



6

Session

Mobile Forensics

Điều tra thiết bị di động

**Tài liệu Thực hành
Pháp chứng Kỹ thuật số**

GVTH: ThS. Nghi Hoàng Khoa

Học kỳ II – Năm học 2021-2022

Tp. HCM, 05.2022

Lưu hành nội bộ

A. TỔNG QUAN

Mục tiêu

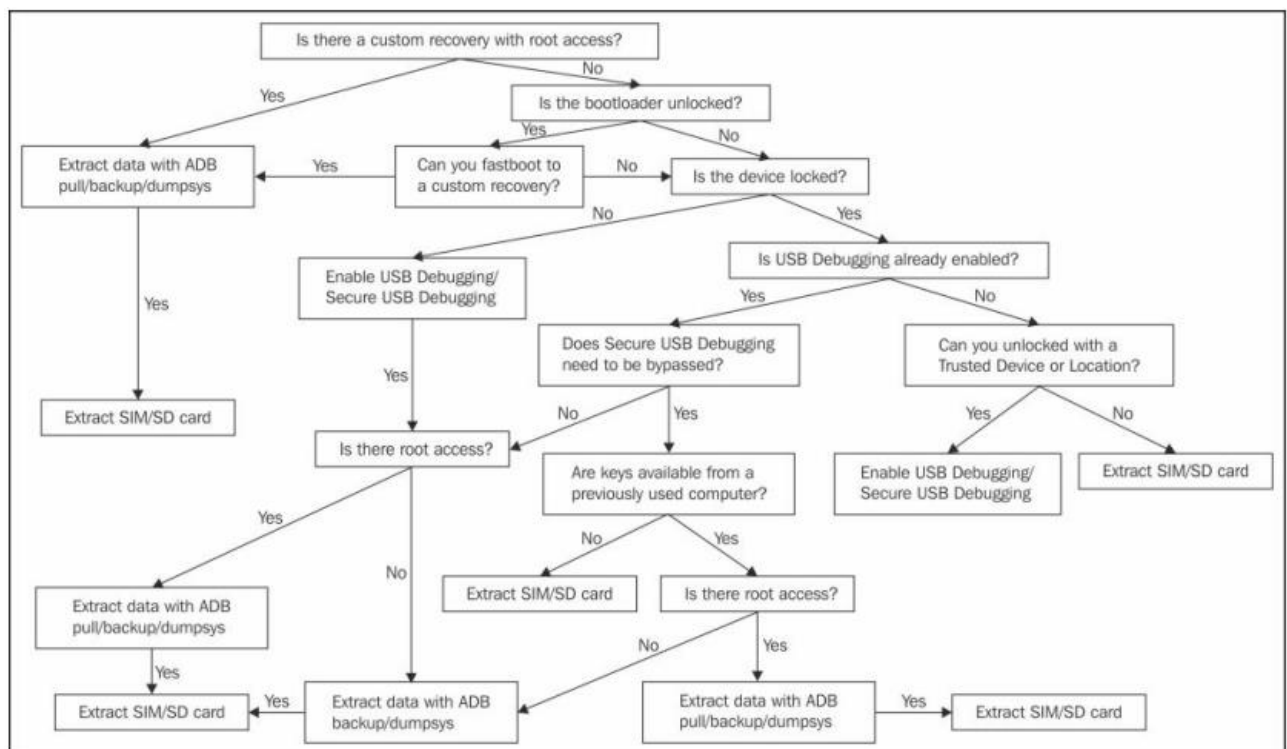
Bài thực hành này giúp sinh viên được làm quen, sử dụng, tăng cường kiến thức về các kỹ năng điều tra kỹ thuật số liên quan đến việc phân tích dữ liệu trên các thiết bị di động (mobile forensics). Trong nội dung bài thực hành này, các thiết bị **Android** sẽ được tập trung phân tích và điều tra.

Giới thiệu kỹ thuật điều tra thiết bị di động

Điều tra thiết bị di động

Kỹ thuật thiết bị di động (Mobile Forensics) là một nhánh của khoa học điều tra số liên quan đến việc giám sát và trích xuất, phân tích nhằm phục vụ cho việc thu thập thông tin, chứng cứ pháp lý hay phát hiện các hành vi của người dùng hay ứng dụng trên thiết bị di động.

Quy trình điều tra thiết bị Android



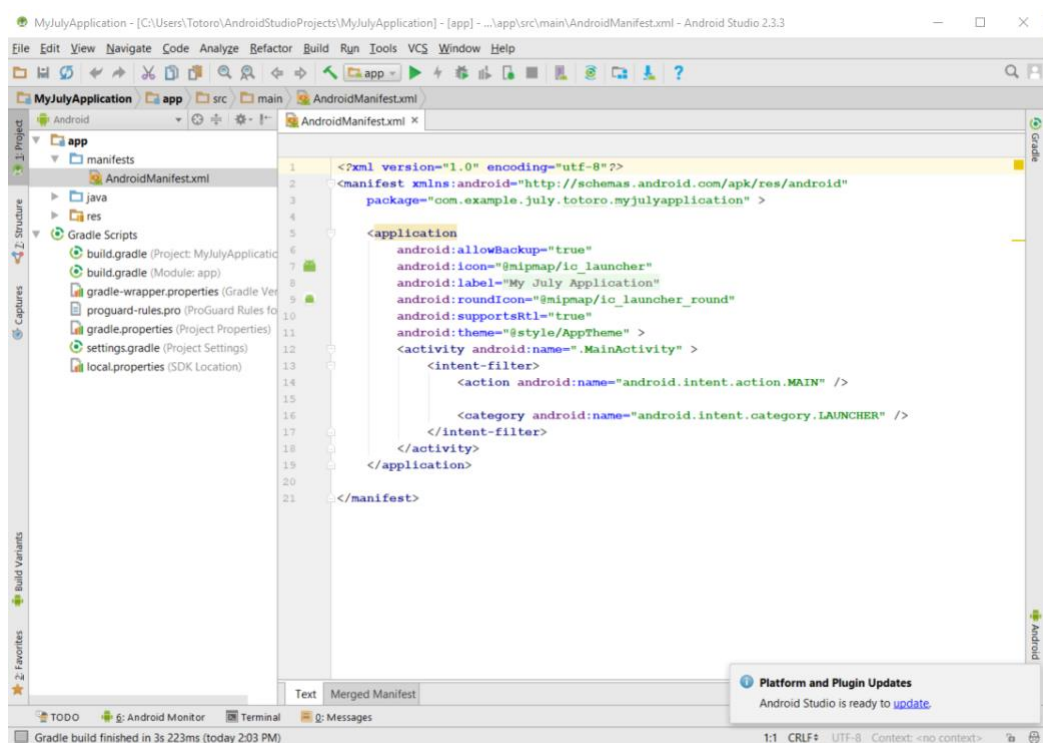
Công cụ điều tra trên thiết bị di động

Một số công cụ dùng điều tra bằng chứng trên các thiết bị di động:

- Dex2jar, JD-GUI,...
- Apktool, APK_OneClick



- Android Studio, Autopsy



- Oxygen Forensic Suite, Cellebrite UFED (Universal Forensic Extraction Device)



- ViaExtract, ViaLab (công cụ cho thiết bị Android)





Môi trường & cấu hình

- Sử dụng các thiết bị và tài liệu, khuyến cáo được cung cấp bởi GVTH, yêu cầu tác phong nghiêm túc trong quá trình thực hiện.
- Công cụ gợi ý: Dex2jar, Apktool, JD-GUI, Oxygen Forensic Suite...
- Tài liệu nên đọc:
 - Sách ***“Practical Mobile Forensics”*** (tác giả: Satish Bommisetty, Rohit Tamma, Heather Mahalik - 2014),
 - Sách ***“Learning Android Forensics”*** (tác giả: Rohit Tamma, Donnie Tindall - 2015),
 - Sách ***“Learning Android Forensics: Analyze Android devices with the latest forensic tools and techniques, 2nd Edition”*** (tác giả: Oleg Skulkin, Donnie Tindall, Rohit Tamma - 2018),
 - Sách ***“Learning iOS Forensics”*** (tác giả: Mattia Epifani, Pasquale Stirparo - 2015).

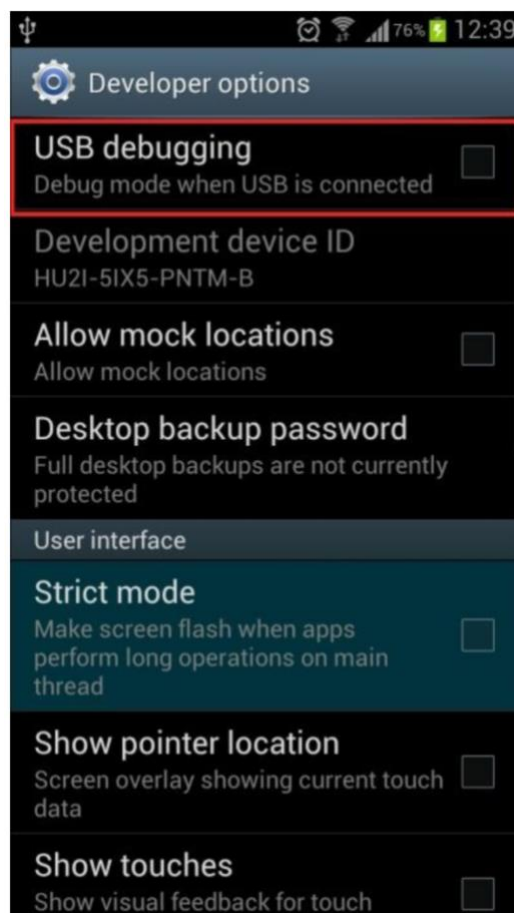
B. THỰC HÀNH

Sinh viên thực hiện điều tra theo yêu cầu của GVHD, làm theo nhóm thực hành đã đăng ký trên lớp trong buổi thực hành.

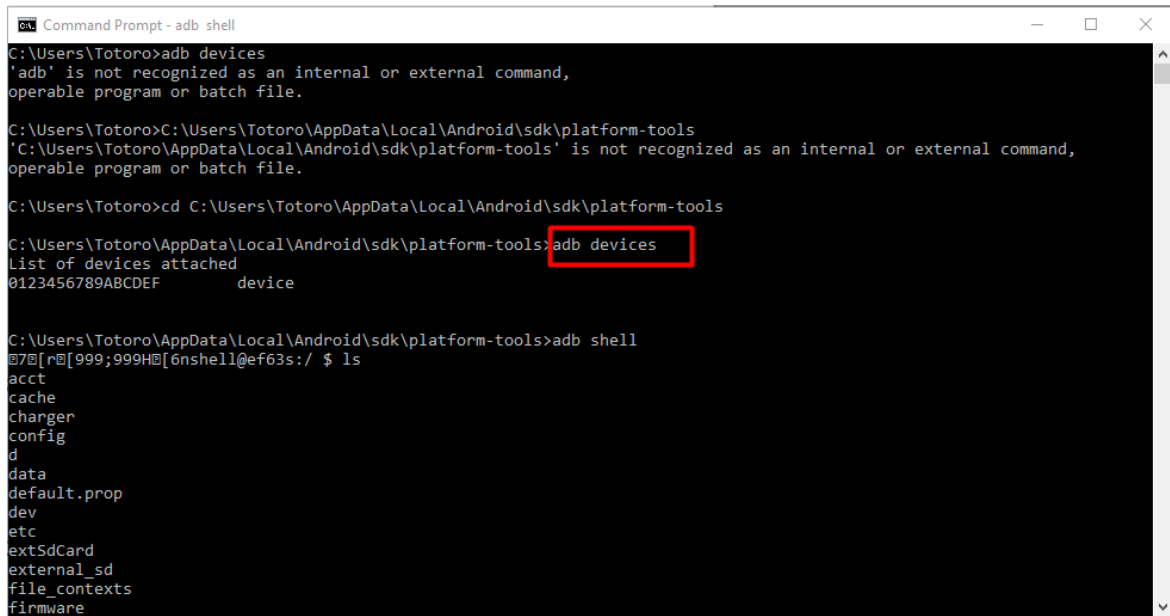
B1. Thiết lập môi trường điều tra thiết bị Android

- Chuẩn bị máy tính điều tra (máy sẽ phân tích và lưu giữ chứng cứ)
- Cài đặt Android SDK
- Thiết bị Android cần điều tra
- Kết nối thiết bị với máy tính qua cổng USB với chế độ hỗ trợ USB debugging/Android debugging. Chọn Settings | Developer để hiển thị. Màn hình dưới đây phụ thuộc vào từng dòng thiết bị khác nhau. Android Debug Bridge (ADB) là một công cụ đóng vai trò quan trọng trong điều tra kỹ thuật số trên thiết bị Android. Trình ADB nằm tại thư mục <sdk_path>/platform-tools.

Ở một số thiết bị, tùy chọn Developer Option bị ẩn, cần bật lên bằng cách nhấn nhiều lần Build Number (chọn Settings | About Device).



- Sử dụng adb để truy cập thiết bị. Kiểm tra thiết bị đã kết nối bằng cách mở cmd và gõ lệnh.



```
Command Prompt - adb shell
C:\Users\Totoro>adb devices
'adb' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Totoro>C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools
'C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Totoro>cd C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb devices
List of devices attached
0123456789ABCDEF      device

C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb shell
070[r0[999;999H0[6nshell@ef63s:/ $ ls
acct
cache
charger
config
d
data
default.prop
dev
etc
extSdCard
external_sd
file_contexts
firmware
```

- Nếu có nhiều thiết bị kết nối, thực hiện chỉ định thực hiện các lệnh trên thiết bị mong muốn bằng cách thêm option -s trước định danh thiết bị thay vì gõ adb shell:

```
C:\Program Files (x86)\Android\android-sdk\platform-tools>adb.exe devices
List of devices attached
4df16ac5115e4e04      device
7f1c86454445606e      device
```

```
adb shell -s4df16ac5115e4e04
```

- Do Android được phát triển trên nhân Linux do đó, có thể thực hiện các lệnh cơ bản như trong các hệ điều hành Linux. Thí dụ:

```

C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb shell
shell@ef63s:/ $ ls -l
drwxr-xr-x root root 1970-04-08 05:42 acct
drwxrwx--- system cache 2019-06-03 15:58 cache
lrwxrwxrwx root root 1970-01-01 07:00 charger -> /sbin/healthd
dr-x----- root root 1970-04-08 05:42 config
lrwxrwxrwx root root 1970-04-08 05:42 d -> /sys/kernel/debug
drwxrwx-x system system 2019-06-03 14:55 data
-rw-r--r-- root root 329 1970-01-01 07:00 default.prop
drwxr-xr-x root root 1970-04-08 05:42 dev
lrwxrwxrwx root root 1970-04-08 05:42 etc -> /system/etc
lrwxrwxrwx root root 1970-04-08 05:42 extSdCard -> /storage/sdcard1
lrwxrwxrwx root root 1970-04-08 05:42 external_sd -> /storage/sdcard1
-rw-r--r-- root root 34983 1970-01-01 07:00 file_contexts
dr-xr-x-- system system 1970-01-01 07:00 firmware
-rw-r----- root root 1328 1970-01-01 07:00 fstab.qcom
-rwxr-x-- root root 324332 1970-01-01 07:00 init
-rwxr-x-- root root 6741 1970-01-01 07:00 init.cm.rc
-rwxr-x-- root root 1064 1970-01-01 07:00 init.envIRON.rc
-rwxr-x-- root root 202 1970-01-01 07:00 init.pantech.ps.wifi.rc
-rwxr-x-- root root 39076 1970-01-01 07:00 init.pantech.usb.rc
-rwxr-x-- root root 269 1970-01-01 07:00 init.pantech.usb.sh
-rwxr-x-- root root 35390 1970-01-01 07:00 init.qcom.post_boot.sh
-rwxr-x-- root root 28388 1970-01-01 07:00 init.qcom.rc
-rwxr-x-- root root 11468 1970-01-01 07:00 init.qcom.sh
-rwxr-x-- root root 269 1970-01-01 07:00 init.qcom.usb.rc
-rwxr-x-- root root 22443 1970-01-01 07:00 init.rc
-rwxr-x-- root root 330 1970-01-01 07:00 init.superuser.rc
-rwxr-x-- root root 13764 1970-01-01 07:00 init.target.rc

```

B2. Trích xuất dữ liệu trên thiết bị Android

- Thực hiện tải dữ liệu /ứng dụng trên thiết bị bằng lệnh adb pull (xem ở các mục sau).
- Xem danh sách các ứng dụng hệ thống/ các ứng dụng cài sẵn:

```

vendor
shell@ef63s:/ $ pwd
/
shell@ef63s:/ $ cd /system/app
shell@ef63s:/system/app $ ls
AntHalService
BasicDreams
Bluetooth
BluetoothExt
Books
CMFileManager
CMWallpapers
Calculator
CalendarGooglePrebuilt
CaptivePortalLogin
CertInstaller
Chrome
CloudPrint2
DeskClock
Development
DocumentsUI
DownloadProviderUi
Drive
EditorsDocs
EditorsSheets
EditorsSlides
Eleven
FaceLock
Galaxy4
Gallery2

```

- Xem dữ liệu các ứng dụng, nằm trong thư mục **/data/data**. Để xem cần có quyền root trên thiết bị.


```

C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb root
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb shell
error: device offline

C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb shell
error: device offline

C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb shell
root@ef63s:/data/data> # cd /data/data
root@ef63s:/data/data> # ls
com.android.apps.tag
com.android.backupconfirm
com.android.bluetooth
com.android.calculator2
com.android.captiveportallogin
com.android.cellbroadcastreceiver
com.android.certinstaller
com.android.chrome
com.android.contacts
com.android.defcontainer
com.android.deskclock
com.android.development
com.android.dialer
com.android.documentsui
com.android.dreams.basic
com.android.dreams.phototable
com.android.externalstorage
com.android.facelock
com.android.galaxy4

```

- Đối với từng ứng dụng được liệt kê bên trên, để xem các giá trị tham chiếu quan trọng thì tìm trong thư mục của nó và được lưu dưới dạng tập tin .xml: /data/data/<package_name>/shared_prefs

```

shell@android:/ # cat /data/data/com.android.email/shared_prefs/com.android.email_preferences.xml
il/shared_prefs/com.android.email_preferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <boolean name="account_sync_email" value="true" />
  <string name="account_settings_cc_bcc">none</string>
  <string name="seven_while_power_low">0</string>
  <boolean name="forward_with_files" value="true" />
  <string name="recent_messages">25</string>
  <boolean name="account_sync_email_legacy" value="true" />
  <string name="account_auto_retry_times_imap">3</string>
  <boolean name="account_default" value="true" />
  <boolean name="account_sync_tasks" value="true" />
  <string name="account_password">gULc[REDACTED]!L0a[REDACTED]kwUg==
</string>
  <string name="account_name">rondr[REDACTED]</string>
  <string name="seven_while_roaming">0</string>
  <string name="account_ringtone_select">/system/media/audio/notifications/S_Postm
an.ogg</string>
  <string name="account_email_retrieve_size">51200</string>
  <string name="account_sync_period">0</string>
  <boolean name="account_notify" value="false" />
  <boolean name="account_sync_calendar" value="true" />
  <string name="account_description">rondr[REDACTED]@gmail.com</string>
  <boolean name="account_sync_contacts" value="true" />
</map>
shell@android:/ #

```

Ví dụ xem thông tin ứng dụng Chrome:

```

0x Command Prompt
fr.playsoft.vnexpress
vt.vtvgo
media
org.codeaurora.bluetooth
org.cyanogenmod.audiofx
org.cyanogenmod.theme chooser
org.cyanogenmod.themes.provider
org.cyanogenmod.wallpapers.photopase
org.whispersystems.whisperpush
vn.vtv.vtvgo
at com.android.chrome/shared_prefs/com.android.chrome.preferences.xml
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<map>
  <boolean name="precache.is_precaching_enabled" value="false" />
  <boolean name="first_run_tos_accepted" value="true" />
  <string name="first_run_signin_account_name">[REDACTED]@gmail.com</string>
  <boolean name="LocaleManager.WAS_IN_SPECIAL_LOCALE" value="false" />
  <int name="opt_out_previous_state" value="0" />
  <boolean name="org.chromium.chrome.browser.tabmodel.TabPersistentStore.HAS_RUN_MULTI_INSTANCE_FILE_MIGRATION" value="true" />
  <int name="browser_crash_success_upload" value="0" />
  <int name="contextual_search_tap_count" value="1" />
  <boolean name="first_backup_done" value="true" />
  <int name="org.chromium.chrome.browser.webapps.extracted_dex_version" value="5" />
  <boolean name="migration_on_upgrade_attempted" value="true" />
  <int name="contextual_search_current_week_number" value="2564" />
  <int name="browser_crash_failure_upload" value="0" />
  <string name="sync_tango_internal_state">3cHe7Ac5G6HJ1RPULLfrcVNRVRfX8RJUKVDVE1WRQoNCOwHeHgQQVTV959AaQCOwHeGtFWFBF
Uk1MRU9UzCz6H8R9U9R9VXfTVJ2FUBAVUf10wPcWHeGpVU0VSXWVRU9UGcB7Ia5
CE3PTaTbQVQLChQ17Ac5SD1dBTExFVF0NRVRBfUQoQLCOwHeG20SUDPUkkkE0j5BxIMWNUFJ10
Tb5TR5UcG4I7Ac5CVRZUVEV1XSTa0VCOwHeHBBVVBPRK1MTf90UK96SUXfChQ17Ac5C0RfV1d

```

```

C:\ Command Prompt - adb shell
com.google.android.talk
com.google.android.tts
com.google.android.youtube
com.somestudio.lichvietnam
com.ss.android.ugc.trill
com.vng.inputmethod.labankey
com.zing.mp3
com.zing.zalo
com.zing.znews
eu.chainfire.supersu
fr.playsoft.vnexpress
ht.nct
media
org.codeaurora.bluetooth
org.cyanogenmod.audiofx
org.cyanogenmod.theme.chooser
org.cyanogenmod.themes.provider
org.cyanogenmod.wallpapers.photophase
org.whispersystems.whisperpush
vn.vtv.vtvg
root@ef63s:/data/data # cd com.zing.mp3
root@ef63s:/data/data/com.zing.mp3 # ls
app_webview
cache
databases
files
lib
no_backup
shared_prefs
root@ef63s:/data/data/com.zing.mp3 #

```

```
Command Prompt - adb shell
org.cyanogenmod.themes.provider
org.cyanogenmod.wallpapers.photophase
org.whispersystems.whisperpush
vn.vtv.vtvgo
root@ef63s:/data/data # cd com.zing.mp3
root@ef63s:/data/data/com.zing.mp3 # ls
app_webview
cache
databases
files
lib
no_backup
shared_prefs
root@ef63s:/data/data/com.zing.mp3 # cd databases/
root@ef63s:/data/data/com.zing.mp3/databases # ls
ads.db
ads.db-journal
com.zing.mp3.session.db
com.zing.mp3.session.db-journal
com.zing.mp3:player.session.db
com.zing.mp3:player.session.db-journal
google_app_measurement_local.db
google_app_measurement_local.db-journal
sp
sp-journal
transactionGoogle.db
transactionGoogle.db-journal
zingmp3.db
zingmp3.db-journal
root@ef63s:/data/data/com.zing.mp3/databases #
```

Các dữ liệu này, ví dụ như CSDL có thể được xem bằng SQLite Browser.

- Tải dữ liệu từ thiết bị di động về máy tính điều tra:

```
adb pull [-p] [-a] <remote> [<local>]
```

```
adb pull -p /data/data/com.android.providers.telephony/databases/mmssms.db
C:/Users/Cases/Case_0001
```

Ví dụ dưới đây tải CSDL tin nhắn SMS trên máy di động về máy tính điều tra.

This PC > Local Disk (C:) > Users > Totoro > AppData > Local > Android > sdk > platform-tools

Name	Date modified	Type	Size
api	26-Jul-17 3:13 PM	File folder	
lib64	26-Jul-17 3:13 PM	File folder	
systrace	26-Jul-17 3:14 PM	File folder	
adb.exe	26-Jul-17 3:13 PM	Application	1,507 KB
AdbWinApi.dll	26-Jul-17 3:13 PM	Application extension	96 KB
AdbWinUsbApi.dll	26-Jul-17 3:13 PM	Application extension	62 KB
dmtracedump.exe	26-Jul-17 3:13 PM	Application	142 KB
etc1tool.exe	26-Jul-17 3:13 PM	Application	321 KB
fastboot.exe	26-Jul-17 3:13 PM	Application	793 KB
hprof-conv.exe	26-Jul-17 3:13 PM	Application	41 KB
libwinpthread-1.dll	26-Jul-17 3:13 PM	Application extension	139 KB
mmsms.db	03-Jun-19 5:04 PM	Data Base File	136 KB
NOTICE.txt	26-Jul-17 3:13 PM	TEXT File	719 KB
package.xml	26-Jul-17 3:14 PM	XML Document	18 KB
source.properties	26-Jul-17 3:13 PM	PROPERTIES File	1 KB
sqlite3.exe	26-Jul-17 3:13 PM	Application	744 KB

Command Prompt

```

ads.db
ads.db-journal
com.zing.mp3.session.db
com.zing.mp3.session.db-journal
com.zing.mp3.player.session.db
com.zing.mp3.player.session.db-journal
google_app_measurement_local.db
google_app_measurement_local.db-journal
sp
sp-journal
transactionGoogle.db
transactionGoogle.db-journal
zingmp3.db
zingmp3.db-journal
root@ef63s:/data/data/com.zing.mp3/databases #
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb shell
* daemon not running; starting it now at tcp:5037 *
* daemon started successfully *
error: device unauthorized.
This adb server's $ADB_VENDOR_KEYS is not set
Try 'adb kill-server' if that seems wrong.
Otherwise check for a confirmation dialog on your device.
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb pull -p /data/data/com.android.providers.telephony/databases/mmsms.db C:/Users
adb: error: cannot create 'C:/Users/mmsms.db': No such file or directory
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb pull -p /data/data/com.android.providers.telephony/databases/mmsms.db .
/data/data/com.android.providers.telephony/databases/mmsms.db: 1 file pulled. 4.9 MB/s (139264 bytes in 0.027s)
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>

```

Thực hiện lấy dữ liệu ứng dụng Gmail:

```

C:\Users\Android_Examiner>adb pull -p /data/data/com.google.android.gm Cases\Case_0002
pull: building file list...
skipping special file 'lib'
pull: /data/data/com.google.android.gm/shared_prefs/Folder-donnietindall@gmail.com-^iim.xml -> Cases\Case_0002/shared_prefs/Folder-donnietindall@gmail.com-^iim.xml
pull: /data/data/com.google.android.gm/shared_prefs/Account-donnietindall@gmail.com.xml -> Cases\Case_0002/shared_prefs/Account-donnietindall@gmail.com.xml

pull: /data/data/com.google.android.gm/app_sslcache/www.google.com.443 -> Cases\Case_0002/app_sslcache/www.google.com.443
pull: /data/data/com.google.android.gm/app_sslcache/android.clients.google.com.443 -> Cases\Case_0002/app_sslcache/android.clients.google.com.443
31 files pulled. 0 files skipped.
1475 KB/s (1233373 bytes in 0.816s)

```

- Xác định ý nghĩa của câu lệnh sau:

```
adb pull -p /data/data/ \Cases\Case_0003
```

- Yêu cầu sinh viên chọn một ứng dụng và phân tích trên thiết bị di động Android của mình
- Tìm hiểu ADB Dumpsys (không đòi hỏi phải có quyền root), để xem các dịch vụ đang chạy trên máy, thực hiện:

```

Command Prompt

C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb pull -p /data/data/com.google.android.gms case_002
adb: error: failed to copy '/data/data/com.google.android.gms/lib' to 'case_002\lib': remote No such file or directory

C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb shell service list
Found 103 services:
0  sip: [android.net.sip.ISipService]
1  phone: [com.android.internal.telephony.ITelephony]
2  isms: [com.android.internal.telephony.ISms]
3  iphonesubinfo: [com.android.internal.telephony.IPhoneSubInfo]
4  simphonelookup: [com.android.internal.telephony.IIccPhoneBook]
5  isub: [com.android.internal.telephony.ISub]
6  nfc: [android.nfc.INfcAdapter]
7  telecom: [com.android.internal.telecom.ITelecomService]
8  imms: [com.android.internal.telephony.IMms]
9  media_projection: [android.media.projection.IMediaProjectionManager]
10 edgegestureservice: [android.service.gesture.IEdgeGestureService]
11 launcherapps: [android.content.pm.ILauncherApps]
12 cmhw: [android.hardware.ICmHardwareService]
13 fingerprint: [android.service.fingerprint.IFingerprintService]
14 trust: [android.app.trust.ITrustManager]
15 media_router: [android.media.IMediaRouterService]
16 killswitch: [com.android.internal.os.IKillSwitchService]
17 themes: [android.content.res.IThemeService]
18 media_session: [android.media.session.ISessionManager]
19 restrictions: [android.content.IRestrictionsManager]
20 print: [android.print.IPrintManager]
21 assetatlas: [android.view.IAssetAtlas]
22 dreams: [android.service.dreams.IDreamManager]
23 commontime_management: []

```

- Dùng dumsys để xem thông tin các dịch vụ liên quan hệ thống:

- iphonesubinfo
- batterystats
- procstats
- userappops
- Wi-Fi
- notification

```

Select Command Prompt

Wake lock androidx.core:wake:fr.playsoft.vnexpress/com.google.firebase.messaging.FirebaseMessagingService realtime
Wake lock GOOGLE_C2DM realtime
Sensor 0: (not used)
Running for: 1s 57ms
Apk fr.playsoft.vnexpress:
(nothing executed)
u0a88:
Wake lock fiid-sync realtime
Running for: 1s 57ms
u0a90:
Wake lock *job*/com.ss.android.ugc.trill/com.ss.android.message.PushJobService realtime
Wake lock fiid-sync realtime
Wake lock androidx.core:wake:com.ss.android.ugc.trill/com.google.firebase.iid.FirebaseInstanceIdService realtime
Wake lock *alarm* realtime
Job com.ss.android.ugc.trill/com.ss.android.message.PushJobService: (not used)
Foreground for: 1s 57ms
Apk com.ss.android.ugc.trill:
Service com.ss.android.message.NotifyService:
Created for: 1s 56ms uptime
Starts: 0, launches: 0
Service com.ss.android.socialbase.downloader.notification.DownloadNotificationService:
Created for: 1s 56ms uptime
Starts: 0, launches: 0
u0a91:
Wake lock Icing realtime
Running for: 1s 57ms
Apk eu.chainfire.supersu:
(nothing executed)

C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb shell dumsys batterystats

```

Các phần thông tin liên quan đến *Wake up* có thể dùng để điều tra mã độc, hoặc các ứng dụng chạy ngầm trên thiết bị.

Thử các lệnh `dumpsys` khác và ghi nhận kết quả:

+ **Dumpsys procstats**: tình trạng sử dụng bộ xử lý của các ứng dụng đang chạy

```
* com.android.chrome / u0a60:
  TOTAL: 7.8% (52MB-84MB-123MB/48MB-73MB-108MB over 44)
  Top: 7.7% (52MB-84MB-123MB/48MB-73MB-108MB over 44)
  Imp Fg: 0.01%
  Imp Bg: 0.00%
  Service: 0.07%
  Receiver: 0.01%
  (Last Act): 8.2% (53MB-62MB-70MB/49MB-57MB-66MB over 29)
  (Cached): 83% (5.2MB-56MB-69MB/4.2MB-52MB-64MB over 65)
```

+ **Dumpsys user**: hiển thị thông tin người dùng đang sử dụng thiết bị

```
Users:
  UserInfo{0:Amber:13} serialNo=0
  Created: <unknown>
  Last logged in: +1h54m10s900ms ago
  UserInfo{10:Donnie:10} serialNo=10
  Created: +4m9s288ms ago
  Last logged in: +4m1s837ms ago
```

+ **Dumpsys App Ops**: thông tin về quyền hạn có thể truy cập bởi các ứng dụng

```
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb shell dumpsys user
Users:
  UserInfo{0:Chibi sBif hBif u:13} serialNo=0
  Created: <unknown>
  Last logged in: +2h8m4s912ms ago

C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb shell dumpsys appops
Current AppOps Service state:
  Op mode watchers:
    Op COARSE_LOCATION:
      #0: com.android.server.AppOpsService$Callback@816c7cd
      #1: com.android.server.AppOpsService$Callback@3821b882
      #2: com.android.server.AppOpsService$Callback@231f5b93
    Op SYSTEM_ALERT_WINDOW:
      #0: com.android.server.AppOpsService$Callback@28f2f7d0
    Op TOAST_WINDOW:
      #0: com.android.server.AppOpsService$Callback@28f2f7d0
  All mode watchers:
    android.app.AppOpsManager$1@9005345 -> com.android.server.AppOpsService$Callback@28f2f7d0
    android.os.BinderProxy@24f088c5 -> com.android.server.AppOpsService$Callback@231f5b93
    android.app.AppOpsManager$1@3c4f4e63 -> com.android.server.AppOpsService$Callback@816c7cd
  Clients:
    android.os.BinderProxy@190d1b62:
      ClientState{mAppToken=android.os.BinderProxy@190d1b62, pid=377}
    android.os.Binder@1a7f41ef:
```



```

uid u0a60:
Package com.android.chrome:
COARSE_LOCATION: mode=0; duration=0
FINE_LOCATION: mode=0; time=+8h57m51s355ms ago; duration=0
VIBRATE: mode=0; time=+1d7h2m45s243ms ago; duration=+12ms
POST_NOTIFICATION: mode=0; time=+6d7h2m42s380ms ago; duration=0
READ_CLIPBOARD: mode=0; time=+5d8h12m52s649ms ago; duration=0
WRITE_CLIPBOARD: mode=0; time=+10d20h49m23s22ms ago; duration=0
TAKE_MEDIA_BUTTONS: mode=0; time=+176d17h18m19s460ms ago; duration=0
TAKE_AUDIO_FOCUS: mode=0; time=+1h7m12s279ms ago; duration=0
AUDIO_RING_VOLUME: mode=0; time=+23h52m52s671ms ago; duration=0
AUDIO_MEDIA_VOLUME: mode=0; time=+1h31m46s692ms ago; duration=0
WAKE_LOCK: mode=0; time=+17m43s597ms ago; duration=+55ms
MONITOR_LOCATION: mode=0; time=+110d8h9m26s749ms ago; duration=+1s219ms

```

Chú ý thông tin xuất ra đối với ứng dụng Chrome ta thấy: cách thời điểm thực hiện trích xuất 1 giờ 7 phút 12 giây, quyền **TAKE_AUDIO_FOCUS** được ứng dụng này sử dụng, tiếp đó là quyền **AUDIO_MEDIA_VOLUME**. Điều này chứng tỏ rằng Chrome được sử dụng để nghe nhạc và đưa ra thông tin nghe khi nào.

Tương tự, hãy thử phân tích thông tin xuất ra từ dumphsys appops sau đây:

```

uid 1001:
Package com.android.phone:
VIBRATE: mode=0; time=+2h34m31s210ms ago; duration=+1s20ms
READ_CONTACTS: mode=0; time=+44m2s299ms ago; duration=0
WRITE_CONTACTS: mode=0; time=+44m2s201ms ago; duration=0
READ_CALL_LOG: mode=0; time=+4d7h29m35s902ms ago; duration=0
WRITE_CALL_LOG: mode=0; time=+44m2s6ms ago; duration=0
POST_NOTIFICATION: mode=0; time=+1d1h31m34s242ms ago; duration=0
CALL_PHONE: mode=0; time=+1d0h56m59s194ms ago; duration=0
READ_SMS: mode=0; time=+4d7h29m36s362ms ago; duration=0
WRITE_SMS: mode=0; time=+3h5m48s341ms ago; duration=0
WRITE_SETTINGS: mode=0; time=+17m18s147ms ago; duration=0
SYSTEM_ALERT_WINDOW: mode=0; time=+20h41m26s834ms ago; duration=+4s776ms
TAKE_AUDIO_FOCUS: mode=0; time=+53m41s785ms ago; duration=0
WAKE_LOCK: mode=0; time=+1m23s617ms ago; duration=+15ms

```

Dựa vào thông tin xuất ra ở trên, ta có thể đưa ra kết luận như sau: Cách thời điểm điều tra 44 phút, người dùng sử dụng ứng dụng Điện thoại (Phone) trên thiết bị của mình để đọc danh bạ với quyền **READ_CONTACTS**. Liên ngay sau đó người này thực hiện một cuộc gọi với quyền **WRITE_CALL_LOG**. Những thông tin này sẽ được ghi nhận, tìm thấy, điều tra được bằng cách này, thậm chí trong trường hợp người dùng thực hiện xóa lịch sử cuộc gọi trên máy điện thoại của mình.

Hãy thực nghiệm lại trên thiết bị của mình.

+ **Dumphsys Wi-Fi**: hiển thị danh sách các SSID mà thiết bị đã kết nối tới. Điều này hữu ích trong các trường hợp muốn xem người dùng này có thể đã tới những địa điểm nào.

```
ID: 9 SSID: "FOR585" BSSID: null PRI0: 51
KeyMgmt: WPA_PSK Protocols: WPA RSN
AuthAlgorithms:
PairwiseCiphers: TKIP CCMP
GroupCiphers: WEP40 WEP104 TKIP CCMP
PSK: *anonymous_identity NULL
```

+ Dumpsys Notification: hiển thị các thông tin về các thông báo đang được kích hoạt trên thiết bị. Những dữ liệu này sẽ hữu ích trong trường hợp lưu giữ trạng thái của thiết bị khi tịch thu được. Ví dụ dưới đây cho thấy có một thông báo từ ứng dụng Gmail (có 1 email mới nhận), với tiêu đề: "This is a test email" và nội dung thông báo như sau: "To see a test notification".

```
>
NotificationRecord(0x4226a928: pkg=com.google.android.gm user=UserHandle{0}
id=31465589 tag=null score=0: Notification(pri=0 contentView=com.google.android.
gm/0x1090064 vibrate=default sound=content://settings/system/notification_sound
defaults=0x6 flags=0x11 kind=[null] 2 actions))
uid=10068 userId=0
icon=0x7f0200df / com.google.android.gm:drawable/ic_notification_mail_24dp

pri=0 score=0
contentIntent=PendingIntent{42aae7f8: PendingIntentRecord{42ca7258 com.goo
gle.android.gm startActivity}}
deleteIntent=PendingIntent{42ab3e38: PendingIntentRecord{42d97190 com.goog
le.android.gm startService}}
tickerText=Donnie Tindall
contentView=android.widget.RemoteViews@42a18b58
defaults=0x00000006 flags=0x00000011
sound=content://settings/system/notification_sound
vibrate=null
led=0x00000000 onMs=0 offMs=0
actions=<
[0] "Delete" -> PendingIntent{42913958: PendingIntentRecord{42a2f818 com
.google.android.gm startService}}
[1] "Reply" -> PendingIntent{4290bd48: PendingIntentRecord{420f50b0 com.
google.android.gm startActivity}}
>
extras=<
android.title=Donnie Tindall
android.support.actionExtras=<0=Bundle[EMPTY_PARCEL], 1=Bundle[EMPTY_PAR
CEL]>
android.subText=donnietindall@gmail.com
android.showChronometer=false
android.icon=2130837727
android.text=This is a test email
To see a test notification
android.progress=0
android.progressBarMax=0
android.showWhen=true
android.people=[Ljava.lang.String;@41fadfb0 <
mailto:donnietindall@gmail.com
>
android.largeIcon=android.graphics.Bitmap@428a3650 <128x128>
android.infoText=null
android.wearable.EXTENSIONS=Bundle[mParcelledData.dataSize=1200]
android.progressBarIndeterminate=false
android.scoreModified=false
>
```

- Nếu không chỉ định dịch vụ cụ thể, **dumpsys** sẽ trích xuất tất cả các dịch vụ đang chạy, ghi vào tập tin đầu ra, thí dụ:

```
adb shell dumpsys > dumpsys.txt
```

B3. Trích xuất dữ liệu thẻ SIM

- Trích xuất dữ liệu thẻ SIM: Hiện nay có rất nhiều công cụ điều tra khác nhau dùng để lấy dữ liệu từ thẻ SIM của điện thoại di động.

Trước đây, thẻ SIM thường chứa 2 loại dữ liệu chính:

- Dữ liệu người dùng: danh bạ, tin nhắn SMS, nhật ký cuộc gọi.
- Dữ liệu mạng:
 - ✓ Integrated Circuit Card Identifier (ICCID): Serial number of the SIM
 - ✓ International Mobile Subscriber Identity (IMSI): Identifier that ties the SIM to a specific user account
 - ✓ MSISDN: số điện thoại gắn với SIM
 - ✓ Location Area Identity (LAI): Identifies the cell that a user is in
 - ✓ Authentication Key (Ki): Used to authenticate to the mobile network

Tuy nhiên, hiện nay do sự phát triển của công nghệ di động (thẻ nhớ, lưu trữ đám mây), các thẻ SIM hầu như chỉ chứa dữ liệu liên quan tới kết nối mạng di động.

Trong quá trình điều tra, các thẻ SIM luôn được tháo rời để phân tích, tìm bằng chứng riêng.

Tham khảo công cụ: <https://www.mobiledit.com/downloads>

- Độ bảo mật của thẻ SIM: mặc dù thẻ SIM có thể được bảo mật bằng mã PIN trên thiết bị di động (bằng cách sử dụng Settings | Security | Set up SIM card lock), tuy nhiên mã PIN này chỉ bảo vệ được dữ liệu của người dùng (user data), trong khi các dữ liệu về kết nối mạng di động vẫn có thể sử dụng/ phục hồi.

Nếu mã PIN được thiết lập trên SIM, nó sẽ cho phép 3 lần thử nhập vào để mở khóa. Nếu người dùng nhập đúng, bộ đếm sẽ được thiết lập lại. Nếu cả 3 lần đều nhập sai mã PIN, thẻ SIM sẽ chuyển sang chế độ Personal Unblocking Key (PUK). Mã PUK bao gồm 8 chữ số được gán bởi nhà mạng, thường được tìm thấy trên bộ Kit của thẻ SIM khi mua thẻ. Khả năng by-passing PUK gần như không thể ngay cả khi dùng các bộ công cụ điều tra khác nhau. Vì lý do này, các nhân viên điều tra luôn được khuyến cáo không bao giờ nhập mã PIN trên thẻ SIM để tránh thẻ bị chuyển sang chế độ PUK và không thể truy cập dữ liệu trên nó được. Tuy nhiên, mã PIN mặc định đối với các nhà mạng thông thường là 0000 hoặc 1234, người điều tra có thể thử sai dưới 3 lần, nếu đúng sẽ mở khóa được thẻ SIM.

- Sao chép thẻ SIM (SIM cloning): Mã Pin dễ dàng bị by-passing bằng kỹ thuật SIM cloning. Kỹ thuật này là một tính năng được cung cấp bởi hầu hết các công cụ giải pháp điều tra thương mại. Nó cho phép sao chép dữ liệu mạng trên SIM điều tra sang một thẻ SIM khác mà không có mã PIN nào được kích hoạt. Thẻ SIM vừa sao

chép, nhân bản được sẽ được bỏ vào thiết bị điện thoại mà không được yêu cầu nhập vào mã PIN nào, tuy nhiên dữ liệu network trên SIM không thể truy cập vào nhà mạng (tương tự chế độ Máy bay). Nó hữu ích trong trường hợp người điều tra cần truy cập dữ liệu trên SIM (dữ liệu người dùng) thông qua SIM nhân bản, trái ngược với khả năng không thể thực hiện trên SIM gốc bị khóa bởi mã PIN.

B4. Phân tích ứng dụng Android

Giúp sinh viên nắm bắt và hiểu rõ cách điều tra một ứng dụng di động trên nền tảng Android.

- Tổng quan về phân tích ứng dụng
 - Danh bạ, Nhật ký cuộc gọi, SMS
 - Wi-Fi
 - User dictionary
- Các phương pháp khác nhau để lưu trữ các loại dữ liệu phức tạp đa dạng khác nhau:
 - Plain text
 - Epoch time
 - WebKit time
 - Misnaming file extensions
 - Julian dates
 - Base64 encoding
 - Encryption
 - Basic steganography
 - SQLCipher

Khi cần phân tích một ứng dụng Android, người điều tra cần đưa ra tên của package, số phiên bản (version number), các tập tin cần quan tâm. Ví dụ:

- Tên gói: com.android.providers.contacts
- Phiên bản: Phiên bản mặc định trên Android 5.0.1
- Các tập tin cần quan tâm: /files/photos/

Khi đã xác định các thông tin cần thiết, các dữ liệu của các ứng dụng cần phân tích nằm trong đường dẫn:

- /data/data/<com.android.providers.contacts>/ nếu ứng dụng được cài trong bộ nhớ của máy
- /sdcard/<com.facebook.orca> nếu ứng dụng được cài trên thẻ nhớ của điện thoại.

a) Xác định những ứng dụng nào được cài đặt trên thiết bị:

Vào thư mục **/data/data** và chạy câu lệnh **ls** để xem các ứng dụng trên thiết bị. Tuy nhiên, cách này không cung cấp nhiều thông tin để quan sát phục vụ cho điều tra.

Để thu được nhiều thông tin hơn, cần tải (pull) tập tin **/data/system/packages.list** về để xem thông tin của ứng dụng, đường dẫn của nó. Nếu tập tin này không tồn tại trên thiết bị, người điều tra có thể sử dụng câu lệnh: **adb shell pm list packages -f**

```
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb root
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb shell
[7][r][999;999H[6nroot@ef63s:/ # exit
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb pull /data/system/packages.list .
/data/system/packages.list: 1 file pulled. 1.6 MB/s (11424 bytes in 0.007s)
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>
```

Kết quả hiển thị:

```

1 com.android.gallery3d 10040 0 /data/data/com.android.gallery3d platform 3003,1028,1015,1023,3002
2 com.android.backupconfirm 10001 0 /data/data/com.android.backupconfirm platform none
3 com.cyanogenmod.updater 10003 0 /data/data/com.cyanogenmod.updater cmupdater 3003,1028,1015,2001
4 com.cyanogenmod.filemanager 10029 0 /data/data/com.cyanogenmod.filemanager platform 1028,1015,1023
5 com.android.packageinstaller 10049 0 /data/data/com.android.packageinstaller platform 1028
6 com.dsi.ant.server 1000 0 /data/data/com.dsi.ant.server platform 3002,3001,3003,1028,1015
7 com.android.providers.downloads.ui 10009 0 /data/data/com.android.providers.downloads.ui default 2001,3003,1028,1015,3007,1023,1024
8 com.android.providers.userdictionary 10006 0 /data/data/com.android.providers.userdictionary default 3003,1028,1015
9 com.android.externalstorage 10010 0 /data/data/com.android.externalstorage platform 1028,1015,1023
10 com.vng.inputmethod.labankey 10085 0 /data/data/com.vng.inputmethod.labankey default 3003,1028,1015
11 com.android.apps.tag 10016 0 /data/data/com.android.apps.tag default none
12 com.google.android.apps.docs.editors.docs 10065 0 /data/data/com.google.android.apps.docs.editors.docs release 3003,1028,1015
13 com.google.android.launcher 10070 0 /data/data/com.google.android.launcher release none
14 com.google.android.apps.cloudprint 10064 0 /data/data/com.google.android.apps.cloudprint release 3003,1028
15 com.android.dreams.phototable 10052 0 /data/data/com.android.dreams.phototable default 1028
16 com.android.galaxy4 10039 0 /data/data/com.android.galaxy4 default none
17 com.google.android.googlequicksearchbox 10025 0 /data/data/com.google.android.googlequicksearchbox release 3003,3001,1028,3002,1015,1005
18 org.cyanogenmod.wallpapers.photophase 10051 0 /data/data/org.cyanogenmod.wallpapers.photophase default 1028
19 com.cyanogenmod.eleven 10038 0 /data/data/com.cyanogenmod.eleven default 1028,1015,3003
20 com.cyanogenmod.lockclock 10046 0 /data/data/com.cyanogenmod.lockclock default 3003
21 com.android.shell 2000 0 /data/data/com.android.shell platform 3002,1028,1015,1023,3008
22 com.android.calculator2 10031 0 /data/data/com.android.calculator2 default 3003
23 com.android.managedprovisioning 10011 0 /data/data/com.android.managedprovisioning platform 1028,3003
24 com.android.proxyhandler 10013 0 /data/data/com.android.proxyhandler platform 3003
25 com.android.chrome 10043 0 /data/data/com.android.chrome release 3003,1028,1015
26 com.google.android.play.games 10032 0 /data/data/com.google.android.play.games release 3003
27 com.google.android.marvin.talkback 10026 0 /data/data/com.google.android.marvin.talkback default 3003,3002,3001
28 com.google.android.feedback 10024 0 /data/data/com.google.android.feedback release 1007,3003
29 com.google.android.inputmethod.latin 10075 0 /data/data/com.google.android.inputmethod.latin release 3003
30 org.whispersystems.whisperpush 10060 0 /data/data/org.whispersystems.whisperpush platform 3003
31 fr.playsoft.vnexpress 10086 0 /data/data/fr.playsoft.vnexpress default 1028,1015,3003
32 com.google.android.onetimeinitializer 10023 0 /data/data/com.google.android.onetimeinitializer release none
33 com.android.wallpaper.livesticker 10045 0 /data/data/com.android.wallpaper.livesticker platform none
34 com.android.inputdevices 1000 0 /data/data/com.android.inputdevices platform 3002,3001,3003,1028,1015
35 com.android.keychain 1000 0 /data/data/com.android.keychain platform 3002,3001,3003,1028,1015
36 com.android.bluetooth 1002 0 /data/data/com.android.bluetooth platform 3003,3002,3001,1028,1015,3005,1016,3008,1023
37 vn.vtv.vtgo 10089 0 /data/data/vn.vtv.vtgo default 3003,1028,1015
38 com.android.printspooler 10054 0 /data/data/com.android.printspooler default none
39 com.android.smspush 10059 0 /data/data/com.android.smspush default none
40 com.cyanogenmod.account 10002 0 /data/data/com.cyanogenmod.account platform 3003
41 com.google.android.ears 10066 0 /data/data/com.google.android.ears release 3003,1028,1015
42 com.google.android.apps.maps 10033 0 /data/data/com.google.android.apps.maps release 3003,1028,1015
43 com.android.dreams.basic 10027 0 /data/data/com.android.dreams.basic default none
44 com.android.contacts 10006 0 /data/data/com.android.contacts default 3003,1028,1015
45 com.android.noisefield 10047 0 /data/data/com.android.noisefield default none
46 com.android.vpndialogs 10019 0 /data/data/com.android.vpndialogs platform none
47 com.google.android.apps.messaging 10076 0 /data/data/com.google.android.apps.messaging default 3003,1028,1015
48 com.google.android.apps.docs.editors.sheets 10077 0 /data/data/com.google.android.apps.docs.editors.sheets release 3003,1028,1015
49 com.google.android.street 10079 0 /data/data/com.google.android.street release 3003,1028,1015
50 com.android.server.telecom 1001 0 /data/data/com.android.server.telecom platform 3002,3001,3003,1028,1015
51 com.android.phasebeam 10050 0 /data/data/com.android.phasebeam default none
52 com.android.provision 10055 0 /data/data/com.android.provision platform none
53 com.zing.znews 10087 0 /data/data/com.zing.znews default 3003,1028,1015
54 com.android.defcontainer 10007 0 /data/data/com.android.defcontainer platform 1028,1015,1023,2001,1035
55 com.ss.android.ugc.trill 10090 0 /data/data/com.ss.android.ugc.trill default 3003,1028,1015
56 com.google.android.gm 10069 0 /data/data/com.google.android.gm release 3003,1028,1015
57 com.android.systemui 10015 0 /data/data/com.android.systemui platform 1028,1015,1035,3002,3001,3006
58 com.android.phone 1001 0 /data/data/com.android.phone platform 3002,3001,3003,1028,1015
59 com.android.nfc 1027 0 /data/data/com.android.nfc platform 3002,3001,1028,1015,3003
60 com.android.providers.calendar 10004 0 /data/data/com.android.providers.calendar default 3003,1028,1015
61 com.android.vending 10012 0 /data/data/com.android.vending release 3003,1028,1015
62 com.google.android.apps.plus 10071 0 /data/data/com.google.android.apps.plus release 3003,1028,1015
63 android 1000 0 /data/system platform 3002,3001,3003,1028,1015
64 com.android.certinstaller 10035 0 /data/data/com.android.certinstaller platform none
65 com.android.webview 10061 0 /data/data/com.android.webview default none

```

Hoặc kết quả khi gõ lệnh adb shell pm list packages -f:

```

C:\Users\Totoro>cd C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb shell pm list packages -f
package:/system/app/Gallery2/Gallery2.apk=com.android.gallery3d
package:/system/priv-app/BackupRestoreConfirmation/BackupRestoreConfirmation.apk=com.android.backupconfirm
package:/system/app/CMFileManager/CMFileManager.apk=com.cyanogenmod.filemanager
package:/system/priv-app/CMUpdater/CMUpdater.apk=com.cyanogenmod.updater
package:/system/app/UserDictionaryProvider/UserDictionaryProvider.apk=com.android.providers.userdictionary
package:/system/app/DownloadProviderUi/DownloadProviderUi.apk=com.android.providers.downloads.ui
package:/system/app/AnthHalService/AnthHalService.apk=com.dsi.ant.server
package:/system/priv-app/ExternalStorageProvider/ExternalStorageProvider.apk=com.android.externalstorage
package:/data/app/com.vng.inputmethod.labankey-2/base.apk=com.vng.inputmethod.labankey
package:/system/priv-app/Tag/Tag.apk=com.android.apps.tag
package:/data/app/com.google.android.apps.docs.editors.docs-1/base.apk=com.google.android.apps.docs.editors.docs
package:/data/app/com.google.android.launcher-2/base.apk=com.google.android.launcher
package:/data/app/com.google.android.apps.cloudprint-2/base.apk=com.google.android.apps.cloudprint
package:/system/app/PhotoTable/PhotoTable.apk=com.android.dreams.phototable
package:/system/app/Galaxy4/Galaxy4.apk=com.android.galaxy4
package:/data/app/com.google.android.googlequicksearchbox-1/base.apk=com.google.android.googlequicksearchbox
package:/system/app/PhotoPhase/PhotoPhase.apk=org.cyanogenmod.wallpapers.photophase
package:/system/app/Eleven/Eleven.apk=com.cyanogenmod.eleven
package:/system/app/LockClock/LockClock.apk=com.cyanogenmod.lockclock
package:/system/app/Calculator/Calculator.apk=com.android.calculator2
package:/system/priv-app/Shell/Shell.apk=com.android.shell
package:/data/app/com.android.chrome-2/base.apk=com.android.chrome
package:/system/priv-app/ProxyHandler/ProxyHandler.apk=com.android.proxyhandler

```


Để xem lần truy cập gần nhất (timestamp định dạng Linux epoch time – được tính từ 1.1.1970) khi một người nào đó sử dụng ứng dụng, chúng ta xem nội dung trong tập tin **/data/system/package-usage.list**.

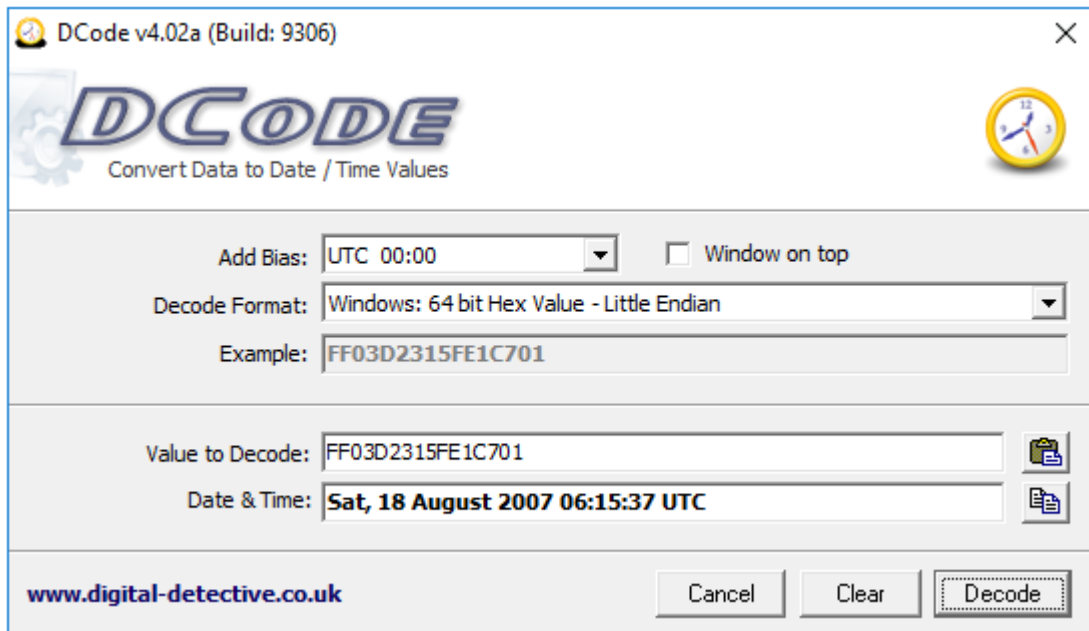
```
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb pull /data/system/package-usage.list .  
/data/system/package-usage.list: 1 file pulled. 1.1 MB/s (3327 bytes in 0.003s)  
  
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>
```



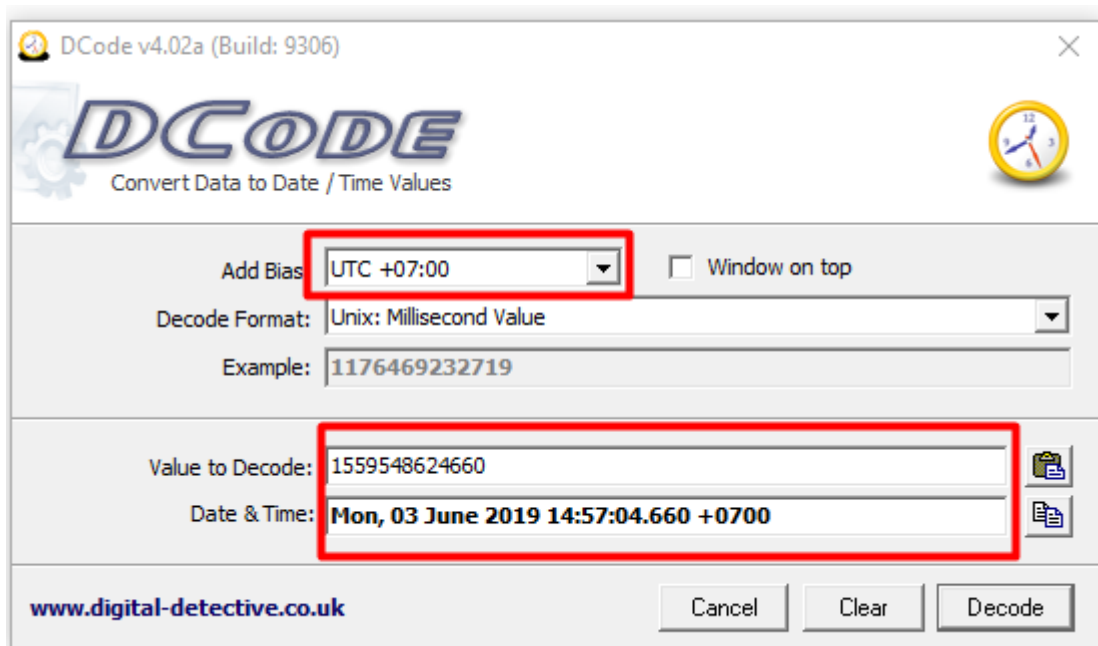
```
1 com.android.gallery3d 1559552992888  
2 com.cyanogenmod.updater 1559560704632  
3 com.android.providers.userdictionary 1559551514579  
4 com.dsi.ant.server 1559548547951  
5 com.vng.inputmethod.labankey 1559560686672  
6 com.google.android.apps.docs.editors.docs 1559548625282  
7 com.google.android.apps.cloudprint 1559548611467  
8 com.google.android.googlequicksearchbox 1559560030650  
9 com.cyanogenmod.eleven 1559548541427  
10 com.cyanogenmod.lockclock 1559560950247  
11 com.android.calculator2 1532385448662  
12 com.android.chrome 1559554488245  
13 com.android.managedprovisioning 1559548546190  
14 com.google.android.play.games 1559548662179  
15 com.google.android.marvin.talkback 1559548543411  
16 com.google.android.inputmethod.latin 1559548702004  
17 org.whispersystems.whisperpush 1559548549039  
18 fr.playsoft.vnexpress 1559560704660  
19 com.google.android.onetimeinitializer 1559548547937  
20 com.android.keychain 1559548745267  
21 com.android.bluetooth 1559553436440  
22 com.android.printspooler 1559548532305  
23 com.android.smspush 1559548543002  
24 com.cyanogenmod.account 1559548671277  
25 com.google.android.apps.maps 1559548904093  
26 com.google.android.apps.docs.editors.sheets 1559548673596  
27 com.google.android.apps.messaging 1559561631661  
28 com.google.android.street 1559548592365  
29 com.android.server.telecom 1559548532728  
30 com.android.provision 1500809402334  
31 com.android.defcontainer 1559549237119  
32 com.ss.android.ugc.trill 1559560724255  
33 com.google.android.gm 1559548676953  
34 com.android.systemui 1559556204611  
35 com.android.nfc 1559548532138  
36 com.android.phone 1559548624660  
37 com.android.providers.calendar 1559548677767  
38 com.google.android.apps.plus 1559560704649  
39 com.android.vending 1559560723985  
40 com.android.webview 1559560722925
```

Để xem chính xác thời gian, tham khảo công cụ DCode:

<https://www.digital-detective.net/digital-forensic-software/free-tools/>



Ví dụ dưới đây cho biết rằng, người dùng đã truy cập ứng dụng Điện thoại (Phone) trên thiết bị gần nhất vào lúc: Mon, 03 June 2019 14:57:04.660 (múi giờ UTC +7)



b) Phân tích Wi-Fi

Dữ liệu Wi-Fi được lưu trong tập tin `/data/misc/wifi/wpa_supplicant.conf`. Thông tin này bao gồm danh sách các access point (điểm truy cập) mà người dùng đã chọn để kết nối. Các điểm truy cập mà người dùng sử dụng chức năng “Forgotten” sẽ không xuất hiện trong tập tin này.

Nếu điểm truy cập có yêu cầu nhập mật khẩu khi kết nối, mật khẩu sẽ được lưu dưới dạng plain text trong tập tin.

```
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb pull /data/misc/wifi/wpa_supplicant.conf .
/data/misc/wifi/wpa_supplicant.conf: 1 file pulled. 0.3 Mb/s (810 bytes in 0.003s)

C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>

vpncclient_tls.c x vpnserv_tls.c x vpnserv_tls_multiclient.c x package-usage.list x wpa_supplicant.conf x
10 device_type=10-0050F204-5
11 config_methods=physical_display virtual_push_button
12 external_sim=1
13 key_mgmt_offload=1
14
15 network={
16     ssid="Healer"
17     psk="XXXXXXXXXX"
18     key_mgmt=WPA-PSK
19     priority=22
20 }
21
22 network={
23     ssid="iSecurityGarden_5G"
24     psk="XXXXXXXXXX"
25     key_mgmt=WPA-PSK
26     priority=48
27 }
28
29 network={
30     ssid="iSecurityGarden"
31     psk="XXXXXXXXXX"
32     key_mgmt=WPA-PSK
33     priority=33
34 }
35
36 network={
37     ssid="UIT"
38     key_mgmt=WPA-EAP IEEE8021X
39     eap=PEAP
40     identity="XXXXXXXXXX"
41     password="XXXXXXXXXX"
42     priority=50
43     proactive_key_caching=1
44 }
45
46 network={
47     ssid="ViVa"
48     psk="XXXXXXXXXX"
49     key_mgmt=WPA-PSK
50     priority=42
51 }
52
```

c) Phân tích danh bạ/ cuộc gọi

- Thông tin về danh bạ, nhật ký cuộc gọi nằm cùng một CSDL. Cụ thể:
 - Tên gói: com.android.providers.contacts
 - Phiên bản: Phiên bản mặc định với Android 5.0.1
 - Tập tin cần quan tâm:

- /files/
 - photos/
 - profile/
- /databases/
 - contacts2.db

- Tìm hiểu, xác định các bảng, trường giá trị lưu trong CSDL này.

d) Phân tích tin nhắn SMS/MMS

- Thông tin về các tin nhắn này được lưu trữ trong

- Gói com.android.providers.telephony
- Tập tin cần quan tâm:

- /app_parts
- /databases/
 - mmssms.db
 - telephony.db

- Tìm hiểu các bảng trong CSDL này: siminfo (trong telephony.db), part, pdu, sms, words, words_content, words_segdir (trong mmssms.db)

e) Phân tích từ điển người dùng (user dictionary)

Tên gói: com.android.providers.userdictionary

Tập tin cần quan tâm: /databases/user_dict.db

Trong CSDL này, Bảng words của user_dict.db sẽ có cột word lưu thông tin các từ mà người dùng đã thêm vào từ điển, tần số (frequency) luôn được hiển thị là 250 bất chấp số lần mà từ này được sử dụng.

_id	word	frequency	locale	appid	shortcut
33	ok	250	en_US	0	
34	reddit	250	en_US	0	
35	snores	250	en_US	0	

f) Phân tích ứng dụng Gmail

Tên package: com.google.android.gm

Các tập tin cần quan tâm:

- /cache
- /databases/
 - mailstore.<username>@gmail.com.db
 - databases/suggestions.db
- /shared_prefs/
 - MailAppProvider.xml
 - Gmail.xml
 - UnifiedEmail.xml

- Thư mục cache trong ứng dụng Gmail chứa các tập tin gần đây được đính kèm vào email (nhận và gửi). Thông tin về các tập tin đính kèm này được lưu trữ ở đây, dù cho người dùng có thực hiện tải về hay không.
- CSDL mailstore.<username>@gmail.com.db chứa rất nhiều thông tin hữu ích trong điều tra, nó bao gồm các bảng sau:
 - attachments: thông tin về kích thước của tệp đính kèm cùng đường dẫn đến trên thiết bị
 - conversations

g) Thực hiện phân tích ứng dụng Google Chrome

Tên gói: com.android.chrome

Các tập tin quan tâm:

- /app_chrome/Default/
 - Sync Data/SyncData.sqlite3
 - Bookmarks
 - Cookies
 - Google Profile Picture.png
 - History
 - Login Data
 - Preferences
 - Top Sites
 - Web Data
- /app_ChromeDocumentActivity/

h) Phân tích ứng dụng Google Maps

Tên gói: com.google.android.apps.maps

Các tập tin cần quan tâm:

- /cache/http/
- /databases/
 - gmm_myplaces.db
 - gmm_storage.db

i) Phân tích ứng dụng Facebook

Tên gói: com.facebook.katana

Tập tin cần quan tâm:

- /files/video-cache/
- /cache/images/
- /databases/
 - bookmarks_db2
 - contacts_db2
 - nearbytiles_db
 - newsfeed_db
 - notifications_db
 - prefs_db
 - threads_db2

j) Phân tích ứng dụng Facebook Messenger

Tên gói: com.facebook.orca

Tập tin cần quan tâm:

- /cache/
 - audio/
 - fb_temp/
 - image/
- /sdcard/com.facebook.orca
- /files/ rti.mqtt.analytics.xml
- /databases/
 - call_log.sqlite
 - contacts_db2
 - prefs_db
 - threads_db2

k) Phân tích ứng dụng Viber

Tên gói: com.viber.voip

Tập tin cần quan tâm:

- /files/preferences/
 - activated_sim_serial
 - display_name
 - reg_viber_phone_num
- /sdcard/viber/media/
 - /User Photos/
 - /Viber Images/
 - /Viber Videos/
- /databases/
 - viber_data
 - viber_messages

l) Phân tích ứng dụng WeChat

Tên gói: com.tencent.mm

Tập tin cần quan tâm:

- /files/host/*.getdns2
- /shared_prefs/
 - com.tencent.mm_preferences.xml
 - system_config_prefs.xml
- /sdcard/tencent/MicroMsg/
 - diskcache/
 - WeChat/
- /sdcard/tencent/MicroMsg/*/
 - image2/
 - video/
 - voice2/
- /MicroMsg/
 - CompatibleInfo.cfg
 - */EnMicroMsg.db

B5. Dịch ngược ứng dụng

a) Thu thập các tập tin APK của ứng dụng

Ứng dụng được cài đặt trên thiết bị Android tồn tại dưới định dạng tập tin .apk. Tập tin cài đặt này vẫn được lưu giữ lại trên ứng dụng cho dù ứng dụng đã cài đặt xong (nó chỉ được xóa khi ứng dụng bị gỡ cài đặt).

Các tập tin apk của các ứng dụng được cài đặt thông qua Google Play có thể tìm thấy trong thư mục **/data/app**.

```

C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb root
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb shell
root@ef63s:/ # cd /data/app
root@ef63s:/data/app # ls
com.android.chrome-1
com.android.vending-1
com.android.vending-2
com.google.android.GoogleCamera-1
com.google.android.apps.books-2
com.google.android.apps.cloudprint-2
com.google.android.apps.docs-2
com.google.android.apps.docs.editors.docs-2
com.google.android.apps.docs.editors.sheets-2
com.google.android.apps.docs.editors.slides-1
com.google.android.apps.maps-1
com.google.android.apps.messaging-1
com.google.android.apps.plus-1
com.google.android.calendar-1
com.google.android.gm-2
com.google.android.gm.exchange-1
com.google.android.gms-1
com.google.android.gms-3
com.google.android.googlequicksearchbox-2
com.google.android.inputmethod.latin-1
com.google.android.keep-1
com.google.android.launcher-2
com.google.android.marvin.talkback-1
com.google.android.play.games-1

```

Ngoài ra, có thể tìm đường dẫn chứa tập tin cài đặt apk của ứng dụng bằng cách sử dụng lệnh **adb pm path <package_name>**.

Tải về tập tin apk bằng cách sử dụng lệnh **pull**.

```

com.google.android.gm-2
com.google.android.gm.exchange-1
com.google.android.gms-1
com.google.android.gms-3
com.google.android.googlequicksearchbox-2
com.google.android.inputmethod.latin-1
com.google.android.keep-1
com.google.android.launcher-2
com.google.android.marvin.talkback-1
com.google.android.play.games-1
com.google.android.street-1
com.google.android.talk-2
com.google.android.tts-2
com.google.android.youtube-1
com.somestudio.lichvietnam-2
com.ss.android.ugc.trill-1
com.vng.inputmethod.labankey-1
com.zing.mp3-1
com.zing.zalo-1
com.zing.znews-1
eu.chainfire.supersu-1
fr.playsoft.vnexpress-1
ht.nct-1
vn.vtv.vtvgo-2
root@ef63s:/data/app # exit
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>adb pull /data/app/vn.vtv.vtvgo-2
/data/app/vn.vtv.vtvgo-2/: 2 files pulled. 3.8 MB/s (14625468 bytes in 3.657s)
C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools>

```

Kết quả tải về là tập tin base.apk trong thư mục của ứng dụng:

s PC > Local Disk (C:) > Users > Totoro > AppData > Local > Android > sdk > platform-tools

Name	Date modified	Type	Size
api	26-Jul-17 3:13 PM	File folder	
case_002	03-Jun-19 5:13 PM	File folder	
lib64	26-Jul-17 3:13 PM	File folder	
systrace	26-Jul-17 3:14 PM	File folder	
vn.vtv.vtvgo-2	04-Jun-19 10:34 AM	File folder	
adb.exe	26-Jul-17 3:13 PM	Application	1,507 KB
AdbWinApi.dll	26-Jul-17 3:13 PM	Application extension	96 KB
AdbWinUsbApi.dll	26-Jul-17 3:13 PM	Application extension	62 KB
dmtracedump.exe	26-Jul-17 3:13 PM	Application	142 KB
etc1tool.exe	26-Jul-17 3:13 PM	Application	321 KB
fastboot.exe	26-Jul-17 3:13 PM	Application	793 KB
hprof-conv.exe	26-Jul-17 3:13 PM	Application	41 KB
libwinpthread-1.dll	26-Jul-17 3:13 PM	Application extension	139 KB
mmssms.db	03-Jun-19 5:04 PM	Data Base File	136 KB
NOTICE.txt	26-Jul-17 3:13 PM	TXT File	719 KB
package.xml	26-Jul-17 3:14 PM	XML Document	18 KB
packages.list	04-Jun-19 9:14 AM	LIST File	12 KB
package-usage.list	04-Jun-19 9:21 AM	LIST File	4 KB
source.properties	26-Jul-17 3:13 PM	PROPERTIES File	1 KB
sqlite3.exe	26-Jul-17 3:13 PM	Application	744 KB
wpa_supplicant.conf	04-Jun-19 9:48 AM	CONF File	1 KB

View

is PC > Local Disk (C:) > Users > Totoro > AppData > Local > Android > sdk > platform-tools > vn.vtv.vtvgo-2

Name	Date modified	Type	Size
lib	04-Jun-19 10:34 AM	File folder	
base.apk	04-Jun-19 10:34 AM	APK File	14,161 KB

- Tập tin cài đặt APK thực chất là một tập tin nén, có thể đổi định dạng .apk thành .zip, sau đó giải nén, thu được cấu trúc của ứng dụng:

Copy View

This PC > Local Disk (C:) > Users > Totoro > AppData > Local > Android > sdk > platform-tools > vn.vtv.vtgo-2 > base - Copy

Name	Date modified	Type	Size
android	04-Jun-19 10:38 AM	File folder	
assets	04-Jun-19 10:38 AM	File folder	
fabric	04-Jun-19 10:38 AM	File folder	
kotlin	04-Jun-19 10:38 AM	File folder	
lib	04-Jun-19 10:38 AM	File folder	
META-INF	04-Jun-19 10:38 AM	File folder	
okhttp3	04-Jun-19 10:38 AM	File folder	
org	04-Jun-19 10:38 AM	File folder	
res	04-Jun-19 10:38 AM	File folder	
AndroidManifest.xml	04-Jun-19 10:38 AM	XML Document	27 KB
androidsupportmultidexversion.txt	04-Jun-19 10:38 AM	TXT File	1 KB
classes.dex	04-Jun-19 10:38 AM	DEX File	8,300 KB
classes2.dex	04-Jun-19 10:38 AM	DEX File	6,038 KB
firebase-abt.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-analytics.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-analytics-impl.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-common.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-config.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-core.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-iid.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-iid-interop.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-measurement-connector.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-measurement-connector-impl.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-messaging.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-ads.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-ads-base.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-ads-identifier.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-ads-lite.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-analytics.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-analytics-impl.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-base.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-basement.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-gass.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-gcm.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-iid.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-location.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-maps.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-measurement-base.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-phenotype.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-places-placereport.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-stats.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-tagmanager.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-tagmanager-api.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-tagmanager-v4-impl.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
play-services-tasks.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
resources.arsc	04-Jun-19 10:38 AM	ARSC File	1,044 KB

- Các quyền hạn được cấp cho ứng dụng sẽ được hiển thị trong tập tin AndroidManifest.xml. Để xem nội dung của tập tin này, cần giải nén tập tin .apk bằng các công cụ chuyên dụng như APK_OneClick, JDAX, JD-GUI, dex2jar... (Xem Phần tiếp theo – Kịch bản 1). Cấu trúc của tập xml này như ví dụ sau:


```

<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.VIBRATE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.WAKE_LOCK" />
<uses-permission android:name="android.permission.GET_ACCOUNTS" />
<uses-permission android:name="kik.android.permission.CONTACT" />
<uses-permission android:name="com.android.vending.BILLING" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.CAMERA" />

```

Tải APK_OneClick ở liên kết sau: <https://forum.xda-developers.com/showthread.php?t=873466>

- Để đọc code Java của ứng dụng, cần chú ý đến tập tin classes.dex. Chúng ta cần chuyển định dạng .dex sang các định dạng code có thể đọc được (vd: Java, Smali,...)

android	04-Jun-19 10:38 AM	File folder	
assets	04-Jun-19 10:38 AM	File folder	
fabric	04-Jun-19 10:38 AM	File folder	
kotlin	04-Jun-19 10:38 AM	File folder	
lib	04-Jun-19 10:38 AM	File folder	
META-INF	04-Jun-19 10:38 AM	File folder	
okhttp3	04-Jun-19 10:38 AM	File folder	
org	04-Jun-19 10:38 AM	File folder	
res	04-Jun-19 10:38 AM	File folder	
AndroidManifest.xml	04-Jun-19 10:38 AM	XML Document	27 KB
androidsupportmultidexversion.txt	04-Jun-19 10:38 AM	TXT File	1 KB
classes.dex	04-Jun-19 10:38 AM	DEX File	8,300 KB
classes2.dex	04-Jun-19 10:38 AM	DEX File	6,038 KB
firebase-abt.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-analytics.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-analytics-impl.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-common.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-config.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB
firebase-core.properties	04-Jun-19 10:38 AM	PROPERTIES File	1 KB

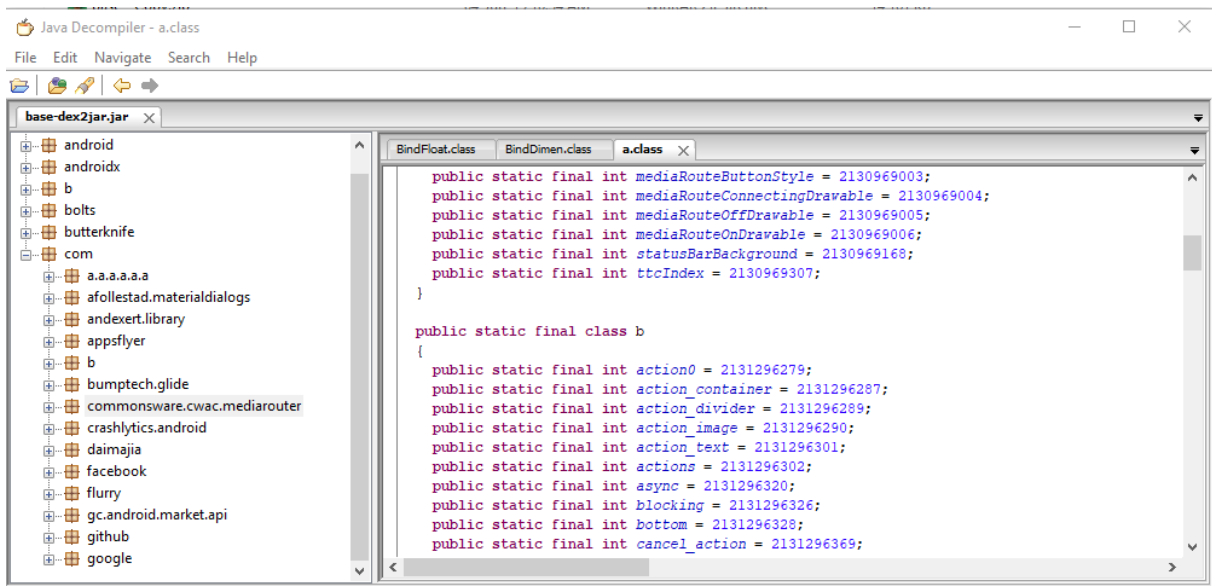
Có thể dùng APK_OneClick để xem code Java của ứng dụng. Sau khi cài đặt ứng dụng, Chọn Nhấp phải vào tập tin APK → Chọn Browse Java Code of APK.

base.apk 04-Jun-19 10:34 AM APK File 14,161 KB

```

C:\WINDOWS\system32\cmd.exe
dex2jar C:\Users\Totoro\AppData\Local\Android\sdk\platform-tools\vn.vtv.vtgo-2\base.apk -> C:\Users\Totoro\AppData\Local\Temp\base-dex2jar.jar

```



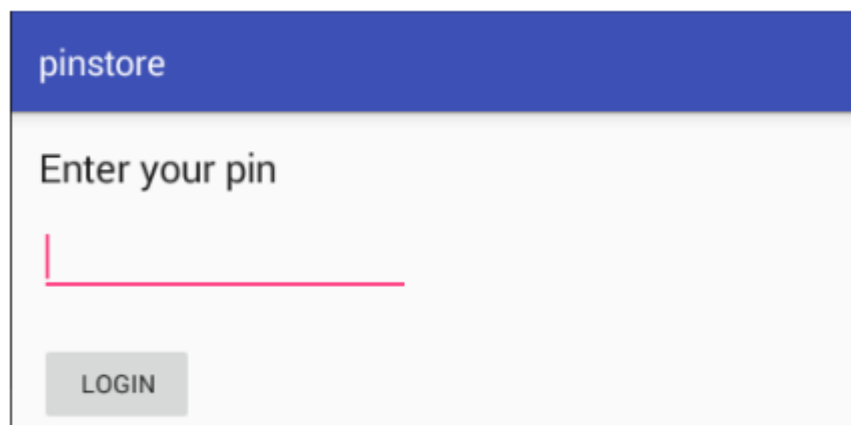
B6. Kịch bản tổng hợp

1. Kịch bản 01. Thực hiện phân tích ứng dụng Android

- Mô tả: Phân tích ứng dụng Android, tìm mã PIN trong ứng dụng để tìm flag.
- Tài nguyên thực hiện: pinstore.zip
- Yêu cầu – Gợi ý: Sử dụng các công cụ dịch ngược (decompile) trên mã nguồn Android để phân tích.

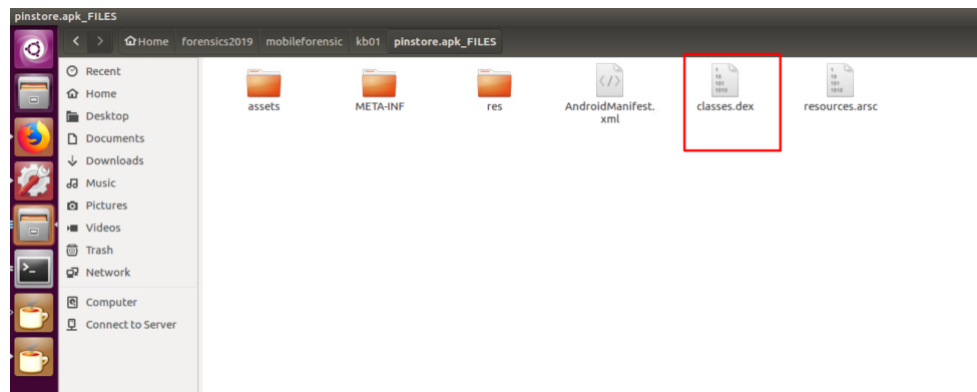
Đáp án:

Gợi ý:

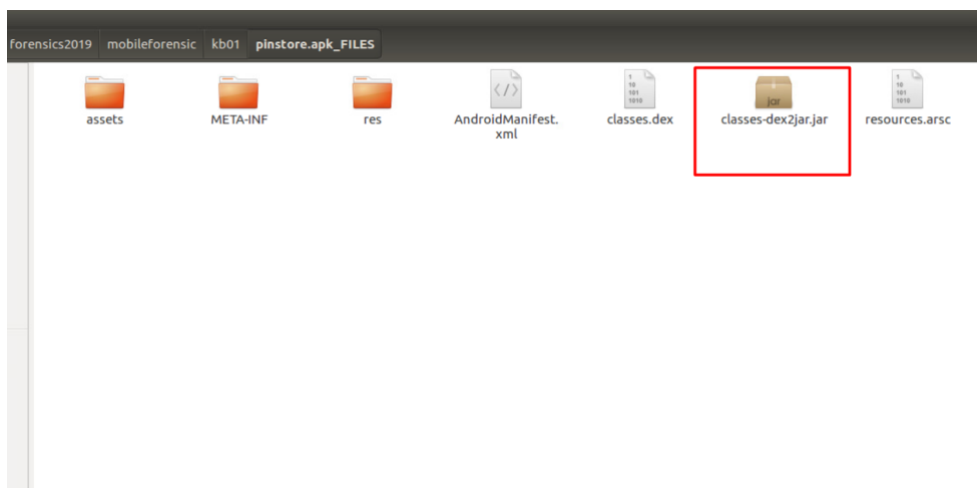


Hình 1. Ứng dụng Pinstore

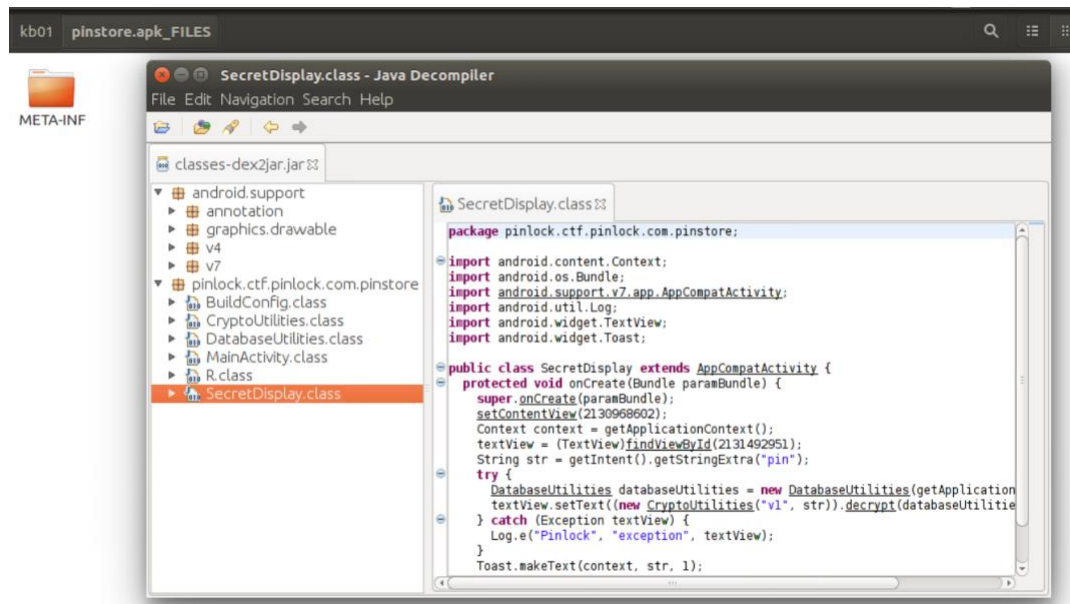
- Giải nén tập tin .zip, và giải nén tập tin .apk. Sau khi thu được tập tin classes.dex thì chuyển đổi thành tập tin JAR.



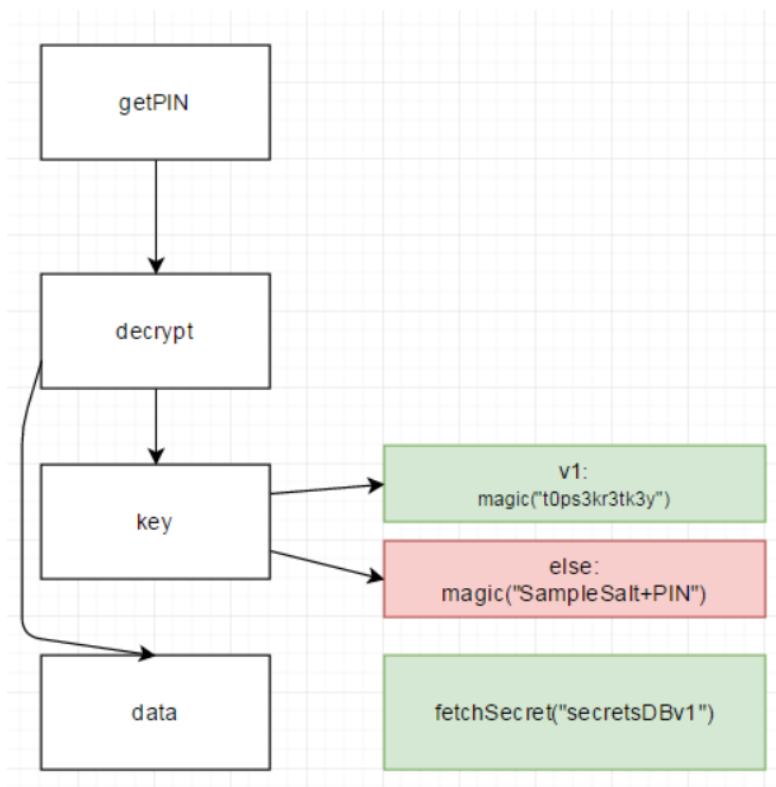
```
insecclab@uSense:~/forensics2019/mobileforensic/kb01/dex2jar-2.0$ sh d2j-dex2jar
.sh classes.dex
./classes-dex2jar.jar exists, use --force to overwrite
insecclab@uSense:~/forensics2019/mobileforensic/kb01/dex2jar-2.0$ sh d2j-dex2jar
.sh classes.dex
dex2jar classes.dex -> ./classes-dex2jar.jar
insecclab@uSense:~/forensics2019/mobileforensic/kb01/dex2jar-2.0$
```



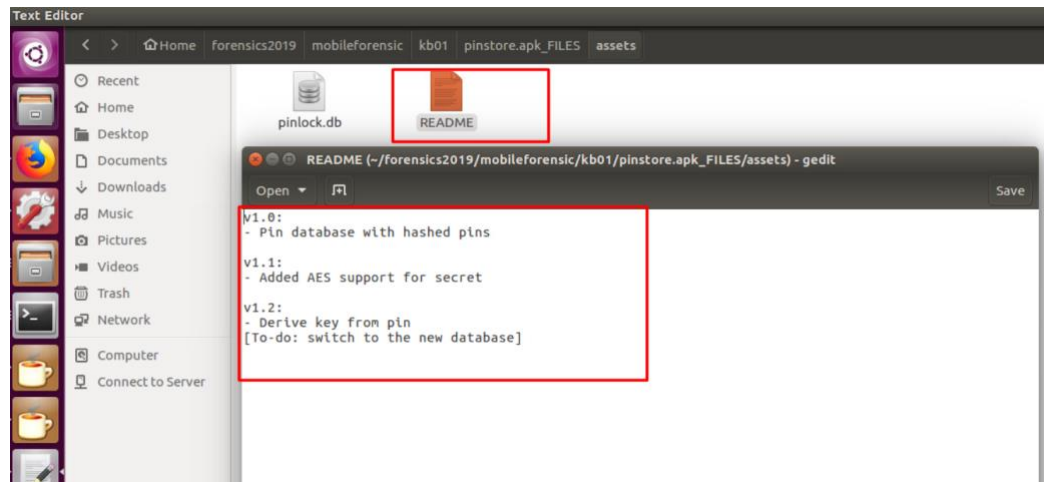
- Cài đặt JD-GUI (hoặc JADX) để decompile tập tin .jar
<https://github.com/java-decompiler/jd-gui/releases>
<https://github.com/skylot/jadx>
- Dùng JD-GUI để mở tập tin .jar, quan sát:



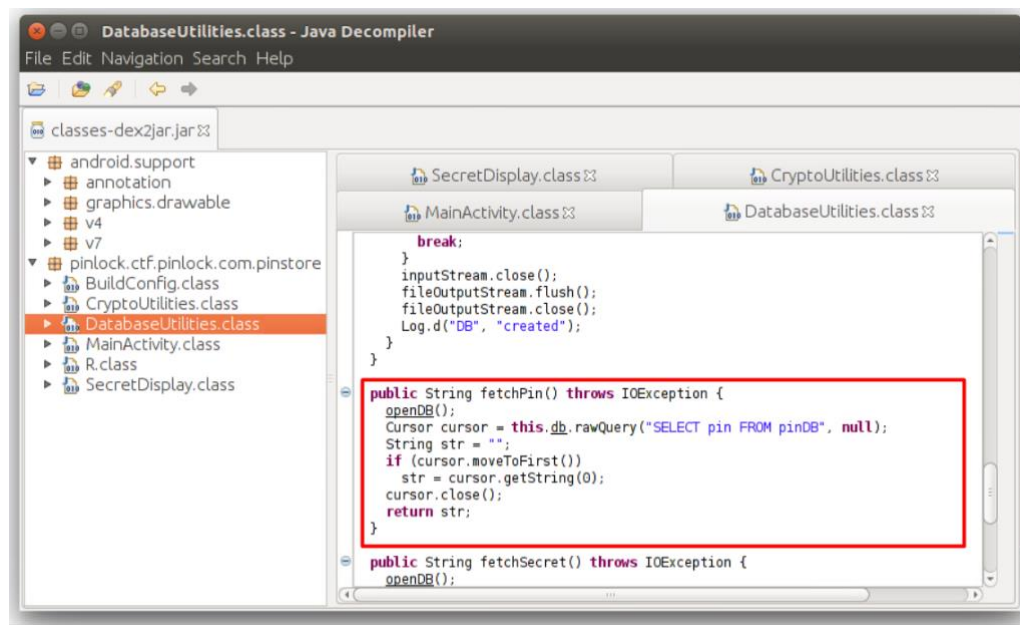
- Đọc code và thu được luồng hoạt động của mã PIN cùng dữ liệu mã hóa như sau:



- Ngoài ra, chú ý đến tập tin README trong thư mục assets. Thông tin này nói lên điều gì?



- Dựa vào cơ sở dữ liệu, trích xuất tất cả các giá trị của 2 bảng secretsDBv1 và secretsDBv2.
- Chú ý nội dung của hàm lấy mã PIN từ CSDL, phân tích cách hoạt động:



- Xác định mã PIN, sau đó viết code để giải mã tìm flag, giải thích cách làm, giá trị các tham số SECRET, salt, pin:

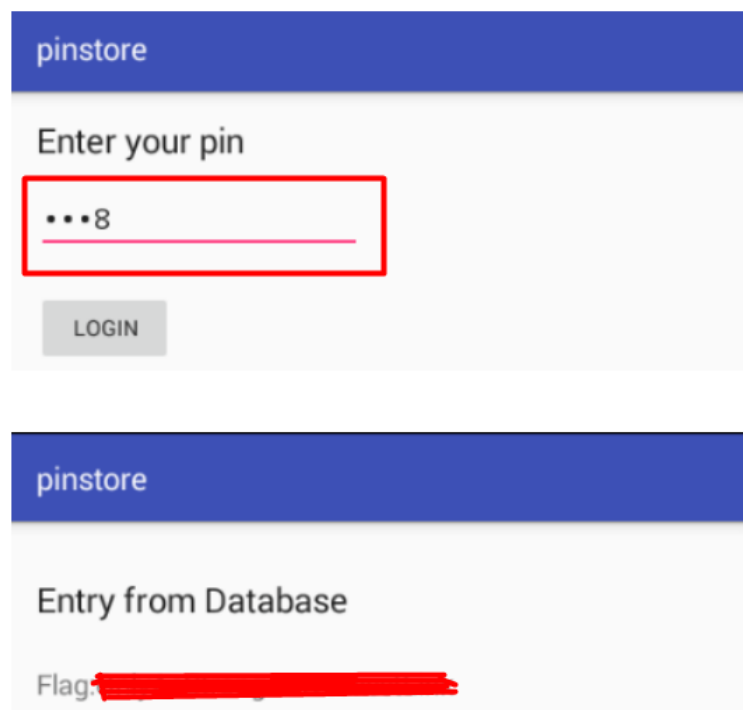
```
// rename as HelloWorld.java :)
import java.io.UnsupportedEncodingException;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.util.Arrays;
import javax.crypto.Cipher;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.PBEKeySpec;
import javax.crypto.spec.SecretKeySpec;
import sun.misc.BASE64Decoder;

public class HelloWorld{

    public static void main(String[] args) throws Exception
    {
        String SECRET = "B1528nD1NbCX9bCC+ZqGQo10z01+GOWSmvxRj7jglg=";

        Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
        byte[] salt = "SampleSalt".getBytes();
        String pin = "...8";
        SecretKeySpec key = new SecretKeySpec(SecretKeyFactory.getInstance("PBKDF2WithHmacSHA1").generateSecret(new PBEKeySpec(pin.toCharArray(), salt, 1000, 128)).getEncoded(), "AES");
        cipher.init(2, key);
        BASE64Decoder decoder = new BASE64Decoder();
        System.out.println(new String(cipher.doFinal(decoder.decodeBuffer(SECRET)), "UTF-8"));
    }
}
```

- Có thể kiểm tra lại kết quả bằng cách sau:



2. Kịch bản 02. Thực hiện phân tích tập tin ứng dụng thu được.

- Mô tả: Ứng dụng kb02 cần được phân tích thành mã smali để tìm flag.
- Tài nguyên thực hiện: kb02_zha.apk
- Yêu cầu – Gợi ý: sử dụng công cụ APKTool/ JADX/ dex2jar/ jdgui/ Android Studio, flag có dạng CTF{....}

Đáp án:

Gợi ý:

- Xem nội dung tập tin AndroidManifest.xml, phân tích cấu trúc ứng dụng, đánh giá các điểm đáng ngờ.

```
<?xml version="1.0" encoding="utf-8"?>
2 <manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" ar
7 <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="27"/>
11 <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon='
19 <activity android:theme="@style/AppTheme_NoActionBar" android:label="@string/title_activity_r2
23 <activity android:name="com.example.blink.MainActivity">
24 <intent-filter>
25 <action android:name="android.intent.action.MAIN"/>
27 <category android:name="android.intent.category.LAUNCHER"/>
24 </intent-filter>
23 </activity>
11 </application>
2 </manifest>
```

3. Kịch bản 03. Thực hiện phân tích tập tin ứng dụng thu được.

- Mô tả: Một ứng dụng có tính năng ghi nhớ các địa điểm mà người dùng muốn hay không muốn tham quan chỉ bằng dấu tick đơn giản trên bản đồ. Tìm flag.
- Tài nguyên: kb03_yon.apk
- Yêu cầu – Gợi ý: Decompile, chú ý CSDL của ứng dụng.

Gợi ý:

4. Kịch bản 04. Điều tra trên tập tin ứng dụng thu được.

- Mô tả: Một ứng dụng thời tiết đơn giản có tính năng thu thập và hiển thị thông tin thời tiết.
- Tài nguyên: kb04_tianqi.apk
- Yêu cầu – Gợi ý: Xác định phiên bản Android đang chạy của ứng dụng. Sử dụng một số công cụ decompile apk như Jadx để phân tích code ứng dụng. Flag có định dạng CTF{...}

Đáp án:

C. THAM KHẢO

<https://www.sciencedirect.com/topics/computer-science/mobile-forensics>

<https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/>

<https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/common-mobile-forensics-tools-and-techniques/#gref>

<https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/#gref>

D. YÊU CẦU

Bài thực hành được chia làm 2 phần riêng biệt.

- **Class Part (CP):** Sinh viên hoàn thành trên lớp (Bắt buộc).
0% <= CP < 50%: 1đ
50% <= CP < 90 %: 5đ
90% <= CP <= 100%: 10đ
- **Home Part (HP):** Hoàn thành phần còn lại và làm báo cáo sau khi kết thúc buổi thực hành (nộp trên Course môn học theo deadline).
- Điểm Thực hành của mỗi Buổi (Session): **$S = (CP + HP)/2$**

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả gồm chi tiết những việc bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.DOCX và .PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Chỉ dùng duy nhất 1 loại Font chữ (**Times New Roman – cỡ chữ 12**)
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).
Ví dụ: [NT101.H11.1]-Session1_Group3.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài Lab.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

Bài sao chép, nộp trễ, thực hiện không nghiêm túc ... sẽ được xử lý tùy mức độ vi phạm.



HẾT