

BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Kỳ báo cáo: Buổi 5

Tên chủ đề: Mobile Forensics

GVHD: Lê Đức Thịnh

Ngày báo cáo: 12/6/2023

Nhóm: 7

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Nguyễn Bùi Kim Ngân	20520648	20520648@gm.uit.edu.vn
2	Nguyễn Bình Thực Trâm	20520815	20520815@gm.uit.edu.vn
3	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Thực hiện	Thành viên thực hiện	Kết quả tự đánh giá
1	Yêu cầu 0	Tìm hiểu công cụ	Kiệt Trâm Ngân	100%
2	Yêu cầu 1	Tìm flag		100%
3	Yêu cầu 2	Tìm flag		100%
4	Yêu cầu 3	Tìm flag		100%
5	Yêu cầu 4	Tìm flag		100%

Lưu ý: Chỉ ghi Kịch bản thực hành được GVTTH chỉ định phải làm báo cáo

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

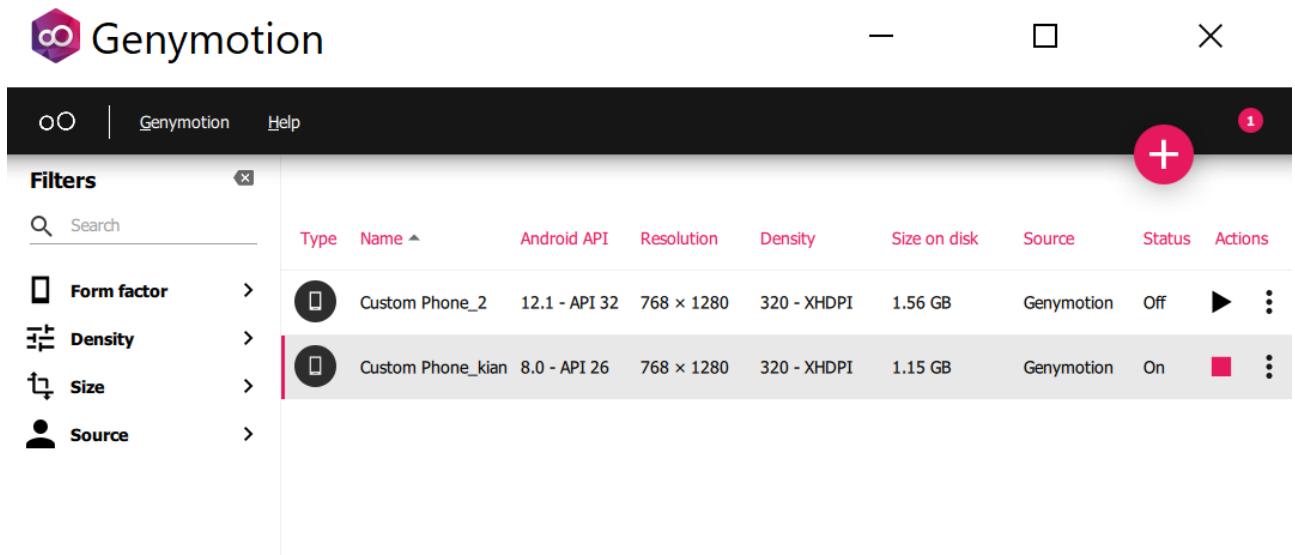
(Xem trang kế tiếp)

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành,

BÁO CÁO CHI TIẾT

1. Kịch bản 0

Dùng genymotion và Oracle VM để tạo điện thoại android ảo như dưới với phiên bản android là 8.0



Kiểm tra device

```
E:\NT213-BaoMatWeb&App\tool\platform-tools>adb devices
List of devices attached
192.168.227.101:5555    device
```

Cài đặt ứng dụng kb2_zha.apk

```
E:\NT213-BaoMatWeb&App\tool\platform-tools>adb install kb02_zha.apk
Performing Streamed Install
Success
```

Vào shell của điện thoại

```
E:\NT213-BaoMatWeb&App\tool\platform-tools>adb shell
genymotion:/ # ls -l
total 2416
dr-xr-xr-x 48 root root 0 2023-06-12 06:42 acct
lrwxrwxrwx 1 root root 50 1970-01-01 00:00 bugreports -> /data/user_0/com.android.shell/files/bugreports
drwxrwx--- 6 system cache 4096 2023-05-09 18:01 cache
lrwxrwxrwx 1 root root 13 1970-01-01 00:00 charger -> /sbin/charger
dr-x----- 2 root root 40 1970-01-01 00:00 config
lrwxrwxrwx 1 root root 17 1970-01-01 00:00 d -> /sys/kernel/debug
drwxrwx--x 36 system system 4096 2023-05-09 18:01 data
-rw----- 1 root root 787 1970-01-01 00:00 default.prop
drwxr-xr-x 16 root root 2740 2023-06-12 06:42 dev
lrwxrwxrwx 1 root root 11 1970-01-01 00:00 etc -> /system/etc
-rw-r----- 1 root root 399 1970-01-01 00:00 fstab.vbox86
-rwxr-x--- 1 root root 1882604 1970-01-01 00:00 init
-rwxr-x--- 1 root root 996 1970-01-01 00:00 init.environ.rc
-rwxr-x--- 1 root root 28033 1970-01-01 00:00 init.rc
-rwxr-x--- 1 root root 7623 1970-01-01 00:00 init.usb.configfs.rc
-rwxr-x--- 1 root root 5632 1970-01-01 00:00 init.usb.rc
-rwxr-x--- 1 root root 2992 1970-01-01 00:00 init.vbox86.rc
-rwxr-x--- 1 root root 497 1970-01-01 00:00 init.zygote32.rc
drwxr-xr-x 11 root system 240 2023-06-12 06:42 mnt
-rw-r--r-- 1 root root 4369 1970-01-01 00:00 nonplat_file_contexts

```

Xem danh sách các ứng dụng hệ thống/ các ứng dụng cài sẵn

```
C:\Windows\System32\cmd.exe - adb shell
genymotion:/ # pwd
/
genymotion:/ # cd /system/app
genymotion:/system/app # ls
Amaze Development PacProcessor
BasicDreams DevelopmentSettings PhotoTable
Bluetooth DownloadProviderUi PicoTts
BluetoothMidiService EasterEgg PrintRecommendationService
BookmarkProvider Email PrintSpooler
Browser2 ExactCalculator QuickSearchBox
BuiltInPrintService ExtShared SettingsService
Calendar Gallery2 Superuser
Camera2 GenyMotionLayout SystemPatcher
CaptivePortalLogin KeyChain UserDictionaryProvider
CarrierDefaultApp HTMLViewer WAPPushManager
CertInstaller LatinIME WallpaperBackup
CompanionDeviceManager LiveWallpapersPicker WallpaperPicker
CtsShimPrebuilt Music messaging
CubeLiveWallpapers NfcNci webview
CustomLocale OpenWnn
DeskClock genymotion:/system/app #
```

Xem dữ liệu các ứng dụng, nằm trong thư mục /data/data

```
C:\Windows\System32\cmd.exe - adb shell
genymotion:/ # cd /data/data
genymotion:/data/data # ls
android
android.ext.services
android.ext.shared
com.amaze.filemanager
com.android.backupconfirm
com.android.bips
com.android.bluetooth
com.android.bluetoothmidiservice
com.android.bookmarkprovider
com.android.calculator2
com.android.calendar
com.android.calllogbackup
com.android.camera2
com.android.captiveportallogin
com.android.carrierconfig
com.android.carrierdefaultapp
com.android.cellbroadcastreceiver
com.android.certinstaller
com.android.companiondevicemanager
com.android.contacts
com.android.cts.ctsshim
com.android.cts.priv.ctsshim
com.android.customlocale2
```

Thư mục của ứng dụng đã cài ở trên

```
genymotion:/data/data # cd com.example.blink
genymotion:/data/data/com.example.blink # ls
cache code_cache
genymotion:/data/data/com.example.blink #
```

Xem database của email

```
genymotion:/data/data # cd com.android.email
genymotion:/data/data/com.android.email # ls
cache code_cache databases files shared_prefs
genymotion:/data/data/com.android.email # cd databases
genymotion:/data/data/com.android.email/databases # ls
EmailProvider.db EmailProviderBody.db
EmailProvider.db-journal EmailProviderBody.db-journal
genymotion:/data/data/com.android.email/databases/EmailProvider.db E:\NT334-PhapChungKTS
```

Dump database của email về máy

```
E:\NT213-BaoMatWeb&App\tool\platform-tools>adb pull -p /data/data/com.android.email/databases/EmailProvider.db E:\NT334-PhapChungKTS
/data/data/com.android.email/databases/EmailProvider.db: 1 file pulled, 0 skipped. 19.2 MB/s (135168 bytes in 0.007s)
```

This PC > STUDY (E:) > NT334-PhapChungKTS >		▼	↻	Search NT334-PhapChungKTS
Name	Date modified	Type	Size	
Slides	6/5/2023 10:35 AM	File folder		
ThucHanh	4/26/2023 5:55 PM	File folder		
[NT334.N21.ANTN-BT.docx	5/24/2023 4:39 PM	Microsoft Word D...	2,369 K	
EmailProvider.db	6/12/2023 2:18 PM	Data Base File	132 K	

Dùng dumpsys để xem thông tin về pin

```
ls Select C:\Windows\System32\cmd.exe
E:\NT213-BaoMatWeb&App\tool\platform-tools>adb shell dumpsys batterystats
Battery History (2% used, 5464 used of 256KB, 39 strings using 2112):
  0 (10) RESET:TIME: 2023-05-16-11-39-13
    0 (3) 095 status=discharging health=unknown plug=none temp=0 volt=10000 charge=0 +running +wake_lock +sensor +screen data_conn=lte phone_signal_strength=moderate brightness=medium +wifi_running +wifi wifi_signal_strength=4 wifi_suppl=completed top=u0:a71:"com.hellocmu.picotf"
    Details: cpu=0u0v0s
      /proc/stat=0 usr, 0 sys, 0 io, 0 irq, 0 sirq, 0 idle, PlatformIdleStat null
      0 (2) 095 user=0:"0"
      0 (2) 095 userfg=0:"0"
    +2ms (8) START
    +2ms (10) TIME: 2023-05-16-11-41-26
    +8ms (8) START
    +8ms (10) TIME: 2023-05-16-14-15-34
    +12ms (8) START
    +12ms (10) TIME: 2023-05-16-14-16-35
    +18ms (8) START
    +18ms (10) TIME: 2023-05-16-14-23-53
    +2s995ms (3) 071 status=charging health=unknown plug=ac temp=0 volt=10000 charge=0 +running +plugged +charging
    +4s121ms (2) 071 +screen
    +4s121ms (3) 071 +wake_lock=1:"screen" brightness=bright
    +4s122ms (3) 071 brightness=medium +wifi_running +wifi stats=0:"network-stats-enabled"
    +5s121ms (2) 071 stats=0:"wifi-running"
    +5s133ms (2) 071 stats=0:"wifi-off"
    +5s510ms (2) 071 +user=0:"0"
    +5s510ms (2) 071 +userfg=0:"0"
    +5s548ms (3) 071 +phone_scanning phone_state=out +top=1000:"com.android.settings"
    +6s736ms (3) 071 +sensor +wifi_scan +top=1000:"com.android.settings"
    +7s698ms (2) 071 +top=u0:a14:"com.android.launcher3"
    +8s898ms (2) 071 -phone_scanning phone_state=in
    +9s398ms (3) 072 stats=0:"battery-level"
    +10s612ms (3) 072 +mobile_radio data_conn=lte conn=0:"CONNECTED"
    +10s896ms (2) 072 +job=u0:a13:"com.android.dialer/com.android.voicemail.impl.StatusCheckJobService"
    +10s903ms (2) 072 -wifi_scan wifi_suppl=authenticating -job=u0:a13:"com.android.dialer/com.android.voicemail.impl.StatusCheckJobService"
    +11s100ms (3) 072 wifi_suppl=associating
    +11s101ms (1) 072 wifi_signal_strength=4 wifi_suppl=associated
    +11s126ms (2) 072 +wifi_radio wifi_suppl=completed stats=0:"wifi-state"
    +11s408ms (2) 072 conn=0:"DISCONNECTED"
    +11s408ms (2) 072 conn=1:"CONNECTED"
    +11s693ms (2) 072 +job=u0:a13:"com.android.dialer/com.android.voicemail.impl.scheduling.TaskSchedulerJobService"
    +11s725ms (2) 072 -job=u0:a13:"com.android.dialer/com.android.voicemail.impl.scheduling.TaskSchedulerJobService"
    +11s727ms (2) 072 +job=u0:a13:"com.android.dialer/com.android.voicemail.impl.scheduling.TaskSchedulerJobService"
    +11s853ms (10) TIME: 2023-05-16-14-24-04
    +27s556ms (1) 072 +wifi_scan
```

Xem tình trạng sử dụng bộ xử lý của các ứng dụng đang chạy

```
C:\Windows\System32\cmd.exe
E:\NT213-BaoMatWeb&App\tool\platform-tools>adb shell dumpsys procstats
CURRENT STATS:
* system / 1000 / v26:
    TOTAL: 100% (87MB-97MB-113MB/73MB-81MB-95MB over 3)
    Persistent: 100% (87MB-97MB-113MB/73MB-81MB-95MB over 3)
* com.android.systemui / u0a26 / v26:
    TOTAL: 100% (65MB-85MB-124MB/50MB-72MB-110MB over 3)
    Persistent: 100% (65MB-85MB-124MB/50MB-72MB-110MB over 3)
* com.android.inputmethod.latin / u0a55 / v26:
    TOTAL: 100% (13MB-13MB-13MB/7.2MB-7.9MB-9.3MB over 3)
    Imp Fg: 0.10%
    Imp Bg: 100% (13MB-13MB-13MB/7.2MB-7.9MB-9.3MB over 3)
* com.android.phone / 1001 / v26:
    TOTAL: 100% (23MB-24MB-25MB/17MB-17MB-18MB over 3)
    Persistent: 100% (23MB-24MB-25MB/17MB-17MB-18MB over 3)
* com.genymotion.settings / 1000 / v26:
    TOTAL: 100% (5.7MB-6.0MB-6.2MB/3.1MB-3.1MB over 3)
    Persistent: 100% (5.7MB-6.0MB-6.2MB/3.1MB-3.1MB over 3)
* com.genymotion.systempatcher / 1000 / v26:
    TOTAL: 100% (6.4MB-6.7MB-6.9MB/4.0MB-4.0MB-4.0MB over 3)
    Persistent: 100% (6.4MB-6.7MB-6.9MB/4.0MB-4.0MB-4.0MB over 3)
* com.genymotion.genynd / 1000 / v26:
    TOTAL: 100% (5.5MB-6.4MB-7.0MB/3.1MB-3.7MB-4.1MB over 3)
    Persistent: 100% (5.5MB-6.4MB-7.0MB/3.1MB-3.7MB-4.1MB over 3)
* com.android.smspush / u0a62 / v26:
    TOTAL: 100% (3.9MB-4.2MB-4.5MB/1.8MB-1.9MB-1.9MB over 3)
    Imp Fg: 100% (3.9MB-4.2MB-4.5MB/1.8MB-1.9MB-1.9MB over 3)
* com.example.blink / u0a78 / v1:
    TOTAL: 34% (17MB-17MB-18MB/13MB-13MB-13MB over 7)
    Top: 34% (17MB-17MB-18MB/13MB-13MB-13MB over 7)
* com.android.launcher3 / u0a14 / v26:
    TOTAL: 23% (25MB-28MB-34MB/16MB-18MB-21MB over 8)
    Top: 23% (25MB-28MB-34MB/16MB-18MB-21MB over 8)
    (Home): 77% (24MB-26MB-26MB/17MB-17MB-18MB over 5)
* com.example.blink / u0a77 / v1:
    TOTAL: 21% (18MB-18MB-18MB/13MB-13MB-13MB over 4)
    Top: 21% (18MB-18MB-18MB/13MB-13MB-13MB over 4)
    (Cached): 3.9% (17MB-17MB-17MB/13MB-13MB-13MB over 1)
* com.android.dialer / u0a13 / v130000:
    TOTAL: 13% (12MB-12MB-12MB/7.0MB-7.0MB-7.0MB over 1)
    Imp Bg: 13% (12MB-12MB-12MB/7.0MB-7.0MB-7.0MB over 1)
```

Hiển thị thông tin người dùng đang sử dụng thiết bị

```
C:\Windows\System32\cmd.exe
E:\NT213-BaoMatWeb&App\tool\platform-tools>adb shell dumpsys user
Users:
UserInfo{0:null:13} serialNo=0
State: RUNNING_UNLOCKED
Created: <unknown>
Last logged in: +44m4s830ms ago
Last logged in fingerprint: google/vbox86p/vbox86p:8.0.0/OPR6.170623.017/434:userdebug/test-keys
Has profile owner: false
Restrictions:
    none
Device policy global restrictions:
    null
Device policy local restrictions:
    null
Effective restrictions:
    none
Device owner id:-10000
Guest restrictions:
    no_sms
    no_install_unknown_sources
    no_config_wifi
    no_outgoing_calls
Device managed: false
Started users state: {0=3}
Max users: 4
Supports switchable users: true
All guests ephemeral: false
E:\NT213-BaoMatWeb&App\tool\platform-tools>
```

Xem thông tin về quyền hạn có thể truy cập bởi các ứng dụng

```
C:\Windows\System32\cmd.exe
E:\NT213-BaoMatWeb&App\tool\platform-tools>adb shell dumpsys appops
Current AppOps Service state:
Op mode watchers:
Op COARSE_LOCATION:
#0: com.android.server.AppOpsService$Callback@f1ac46b
Op SYSTEM_ALERT_WINDOW:
#0: com.android.server.AppOpsService$Callback@fb7a70
Op PLAY_AUDIO:
#0: com.android.server.AppOpsService$Callback@4446b65
#1: com.android.server.AppOpsService$Callback@8dc859d
Op TOAST_WINDOW:
#0: com.android.server.AppOpsService$Callback@fb7a70
Op GET_ACCOUNTS:
#0: com.android.server.AppOpsService$Callback@12d7a86
Op RUN_IN_BACKGROUND:
#0: com.android.server.AppOpsService$Callback@e8ea7a5
Package mode watchers:
Pkg com.android.systemui:
#0: com.android.server.AppOpsService$Callback@8dc859d
All mode watchers:
android.app.AppOpsManager$1@0b7ff61 -> com.android.server.AppOpsService$Callback@12d7a86
com.android.server.am.ActivityManagerService$3@ae1419c -> com.android.server.AppOpsService$Callback@e8ea7a5
android.app.AppOpsManager$1@03c4b3 -> com.android.server.AppOpsService$Callback@fb7a70
android.media.PlayerBase$IAudioPcmCallbackWrapper@08bc5c -> com.android.server.AppOpsService$Callback@4446b65
android.os.BinderProxy@947c74 -> com.android.server.AppOpsService$Callback@8dc859d
android.app.AppOpsManager$1@fa85dba -> com.android.server.AppOpsService$Callback@f1ac46b
Clients:
android.os.Binder@b08ea12:
ClientState{mAppToken=android.os.Binder@b08ea12, local}
android.os.BinderProxy@c9678aa:
ClientState{mAppToken=android.os.BinderProxy@c9678aa, pid=232}

Uid 1000:
Package com.genymotion.settings:
READ_EXTERNAL_STORAGE: mode=0; time=+45m0s653ms ago
WRITE_EXTERNAL_STORAGE: mode=0; time=+45m0s653ms ago
Package com.genymotion.systempatcher:
READ_EXTERNAL_STORAGE: mode=0; time=+45m0s642ms ago
WRITE_EXTERNAL_STORAGE: mode=0; time=+45m0s642ms ago
Package android:
COARSE_LOCATION: mode=0; time=+45m1s643ms ago
READ_CALENDAR: mode=0; time=+45m4s773ms ago
```

Hiển thị danh sách các SSID mà thiết bị đã kết nối tới

```
C:\Windows\System32\cmd.exe
E:\NT213-BaoMatWeb&App\tool\platform-tools>adb shell dumpsys wifi
Wi-Fi is enabled
Stay-aware conditions: 1
minidleMode false
mScanPending false
WifiController:
total records=14
rec[0]: time=06-12 06:42:59.063 processed=ApStaDisabledState org=ApStaDisabledState dest=<null> what=155656(0x26008)
rec[1]: time=06-12 06:42:59.570 processed=ApStaDisabledState org=ApStaDisabledState dest=<null> what=155659(0x2600b)
rec[2]: time=06-12 06:42:59.570 processed=ApStaDisabledState org=ApStaDisabledState dest=DeviceActiveState what=155656(0x26008)
rec[3]: time=06-12 06:43:00.083 processed=DefaultState org=DeviceActiveState dest=<null> what=155652(0x26004)
rec[4]: time=06-12 06:43:00.096 processed=DefaultState org=DeviceActiveState dest=<null> what=155652(0x26004)
rec[5]: time=06-12 06:43:00.624 processed=DeviceActiveState org=DeviceActiveState dest=<null> what=155660(0x2600c)
rec[6]: time=06-12 06:43:02.252 processed=DeviceActiveState org=DeviceActiveState dest=<null> what=155660(0x2600c)
rec[7]: time=06-12 07:00:20.538 processed=DeviceActiveState org=DeviceActiveState dest=<null> what=155652(0x26004)
rec[8]: time=06-12 07:00:50.533 processed=DefaultState org=DeviceActiveState dest=<null> what=155652(0x26004)
rec[9]: time=06-12 07:03:14.603 processed=DefaultState org=DeviceActiveState dest=<null> what=155652(0x26004)
rec[10]: time=06-12 07:06:12.532 processed=DefaultState org=DeviceActiveState dest=<null> what=155652(0x26004)
rec[11]: time=06-12 07:08:54.537 processed=DefaultState org=DeviceActiveState dest=<null> what=155652(0x26004)
rec[12]: time=06-12 07:12:02.537 processed=DefaultState org=DeviceActiveState dest=<null> what=155652(0x26004)
rec[13]: time=06-12 07:26:08.544 processed=DefaultState org=DeviceActiveState dest=<null> what=155652(0x26004)
currState=DeviceActiveState
mScreenOff false
mDeviceIdle false
mPluggedType 1
mIdleMillis 900000
mSleepPolicy 2
mPersistWifiState 1
mAirplaneModeOn false
mNotificationEnabled true
mNotificationRepeatTime 0
mNotificationShown false
mNumScansSinceNetworkStateChange 0
mEnableTrafficStatsPoll true
mTrafficStatsPollToken 8
mTxPkts 104
mRxPkts 97
mDataActivity 0

Locks held:
Locks acquired: 0 full, 0 full high perf, 0 scan
Locks released: 0 full, 0 full high perf, 0 scan
```

2. Set up

Dịch ngược bằng MobSF kb01



APP SCORES

FILE INFORMATION

APP INFORMATION

SCANNER OPTIONS

DECOMPILED CODE

Detailed description: This screenshot shows the MobSF static analysis interface for the APK file 'pinstore.apk'. The 'APP SCORES' section indicates a high security score of 45/100 and 0 tracked detections. The 'FILE INFORMATION' section provides details like file name, size (1.18MB), MD5, SHA1, and SHA256. The 'APP INFORMATION' section lists the app's name as 'pinstore', package name as 'pinlock.ctf.pinlock.com.pinstore', and main activity as 'pinlock.ctf.pinlock.com.pinstore.MainActivity'. Below these are four cards showing activity, service, receiver, and provider counts, all of which are zero.

Dịch ngược bằng MobSF kb02

APP SCORES

FILE INFORMATION

APP INFORMATION

SCANNER OPTIONS

DECOMPILED CODE

Detailed description: This screenshot shows the MobSF static analysis interface for the APK file 'kb02_zha.apk'. The 'APP SCORES' section shows a moderate security score of 38/100 and 0 tracked detections. The 'FILE INFORMATION' section provides details like file name, size (2.05MB), MD5, SHA1, and SHA256. The 'APP INFORMATION' section lists the app's name as 'Droids', package name as 'com.example.blink', and main activity as 'com.example.blink.MainActivity'. Below these are four cards showing activity, service, receiver, and provider counts, all of which are zero.

Dịch ngược bằng MobSF kb03

APP SCORES

FILE INFORMATION

APP INFORMATION

SCANNER OPTIONS

DECOMPILED CODE

Detailed description: This screenshot shows the MobSF static analysis interface for the APK file 'kb03_yon.apk'. The 'APP SCORES' section shows a high security score of 46/100 and 0 tracked detections. The 'FILE INFORMATION' section provides details like file name, size (2.03MB), MD5, SHA1, and SHA256. The 'APP INFORMATION' section lists the app's name as 'Yay or Nay?', package name as 'com.example.yayornay', and main activity as 'com.example.yayornay.MainActivity'. Below these are four cards showing activity, service, receiver, and provider counts, all of which are zero.

Dịch ngược bằng MobSF kb04

The screenshot shows the MobSF static analysis interface. On the left, there's a sidebar with various analysis options like Information, Scan Options, Signer Certificate, Permissions, Android API, Browseable Activities, Security Analysis, Malware Analysis, Reconnaissance, Components, PDF Report, Print Report, and Start Dynamic Analysis. The main area has tabs for RECENT SCANS, STATIC ANALYZER, DYNAMIC ANALYZER, REST API, DONATE, DOCS, and ABOUT. The current tab is STATIC ANALYZER. Under this tab, there are sections for APP SCORES, FILE INFORMATION, APP INFORMATION, SCAN OPTIONS, and DECOMPILATED CODE. The FILE INFORMATION section shows the file name as kb04_tianqi.apk, size as 1.63MB, and MD5, SHA1, SHA256 checksums. The APP INFORMATION section provides details about the app: App Name (Weather Companion), Package Name (com.example.myapplication), Main Activity (com.example.myapplication.MainActivity), Target SDK (27), Min SDK (26), Max SDK (30), and Android Version Name (1.0). Below these are four cards: ACTIVITIES (1), SERVICES (0), RECEIVERS (0), and PROVIDERS (0), each with a 'View' button. The SCAN OPTIONS tab is currently selected.

Dịch ngược bằng apktool

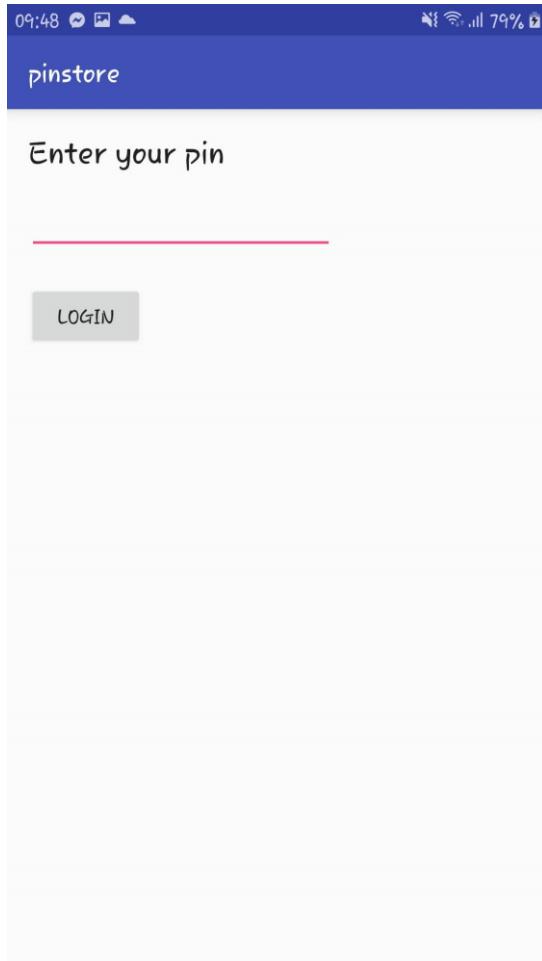
```

File Edit View Search Terminal Help
[1] kiet@parrot:[~/Downloads/nhombay_lab]
└─$ apktool d pinstore.apk
I: Using Apktool 2.7.0 on pinstore.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/kiet/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
[1] kiet@parrot:[~/Downloads/nhombay_lab]
└─$ apktool d kb03_yon.apk
I: Using Apktool 2.7.0 on kb03_yon.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/kiet/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
[1] kiet@parrot:[~/Downloads/nhombay_lab]
└─$ apktool d kb04_tianqi.apk \
> ^C
[1] kiet@parrot:[~/Downloads/nhombay_lab]
└─$ apktool d kb04_tianqi.apk
I: Using Apktool 2.7.0 on kb04_tianqi.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/kiet/.local/share/apktool/framework/1.apk

```

3. Kịch bản 01

Đầu tiên ta cài chương trình vào thiết bị thì ta thấy cần nhập mã pin



Ta sẽ đọc code thì thấy ta cần nhập mã pin để lấy flag



The screenshot shows the Android Studio interface with the following details:

- File Structure (Left):** Shows the project structure with files like `MainActivity.java`, `pinlock.ctf.pinlock`, `BuildConfig.java`, `CryptoUtilities.java`, `DatabaseUtilities.java`, `R.java`, and `SecretDisplay.java`.
- Code Editor (Right):** Displays the `MainActivity.java` code. The code handles pin entry logic, including hashing entered pins and comparing them against a database pin.

```
pinlock > ctf > pinlock > com > pinstore > MainActivity.java > { }-pinlock.ctf.pinlock.com.pinstore
button.setOnClickListener(new View.OnClickListener() { // from class: pinlock.ctf.pinlock.MainActivity
    @Override // android.view.View.OnClickListener
    public void onClick(View view) {
        String enteredPin = MainActivity.this.pinEditText.getText().toString();
        String pinFromDB = null;
        String hashOfEnteredPin = null;
        try {
            DatabaseUtilities dbUtil = new DatabaseUtilities(MainActivity.this.getApplicationContext());
            pinFromDB = dbUtil.fetchPin();
        } catch (IOException e) {
            e.printStackTrace();
        }
        try {
            hashOfEnteredPin = CryptoUtilities.getHash(enteredPin);
        } catch (UnsupportedEncodingException e2) {
            e2.printStackTrace();
        } catch (NoSuchAlgorithmException e3) {
            e3.printStackTrace();
        }
        if (pinFromDB.equalsIgnoreCase(hashOfEnteredPin)) {
            Intent intent = new Intent(MainActivity.this, SecretDisplay.class);
            intent.putExtra("pin", enteredPin);
            MainActivity.this.startActivity(intent);
            return;
        }
        MainActivity.this.pinEditText.setText("");
        Toast.makeText(MainActivity.this, "Incorrect Pin, try again", 1).show();
    }
});
```

Ta sẽ vào mục assets và mở pinlock database để xem thông tin trong database, ta sẽ lấy thông tin trong mục pinDB

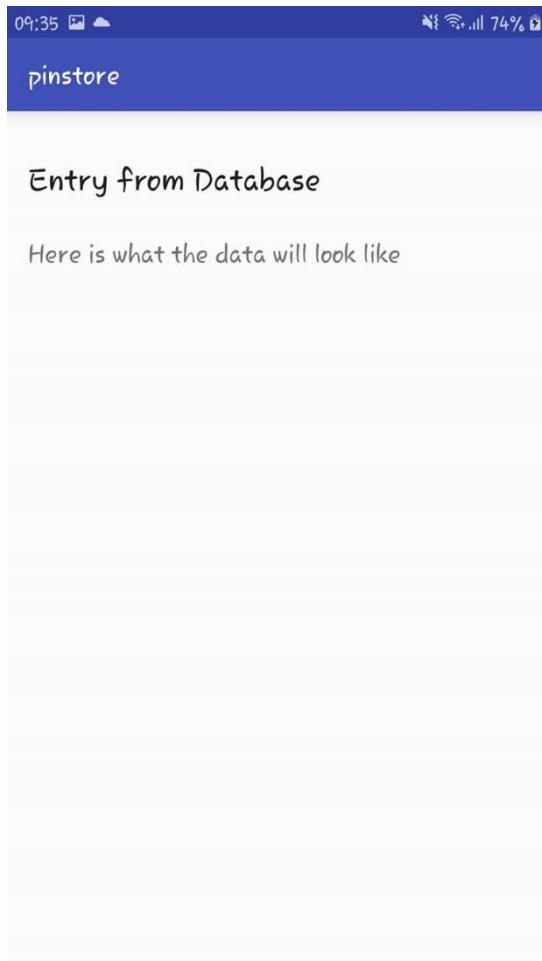
```
[kiet@parrot] -[~/Downloads/nhombay_lab/pinstore/assets]
└─$sqlite3 pinlock.db
SQLite version 3.34.1 2021-01-20 14:10:07
Enter ".help" for usage hints.
sqlite> .databases
main: /home/kiet/Downloads/nhombay_lab/pinstore/assets/pinlock.db r/w
sqlite> .table
android_metadata pinDB secretsDBv1 secretsDBv2
sqlite> select * from android_metadata
...>;
en_US ADME.license
sqlite> select * from pinDB
...>;
1|d8531a519b3d4dfbebe0259f90b466a23efc57b
sqlite> select * from secretsDBv1
...>;
1|hcsvUnln5jMdw3GeI4o/txB5vaEf1PFAKQ3kPsRW2o5rR0a1JE54d0BLkzXPtqB
sqlite> select * from secretsDBv2
...>;
1|Bi528nDlNBcX9BcCC+ZqGQo10z01+GOWSmvxRj7jg1g=
sqlite> █
```

Ta sẽ sử dụng crackstation để dịch thì ta có được pin là 7498

The screenshot shows the CrackStation website interface. At the top, it says "CrackStation" and "Free Password Hash Cracker". Below that, there's a text input field containing the hash "hcsvUnln5jMdw3GeI4o/txB5vaEf1PFAKQ3kPsRW2o5rR0a1JE54d0BLkzXPtqB". To the right of the input field is a CAPTCHA challenge with the text "I'm not a robot" and a reCAPTCHA button. Below the input field is a "Crack Hashes" button. Further down, there's some small text about supported hash types and a legend for color codes: green for exact match, yellow for partial match, and red for not found.

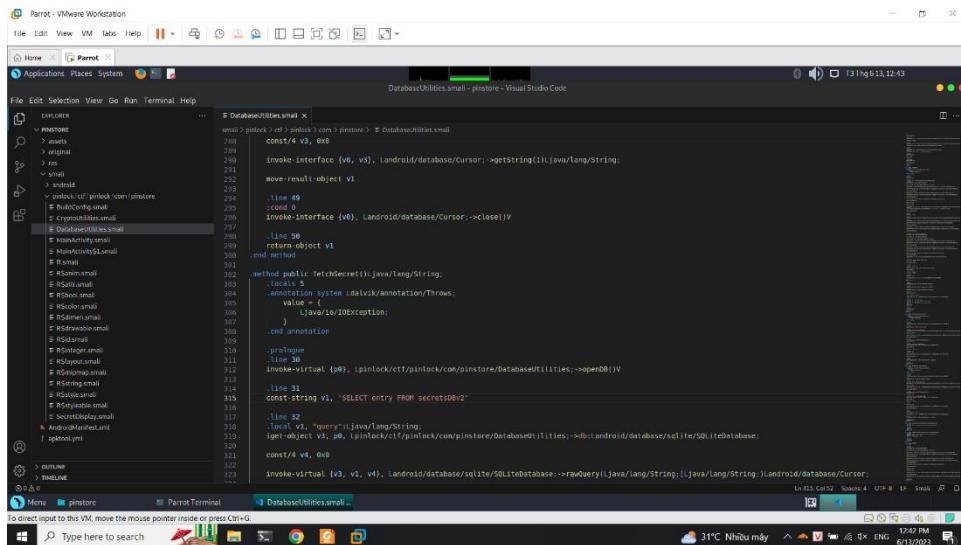
Hash	Type	Result
hcsvUnln5jMdw3GeI4o/txB5vaEf1PFAKQ3kPsRW2o5rR0a1JE54d0BLkzXPtqB	sha1	7498

Nhập pin vào thì truy cập được database

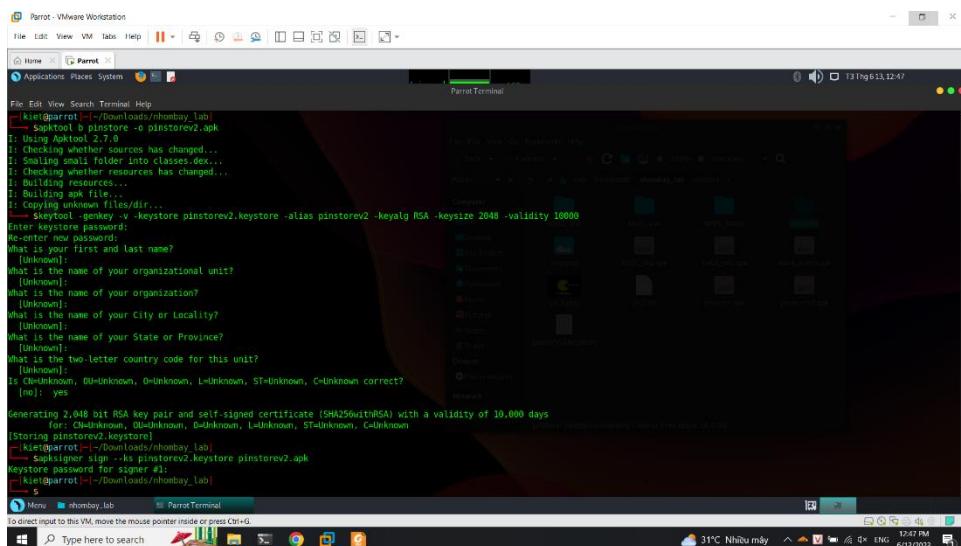


Tiếp tục thực hiện chỉnh code smali, đầu tiên ở phần chỉnh dòng 74 của secret display thành v2

Tiếp tục chỉnh dòng 315 của file DatabaseUtilities thành v2



Thực hiện build, tạo chữ ký, ký file và cài vào máy



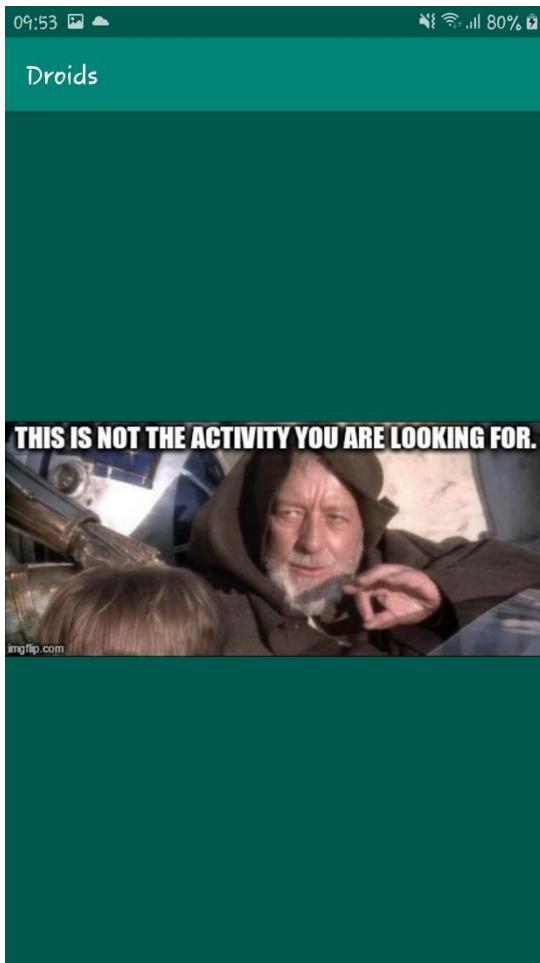
Vào lai máy nhập lai pin và ta có flag



Flag: OnlyAsStrongAsWeakestLink

4. Kịch bản 02

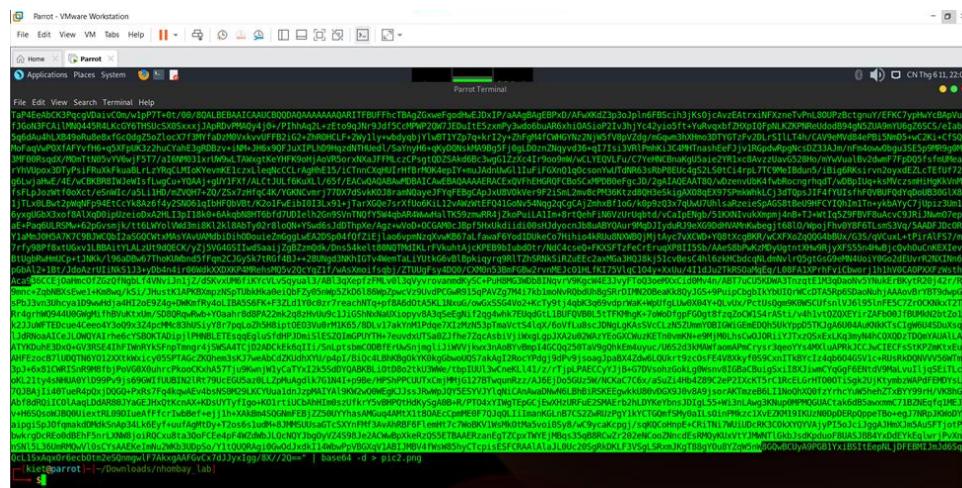
Đầu tiên ta vào code dịch ngược thì ta thấy chương trình này chỉ có file hình



Kiểm tra code thì ta không thấy có chuyển trang dựa trên intent

Kiểm tra code r2d2 thì ta có bảng mã base64

Thực hiện chuyển base 64 thành hình bằng lệnh: echo "/9j/4AA..." > base64 -d pic2.png



Mở ảnh lên và thấy flag



Flag: CTF{PUCKMAN}

5. Kịch bản 03

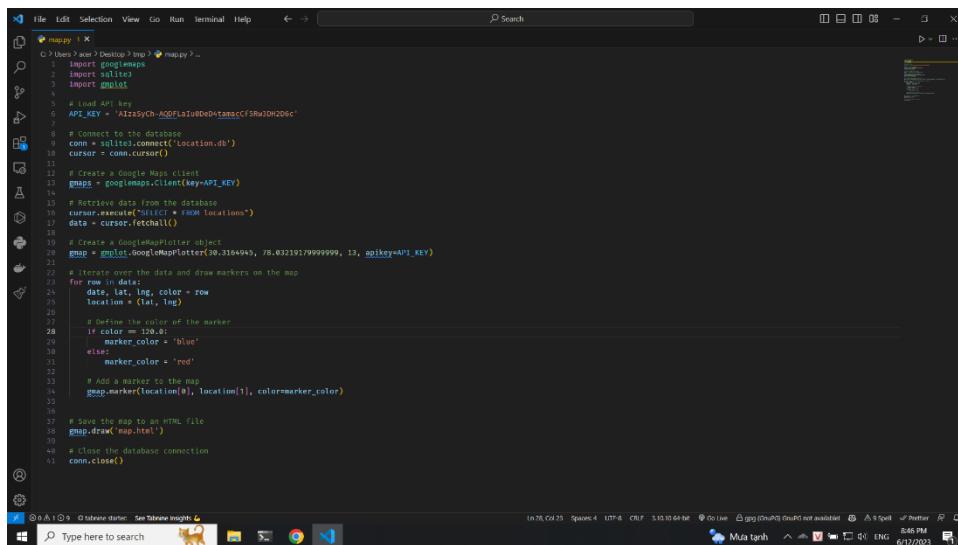
Đầu tiên ta cần file assets và mở file Locations.db lên và xem thông tin bên trong thì ta thấy được thông tin ngày tháng, toa độ X, toa độ Y và màu 120 và 0

The screenshot shows a terminal window titled "Parrot Terminal" running on Parrot OS. The user is executing an SQLite command to select all rows from the "Locations" table. The output displays numerous rows of location data, including names like "Amberley Woods", "Clevedon", "Dunedin", etc., along with their coordinates and other attributes. The terminal interface includes standard Windows-style icons at the top and a taskbar at the bottom.

```
[kiel@parrot:~/Downloads/nomadbay_lab/kb03_yon/assets]$ sqlite3 Location.db
SQLite version 3.34.2 2020-01-20 14:10:07
Copyright (c) 2020, SQLite.  All rights reserved.
This is free software; see the source for details.
sqlite3> .quit
```

id	name	lat	lon	active
0	Amberley Woods	-37.7760	174.7768	1
1	Clevedon	-37.7758	174.7765	1
2	Dunedin	-37.7755	174.7762	1
3	Wellington	-37.7752	174.7758	1
4	Auckland	-37.7750	174.7755	1
5	Tauranga	-37.7748	174.7752	1
6	Gisborne	-37.7745	174.7748	1
7	Nelson	-37.7742	174.7745	1
8	Christchurch	-37.7740	174.7742	1
9	Saint Kilda	-37.7738	174.7738	1
10	Mt Maunganui	-37.7735	174.7735	1
11	Bluff	-37.7732	174.7732	1
12	Wanganui	-37.7730	174.7728	1
13	Waiheke Island	-37.7728	174.7725	1
14	Waikanae	-37.7725	174.7722	1
15	Te Anau	-37.7722	174.7718	1
16	Queenstown	-37.7718	174.7715	1
17	Hamilton	-37.7715	174.7712	1
18	Rotorua	-37.7712	174.7708	1
19	Wanganui	-37.7708	174.7705	1
20	Waihi	-37.7705	174.7702	1
21	Wairoa	-37.7702	174.7700	1
22	Wanaka	-37.7698	174.7697	1
23	Wanaka	-37.7695	174.7694	1
24	Wanaka	-37.7692	174.7691	1
25	Wanaka	-37.7689	174.7688	1
26	Wanaka	-37.7686	174.7685	1
27	Wanaka	-37.7683	174.7682	1
28	Wanaka	-37.7680	174.7679	1
29	Wanaka	-37.7677	174.7676	1
30	Wanaka	-37.7674	174.7673	1
31	Wanaka	-37.7671	174.7670	1
32	Wanaka	-37.7668	174.7667	1
33	Wanaka	-37.7665	174.7664	1
34	Wanaka	-37.7662	174.7661	1
35	Wanaka	-37.7659	174.7658	1
36	Wanaka	-37.7656	174.7655	1
37	Wanaka	-37.7653	174.7652	1
38	Wanaka	-37.7650	174.7649	1
39	Wanaka	-37.7647	174.7646	1
40	Wanaka	-37.7644	174.7643	1
41	Wanaka	-37.7641	174.7640	1
42	Wanaka	-37.7638	174.7637	1
43	Wanaka	-37.7635	174.7634	1
44	Wanaka	-37.7632	174.7631	1
45	Wanaka	-37.7629	174.7628	1
46	Wanaka	-37.7626	174.7625	1
47	Wanaka	-37.7623	174.7622	1
48	Wanaka	-37.7620	174.7619	1
49	Wanaka	-37.7617	174.7616	1
50	Wanaka	-37.7614	174.7613	1
51	Wanaka	-37.7611	174.7610	1
52	Wanaka	-37.7608	174.7607	1
53	Wanaka	-37.7605	174.7604	1
54	Wanaka	-37.7602	174.7601	1
55	Wanaka	-37.7599	174.7598	1
56	Wanaka	-37.7596	174.7595	1
57	Wanaka	-37.7593	174.7592	1
58	Wanaka	-37.7590	174.7589	1
59	Wanaka	-37.7587	174.7586	1
60	Wanaka	-37.7584	174.7583	1
61	Wanaka	-37.7581	174.7580	1
62	Wanaka	-37.7578	174.7577	1
63	Wanaka	-37.7575	174.7574	1
64	Wanaka	-37.7572	174.7571	1
65	Wanaka	-37.7569	174.7568	1
66	Wanaka	-37.7566	174.7565	1
67	Wanaka	-37.7563	174.7562	1
68	Wanaka	-37.7560	174.7559	1
69	Wanaka	-37.7557	174.7556	1
70	Wanaka	-37.7554	174.7553	1
71	Wanaka	-37.7551	174.7550	1
72	Wanaka	-37.7548	174.7547	1
73	Wanaka	-37.7545	174.7544	1
74	Wanaka	-37.7542	174.7541	1
75	Wanaka	-37.7539	174.7538	1
76	Wanaka	-37.7536	174.7535	1
77	Wanaka	-37.7533	174.7532	1
78	Wanaka	-37.7530	174.7529	1
79	Wanaka	-37.7527	174.7526	1
80	Wanaka	-37.7524	174.7523	1
81	Wanaka	-37.7521	174.7520	1
82	Wanaka	-37.7518	174.7517	1
83	Wanaka	-37.7515	174.7514	1
84	Wanaka	-37.7512	174.7511	1
85	Wanaka	-37.7509	174.7508	1
86	Wanaka	-37.7506	174.7505	1
87	Wanaka	-37.7503	174.7502	1
88	Wanaka	-37.7500	174.7500	1
89	Wanaka	-37.7497	174.7497	1
90	Wanaka	-37.7494	174.7494	1
91	Wanaka	-37.7491	174.7491	1
92	Wanaka	-37.7488	174.7488	1
93	Wanaka	-37.7485	174.7485	1
94	Wanaka	-37.7482	174.7482	1
95	Wanaka	-37.7479	174.7479	1
96	Wanaka	-37.7476	174.7476	1
97	Wanaka	-37.7473	174.7473	1
98	Wanaka	-37.7470	174.7470	1
99	Wanaka	-37.7467	174.7467	1
100	Wanaka	-37.7464	174.7464	1
101	Wanaka	-37.7461	174.7461	1
102	Wanaka	-37.7458	174.7458	1
103	Wanaka	-37.7455	174.7455	1
104	Wanaka	-37.7452	174.7452	1
105	Wanaka	-37.7449	174.7449	1
106	Wanaka	-37.7446	174.7446	1
107	Wanaka	-37.7443	174.7443	1
108	Wanaka	-37.7440	174.7440	1
109	Wanaka	-37.7437	174.7437	1
110	Wanaka	-37.7434	174.7434	1
111	Wanaka	-37.7431	174.7431	1
112	Wanaka	-37.7428	174.7428	1
113	Wanaka	-37.7425	174.7425	1
114	Wanaka	-37.7422	174.7422	1
115	Wanaka	-37.7419	174.7419	1
116	Wanaka	-37.7416	174.7416	1
117	Wanaka	-37.7413	174.7413	1
118	Wanaka	-37.7410	174.7410	1
119	Wanaka	-37.7407	174.7407	1
120	Wanaka	-37.7404	174.7404	1
121	Wanaka	-37.7401	174.7401	1
122	Wanaka	-37.7398	174.7398	1
123	Wanaka	-37.7395	174.7395	1
124	Wanaka	-37.7392	174.7392	1
125	Wanaka	-37.7389	174.7389	1
126	Wanaka	-37.7386	174.7386	1
127	Wanaka	-37.7383	174.7383	1
128	Wanaka	-37.7380	174.7380	1
129	Wanaka	-37.7377	174.7377	1
130	Wanaka	-37.7374	174.7374	1
131	Wanaka	-37.7371	174.7371	1
132	Wanaka	-37.7368	174.7368	1
133	Wanaka	-37.7365	174.7365	1
134	Wanaka	-37.7362	174.7362	1
135	Wanaka	-37.7359	174.7359	1
136	Wanaka	-37.7356	174.7356	1
137	Wanaka	-37.7353	174.7353	1
138	Wanaka	-37.7350	174.7350	1
139	Wanaka	-37.7347	174.7347	1
140	Wanaka	-37.7344	174.7344	1
141	Wanaka	-37.7341	174.7341	1
142	Wanaka	-37.7338	174.7338	1
143	Wanaka	-37.7335	174.7335	1
144	Wanaka	-37.7332	174.7332	1
145	Wanaka	-37.7329	174.7329	1
146	Wanaka	-37.7326	174.7326	1
147	Wanaka	-37.7323	174.7323	1
148	Wanaka	-37.7320	174.7320	1
149	Wanaka	-37.7317	174.7317	1
150	Wanaka	-37.7314	174.7314	1
151	Wanaka	-37.7311	174.7311	1
152	Wanaka	-37.7308	174.7308	1
153	Wanaka	-37.7305	174.7305	1
154	Wanaka	-37.7302	174.7302	1
155	Wanaka	-37.7299	174.7299	1
156	Wanaka	-37.7296	174.7296	1
157	Wanaka	-37.7293	174.7293	1
158	Wanaka	-37.7290	174.7290	1
159	Wanaka	-37.7287	174.7287	1
160	Wanaka	-37.7284	174.7284	1
161	Wanaka	-37.7281	174.7281	1
162	Wanaka	-37.7278	174.7278	1
163	Wanaka	-37.7275	174.7275	1
164	Wanaka	-37.7272	174.7272	1
165	Wanaka	-37.7269	174.7269	1
166	Wanaka	-37.7266	174.7266	1
167	Wanaka	-37.7263	174.7263	1
168	Wanaka	-37.7260	174.7260	1
169	Wanaka	-37.7257	174.7257	1
170	Wanaka	-37.7254	174.7254	1
171	Wanaka	-37.7251	174.7251	1
172	Wanaka	-37.7248	174.7248	1
173	Wanaka	-37.7245	174.7245	1
174	Wanaka	-37.7242	174.7242	1
175	Wanaka	-37.7239	174.7239	1
176	Wanaka	-37.7236	174.7236	1
177	Wanaka	-37.7233	174.7233	1
178	Wanaka	-37.7230	174.7230	1
179	Wanaka	-37.7227	174.7227	1
180	Wanaka	-37.7224	174.7224	1
181	Wanaka	-37.7221	174.7221	1
182	Wanaka	-37.7218	174.7218	1
183	Wanaka	-37.7215	174.7215	1
184	Wanaka	-37.7212	174.7212	1
185	Wanaka	-37.7209	174.7209	1
186	Wanaka	-37.7206	174.7206	1
187	Wanaka	-37.7203	174.7203	1
188	Wanaka	-37.7200	174.7200	1
189	Wanaka	-37.7197	174.7197	1
190	Wanaka	-37.7194	174.7194	1
191	Wanaka	-37.7191	174.7191	1
192	Wanaka	-37.7188	174.7188	1
193	Wanaka	-37.7185	174.7185	1
194	Wanaka	-37.7182	174.7182	1
195	Wanaka	-37.7179	174.7179	1
196	Wanaka	-37.7176	174.7176	1
197	Wanaka	-37.7173	174.7173	1
198	Wanaka	-37.7170	174.7170	1
199	Wanaka	-37.7167	174.7167	1
200	Wanaka	-37.7164	174.7164	1
201	Wanaka	-37.7161	174.7161	1
202	Wanaka	-37.7158	174.7158	1
203	Wanaka	-37.7155	174.7155	1
204	Wanaka	-37.7152	174.7152	1
205	Wanaka	-37.7149	174.7149	1
206	Wanaka	-37.7146	174.7146	1
207	Wanaka	-37.7143	174.7143	1
208	Wanaka	-37.7140	174.7140	1
209	Wanaka	-37.7137	174.7137	1
210	Wanaka	-37.7134	174.7134	1
211	Wanaka	-37.7131	174.7131	1
212	Wanaka	-37.7128	174.7128	1
213	Wanaka	-37.7125	174.7125	1
214	Wanaka	-37.7122	174.7122	1
215	Wanaka	-37.7119	174.7119	1
216	Wanaka	-37.7116	174.7116	1
217	Wanaka	-37.7113	174.7113	1
218	Wanaka	-37.7110	174.7110	1
219	Wanaka	-37.7107	174.7107	1
220	Wanaka	-37.7104	174.7104	1
221	Wanaka	-37.7101	174.7101	1
222	Wanaka	-37.7098	174.7098	1
223	Wanaka	-37.7095	174.7095	1
224	Wanaka	-37.7092	174.7092	1
225	Wanaka	-37.7089	174.7089	1
226	Wanaka	-37.7086	174.7086	1
227	Wanaka	-37.7083	174.7083	1
228	Wanaka	-37.7080	174.7080	1
229	Wanaka	-37.7077	174.7077	1
230	Wanaka	-37.7074	174.7074	1
231	Wanaka	-37.7071	174.7071	1
232	Wanaka	-37.7068	174.7068	1
233	Wanaka	-37.7065	174.7065	1
234	Wanaka	-37.7062	174.7062	1
235	Wanaka	-37.7059	174.7059	1
236	Wanaka	-37.7056	174.7056	1
237	Wanaka	-37.7053	174.7053	1
238	Wanaka	-37.7050	174.7050	1
239	Wanaka	-37.7047	174.7	

Thực hiện code để đọc data từ file Location và kết hợp api của google maps để thực hiện visualize lên google maps

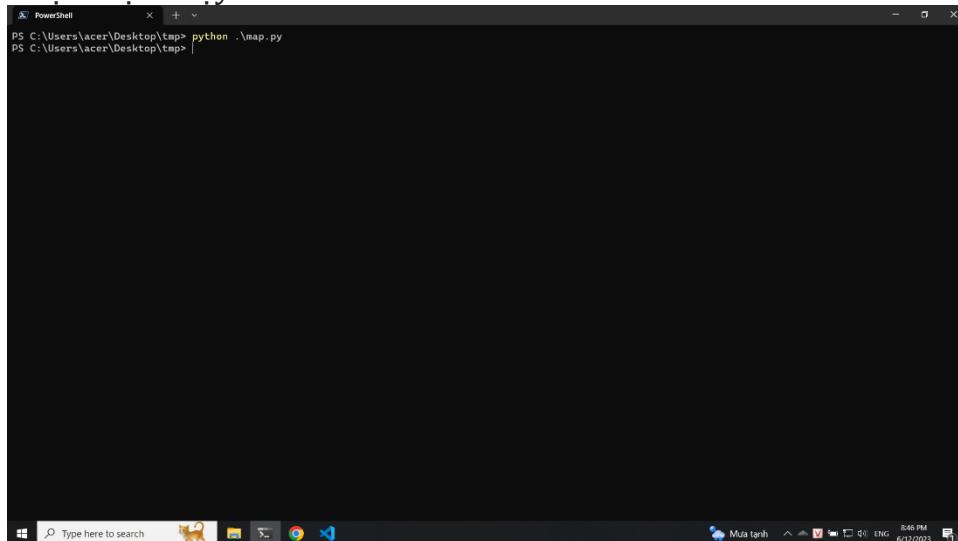


```

File Edit Selection View Go Run Terminal Help Search
C:\Users\xor\Desktop\map.py
1 import os
2 import googlemaps
3 import sqlite3
4 import googlemaps
5
6 # Load API key
7 API_KEY = 'AIzaSyCh-AQFlaIuNdeDatauccf3RwJ0H206c'
8
9 # Connect to the database
10 conn = sqlite3.connect('location.db')
11 cursor = conn.cursor()
12
13 # Create a Google Maps client
14 gmaps = googlemaps.Client(key=API_KEY)
15
16 # Retrieve data from the database
17 cursor.execute("SELECT * FROM locations")
18 data = cursor.fetchall()
19
20 # Create a GoogleMapPlotter object
21 gmap = googlemaps.GoogleMapPlotter(30.3184945, -78.0321917999999, 13, key=API_KEY)
22
23 # Iterate over the data and draw markers on the map
24 for row in data:
25     lat, lon, color = row
26     location = (lat, lon)
27
28     # Define the color of the marker
29     if color == 100.0:
30         marker_color = 'blue'
31     else:
32         marker_color = 'red'
33
34     # Add a marker to the map
35     gmap.marker(location[0], location[1], color=marker_color)
36
37 # Save the map to an HTML file
38 gmap.draw('map.html')
39
40 # Close the database connection
41 conn.close()

```

Thực hiện chạy code

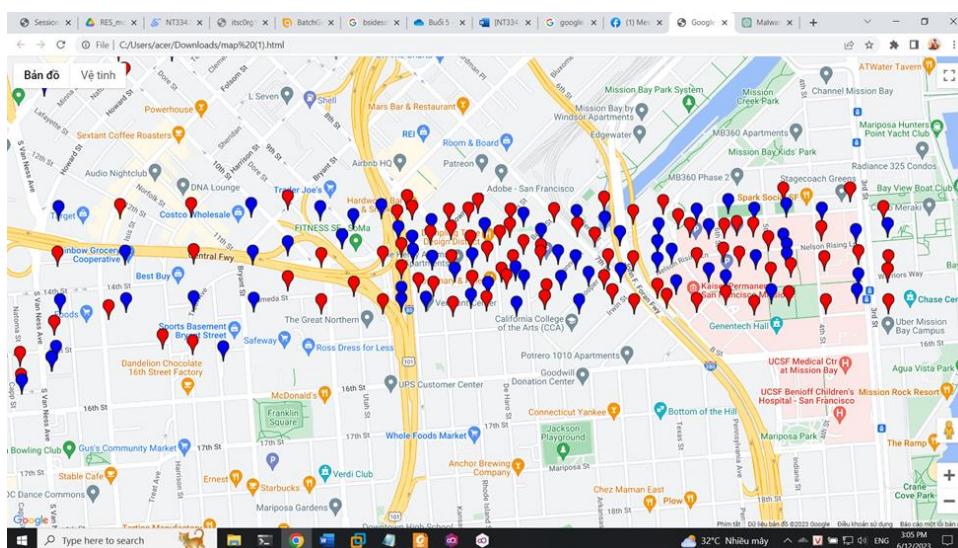


```

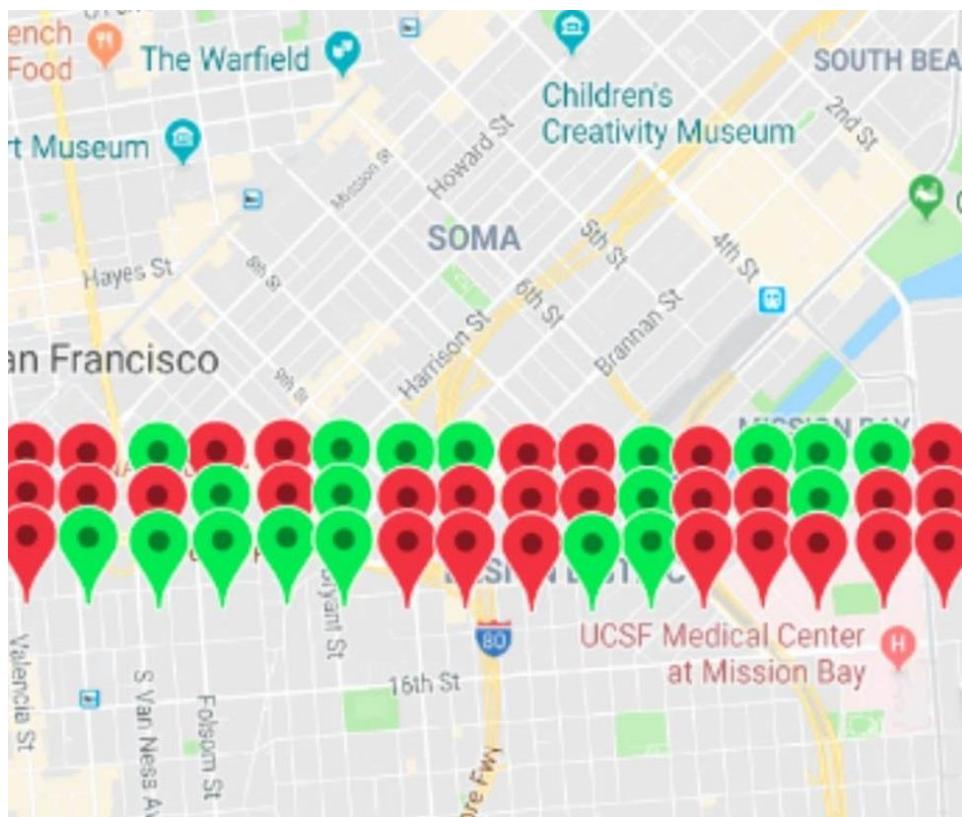
PowerShell
PS C:\Users\acer\Desktop\tmp> python .\map.py
PS C:\Users\acer\Desktop\tmp>

```

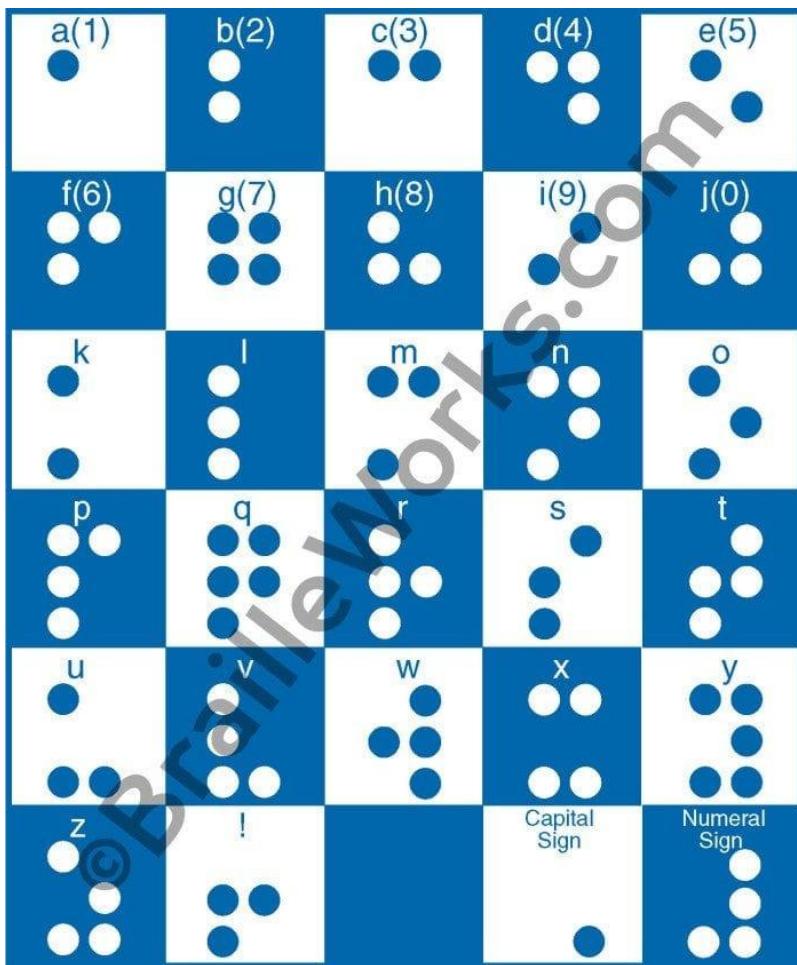
Sau khi chạy code xong ta có những điểm đánh dấu như hình



Tắt bớt thì ta có thông tin như hình, thì đây là dạng chữ nổi của người mù



Thực hiện giải mã theo bảng mã này thì ta có được flag



Flag: Z3Lda

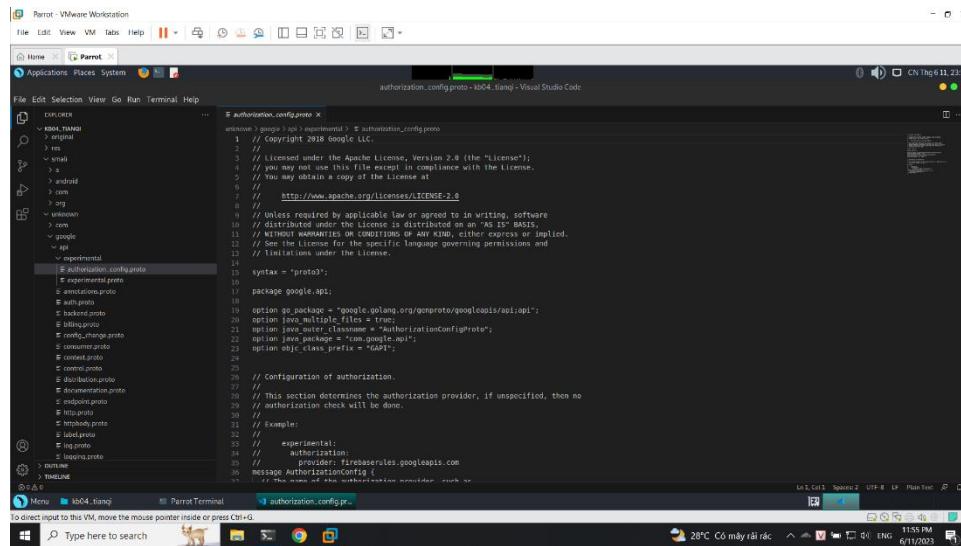
6. Kịch bản 04

Đầu tiên ta thực hiện dịch ngược

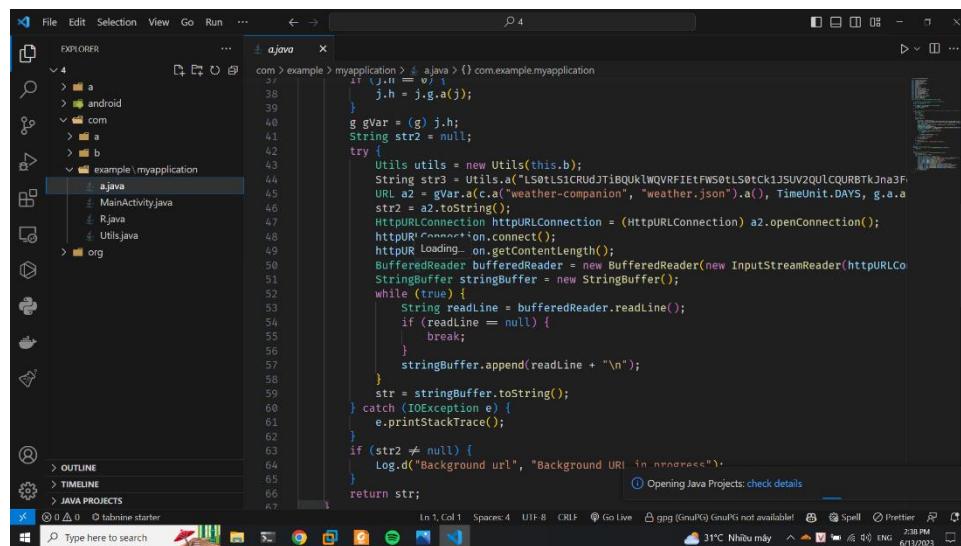
Tiếp theo ta sẽ thực hiện dịch bằng apktool

```
> ^C
[|x|-[kiet@parrot|~/Downloads/nhombay_lab]
$ apktool d kb04_tianqi.apk
I: Using Apktool 2.7.0 on kb04_tianqi.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/kiet/.local/share/apktool/framework/1
Network
```

Tiếp tục ta sẽ thực hiện xem code thì ta thấy chương trình đang sử dụng api key của google thì đây là lab bị outdated nên không thể sử dụng được nữa



Thực hiện phân tích code



Nhưng sau khi đọc code thì ta có thể code frida để thực hiện hooking với idea:

Bypass SSL Unpinning -> Hook toString -> Monitor toString

Sau khi thực hiện hooking thì ta sẽ có được 1 file key.json, ta sẽ dùng key này để truy cập vào hệ thống là lấy flag. Nhưng những dịch vụ liên quan đến google không còn hỗ trợ miễn phí nên lab chỉ có thể làm được đến đây

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) 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.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)** – cỡ **chữ 13**. **Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- 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, trẽ... sẽ được xử lý tùy mức độ vi phạm.

HẾT