

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.

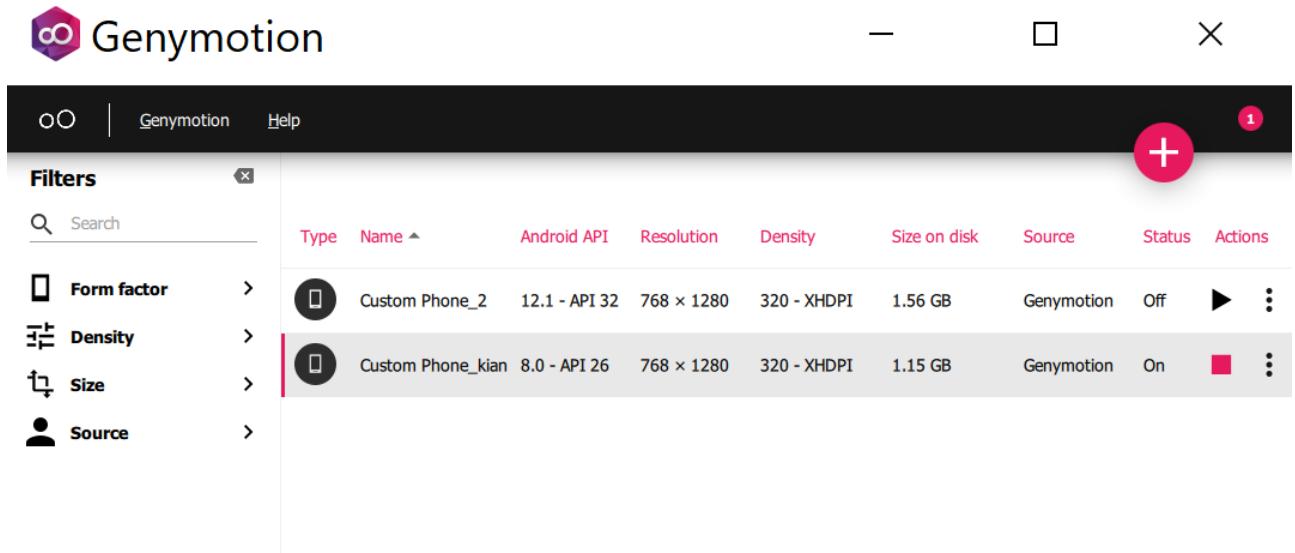
(Xem trang kế tiếp)

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                          GenydService      SystemPatcher
CaptivePortalLogin               GenymotionLayout UserDictionaryProvider
CarrierDefaultApp                HTMLViewer        WAPPushManager
CertInstaller                     KeyChain          WallpaperBackup
CompanionDeviceManager          LatinIME          WallpaperPicker
CtsShimPrebuilt                  LiveWallpapersPicker messaging
CubeLiveWallpapers               Music             webview
CustomLocale                      NfcNci
DeskClock                         OpenWnn
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
E:\NT213-BaoMatWeb&App\tool\platform-tools>adb pull -p /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

```
ca 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$1@1b7ff61 -> com.android.server.AppOpsService$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

Mobile Forensics

The screenshot shows the MobSF static analysis tool. 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 APP SCORES, it shows a Security Score of 73/100 and Trackers Detected 0/428. The FILE INFORMATION section shows the file name as kb04_tianqi.apk, size as 1.63MB, MD5 as c5fdb8dbb0e7c2d4965e9e23dc8f126, SHA1 as e52ae1a8485b13a6ff0a4901e6a0948ae3c2009, and SHA256 as 566ec2724151d73a2303fa3878baff64548dbf774d50b3d4b324de860ab5a29. 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 26, and Android Version Name 1.0, Android Version Code 1. Below these are four cards: ACTIVITIES (1), SERVICES (0), RECEIVERS (0), and PROVIDERS (0). The bottom tabs include SCAN OPTIONS and DECOMPILATED CODE.

Dịch ngược bằng apktool

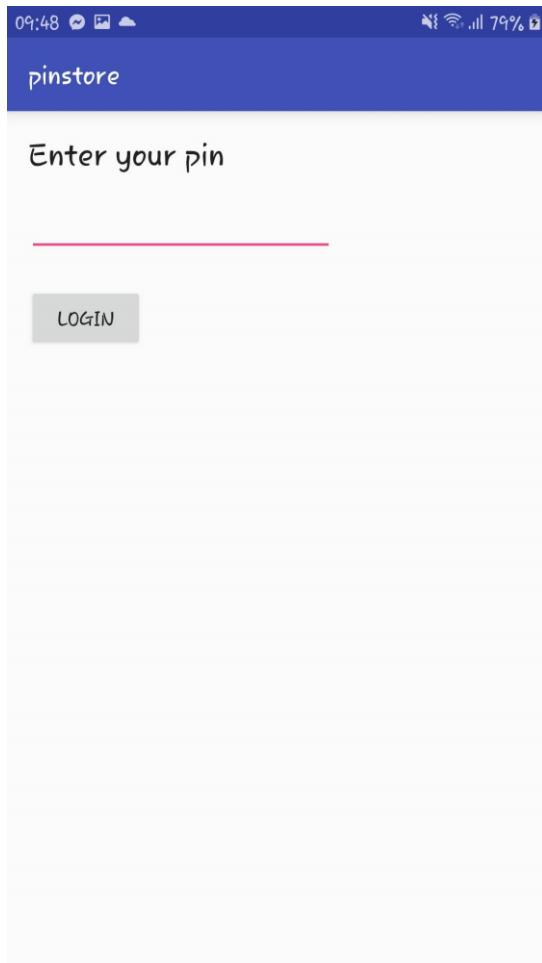
```

File Edit View Search Terminal Help
[+] 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...
[+] 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...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
[+] kiet@parrot:[~/Downloads/nhombay_lab]
└─$ apktool d kb02_zha.apk
I: Using Apktool 2.7.0 on kb02_zha.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...
[+] 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
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...

```

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.getApplication());
            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

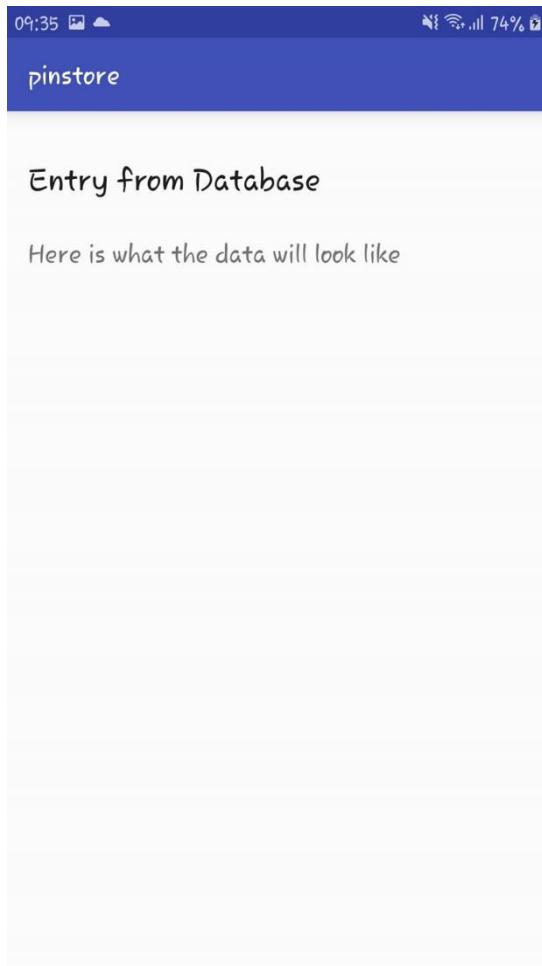
```
[kiet@parrot] -[~/Downloads/nhombay_lab/pinstore/assets]
└─$sqlite3 pinlock.db
SQLite version 3.34.1 2021-01-20 14:10:07
Enter ".help" for usage hints.
sqlite> .databases
main: /home/kiet/Downloads/nhombay_lab/pinstore/assets/pinlock.db r/w
sqlite> .table
android_metadata pinDB secretsDBv1 secretsDBv2
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

Mobile Forensics

The screenshot shows a Parrot OS VM interface. In the foreground, there's a code editor window titled "DatabaseUtilities.smali" showing Java-like assembly code. In the background, the file browser shows a directory structure under "/mnt/sdcard/Android/Database". The status bar at the bottom indicates the date and time as "T3 Thg 6 13, 12:43".

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

The screenshot shows a terminal window on Parrot OS. The user is running the command \$apktool b pinstore -o pinstorev2.apk to build an APK. The terminal also shows the generation of a keystore (pinstorev2.keystore) and the signing of the APK with a key size of 2048 bits and a validity of 10,000 days. The status bar at the bottom indicates the date and time as "T3 Thg 6 13, 12:47".

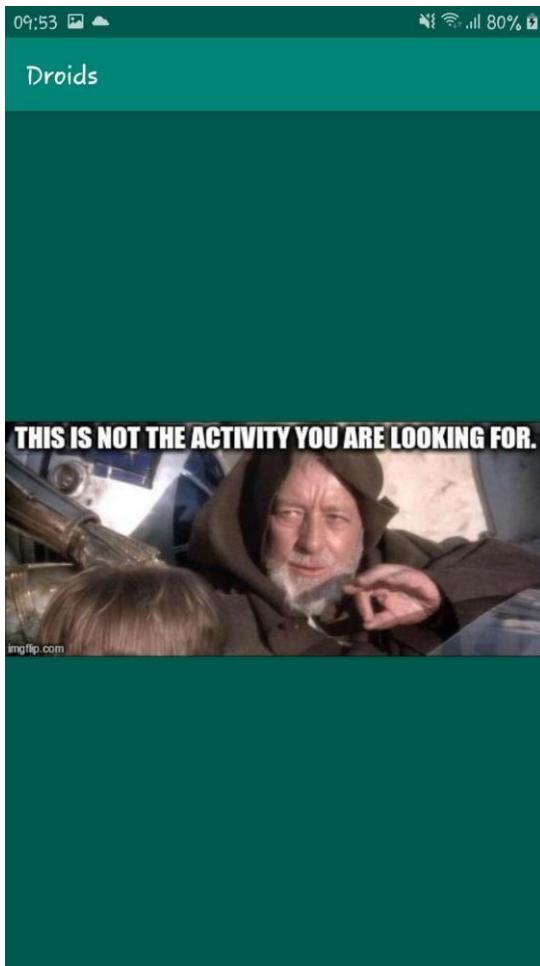
Vào lại máy nhập lại pin và ta có flag



Flag: OnlyAsStrongAsWeakestLink

4. Kịch bản 02

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

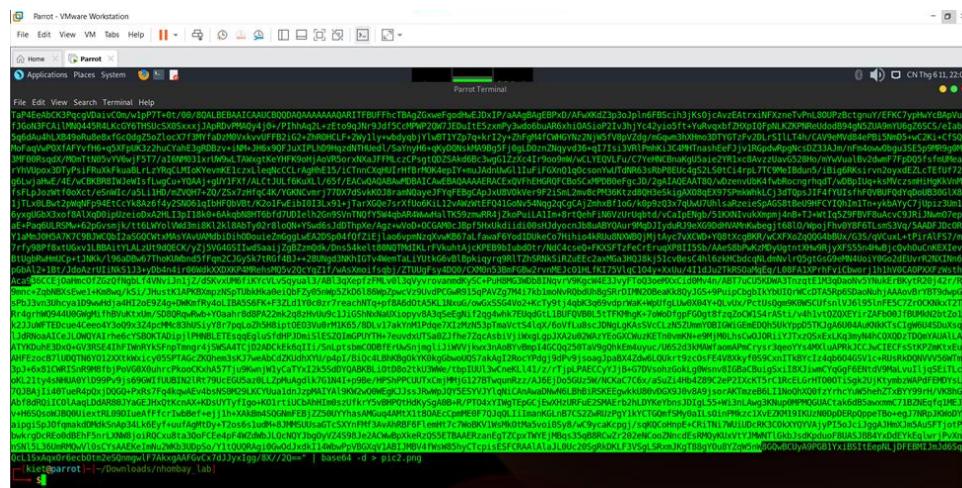


Kiểm tra code thì ta không thấy có chuyển trang dựa trên intent

```
>MainActivity.java 4 x
2 > com > example > blink > MainActivity.java > {} com.example.blink
1 package com.example.blink;
2
3 import android.os.Bundle;
4 import android.support.v7.app.AppCompatActivity;
5 /* loaded from: classes.dex */
6 public class MainActivity extends AppCompatActivity {
7     /* JADX INFO: Access modifiers changed from: protected */
8     @Override // android.support.v7.app.AppCompatActivity, android.support.v4.app.FragmentActi
9     public void onCreate(Bundle savedInstanceState) {
10         super.onCreate(savedInstanceState);
11         setContentView(R.layout.activity_main);
12     }
13 }
```

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

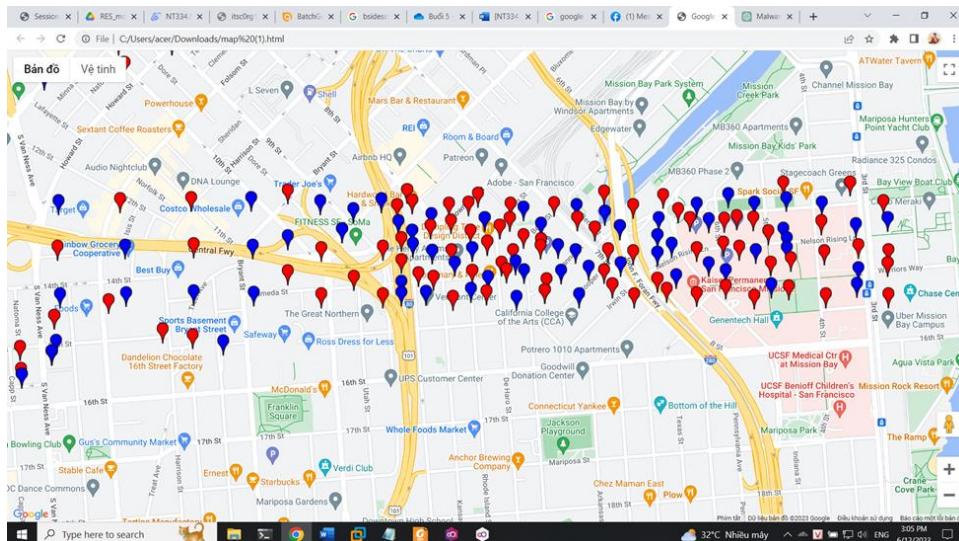
Thực hiện code để đọc data từ file Location và kết hợp api của google maps để thực hiện visualize lên google maps



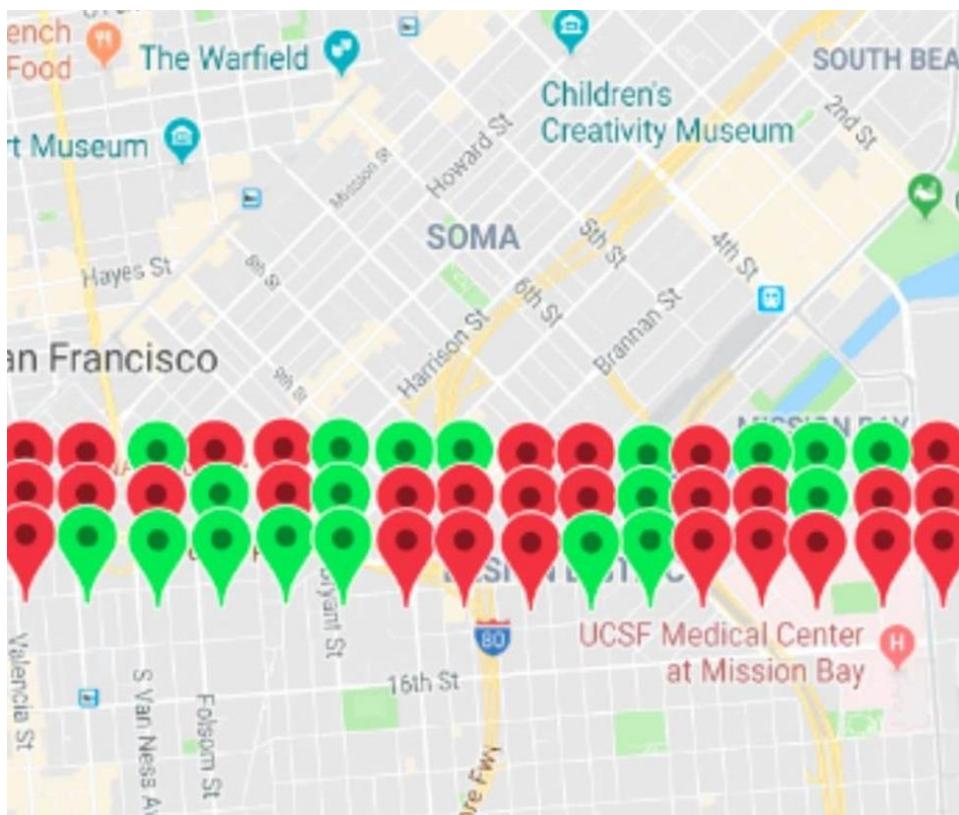
Thực hiện chạy code



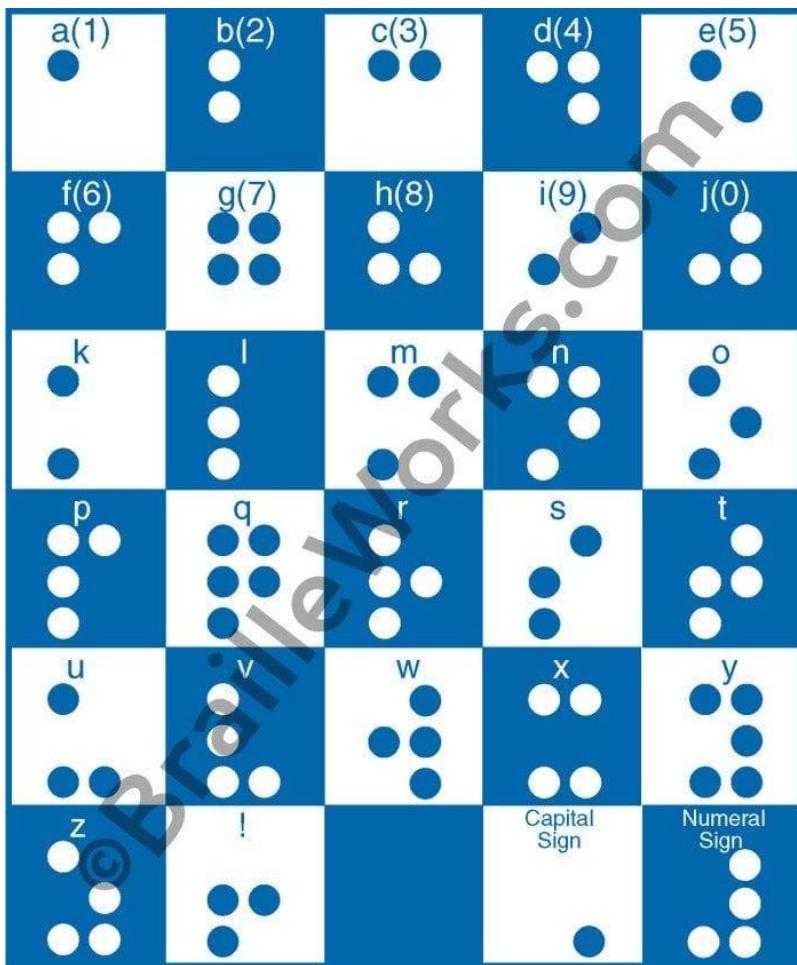
Sau khi chạy code xong ta có những điểm đánh dấu như hình



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

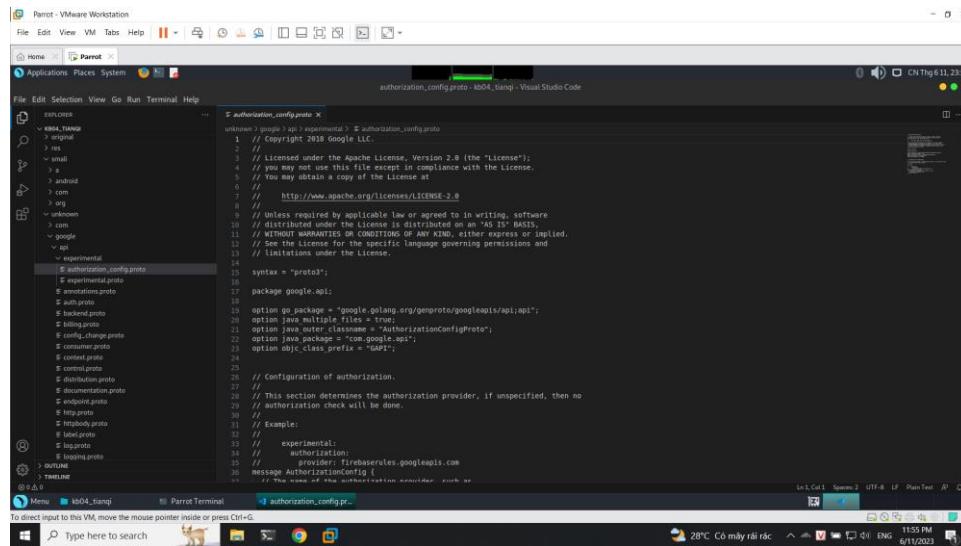
6. Kịch bản 04

Đầu tiên ta thực hiện dịch ngược

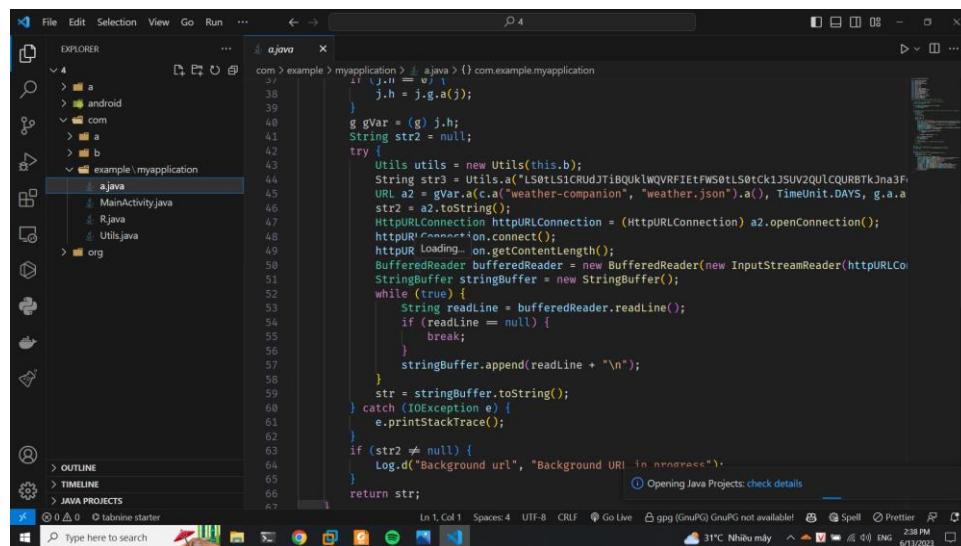
Tiếp theo ta sẽ thực hiện dịch bằng apktool

```
> ^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`

```

1  File Edit Selection View Go Run Terminal Help < - > Search
2  Java.perform(function () {
3      // Step - 1
4
5      var array_list = Java.use("java.util.ArrayList");
6      var ApIClient = Java.use("com.android.org.conscrypt.TrustManagerImpl");
7
8      ApIClient.checkTrustedRecursive.implementation = function (
9          a1,
10         a2,
11         a3,
12         a4,
13         a5,
14         a6
15     ) {
16         var k = array_list.$new();
17         return k;
18     };
19
20     // Step - 2
21     console.log("Hooking Java");
22
23     const StringBuilder = Java.use("java.lang.StringBuilder");
24
25     StringBuilder.$init.overload("java.lang.String").implementation = function (
26         arg
27     ) {
28         var partial = "";
29         var result = this.$init(arg);
30         console.log("new StringBuilder('" + result + "')");
31         return result;
32     };
33
34     console.log("Hooking new StringBuilder(java.lang.String)");
35
36     // Step - 3
37     StringBuilder.toString.implementation = function () {
38         var result = this.toString();
39         console.log("StringBuilder.toString() => '" + result);
40         return result;
41     };
42
43     console.log("Hooking StringBuilder.toString() hooked");
44
45     ...
46 };
47
48 ④ tableau starter
49
50
51
52
53
54
55
56
57
58
59
60
61
62

```

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