BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Lab 5: Mobile Forensics

GVHD: Đoàn Minh Trung

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.O21.ATTN

STT	Họ và tên	MSSV	Email
1	Phạm Ngọc Thơ	21522641	21522641@gm.uit.edu.vn
2	Hà Thị Thu Hiền	21522056	21522056@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Kịch bản 1 (đã báo cáo ở lớp)	100%
2	Kịch bản 2 (đã báo cáo ở lớp)	100%
3	Kịch bản 3 (đã báo cáo ở lớp)	100%
4	Kịch bản 4	100%

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

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

BÁO CÁO CHI TIẾT

Kịch bản 04:

> **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:*

- Thiết bị ảo em sử dụng là Android 5, không thể cài đặt được ứng dụng:

```
C:\Users\ngtho\Downloads\Compressed\resources-session05\resources-session05>adb install kb04_tianqi.apk
Performing Push Install
kb04_tianqi.apk: 1 file pushed, 0 skipped. 779.2 MB/s (1710140 bytes in 0.002s)
        pkg: /data/local/tmp/kb04_tianqi.apk
Failure [INSTALL_FAILED_OLDER_SDK]
```

- Dùng apktool để decompile file apk:

```
┌──(kali㉿kali)-[~/forensic]
└─$ apktool d kb04_tianqi.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty on kb04_tianqi.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/kali/.local/share/apktool/framework/1.apk
I: Regular manifest package...
```

- Kiểm tra file *AndroidManifest.xml*, em tìm được phiên bản Android của app. Ở đây em dùng https://www.decompiler.com/jar/ để dễ xem nội dung của file apk hơn:

kb04_tianqi.apk Delete Download ZIP

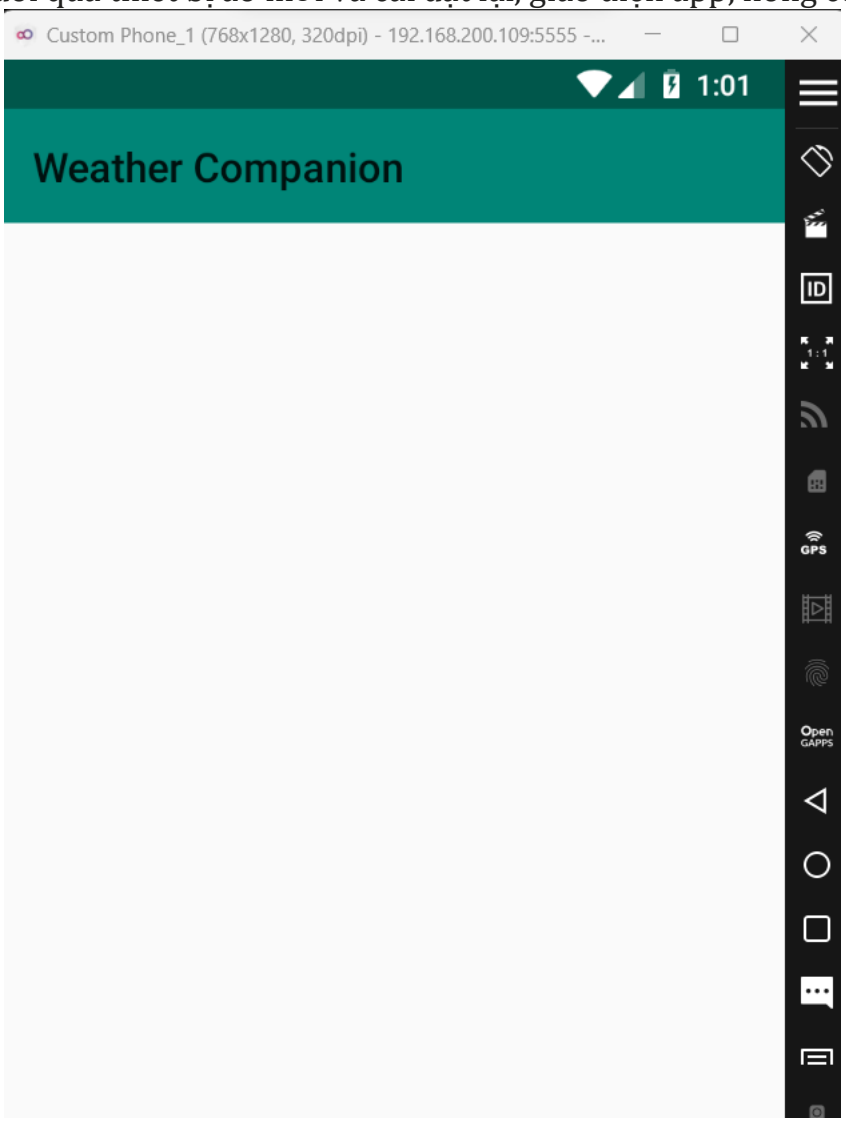
kb04_tianqi.apk / resources / AndroidManifest.xml

Download file

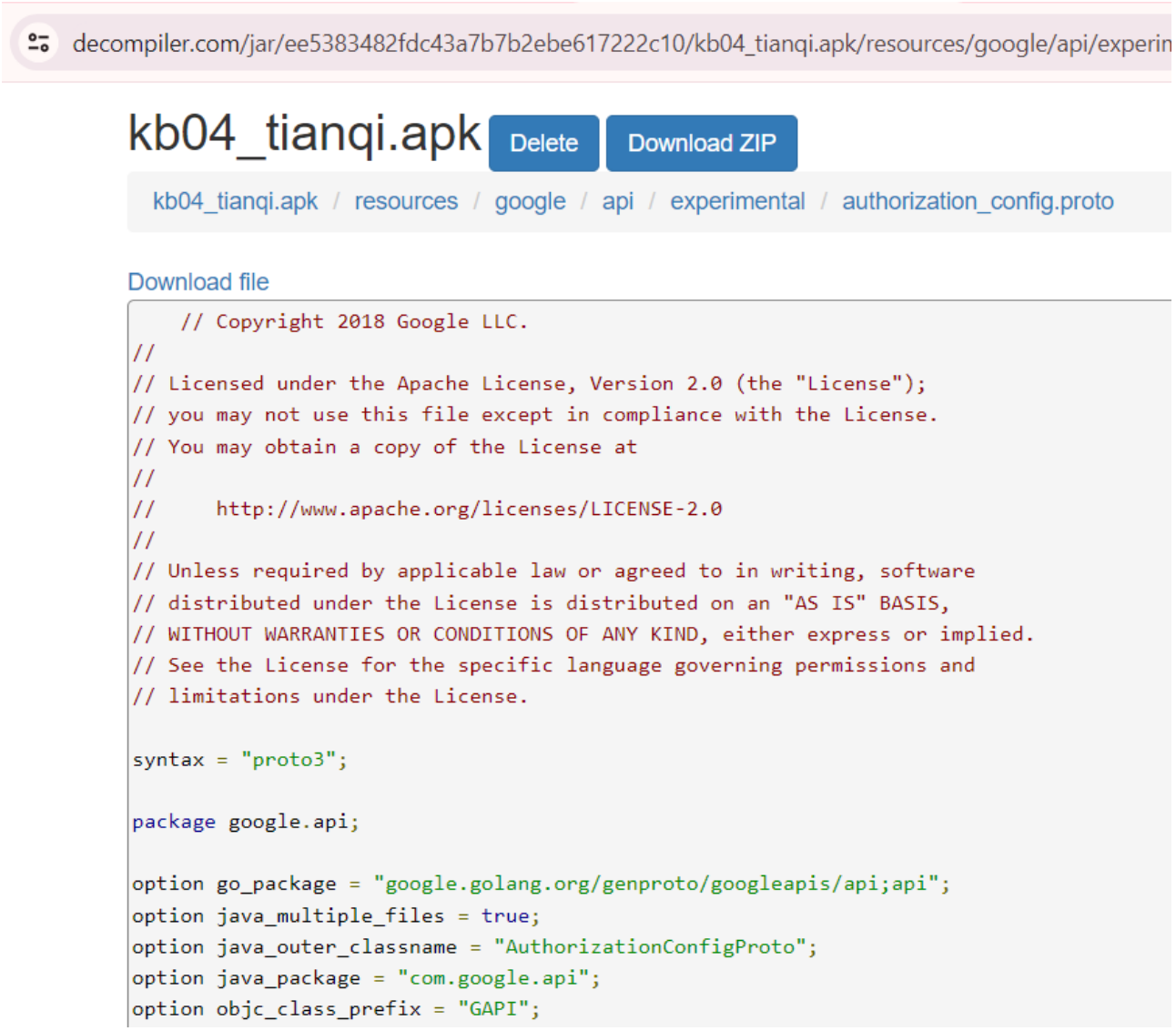
```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1
    <uses-sdk android:minSdkVersion="26" android:targetSdkVersion="27"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <application android:theme="@style/AppTheme" android:label="@string/app_name" android:
        <activity android:theme="@style/AppTheme.NoActionBar" android:label="@string/app_na
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
```

SDK 26, 27 tương ứng với Android version 8.0 và 8.1. App sẽ chạy được trên thiết bị Android có version tối thiểu là 8.0 và tối ưu nhất khi chạy trên thiết bị 8.1.

- Sau khi đổi qua thiết bị ảo mới và cài đặt lại, giao diện app, hổng có gì cả!



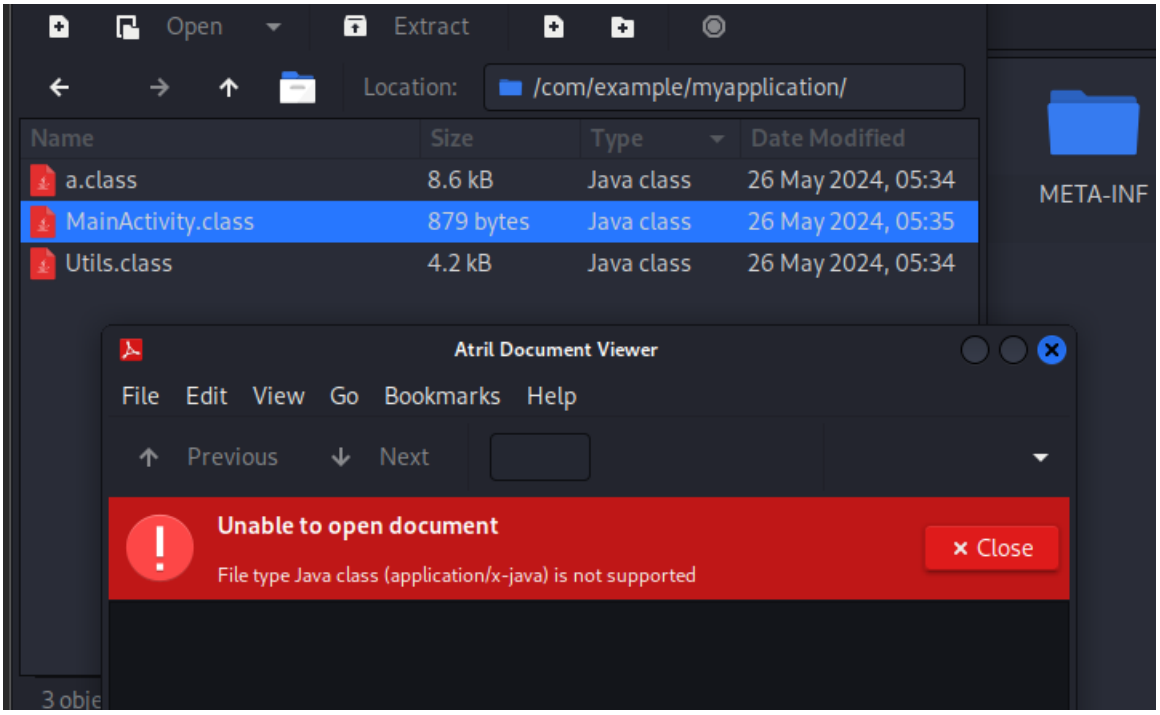
- Em tìm được đoạn mã liên quan đến Google API như sau:



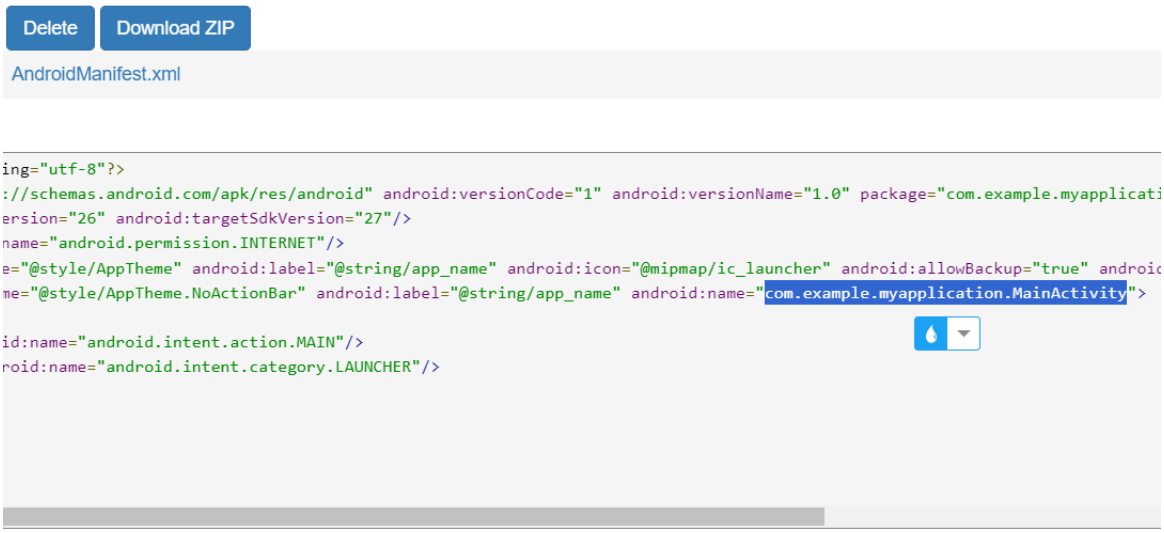
Các dòng được chú thích liên quan đến thông tin bản quyền.
2 dòng lệnh tiếp theo chỉ định rằng file sử dụng cú pháp *proto3* và thuộc gói *google.api.*
Các dòng còn lại là các tùy chọn dùng để tạo mã.

- Em dùng *dex2jar* để chuyển từ file *class.dex* sang *.jar*, tuy nhiên bị lỗi. Do đó không thể thực hiện các bước phân tích tiếp theo:

```
┌──(kali㉿kali)-[~/forensic/kb04]
└─$ d2j-dex2jar classes.dex
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
dex2jar classes.dex → ./classes-dex2jar.jar
Detail Error Information in File ./classes-error.zip
Please report this file to one of following link if possible (any one).
    https://sourceforge.net/p/dex2jar/tickets/
    https://bitbucket.org/pxb1988/dex2jar/issues
    https://github.com/pxb1988/dex2jar/issues
    dex2jar@googlegroups.com
```



- Quay lại file *AndroidManifest.xml* ban đầu:



Activity chính của chương trình là *com.example.myapplication.MainActivity*, nhưng lúc chạy app cũng không thể hiển thị được chức năng gì để phân tích thêm. Do đó, kịch bản 4 dừng lại ở đây.

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

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, 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]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- 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 nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT