Phòng thí nghiệm An toàn Thông tin
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật Web và Ứng dụng

Kỳ báo cáo: Buổi 04 (Session 04)

Tên chủ đề: Pentesting Android Applications

GVHD: Ngô Đức Hoàng Sơn

Ngày báo cáo: 8/05/2024

Nhóm: 07 (ghi số thứ tự nhóm)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.O22.ATCL

STT	Họ và tên	MSSV	Email
1	Nguyễn Thị Kiều Trang	21520489	21520489@gm.uit.edu.vn
2	Trần Đình Huy	21522167	21522167@gm.uit.edu.vn
3	Dương Phú Cường	21521900	21521900@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Phân tích tĩnh (Static Analysis)	100%
2	Dịch ngược (Reverse Engineering)	100%
3	Phân tích động (Dynamic Analysis)	80%
4	Hooking với Frida	100%
5	Challenge CTF	64%

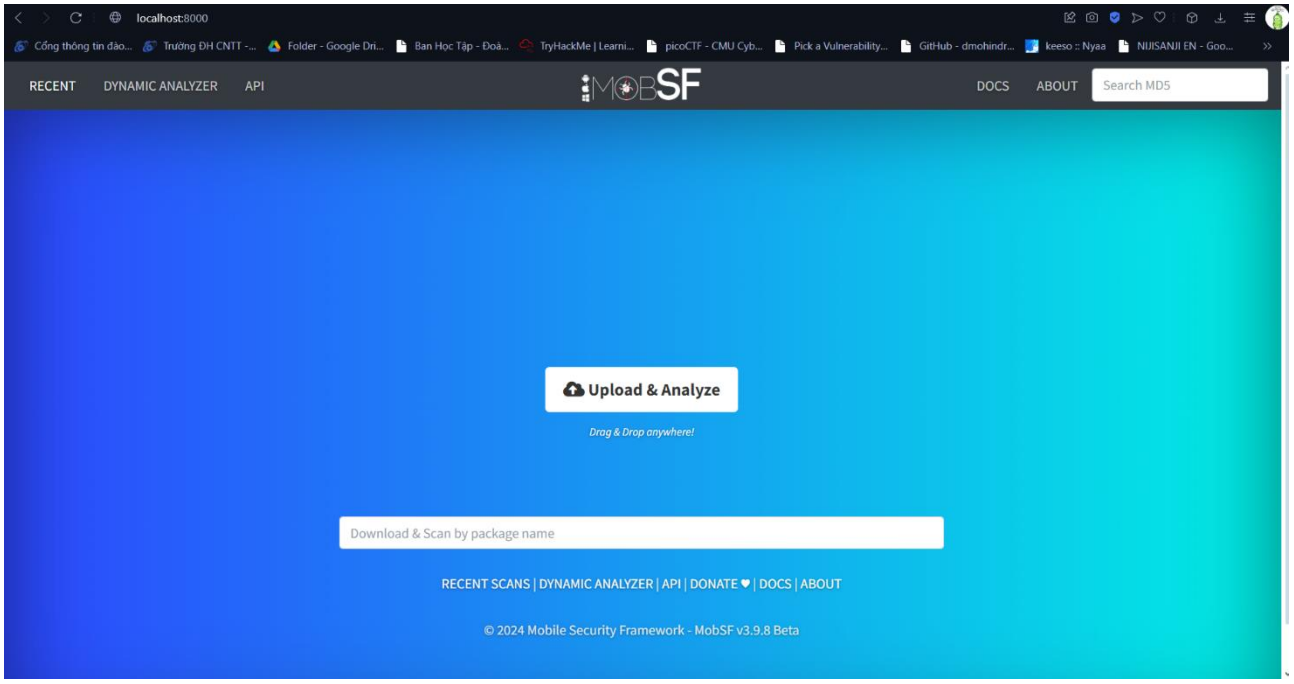
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

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

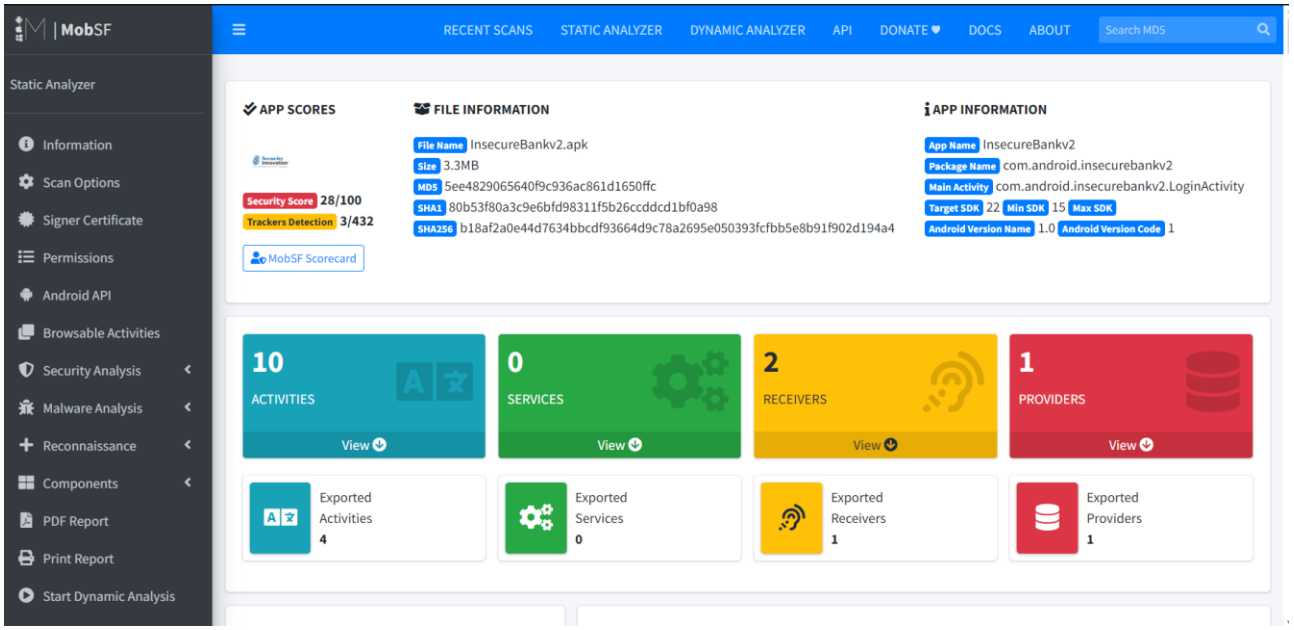
BÁO CÁO CHI TIẾT

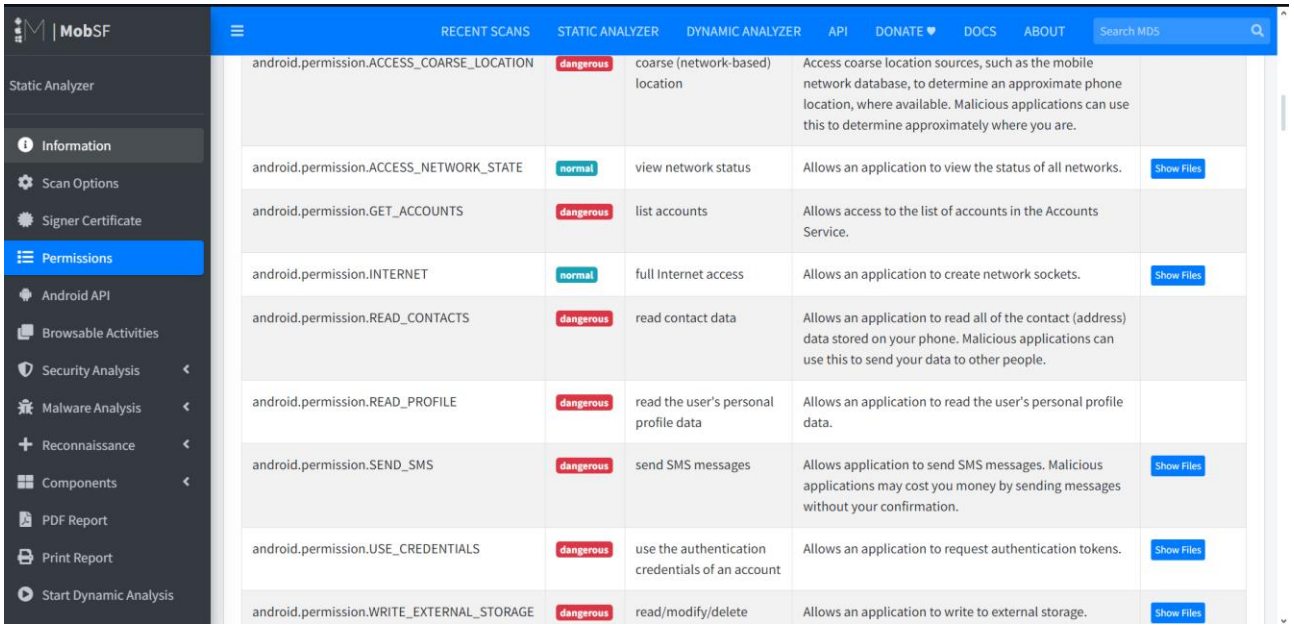
1. Phân tích tĩnh (Static Analysis)

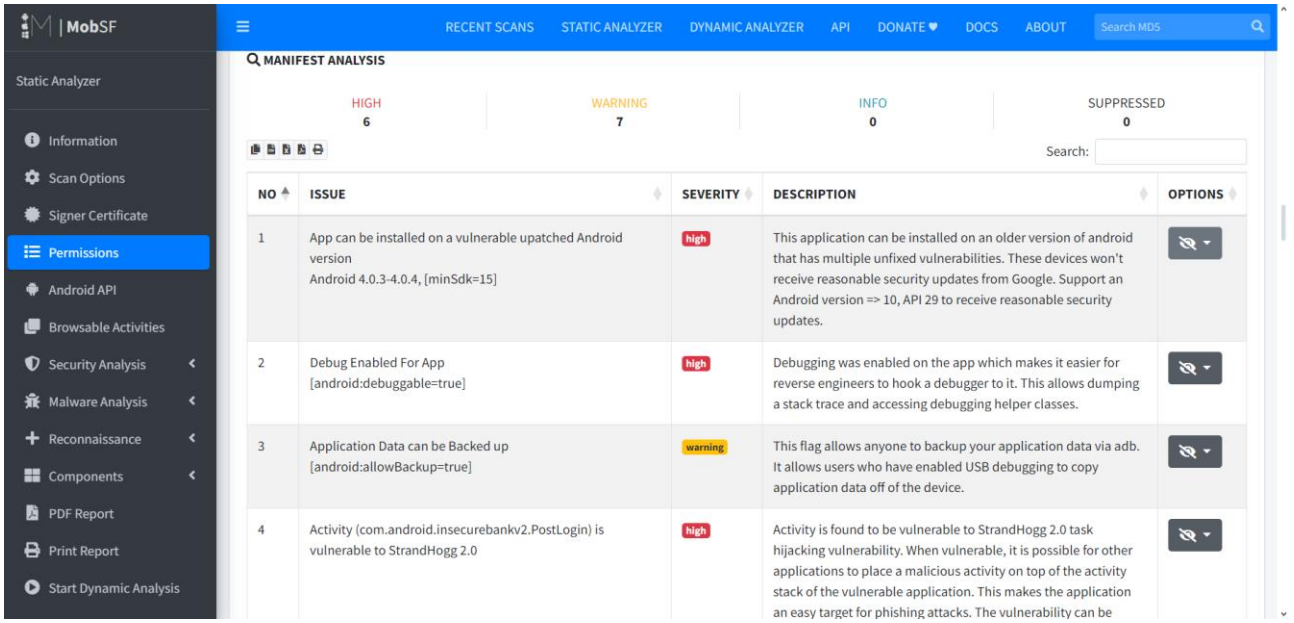
- Sau khi cài đặt và thiết lập môi trường của MobSF ta sẽ truy cập localhost:8000



- Tải lên hoặc kéo thả tập tin *InsecureBankv2.apk* MobSF để tiếnh hành phân tích tĩnh.



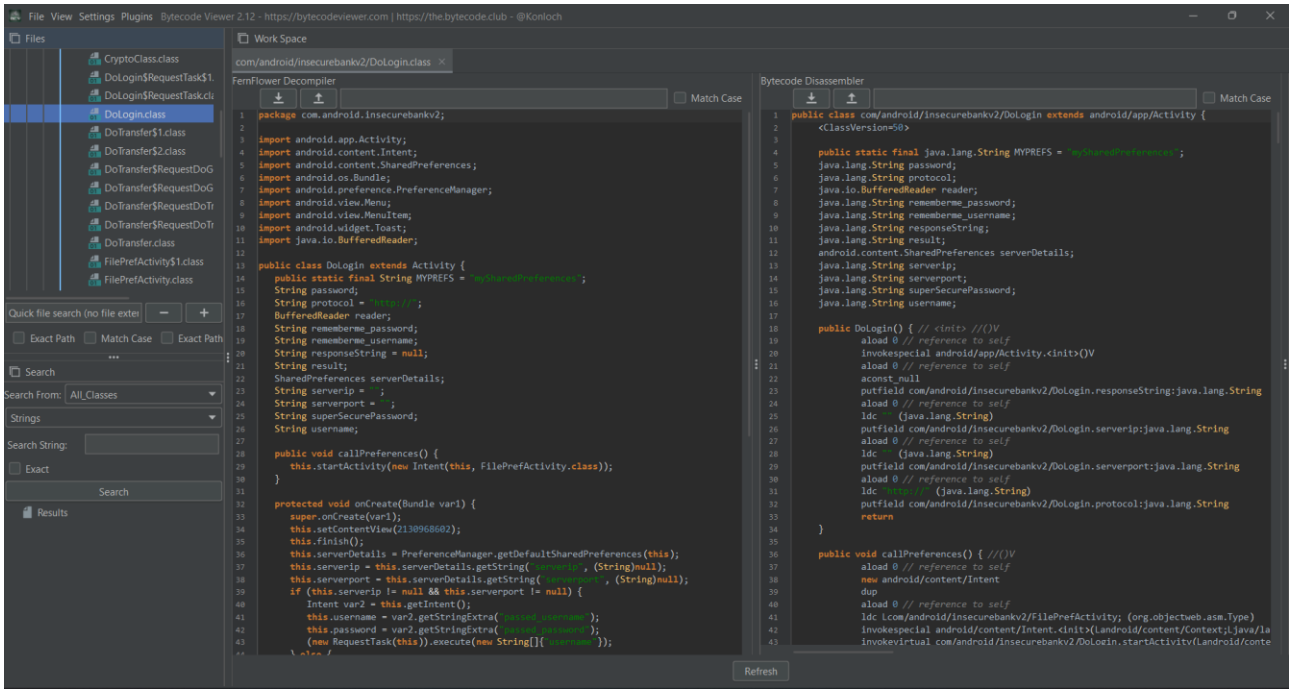




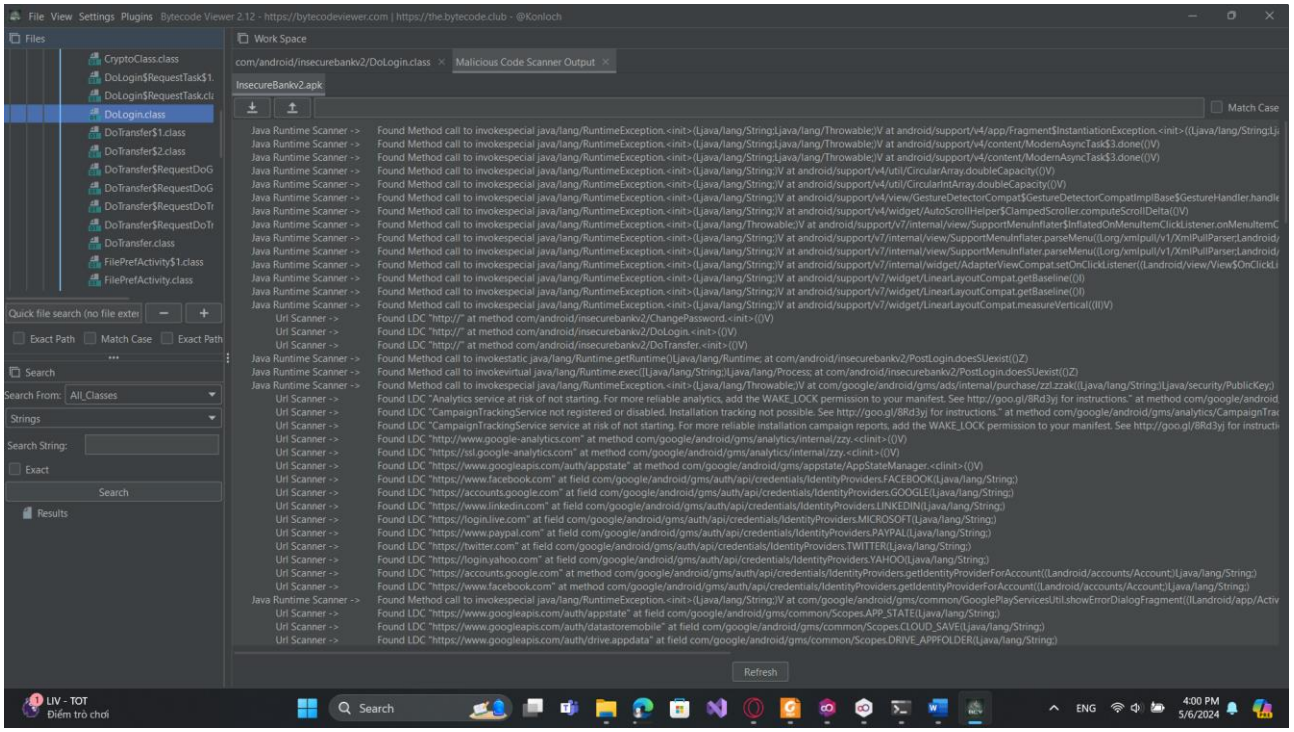
- Ta thấy có mốt số vấn đề đã được hiển thị như SEND_SMS, USE_CREDENTIAL,...

- Một trong các bước quan trong trong phân tích tĩnh là kiểm tra code. Để làm được việc này dùng ByteCode Viewer để xem code nhanh nha trong tập tin apk. Tải tập tin ***Bytecode-Viewer-2.9.x.jar*** từ https://github.com/Konloch/bytecode-viewer/releases

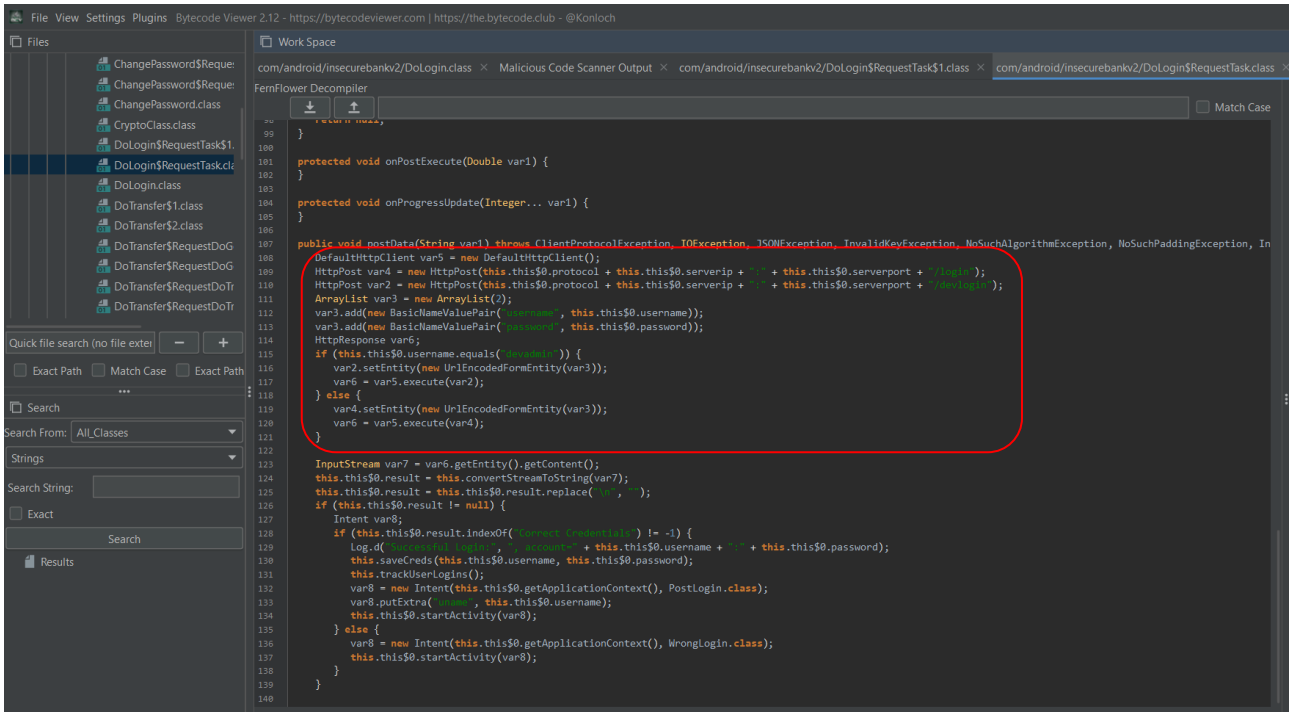
- Kéo thả tập tin apk, ByteCode Viewer sẽ phân tích và hiển thị code.



- Sử dụng *Malicious Code Scanner* ở mục *Plugins* để quét các đoạn code có vẻ nguy hiểm.



com/android/insecurebankv2/DoLogin$RequestTask.class




```
}

protected void onPostExecute(Double var1) {
}

protected void onProgressUpdate(Integer... var1) {
}

public void postData(String var1) throws ClientProtocolException, IOException, JSONException, InvalidKeyException, NoSuchAlgorithmException, NoSuchPaddingException, In
   DefaultHttpClient var5 = new DefaultHttpClient();
   HttpPost var4 = new HttpPost(this.this$0.protocol + this.this$0.serverip + ":" + this.this$0.serverport + "/login");
   HttpPost var2 = new HttpPost(this.this$0.protocol + this.this$0.serverip + ":" + this.this$0.serverport + "/devlogin");
   ArrayList var3 = new ArrayList(2);
   var3.add(new BasicNameValuePair("username", this.this$0.username));
   var3.add(new BasicNameValuePair("password", this.this$0.password));
   HttpResponse var6;
   if (this.this$0.username.equals("devadmin")) {
      var2.setEntity(new UrlEncodedFormEntity(var3));
      var6 = var5.execute(var2);
   } else {
      var4.setEntity(new UrlEncodedFormEntity(var3));
      var6 = var5.execute(var4);
   }

   InputStream var7 = var6.getEntity().getContent();
   this.this$0.result = this.convertStreamToString(var7);
   this.this$0.result = this.this$0.result.replace("\n", "");
   if (this.this$0.result != null) {
      Intent var8;
      if (this.this$0.result.indexOf("Correct Credentials") != -1) {
         Log.d("Successful Login:", ", account=" + this.this$0.username + ":" + this.this$0.password);
         this.saveCreds(this.this$0.username, this.this$0.password);
         this.trackUserLogins();
         var8 = new Intent(this.this$0.getApplicationContext(), PostLogin.class);
         var8.putExtra("uname", this.this$0.username);
         this.this$0.startActivity(var8);
      } else {
         var8 = new Intent(this.this$0.getApplicationContext(), WrongLogin.class);
         this.this$0.startActivity(var8);
      }
   }
```

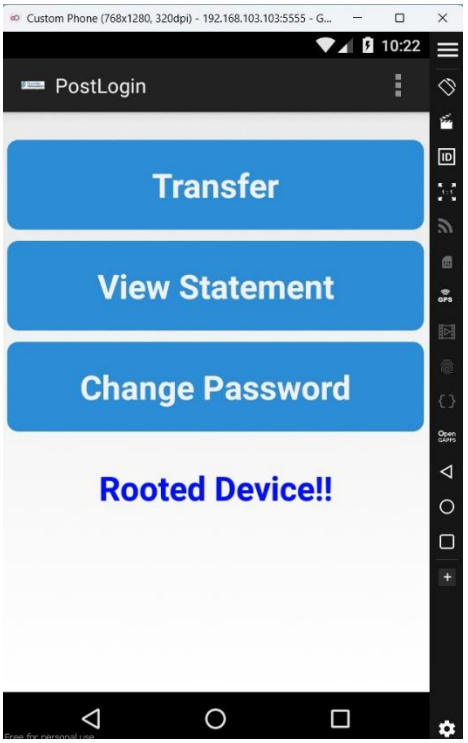
Yêu cầu 1 Phân tích và chỉ ra điểm bất thường của đoạn code trên?

- Đầu tiên ta có thể thấy trong đoạn mã sử dụng HttpPost để post các request đăng nhập. Do phương thức HTTP không có mã hóa nên nếu bắt được gói thì thì username và password có thể bị đọc được.

- Và nếu ta nhập username là devadmin thì có thể login thẳng mà không cần tới password.

Yêu cầu 2 Chỉ ra rằng dữ liệu lưu trữ có an toàn hay không?

- Đầu tiên ta sẽ thử đăng nhập vào chương trình để lưu thông tin.



- Tiếp đến vào command shell của điện thoại ảo di chuyển vào /data/data/com.android.insecurebankv2/databases

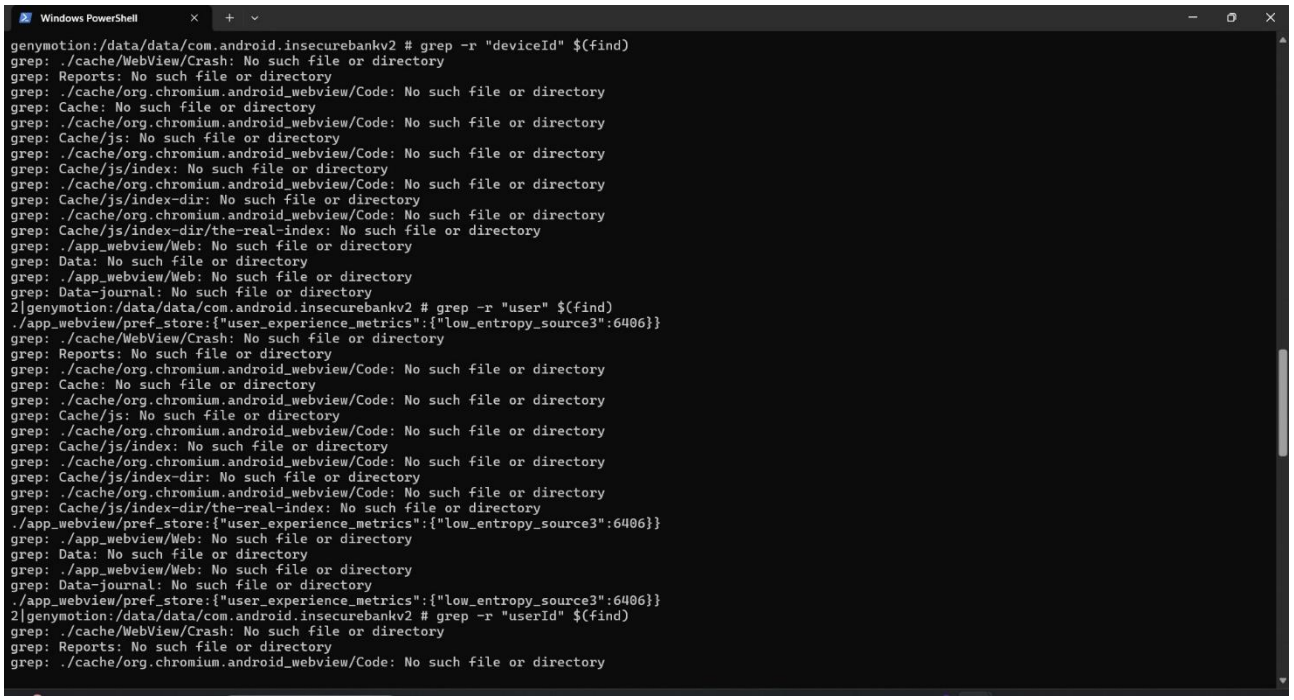
- Sử dụng lệnh sqlite3 mydb để tiến hành kiểm tra mydb. Trong database liệt kê tất cả các table hiện có, ở đây ta thấy có 2 table là android_metadata và names, ta sẽ cho hiển thị toàn bộ các thông tin có trong 2 table đó.

```
PS C:\Users\kieut> adb shell
genymotion:/ # cd /data/data/com.android.insecurebankv2/databases
genymotion:/data/data/com.android.insecurebankv2/databases # sqlite3 mydb
SQLite version 3.18.2 2017-07-21 07:56:09
Enter ".help" for usage hints.
sqlite> .database
main: /data/data/com.android.insecurebankv2/databases/mydb
sqlite> .table
android_metadata  names
sqlite> select * from names
   ...> ;
1|dinesh
2|jack
3|devadmin
sqlite> select * from android_metadata
   ...> ;
en_US
sqlite>
```

- Kết quả chỉ hiển thị các username ở dưới dạng plain text.

Yêu cầu 3 Kiểm tra xem thông tin nhạy cảm có lưu lại trên thiết bị hay không? Một số từkhoá: deviceId, userId, imei, deviceSerialNumber, devicePrint, phone, XDSN, mdn, IMSI, uuid…

- Dùng adb shell để vào command shell của điện thoại ảo sau đó di chuyển đến /data/data/com.android.insecurebankv2.
- Chạy cấu trúc lệnh grep -r "string-to-find" $(find), trong đó là những từ khóa gợi ý trong nội dung yêu cầu 3.
- Trong phần này thì ta không tìm được thông tin nhạy cảm nào cả.



Yêu cầu 4 Theo bạn thư mục sao lưu chứa thông tin nào cần mã hoá, chỉ ra.

- Đầu tiên đăng nhập với tài khoản người dùng bình thường sau đó sử dụng lệnh adb backup -apk -shared com.android.insecurebankv2 để backup dữ liệu

```
PS E:\3\bmweb\th\Lab4> adb backup -apk -shared.com.android.insecurebankv2
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...
```

- Chuyển đổi tập tin sao lưu qua định dạng có thể đọc được (cài gói qpdf)

```
trang@trang-virtual-machine:~$ cat backup.ab | (dd bs=24 count=0 skip=1; cat) |
zlib-flate -uncompress > backup_compressed.tar
0+0 records in
0+0 records out
0 bytes copied, 0,000146494 s, 0,0 kB/s
```

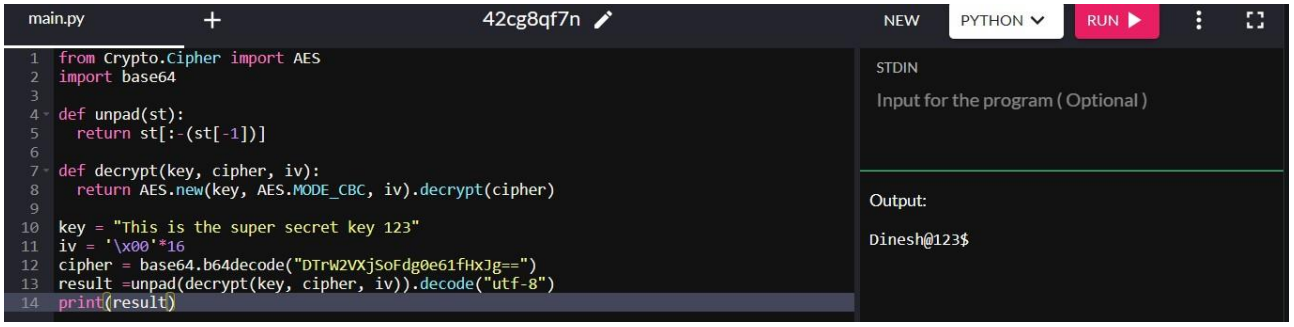
Ta có đoạn dữ liệu được mã hoá, ta có thể thấy thông tin của user đã được mã hóa

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="superSecurePassword">DTrW2VXjSoFdg0e61fHxJg==
    </string>
    <string name="EncryptedUsername">ZGluZXNo
    </string>
</map>
```

Yêu cầu 5 Viết chương trình giải mã đoạn dữ liệu mã hoá (python3 chẳng hạn…)

- Đề bài cũng đã cung cấp cho ta một đoạn mã java dùng thuật toán AES-256 với mode CBC và đệm PKCS5Padding để mã hóa kèm theo đó là key và iv dùng để giải mã.

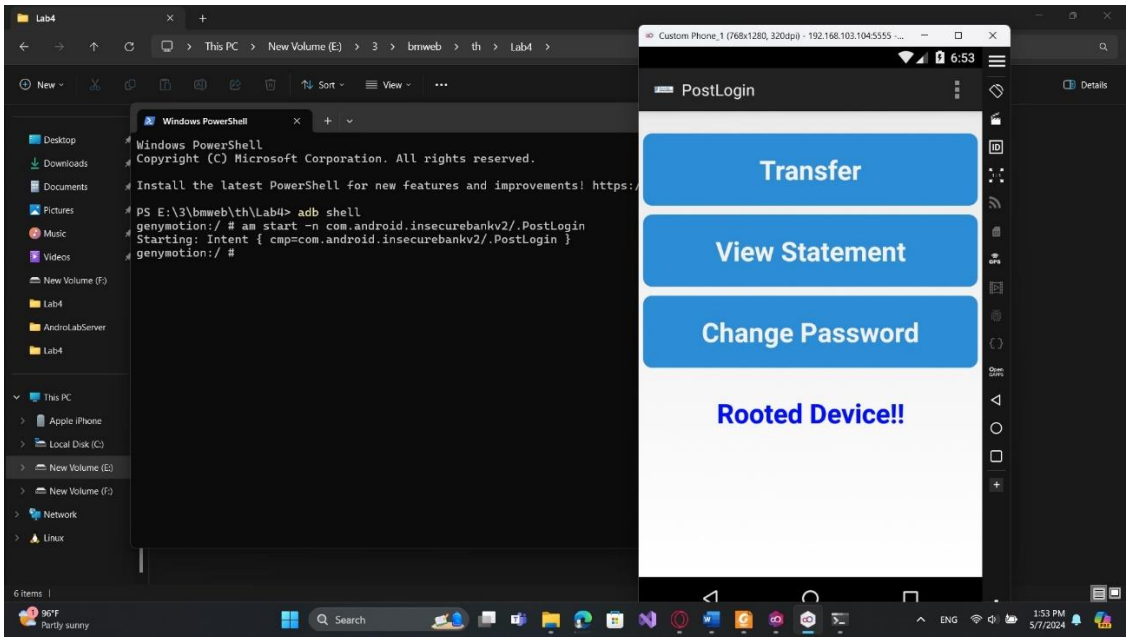
- Từ đó ta có thể viết một chương trình Python dùng để giải mã. Chạy chương trình trên one compiler, kết quả trả về là mật khẩu của user dinesh.



Activity Hijacking

- Gọi Activity Manager (am): là lệnh gọi các lệnh của hệ thống; ví dụ chạy Activity, dừng một tiến trình, sửa đổi các thuộc tính...
- Thử gọi activity PostLogin, dùng lệnh sau:

am start -n com.android.insecurebankv2/.PostLogin



2. Dịch ngược (Reverse Engineering)

- Đầu tiên ta sẽ sử dụng apktool để dịch ngược chương trình.

```
PS E:\3\bmweb\th\Lab4> apktool d InsecureBankv2.apk
I: Using Apktool 2.9.3 on InsecureBankv2.apk
I: Loading resource table...
I: Decoding file-resources...
I: Loading resource table from file: C:\Users\kieut\AppData\Local\apktool\framework\1.apk
I: Decoding values */* XMLs...
I: Decoding AndroidManifest.xml with resources...
I: Regular manifest package...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

- Ta sẽ truy cập vào InsecureBankv2/smali/com/android/insecurebankv2/ PostLogin.smali để sửa đổi tập tin. Thay đổi nhánh else để in ra Rooted Device

PostLogin.smali

E: > 3 > bmweb > th > Lab4 > InsecureBankv2 > smali > com > android > insecurebankv2 > PostLogin.smali

```
422   .method showRootStatus()V
446
447       .line 88
448       .local v0, "isrooted":Z
449       :goto_0
450       if-ne v0, v1, :cond_2
451
452       .line 90
453       iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;->root_status:Landroid/widget/TextView;
454
455       const-string v2, "Rooted Device!!"
456
457       invoke-virtual {v1, v2}, Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V
458
459       .line 96
460       :goto_1
461       return-void
462
463       .line 87
464       .end local v0    # "isrooted":Z
465       :cond_1
466       const/4 v0, 0x0
467
468       goto :goto_0
469
470       .line 94
471       .restart local v0    # "isrooted":Z
472       :cond_2
473       iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;->root_status:Landroid/widget/TextView;
474
475       const-string v2, "Rooted Device!!"
476
477       invoke-virtual {v1, v2}, Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V
478
479       goto :goto_1
480   .end method
```

- Sử dụng apktool để vá lại file apk

```
PS E:\3\bmweb\th\Lab4> apktool b InsecureBankv2 -o InsecureBankv2_1.apk
I: Using Apktool 2.9.3
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk into: InsecureBankv2_1.apk
```

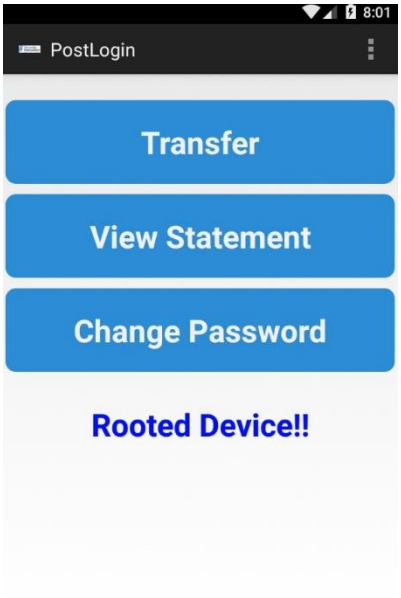
- Android yêu cầu các tập tin APK đều phải được ký bằng một chứng chỉ trước khi được phép cài đặt trên thiết bị. Sau khi chỉnh sửa, tập tin APK sẽ không còn toàn vẹn như ban đầu nên cần phải được ký lại.
- Vì vậy ta cần tạo key và kí

```
PS C:\Users\kieut> keytool -genkeypair -v -keystore E:\3\bmweb\th\Lab4\key.keystore -alias InsecureBankv2_1 -keyalg RSA
-keysize 2048 -validity 1000
Enter keystore password:
Re-enter new password:
Enter the distinguished name. Provide a single dot (.) to leave a sub-component empty or press ENTER to use the default
value in braces.
What is your first and last name?
What is the name of your organizational unit?
What is the name of your organization?
What is the name of your City or Locality?
What is the name of your State or Province?
What is the two-letter country code for this unit?
Is CN=trang nguyen, OU=UIT, O=Group 06, L=HCM, ST=HCM, C=123 correct?
  [no]:  yes
Generating 2,048 bit RSA key pair and self-signed certificate (SHA384withRSA) with a validity of 1,000 days
        for: CN=trang nguyen, OU=UIT, O=Group 06, L=HCM, ST=HCM, C=123
[Storing E:\3\bmweb\th\Lab4\key.keystore]
```

```
PS C:\Program Files\Java\jdk-22\bin> jarsigner -keystore "E:\3\bmweb\th\Lab4\key.keystore" -storepa
ss [redacted] "E:\3\bmweb\th\Lab4\InsecureBankv2_1.apk" InsecureBankv2_1
jar signed.

Warning:
The signer's certificate is self-signed.
```

- Sau khi hoàn thành quá trình kí và tạo key ta sẽ cài đặt lại chương trình và kiểm tra.

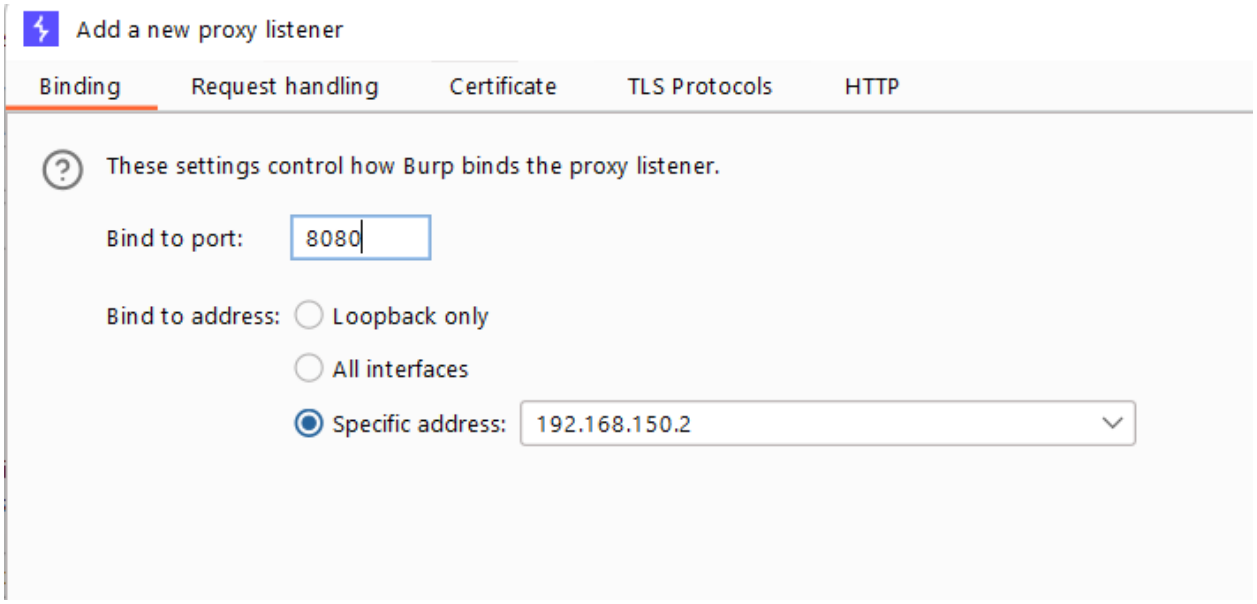


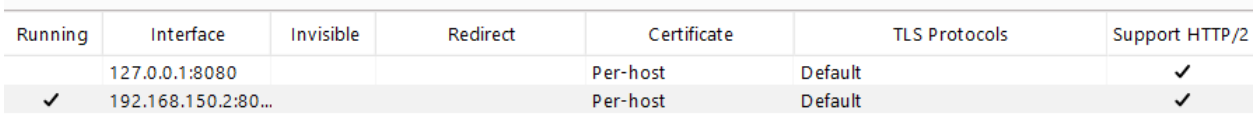
3. Phân tích động (Dynamic Analysis)

- Địa chỉ IP của điện thoại ảo.

```
PS C:\Users\cuong> adb devices
List of devices attached
192.168.150.105:5555    device
```

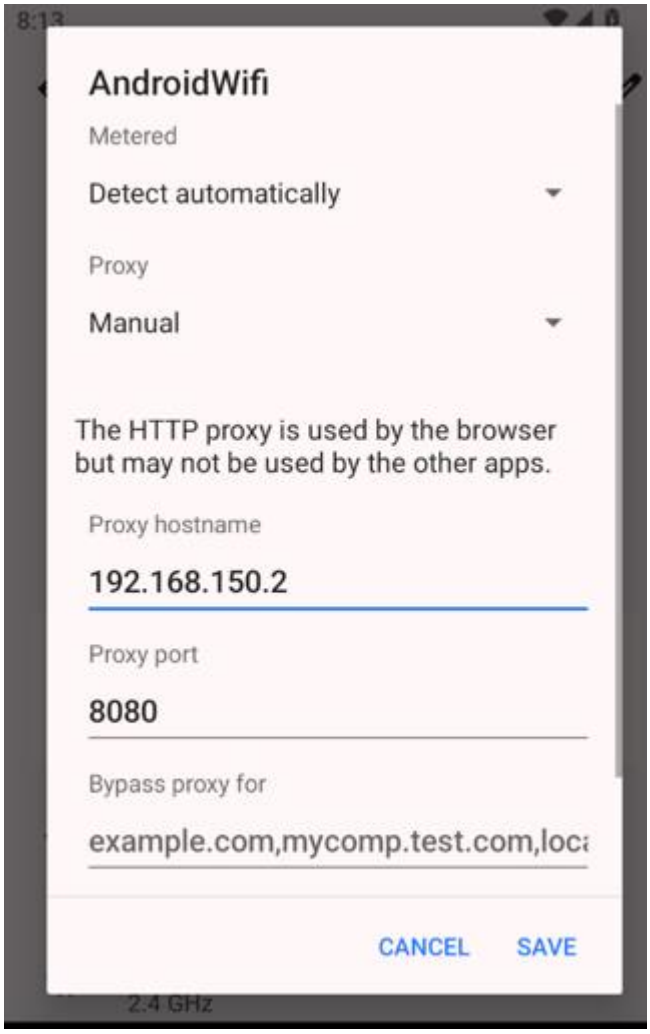
- Tạo proxy cho điện thoại ảo.



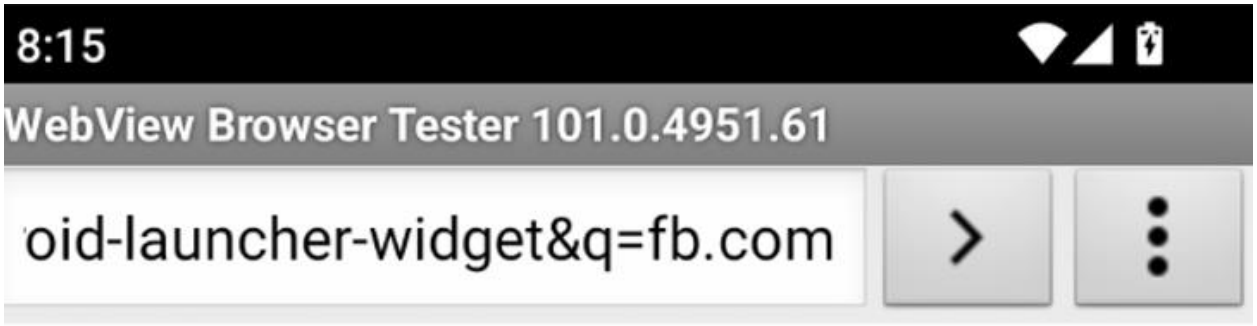


Running	Interface	Invisible	Redirect	Certificate	TLS Protocols	Support HTTP/2
	127.0.0.1:8080			Per-host	Default	✓
✓	192.168.150.2:80...			Per-host	Default	✓

- Cấu hình thông tin proxy điện thoại ảo.

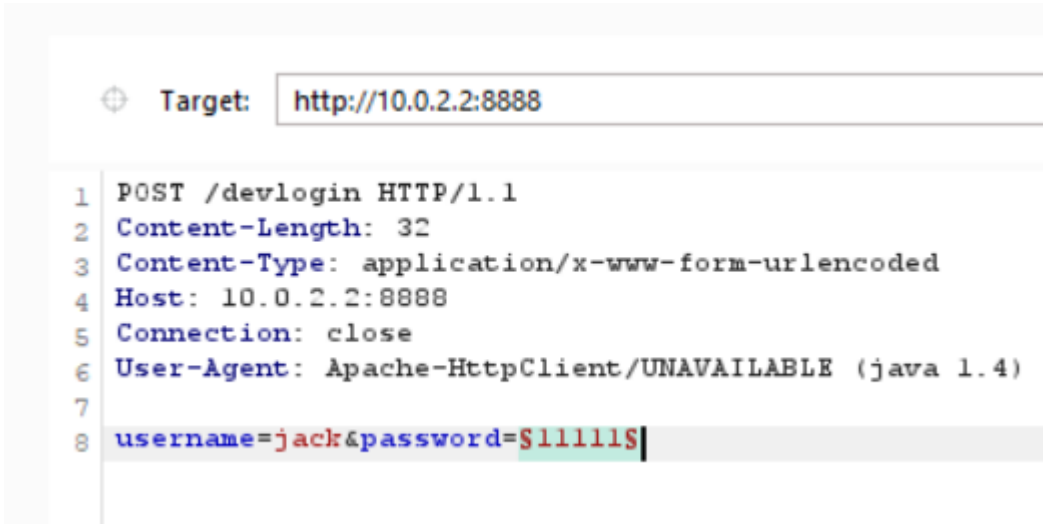


- Truy cập thử trang fb.com.

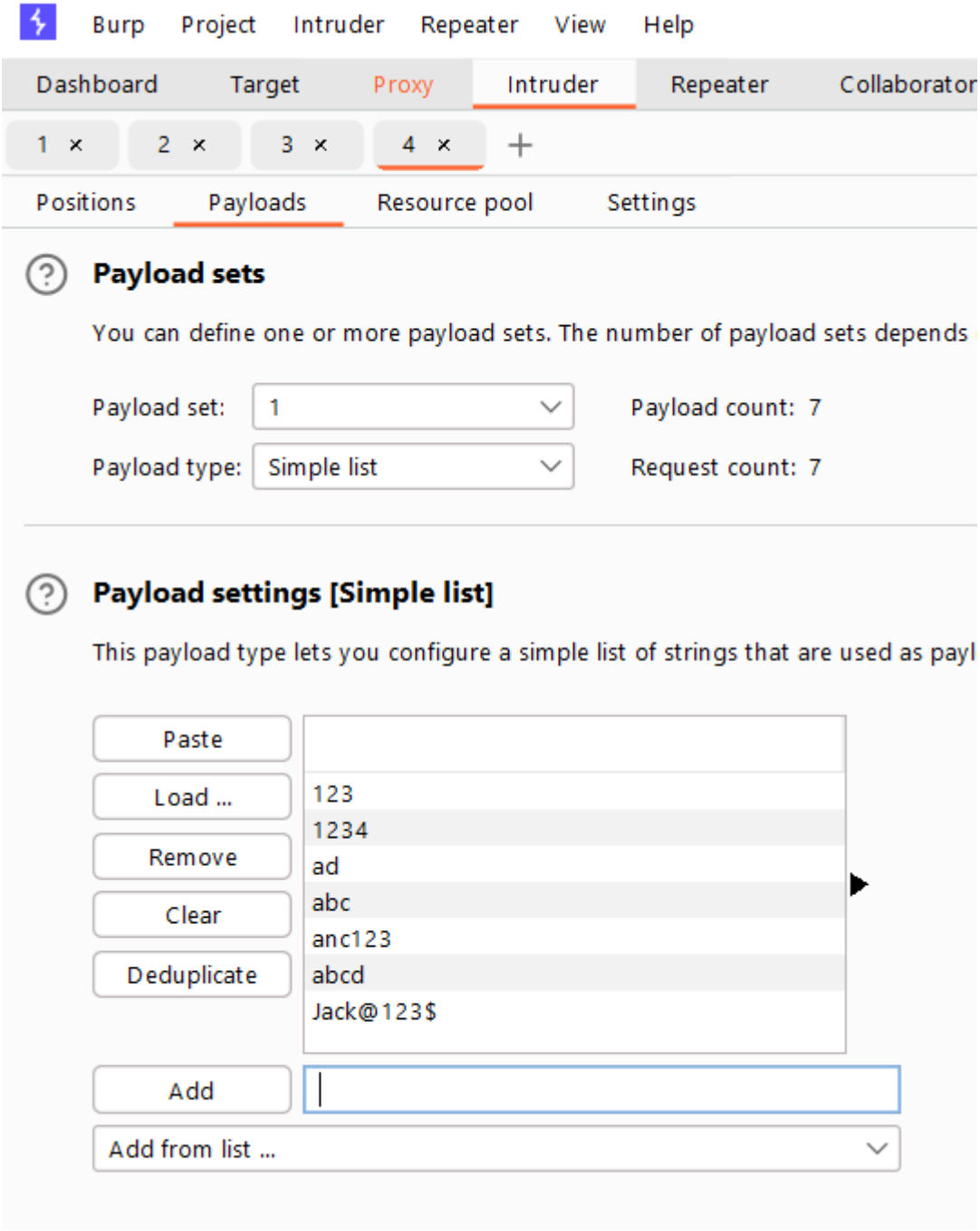


- Ta thấy proxy đã được cấu hình thành công.

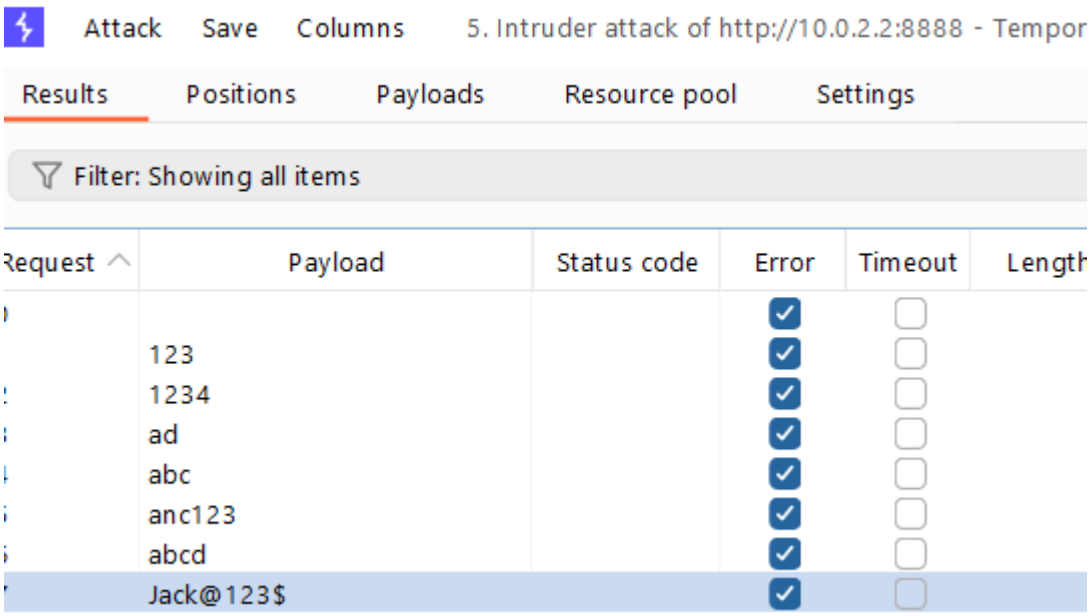
- Tại tab intruder, ta đánh dấu phần nội dung trường password.



- Tại phần payload ta thêm các mật khẩu để tiến hành tấn công vét cạn.



- Kết quả sau khi tấn công vét cạn.



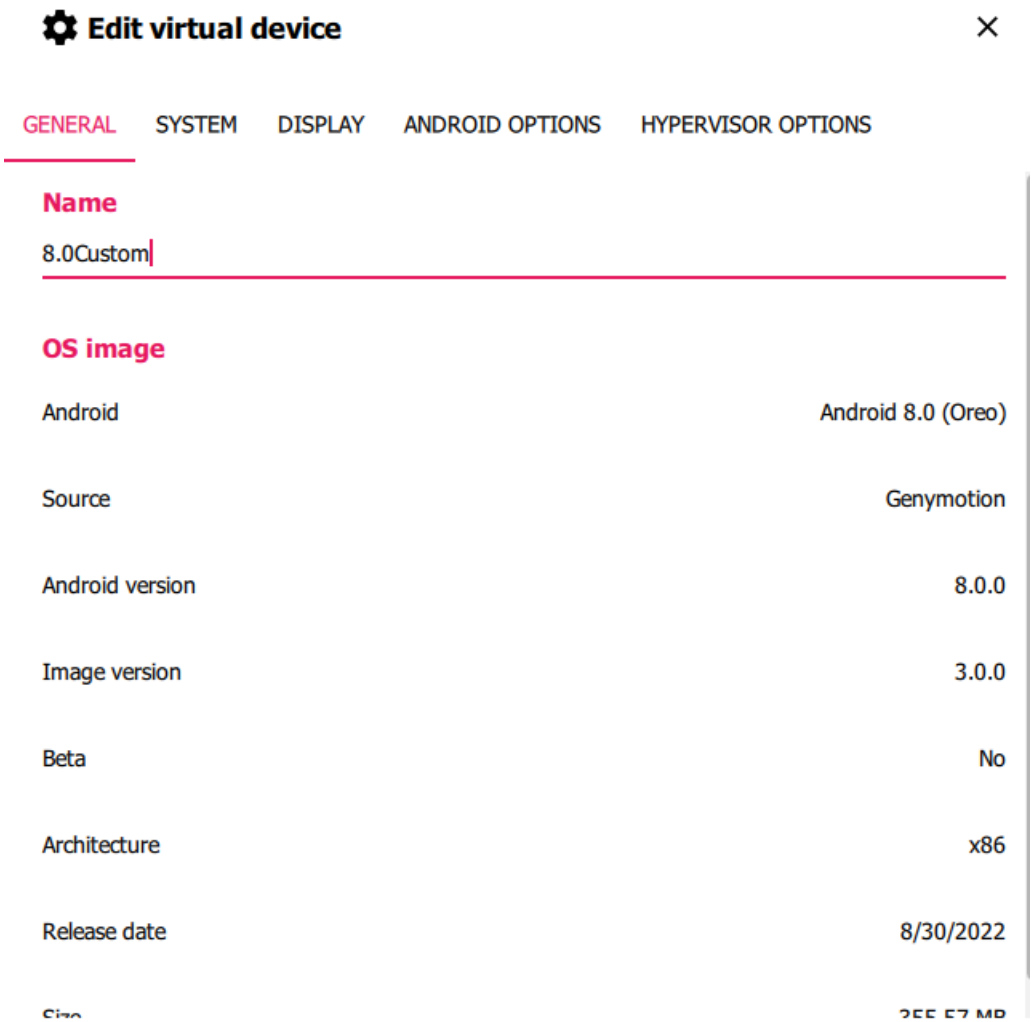
- Phần History hiển thị lịch sử của các request được gửi từ điện thoại ảo.

4. Hooking với Frida:

- Cài đặt Frida tool.

```
C:\Users\cuong>pip3 install frida-tools
Collecting frida-tools
  Downloading frida-tools-12.3.0.tar.gz (200 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 200.5/200.5 kB 715.3 kB/s eta 0:00
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Installing backend dependencies ... done
  Preparing metadata (pyproject.toml) ... done
Requirement already satisfied: colorama<1.0.0,>=0.2.7 in c:\users\cuong\appdata\
-packages (from frida-tools) (0.4.6)
Collecting frida<17.0.0,>=16.0.9 (from frida-tools)
  Downloading frida-16.2.1-cp37-abi3-win_amd64.whl.metadata (2.1 kB)
Collecting prompt-toolkit<4.0.0,>=2.0.0 (from frida-tools)
  Downloading prompt_toolkit-3.0.43-py3-none-any.whl.metadata (6.5 kB)
Collecting pygments<3.0.0,>=2.0.2 (from frida-tools)
  Downloading pygments-2.18.0-py3-none-any.whl.metadata (2.5 kB)
Collecting wcwidth (from prompt-toolkit<4.0.0,>=2.0.0->frida-tools)
  Downloading wcwidth-0.2.13-py2.py3-none-any.whl.metadata (14 kB)
Downloading frida-16.2.1-cp37-abi3-win_amd64.whl (32.7 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 32.7/32.7 MB 14.6 MB/s eta 0:00:00
```

- Ở đây ta thấy kiến trúc điện thoại là x86.



-Do đó ta cần tải Frida-server tương ứng.

frida-server-16.2.1-android-x86.xz 15.1 MB Feb 17

- Cài đặt Frida-server ở điện thoại ảo.

```
PS C:\Users\cuong\Downloads> adb push frida-server-16.2.1-android-x86 /data/local/tmp/frida-server
frida-server-16.2.1-android-x86: 1 file pushed. 102.0 MB/s (51807740 bytes in 0.484s)
PS C:\Users\cuong\Downloads> adb shell
genymotion:/ # chmod +x frida-server
chmod: frida-server: No such file or directory
1|genymotion:/ # cd /data/local/tmp/
genymotion:/data/local/tmp # chmod +x frida-server
genymotion:/data/local/tmp # ./frida-server &
[1] 1900
```

- Cài đặt thành công.

```
PS C:\Users\cuong> frida-ps -U
 PID  Name
----  ------------------------------------------------
1436  Calendar
 952  Clock
1505  Email
1602  Messaging
 997  Phone
1364  Search
 788  Settings
1797  Superuser
 238  adbd
1852  android.ext.services
 468  android.hardware.camera.provider@2.4-service
 469  android.hardware.configstore@1.0-service
 232  android.hardware.gnss@1.0-service
 470  android.hardware.graphics.allocator@2.0-service
 169  android.hardware.keymaster@3.0-service
 471  android.hardware.sensors@1.0-service
 472  android.hardware.wifi@1.0-service
```

Yêu cầu 7 Hoàn thiện đoạn code trên và demo.

- Đoạn script hook1.py

```
import frida
import time

device = frida.get_usb_device()
pid = device.spawn("com.android.insecurebankv2")
device.resume(pid)

time.sleep(1)
session=device.attach(pid)

hook_script="""
Java.perform
(
    function()
    {
        console.log("Inside the hook_script");
        classPostLogin = Java.use('com.android.insecurebankv2.PostLogin');
        classPostLogin.doesSuperuserApkExist.implementation = function()
        {
            return true;
        };
    }
);
"""

script=session.create_script(hook_script)
script.load()

input('...?')
```

- Ở đây ta sẽ ghi đè method doesSuperuserApkExist() bằng cách sử dụng implementation.

```
classPostLogin.doesSuperuserApkExist.implementation = function()
{
    return true;
};
```

- Khi doesSuperuserApkExist() == true thì root detected.

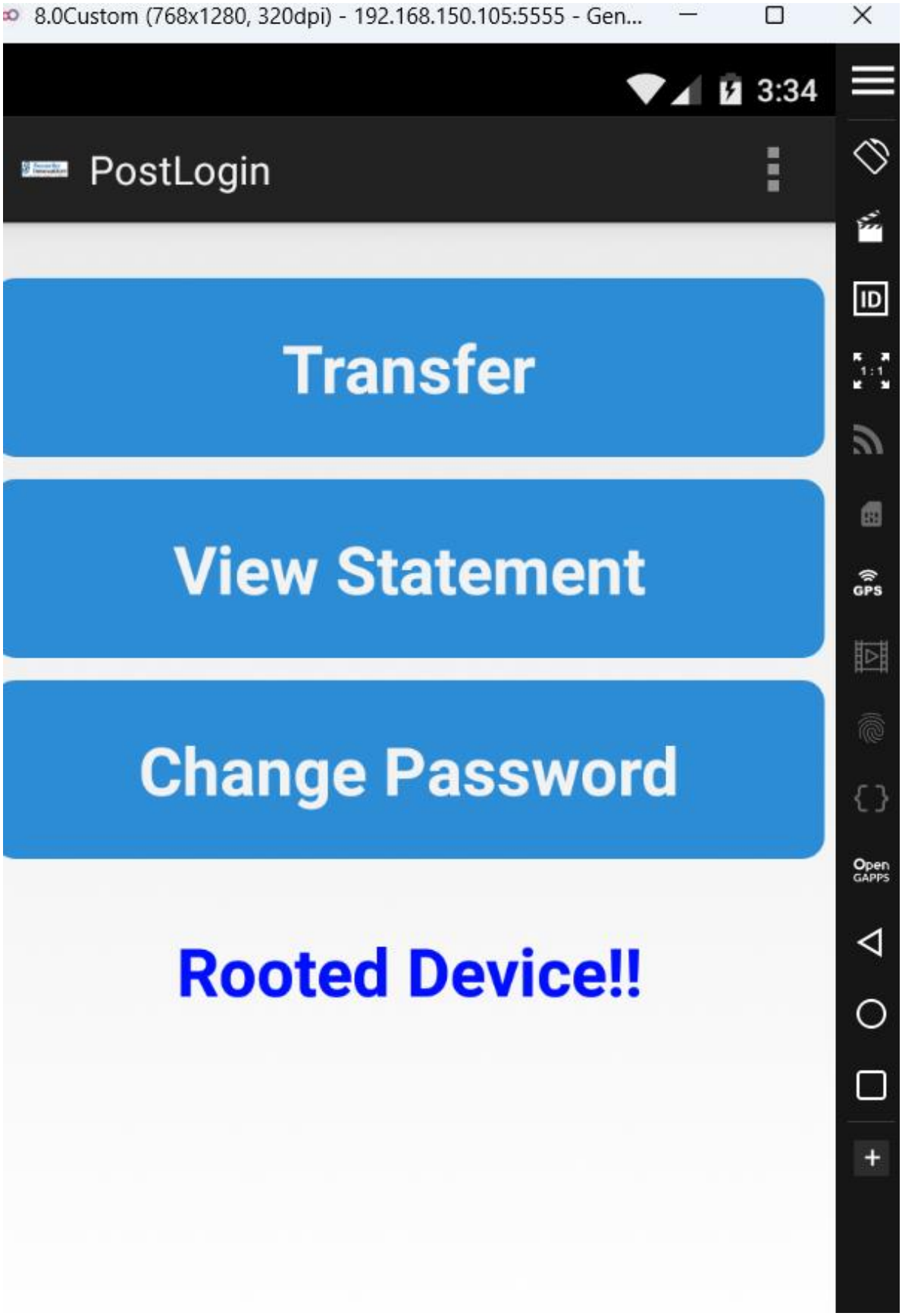
```
void showRootStatus() {
    boolean var1;
    if (!this.doesSuperuserApkExist("/system/app/Superuser.apk") && !this.doesSUexist()) {
      var1 = false;
    } else {
      var1 = true;
    }

    if (var1) {
      this.root_status.setText("Rooted Device!!");
    } else {
      this.root_status.setText("Device not Rooted!!");
    }

  }
```

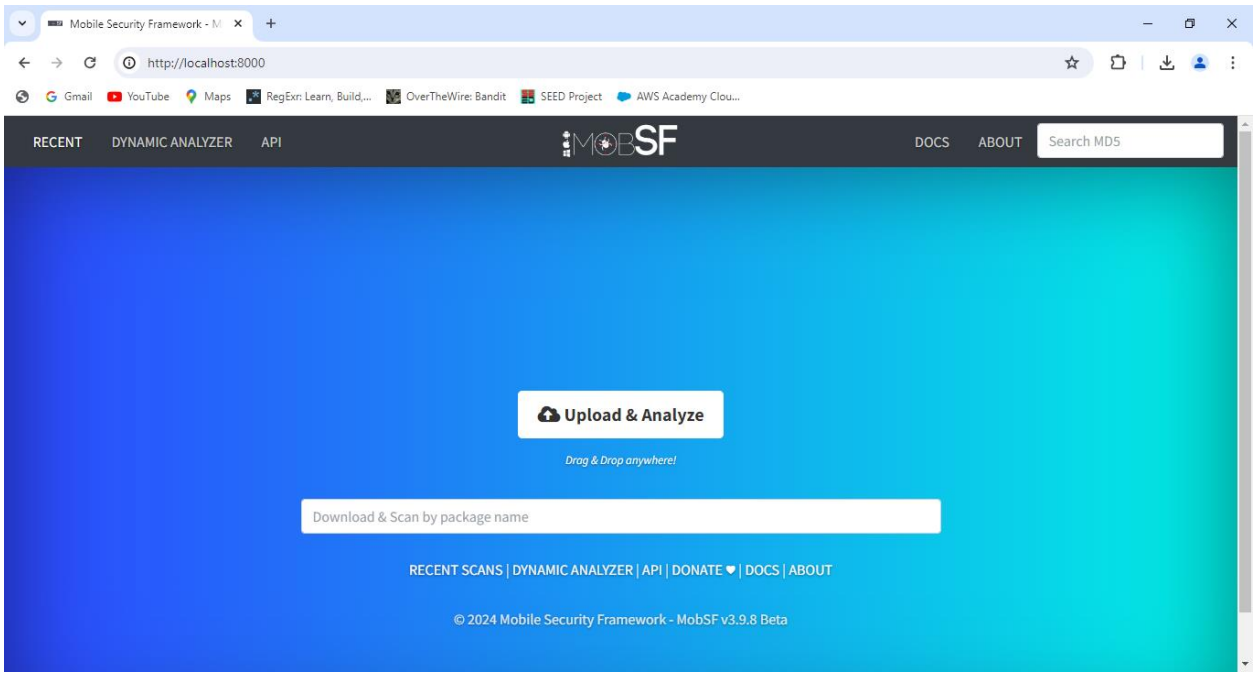
```
PS C:\Users\cuong\Downloads> python hook1.py
Inside the hook_script
...?
```

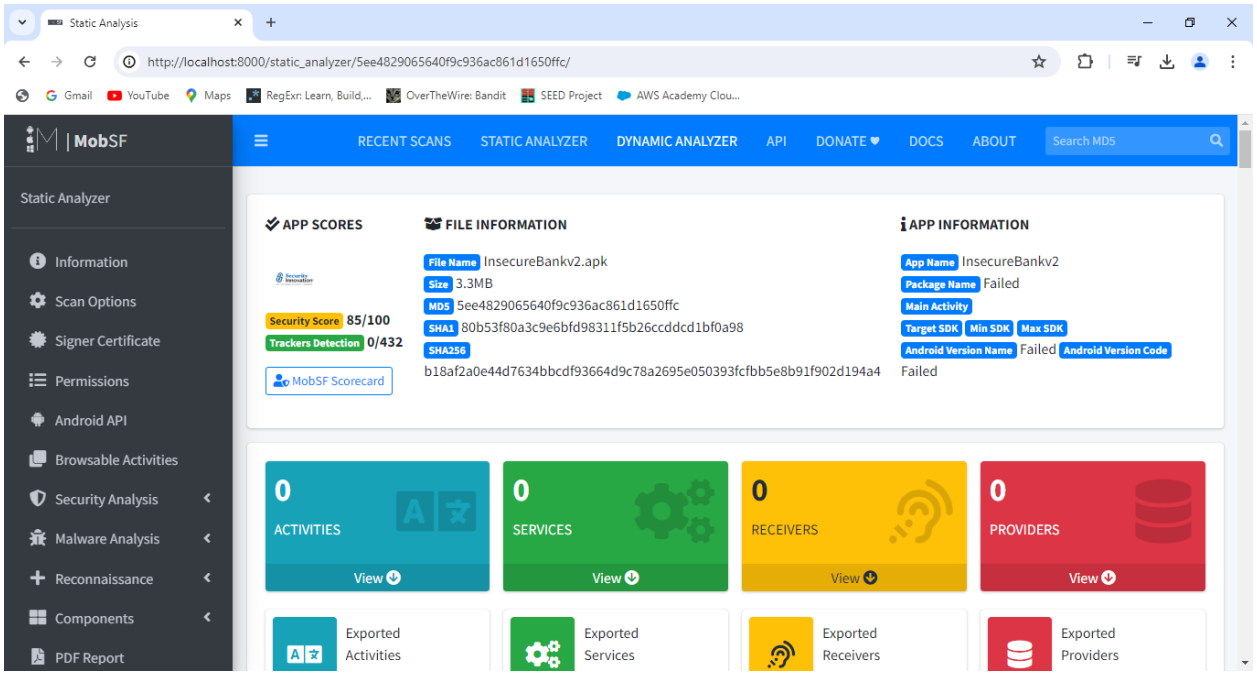
- Kết quả cho thấy ta root device thành công.


8.0Custom (768x1280, 320dpi) - 192.168.150.105:5555 - Gen...
3:34
PostLogin
Transfer
View Statement
Change Password
Rooted Device!!
GPS
Open GAPPS

D. CHALLENGES CTF (BÀI TẬP BẢO MẬT ỨNG DỤNG)

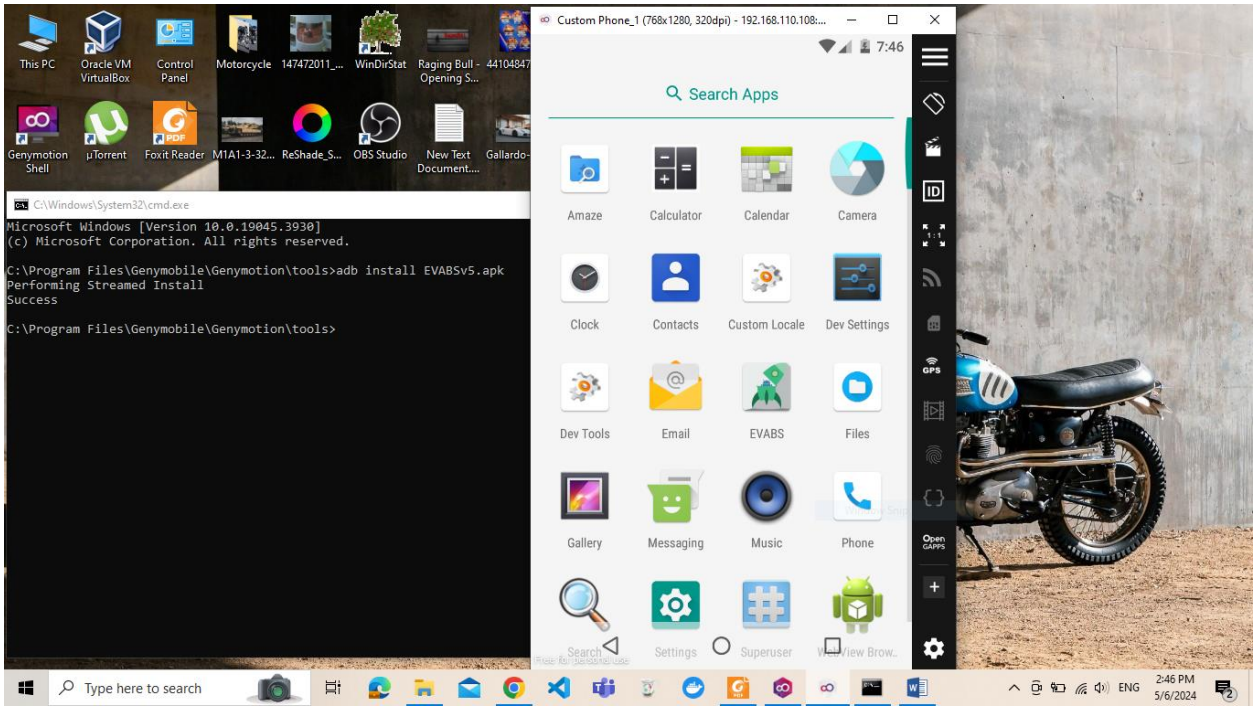
Thiết lập môi trường



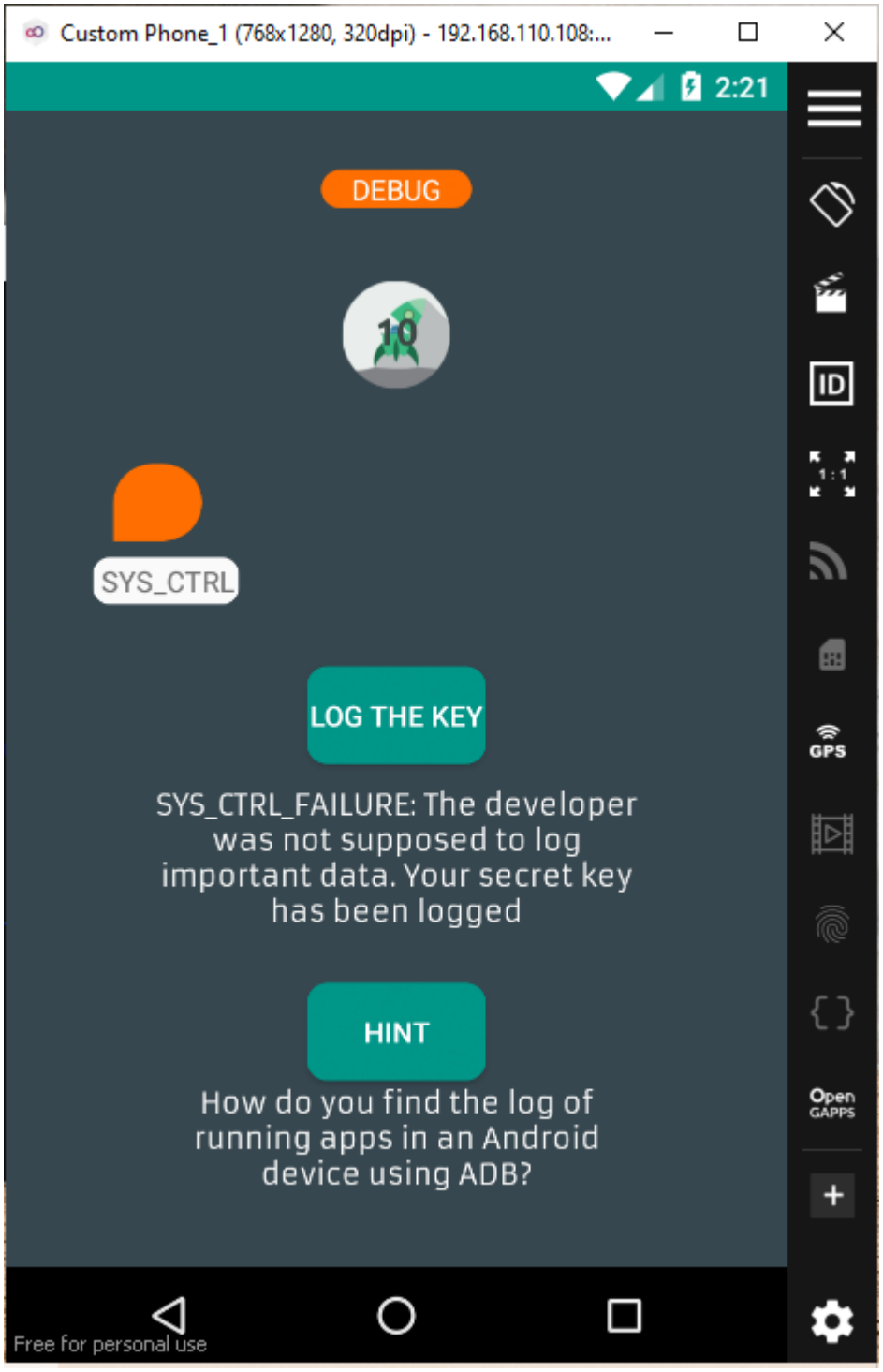


CHALLENGES CTF

EV ABS


This PC
Oracle VM VirtualBox
Control Panel
Motorcycle
WinDirStat
Genymotion Shell
µTorrent
Foxit Reader
OBS Studio
New Text Document....
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.
C:\Program Files\Genymobile\Genymotion\tools>adb install EVABSv5.apk
Performing Streamed Install
Success
C:\Program Files\Genymobile\Genymotion\tools>
Custom Phone_1 (768x1280, 320dpi) - 192.168.110.108:...
7:46
Search Apps
Amaze
Calculator
Calendar
Camera
Clock
Contacts
Custom Locale
Dev Settings
Dev Tools
Email
EVABS
Files
Gallery
Messaging
Music
Phone
Search
Settings
Superuser
Type here to search
ENG
2:46 PM
5/6/2024

Flag1:



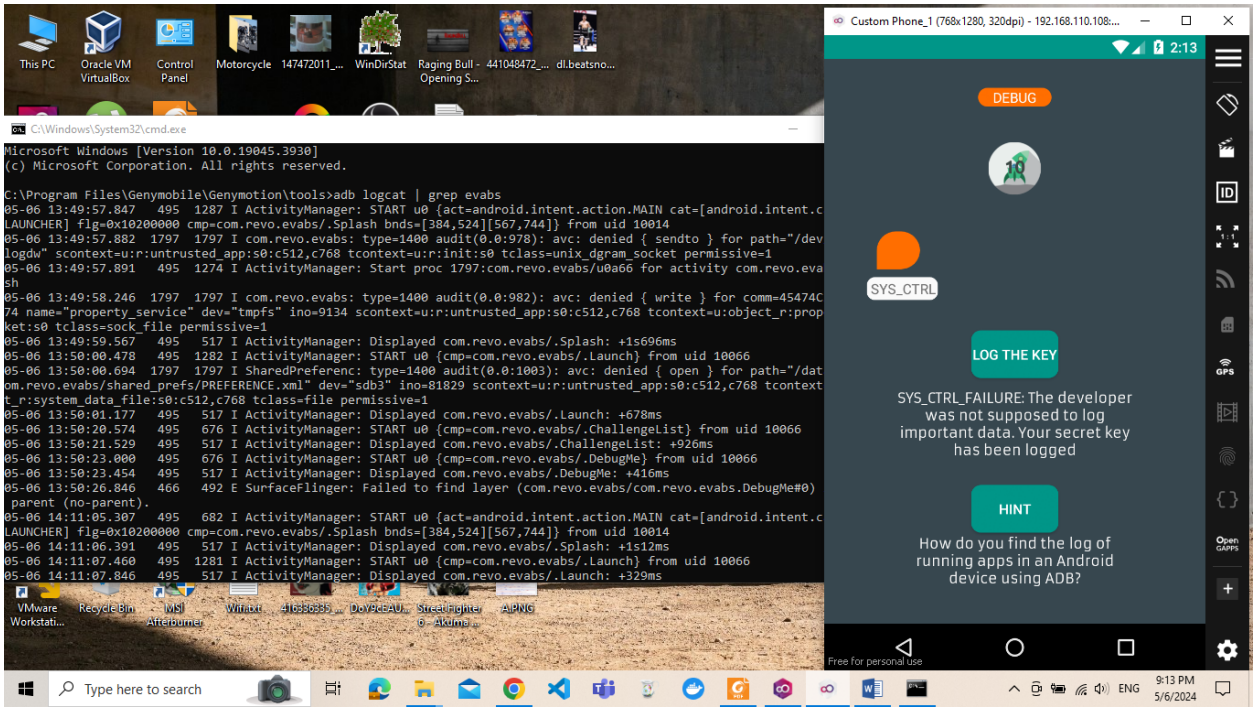
Tiến hành xem log của chương trình

```
C:\Windows\System32\cmd.exe - adb logcat
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Genymobile\Genymotion\tools>adb install EVABSv5.apk
Performing Streamed Install
Success

C:\Program Files\Genymobile\Genymotion\tools>adb logcat
--------- beginning of system
05-06 07:35:12.779   159   159 I vold    : Vold 3.0 (the awakening) firing up
05-06 07:35:12.779   159   159 V vold    : Detected support for: ext4 vfat
05-06 07:35:12.785   159   159 I vold    : [libfs_mgr]fs_mgr_read_fstab_dt(): failed to read fstab from dt
05-06 07:35:12.795   159   172 I vold    : e4crypt_initialize_global_de
05-06 07:35:12.795   159   172 I vold    : Creating new key
05-06 07:35:12.800   159   172 D vold    : Creating key that doesn't need auth token
05-06 07:35:12.803   159   172 D vold    : Created key /data/unencrypted/key
05-06 07:35:12.803   159   172 D vold    : Added key 1010257162 (ext4:7fc5a61ddedfdaf5) to keyring 671894807 in process
159
05-06 07:35:12.858   159   172 D vold    : e4crypt_init_user0
05-06 07:35:12.858   159   172 D vold    : Preparing: /data/misc/vold/user_keys
05-06 07:35:12.858   159   172 D vold    : Preparing: /data/misc/vold/user_keys/ce
05-06 07:35:12.858   159   172 D vold    : Preparing: /data/misc/vold/user_keys/de
05-06 07:35:12.858   159   172 D vold    : Preparing: /data/misc/vold/user_keys/ce/0
05-06 07:35:12.858   159   172 D vold    : Skipping non-key .
05-06 07:35:12.858   159   172 D vold    : Skipping non-key ..
05-06 07:35:12.861   159   172 D vold    : Creating key that doesn't need auth token
05-06 07:35:12.863   159   172 D vold    : Created key /data/misc/vold/user_keys/ce/0/current
05-06 07:35:12.867   159   172 D vold    : Creating key that doesn't need auth token
05-06 07:35:12.872   159   172 D vold    : Created key /data/misc/vold/user_keys/de/0
05-06 07:35:12.873   159   172 D vold    : Added key 26902 (ext4:6c0c1d38fa584250) to keyring 671894807 in process 159
```

Ta thấy được tiến trình chạy lên bằng lệnh grep evabs

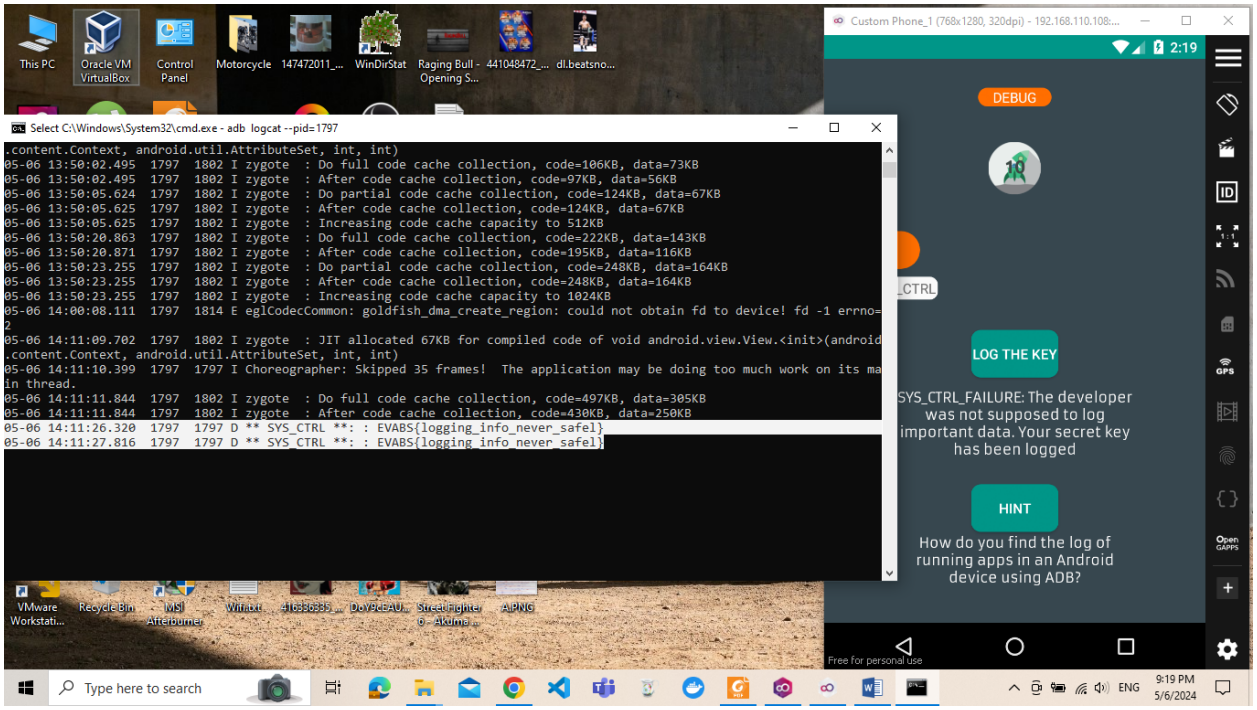


```
C:\Program Files\Genymobile\Genymotion\tools>adb logcat | grep evabs
05-06 13:49:57.847   495  1287 I ActivityManager: START u0 {act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] flg=0x10200000 cmp=com.revo.evabs/.Spl
ash bnds=[384,524][567,744]} from uid 10014
05-06 13:49:57.882  1797  1797 I com.revo.evabs: type=1400 audit(0.0:978): avc: denied { sendto } for path="/dev/socket/logdw" scontext=u:r:untrusted_app:s0:c512,c768 t
context=u:r:init:s0 tclass=unix_dgram_socket permissive=1
05-06 13:49:57.891   495  1274 I ActivityManager: Start proc 1797:com.revo.evabs/u0a66 for activity com.revo.evabs/.Splash
05-06 13:49:58.246  1797  1797 I com.revo.evabs: type=1400 audit(0.0:982): avc: denied { write } for comm=45474C20496E6974 name="property_service" dev="tmpfs" ino=9134
scontext=u:r:untrusted_app:s0:c512,c768 tcontext=u:object_r:property_socket:s0 tclass=sock_file permissive=1
05-06 13:49:59.567   495   517 I ActivityManager: Displayed com.revo.evabs/.Splash: +1s696ms
05-06 13:50:00.478   495  1282 I ActivityManager: START u0 {cmp=com.revo.evabs/.Launch} from uid 10066
05-06 13:50:00.694  1797  1797 I SharedPreferenc: type=1400 audit(0.0:1003): avc: denied { open } for path="/data/data/com.revo.evabs/shared_prefs/PREFERENCE.xml" dev="
sdb3" ino=81829 scontext=u:r:untrusted_app:s0:c512,c768 tcontext=u:object_r:system_data_file:s0:c512,c768 tclass=file permissive=1
05-06 13:50:01.177   495   517 I ActivityManager: Displayed com.revo.evabs/.Launch: +678ms
05-06 13:50:20.574   495   676 I ActivityManager: START u0 {cmp=com.revo.evabs/.ChallengeList} from uid 10066
05-06 13:50:21.529   495   517 I ActivityManager: Displayed com.revo.evabs/.ChallengeList: +926ms
05-06 13:50:23.000   495   676 I ActivityManager: START u0 {cmp=com.revo.evabs/.DebugMe} from uid 10066
05-06 13:50:23.454   495   517 I ActivityManager: Displayed com.revo.evabs/.DebugMe: +416ms
05-06 13:50:26.846   466   492 E SurfaceFlinger: Failed to find layer (com.revo.evabs/com.revo.evabs.DebugMe#0) in layer parent (no-parent).
05-06 14:11:05.307   495   682 I ActivityManager: START u0 {act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] flg=0x10200000 cmp=com.revo.evabs/.Spl
ash bnds=[384,524][567,744]} from uid 10014
05-06 14:11:06.391   495   517 I ActivityManager: Displayed com.revo.evabs/.Splash: +1s12ms
05-06 14:11:07.460   495  1281 I ActivityManager: START u0 {cmp=com.revo.evabs/.Launch} from uid 10066
05-06 14:11:07.846   495   517 I ActivityManager: Displayed com.revo.evabs/.Launch: +329ms
05-06 14:11:09.442   495   813 I ActivityManager: START u0 {cmp=com.revo.evabs/.ChallengeList} from uid 10066
05-06 14:11:10.414   495   517 I ActivityManager: Displayed com.revo.evabs/.ChallengeList: +943ms
05-06 14:11:11.712   495  1287 I ActivityManager: START u0 {cmp=com.revo.evabs/.DebugMe} from uid 10066
05-06 14:11:12.036   495   517 I ActivityManager: Displayed com.revo.evabs/.DebugMe: +289ms
```

Tiếp tục tìm kiếm tiến trình với pid như vậy

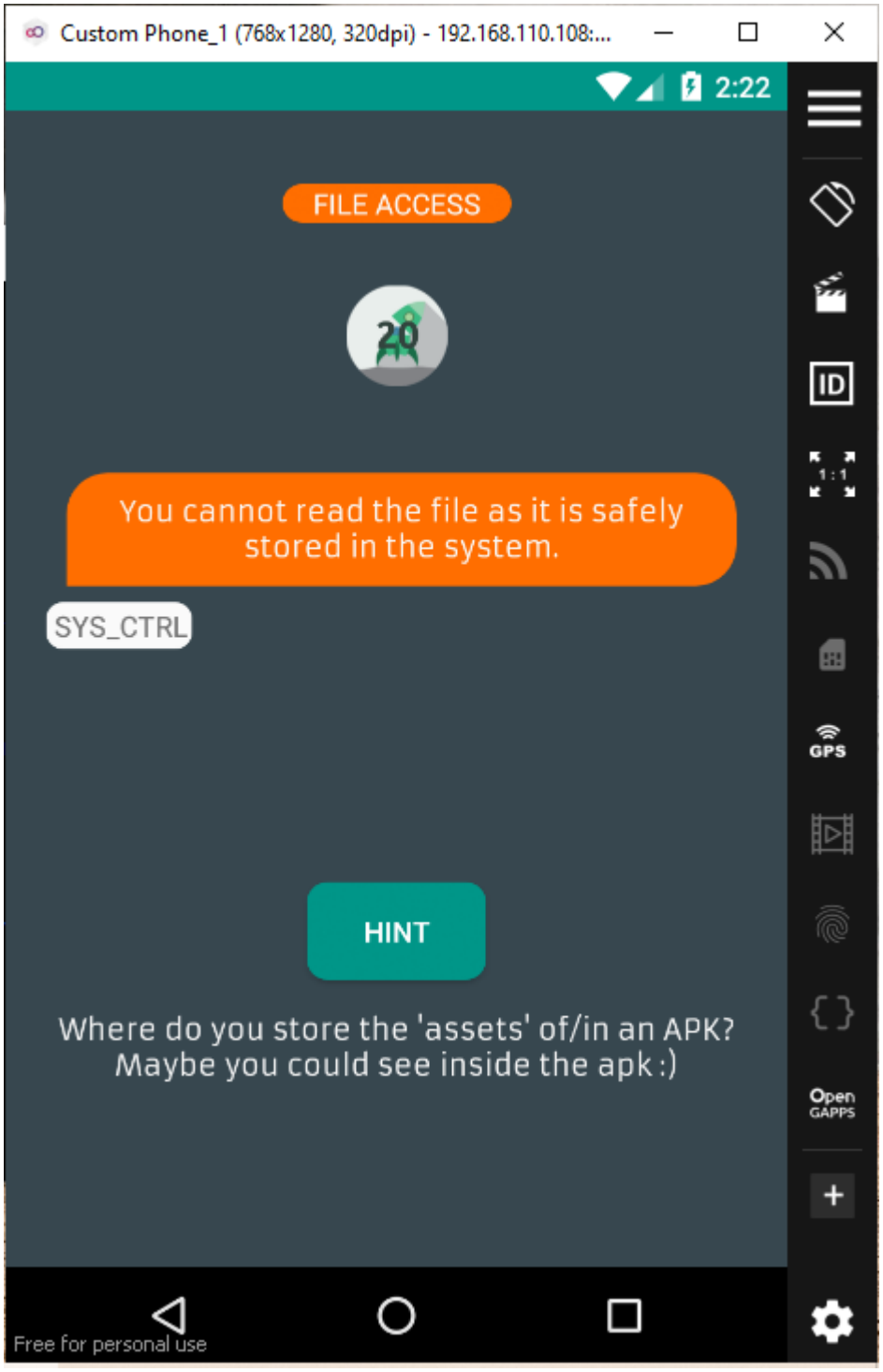
```
C:\Windows\System32\cmd.exe - adb  logcat --pid=1797
C:\Program Files\Genymobile\Genymotion\tools>adb logcat --pid=1797
--------- beginning of main
05-06 13:49:57.882  1797  1797 I com.revo.evabs: type=1400 audit(0.0:978): avc: denied { sendto } for path="/dev/socket/logdw" scontext=u:r:untrusted_app:s0:c512,c768 t
context=u:r:init:s0 tclass=unix_dgram_socket permissive=1
05-06 13:49:57.886  1797  1797 I zygote  : Late-enabling -Xcheck:jni
05-06 13:49:57.915  1797  1797 W zygote  : Unexpected CPU variant for X86 using defaults: x86
05-06 13:49:57.966  1797  1797 I JDWP    : type=1400 audit(0.0:980): avc: denied { connectto } for path=006A6477702D636F6E74726F6C scontext=u:r:untrusted_app:s0:c512,c7
68 tcontext=u:r:init:s0 tclass=unix_stream_socket permissive=1
05-06 13:49:58.246  1797  1797 I com.revo.evabs: type=1400 audit(0.0:982): avc: denied { write } for comm=45474C20496E6974 name="property_service" dev="tmpfs" ino=9134
scontext=u:r:untrusted_app:s0:c512,c768 tcontext=u:object_r:property_socket:s0 tclass=sock_file permissive=1
05-06 13:49:58.250  1797  1812 I vndksupport: sphal namespace is not configured for this process. Loading /vendor/lib/egl/libGLES_emulation.so from the current namespac
e instead.
05-06 13:49:58.250  1797  1812 I vndksupport: sphal namespace is not configured for this process. Loading /vendor/lib/egl/libEGL_emulation.so from the current namespace
 instead.
05-06 13:49:58.252  1797  1812 I vndksupport: sphal namespace is not configured for this process. Loading /vendor/lib/egl/libGLESv1_CM_emulation.so from the current nam
espace instead.
05-06 13:49:58.262  1797  1812 I vndksupport: sphal namespace is not configured for this process. Loading /vendor/lib/egl/libGLESv2_emulation.so from the current namesp
ace instead.
05-06 13:49:58.362  1797  1797 D FirebaseApp: com.google.firebase.iid.FirebaseInstanceId is not linked. Skipping initialization.
05-06 13:49:58.362  1797  1797 D FirebaseApp: com.google.firebase.crash.FirebaseCrash is not linked. Skipping initialization.
05-06 13:49:58.362  1797  1797 D FirebaseApp: com.google.android.gms.measurement.AppMeasurement is not linked. Skipping initialization.
05-06 13:49:58.362  1797  1797 I FirebaseInitProvider: FirebaseApp initialization successful
05-06 13:49:58.502  1797  1814 D OpenGLRenderer: HWUI GL Pipeline
05-06 13:49:58.586  1797  1797 I RenderThread: type=1400 audit(0.0:983): avc: denied { write } for name="local_opengl" dev="tmpfs" ino=11246 scontext=u:r:untrusted_app:
s0:c512,c768 tcontext=u:object_r:socket_device:s0 tclass=sock_file permissive=1
05-06 13:49:58.586  1797  1797 I RenderThread: type=1400 audit(0.0:984): avc: denied { connectto } for path="/dev/socket/local_opengl" scontext=u:r:untrusted_app:s0:c51
2,c768 tcontext=u:r:init:s0 tclass=unix_stream_socket permissive=1
05-06 13:49:58.588  1797  1814 D         : HostConnection::get() New Host Connection established 0xe0824190, pid 1797, tid 1814
05-06 13:49:58.598  1797  1814 D         : HostComposition ext ANDROID_EMU_host_composition_v1 ANDROID_EMU_host_composition_v2 ANDROID_EMU_async_unmap_buffer ANDROID_EM
U_sync_buffer_data GL_OES_EGL_image_external_essl3 GL_OES_vertex_array_object GL_KHR_texture_compression_astc_ldr ANDROID_EMU_host_side_tracing ANDROID_EMU_async_frame_
commands ANDROID_EMU_gles_max_version_3_1
05-06 13:49:58.598  1797  1814 W         : Process pipe failed
05-06 13:49:58.714  1797  1814 I OpenGLRenderer: Initialized EGL, version 1.4
05-06 13:49:58.715  1797  1814 D OpenGLRenderer: Swap behavior 1
05-06 13:49:58.744  1797  1814 W OpenGLRenderer: Failed to choose config with EGL_SWAP_BEHAVIOR_PRESERVED, retrying without...
05-06 13:49:58.744  1797  1814 D OpenGLRenderer: Swap behavior 0
05-06 13:49:58.779  1797  1814 D EGL_emulation: eglCreateContext: 0xe08050c0: maj 3 min 1 rcv 4
05-06 13:49:59.209  1797  1814 I vndksupport: sphal namespace is not configured for this process. Loading /vendor/lib/hw/gralloc.vbox86.so from the current namespace in
stead.
05-06 13:49:59.209  1797  1814 D         : createUnique: call
05-06 13:49:59.210  1797  1814 D         : HostConnection::get() New Host Connection established 0xe0824370, pid 1797, tid 1814
05-06 13:49:59.216  1797  1814 D         : HostComposition ext ANDROID_EMU_host_composition_v1 ANDROID_EMU_host_composition_v2 ANDROID_EMU_async_unmap_buffer ANDROID_EM
U_sync_buffer_data GL_OES_EGL_image_external_essl3 GL_OES_vertex_array_object GL_KHR_texture_compression_astc_ldr ANDROID_EMU_host_side_tracing ANDROID_EMU_async_frame_
commands ANDROID_EMU_gles_max_version_3_1
```

Ta thu được flag

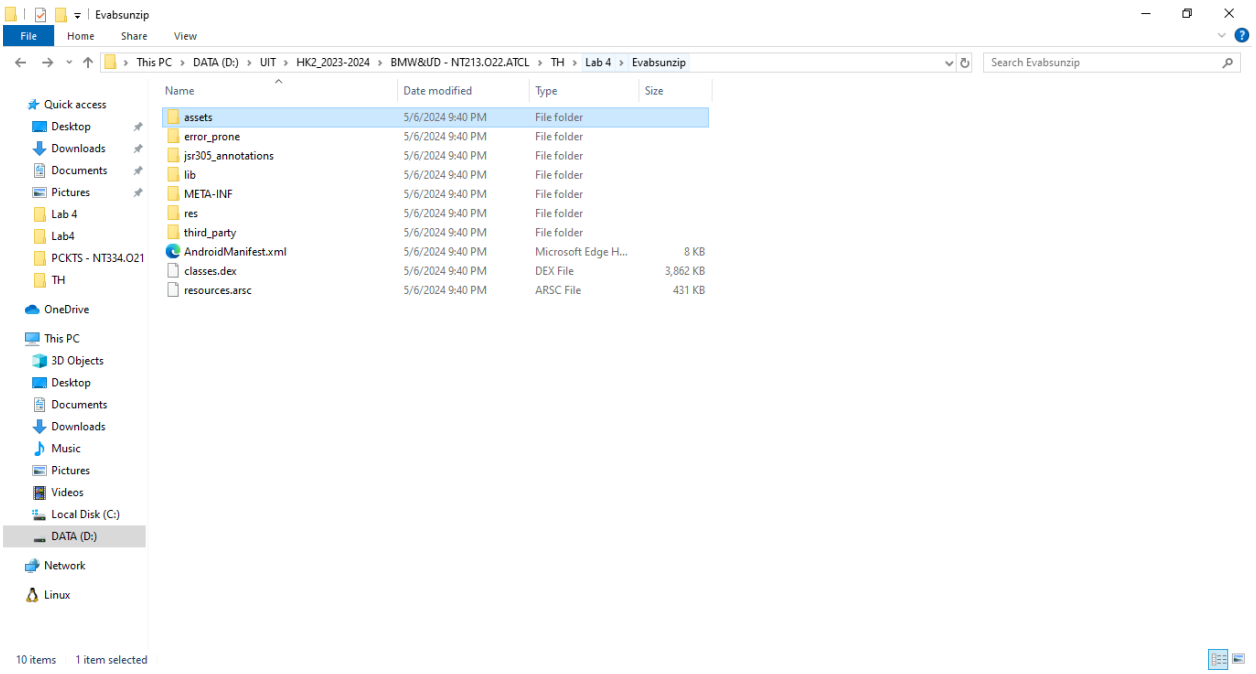


Flag: EVABS{logging_info_never_safel}

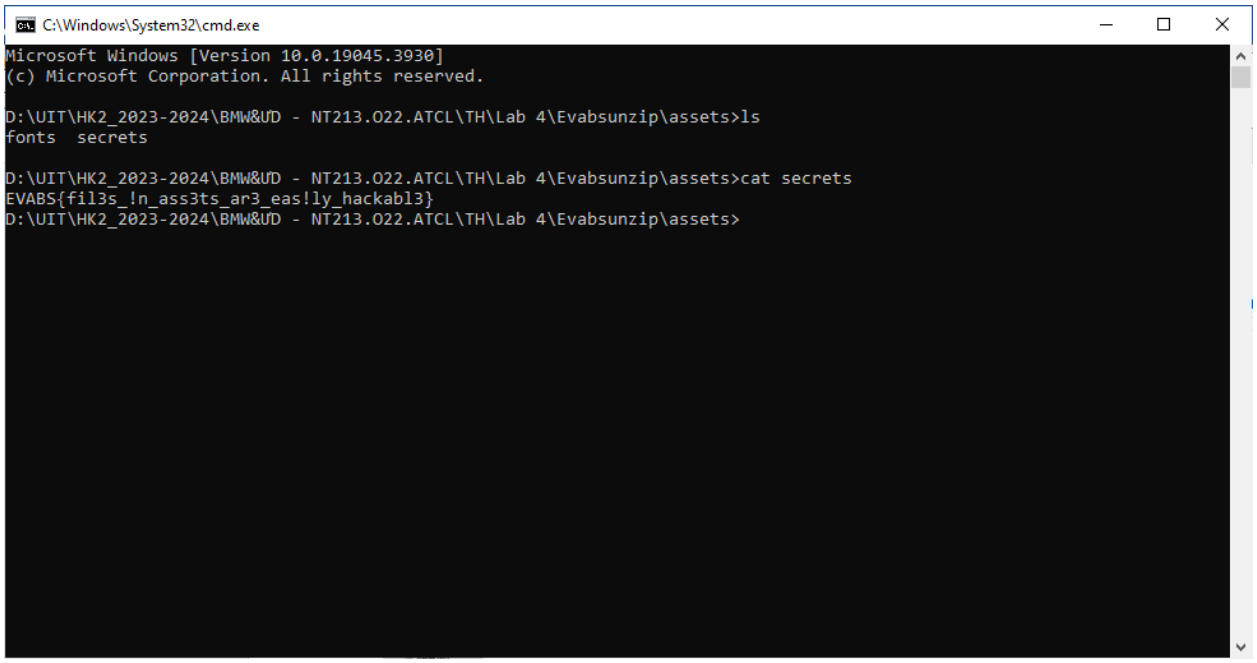
Flag2:



Ta thực hiện giải nén file apk



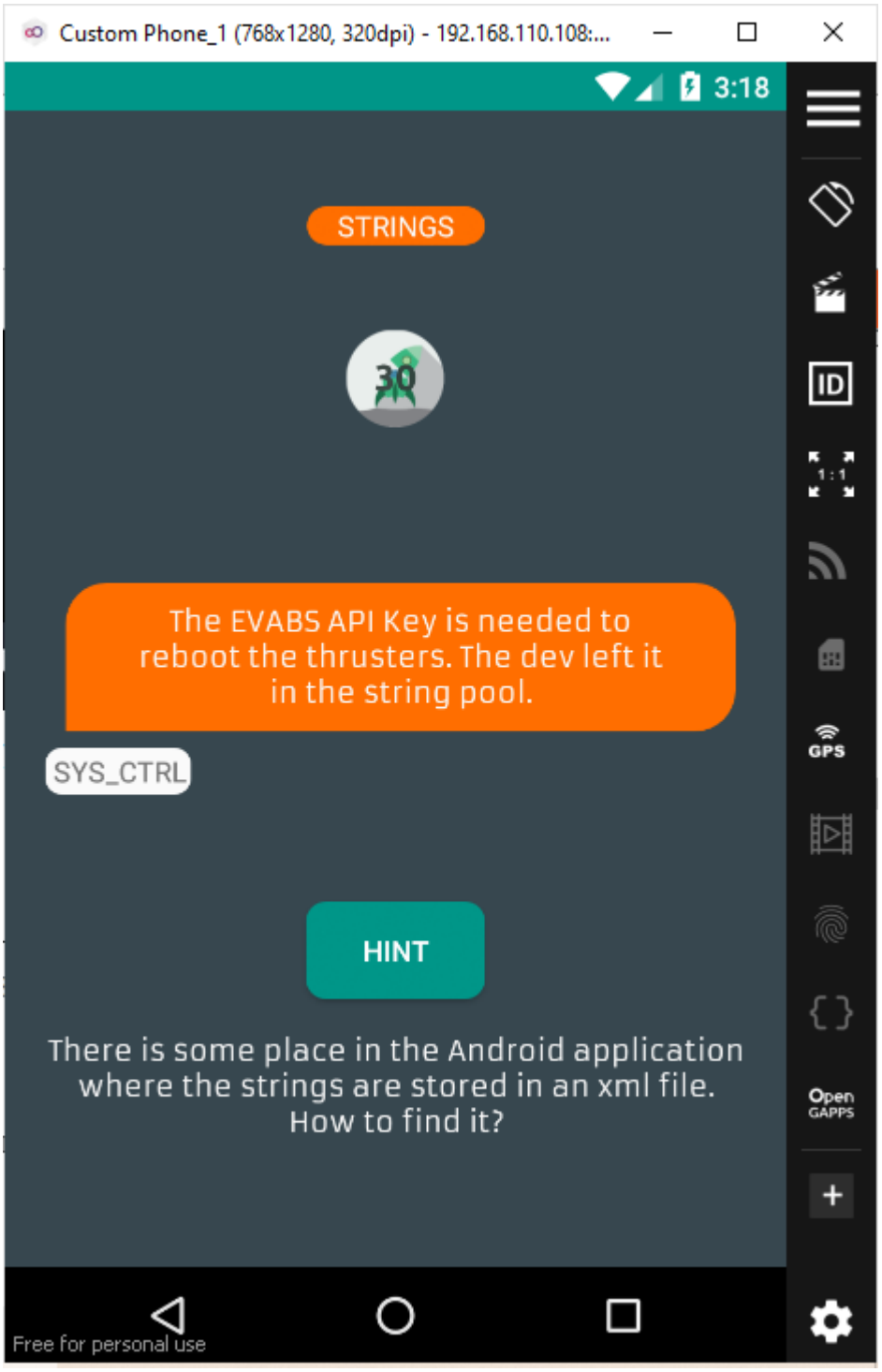
Tiến hành kiểm tra trong assets



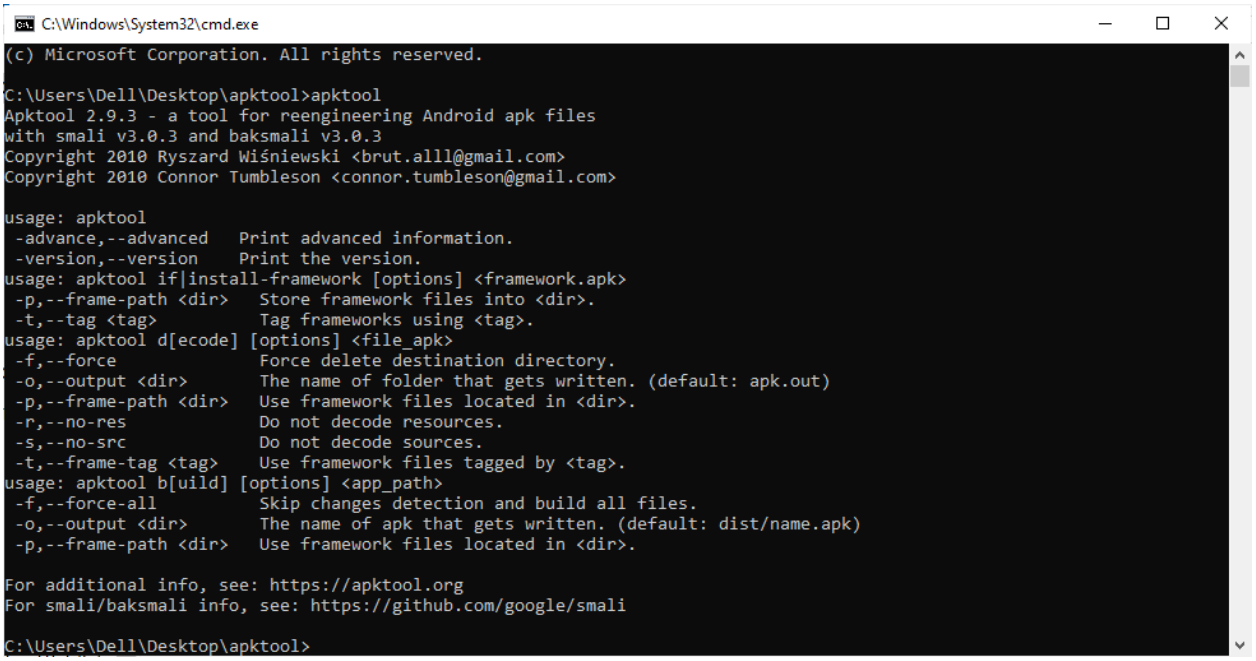
Ta thu được flag

Flag: EVABS{fil3s_!n_ass3ts_ar3_eas!ly_hackabl3}

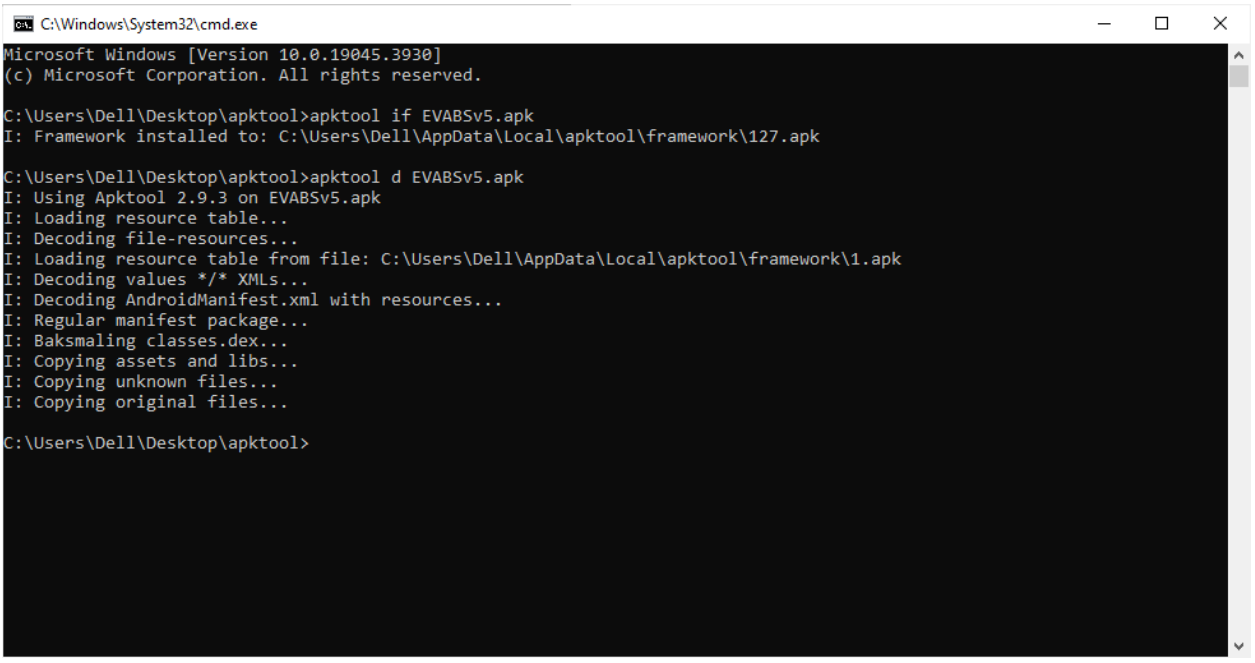
Flag3:



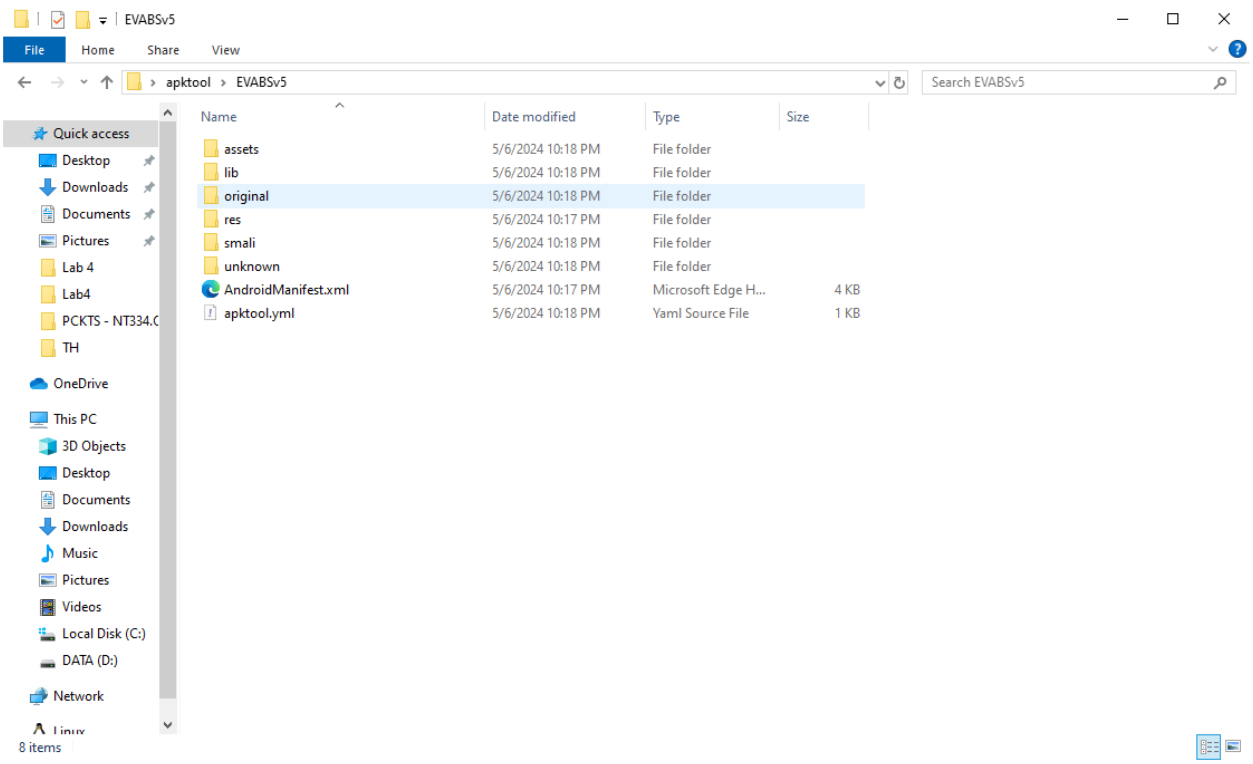
Tiến hành cài đặt apktool



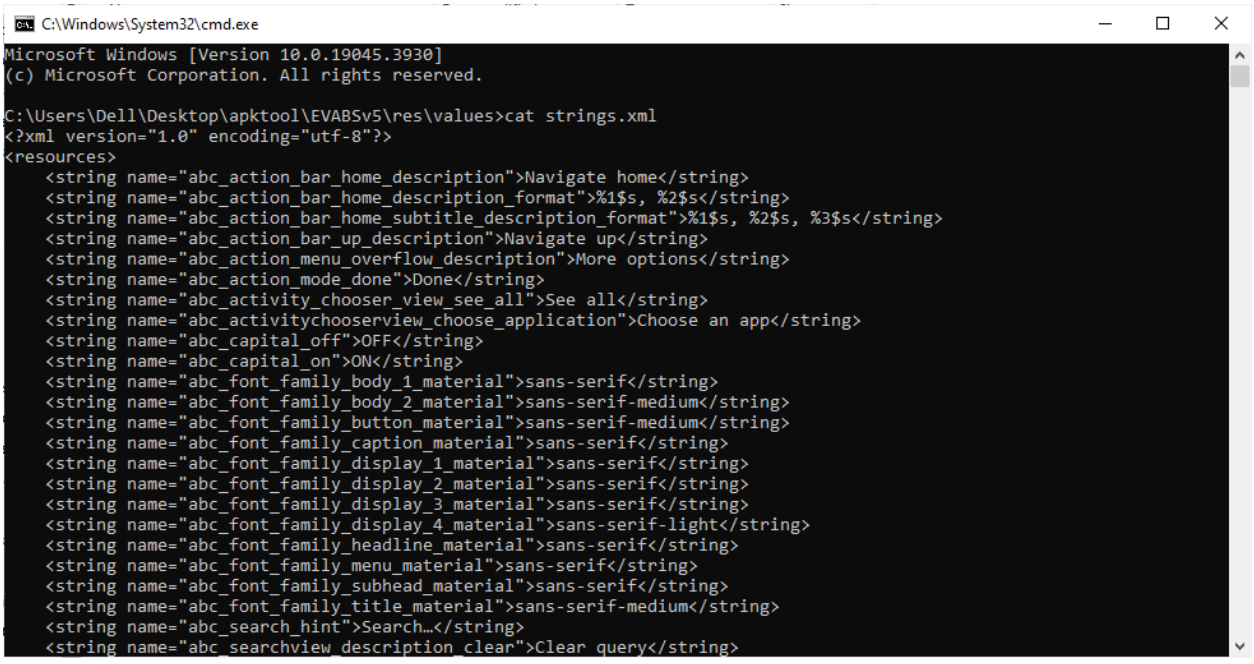
Thực hiện decompile file

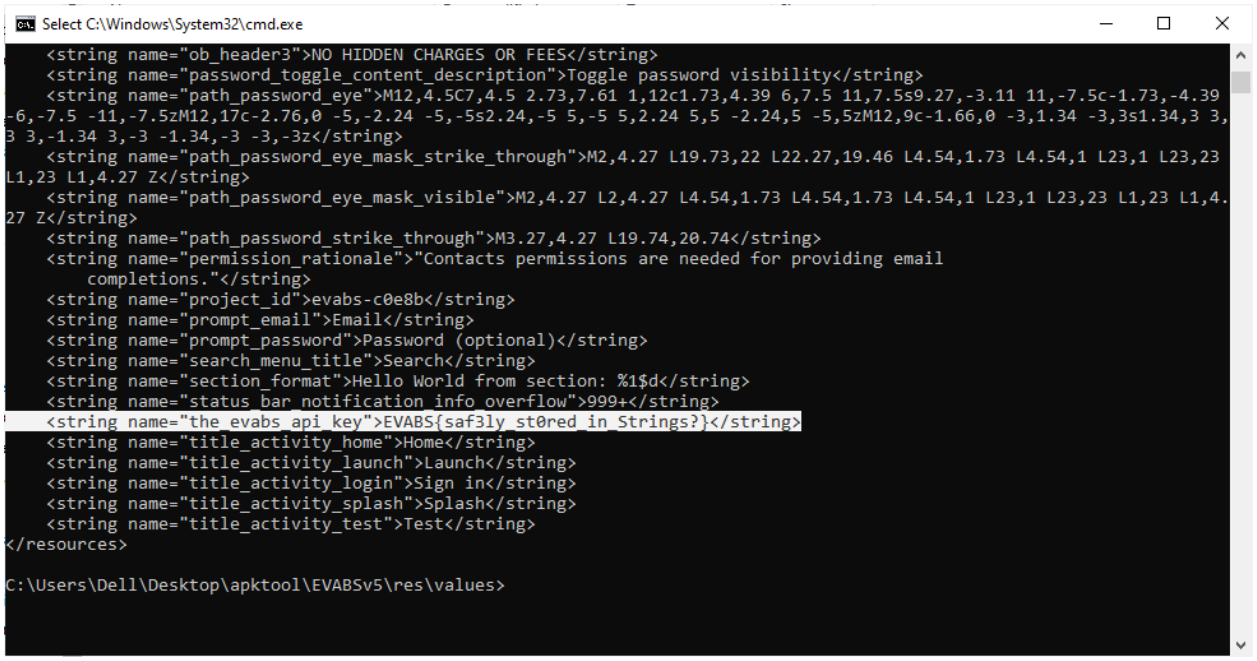


Ta thu được folder



Vào thư mục /res/values và kiểm tra các file strings

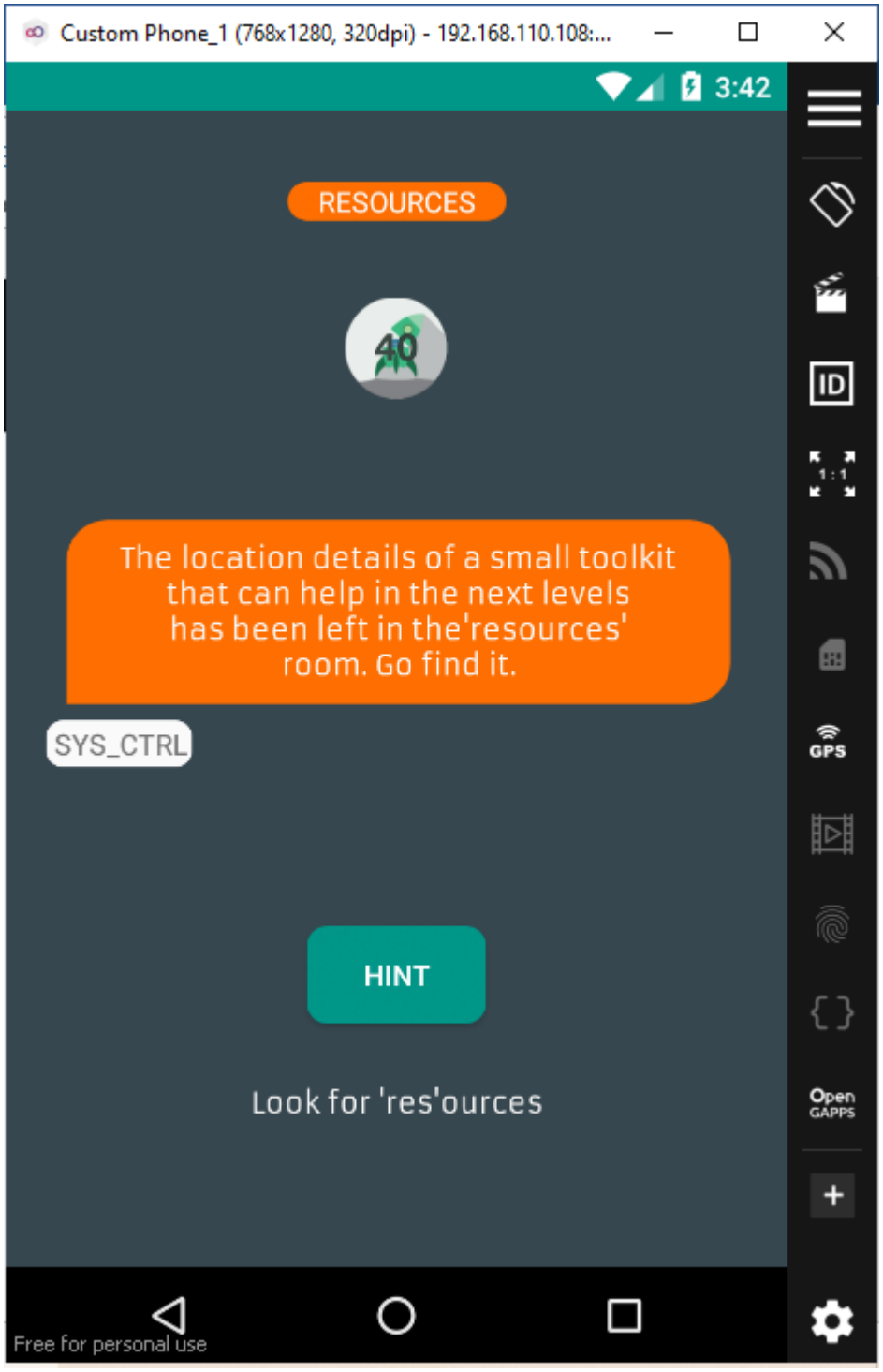




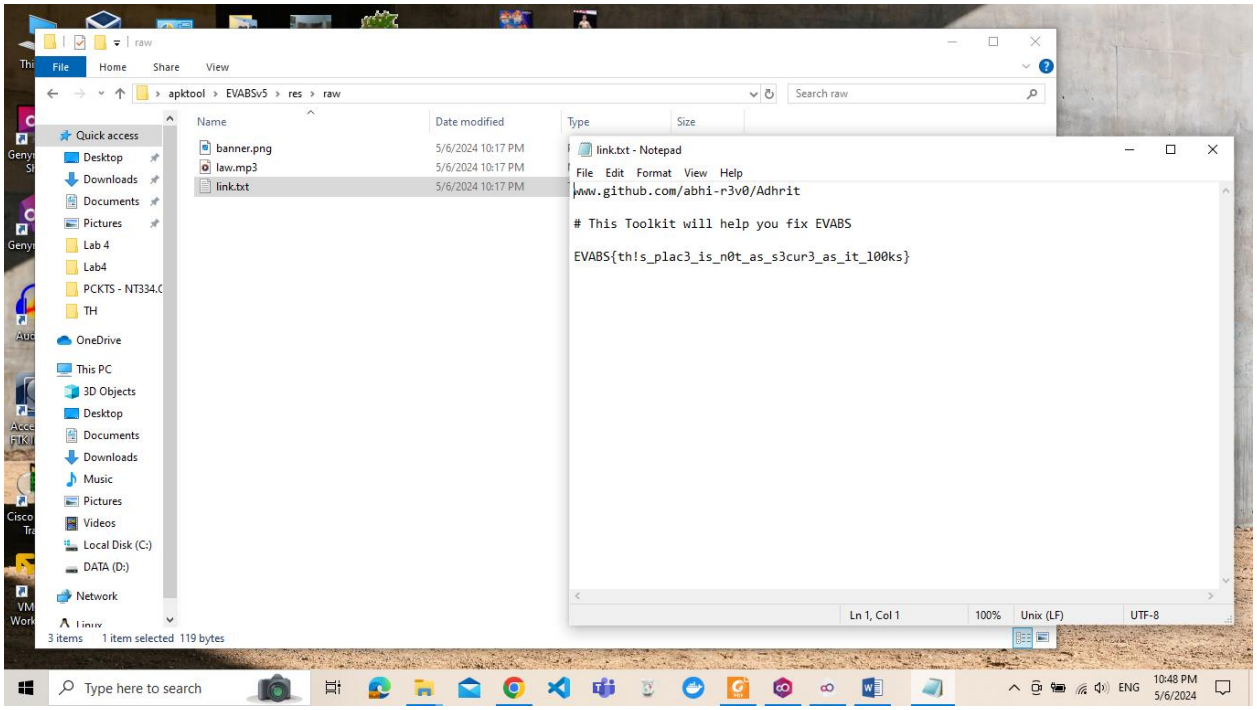
Ta thu được flag

Flag: EVABS{saf3ly_st0red_in_Strings?}

Flag4



Thông qua quá trình tìm kiếm trong /res, ta thu được flag

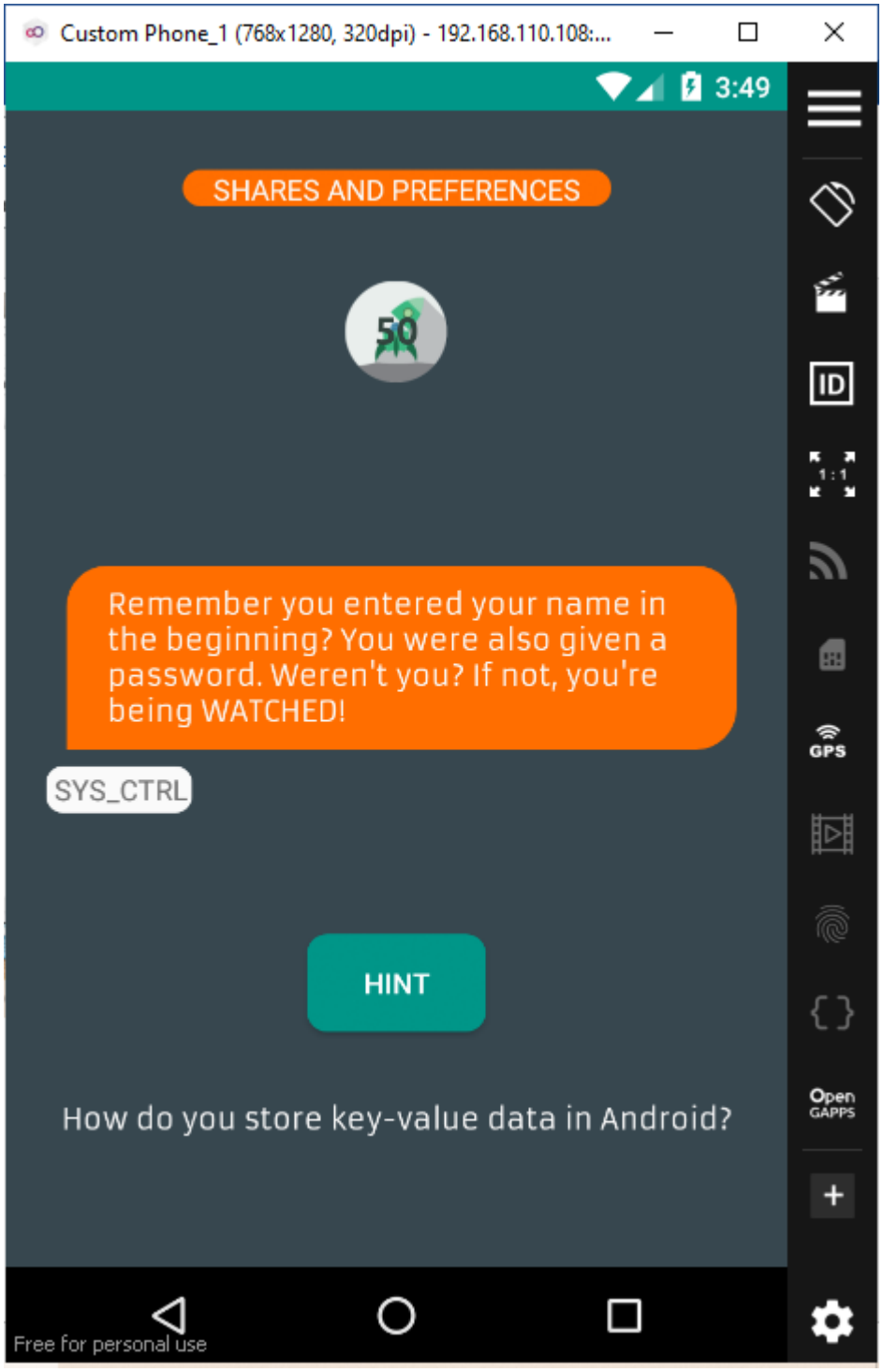


Flag: EVABS{th!s_plac3_is_n0t_as_s3cur3_as_it_l00ks}

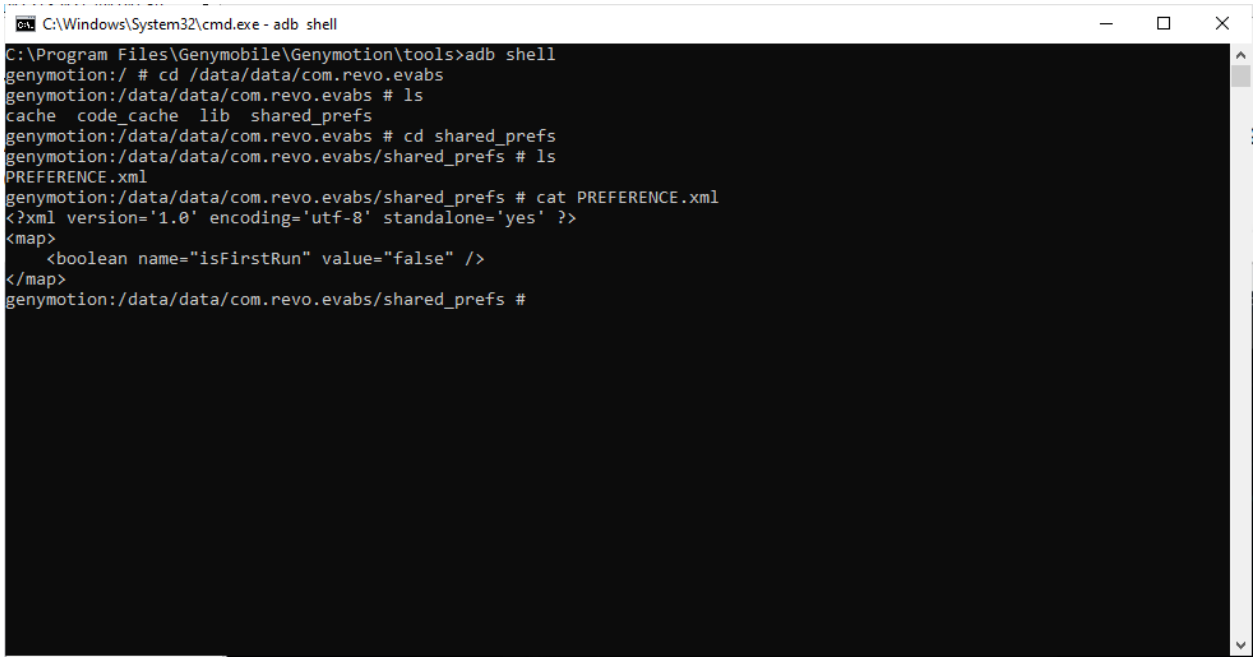
Ngoài ra ta còn thu được thêm 1 flag gợi ý

Flag: EVABS{sOme_t3xt_here}

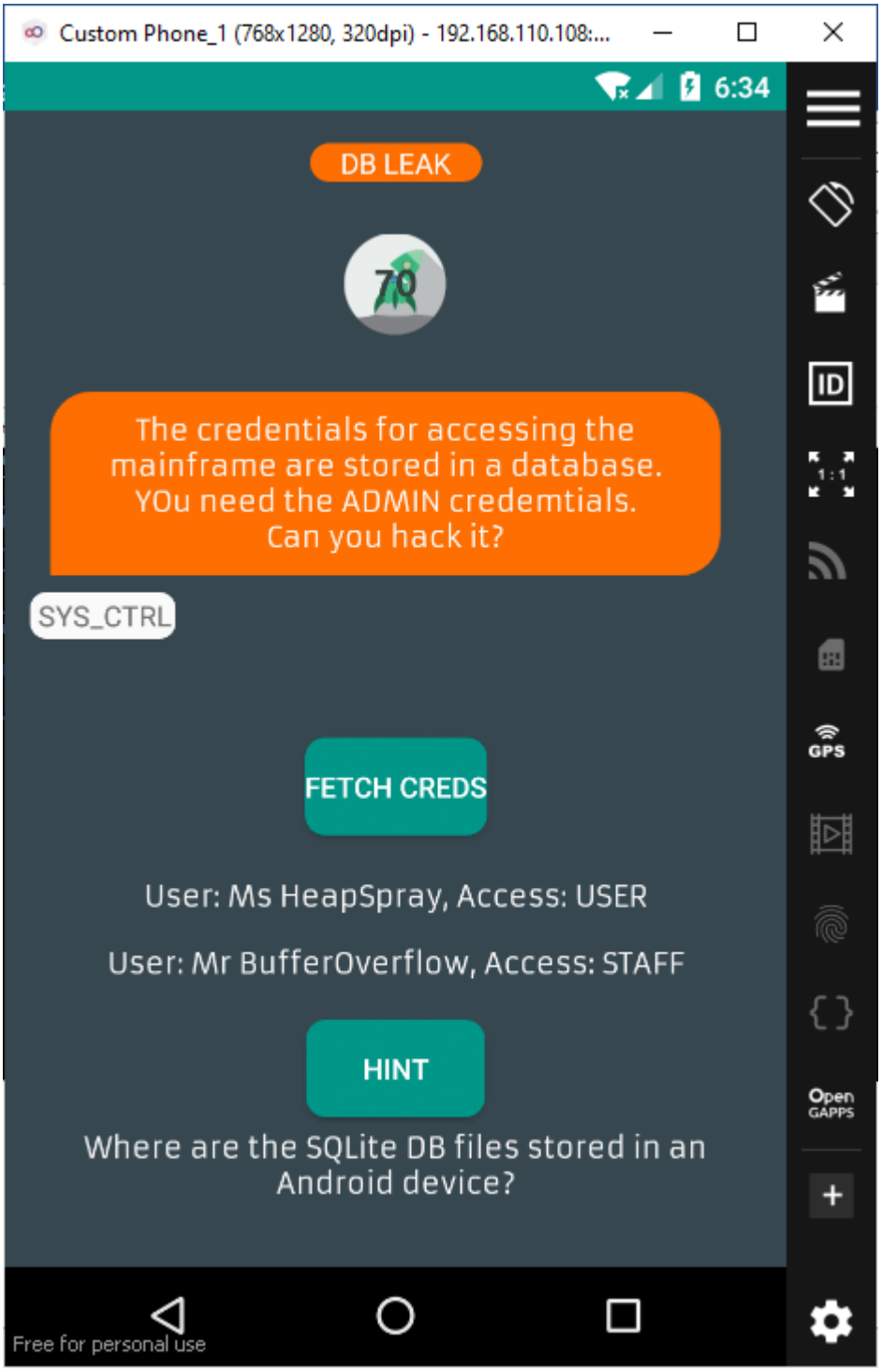
Flag5



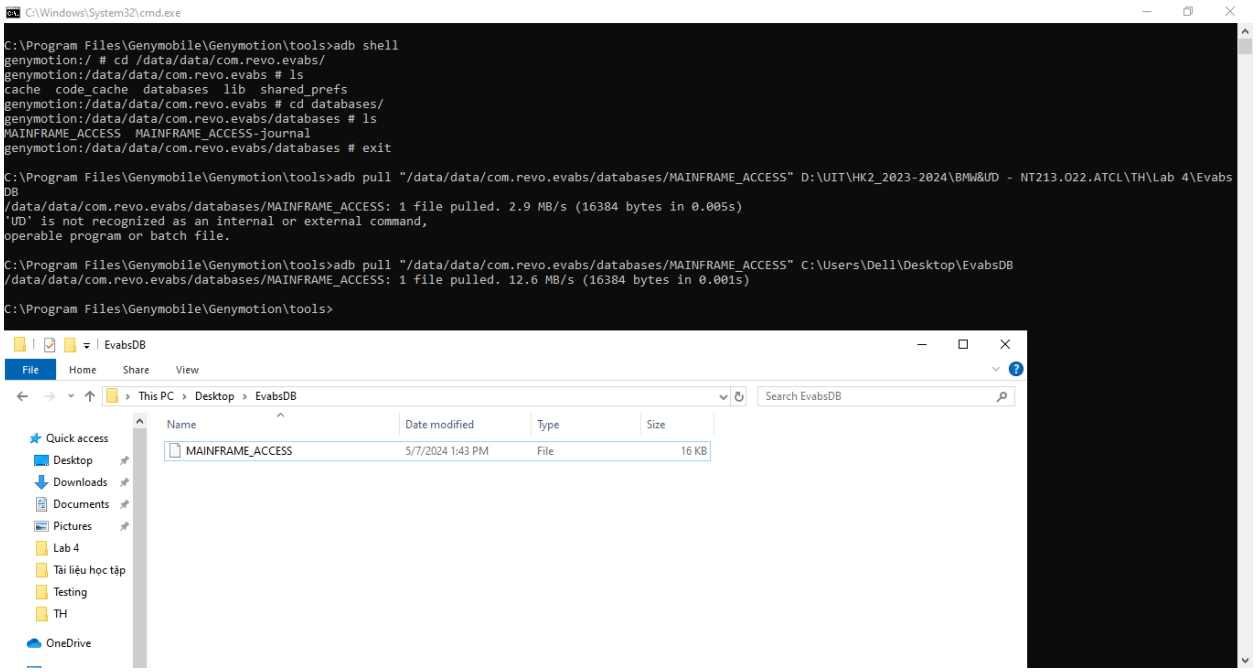
Theo gợi ý, ta vào folder shared_prefs


C:\Windows\System32\cmd.exe - adb shell
C:\Program Files\Genymobile\Genymotion\tools>adb shell
genymotion:/ # cd /data/data/com.revo.evabs
genymotion:/data/data/com.revo.evabs # ls
cache code_cache lib shared_prefs
genymotion:/data/data/com.revo.evabs # cd shared_prefs
genymotion:/data/data/com.revo.evabs/shared_prefs # ls
PREFERENCE.xml
genymotion:/data/data/com.revo.evabs/shared_prefs # cat PREFERENCE.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<boolean name="isFirstRun" value="false" />
</map>
genymotion:/data/data/com.revo.evabs/shared_prefs #

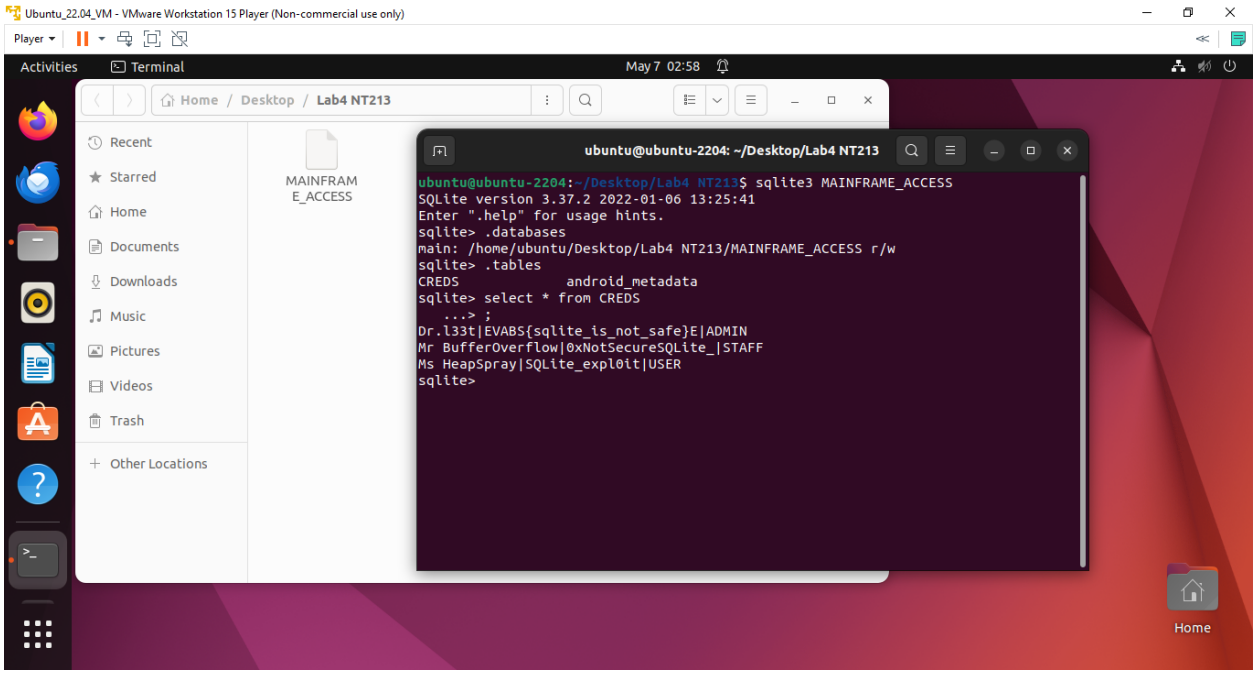
Flag6



Tiến hành pull về máy



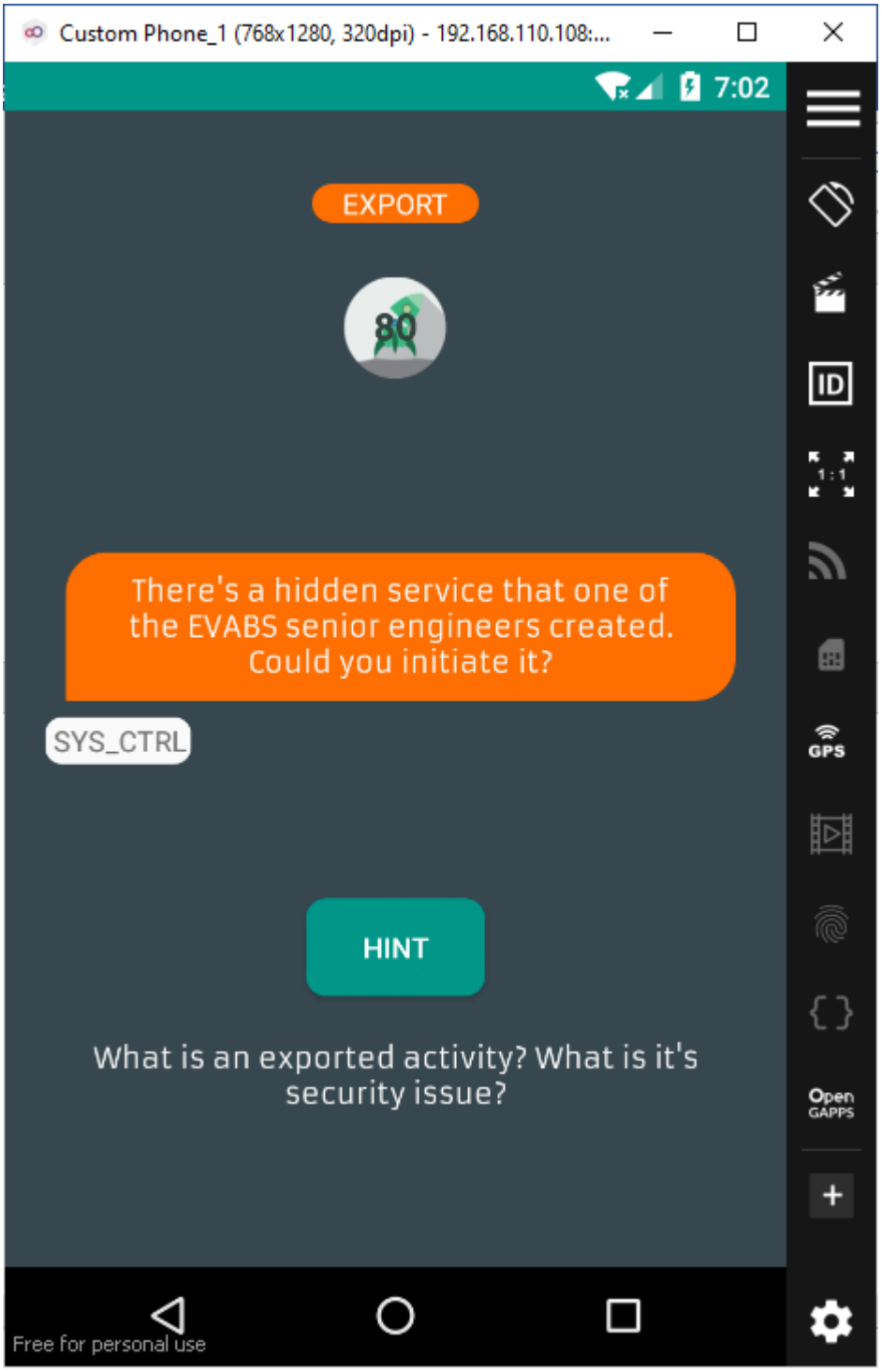
Sử dụng sqlite3 để kiểm tra file



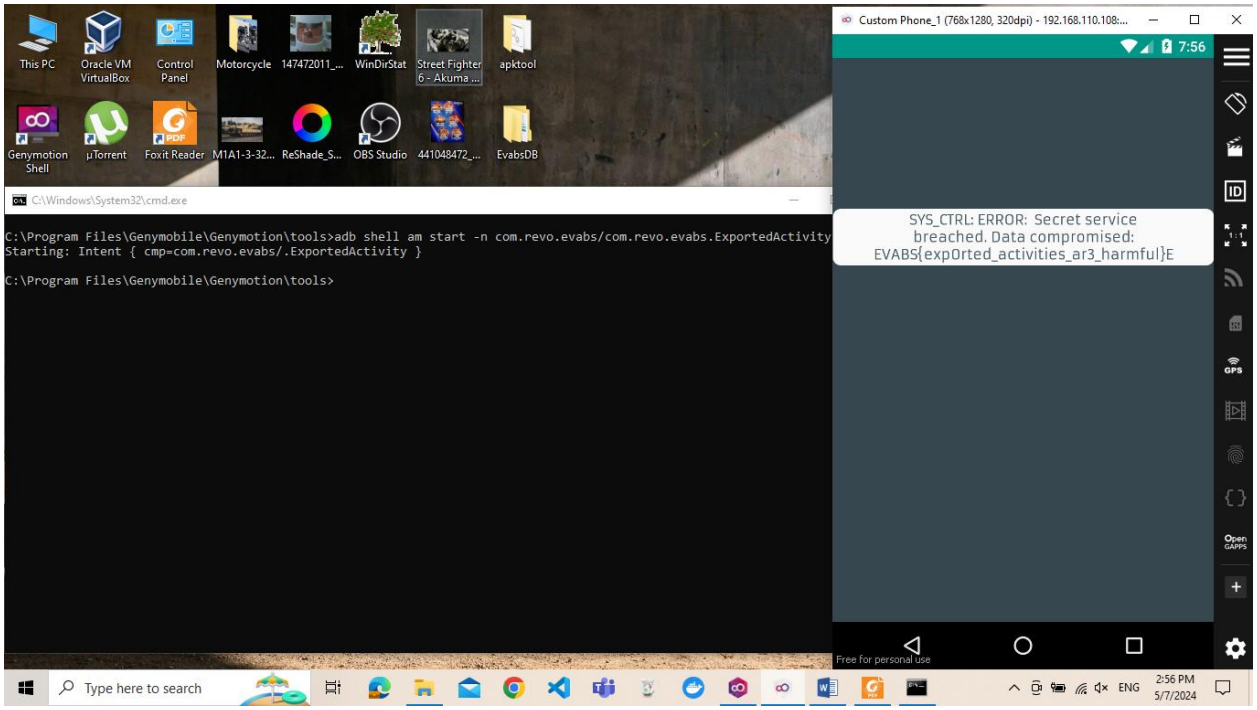
Ta thu được flag

Flag: EVABS{sqlite_is_not_safe}

Flag7


Custom Phone_1 (768x1280, 320dpi) - 192.168.110.108:...
7:02
EXPORT
There's a hidden service that one of the EVABS senior engineers created. Could you initiate it?
SYS_CTRL
HINT
What is an exported activity? What is it's security issue?
Free for personal use

Từ gợi ý



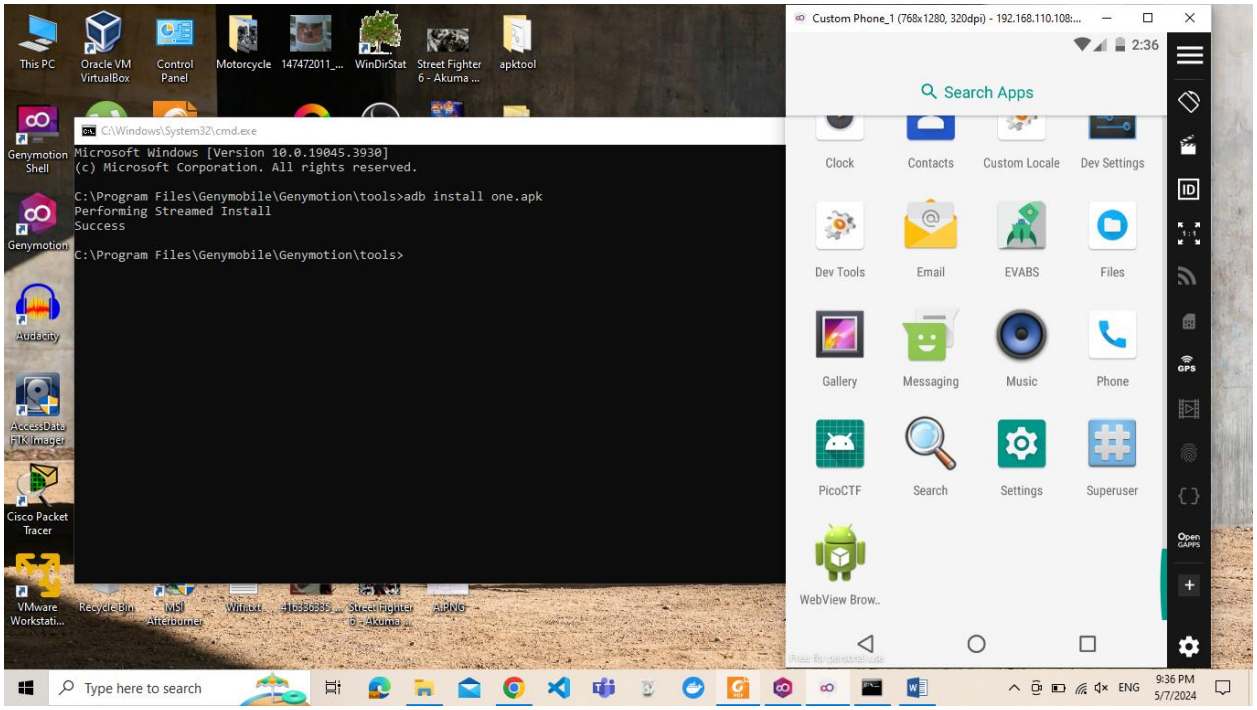
Ta thu được flag

Flag: EVABS{exported_activities_ar3_harmful}

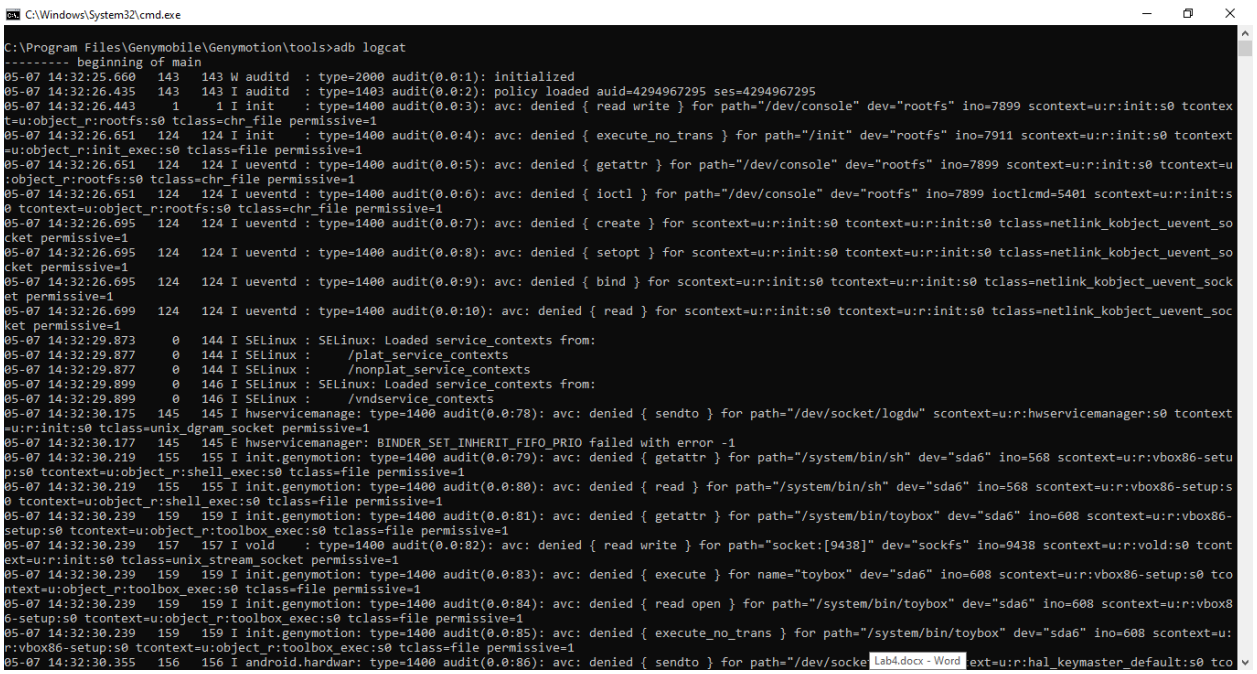
Flag8

picoCTF

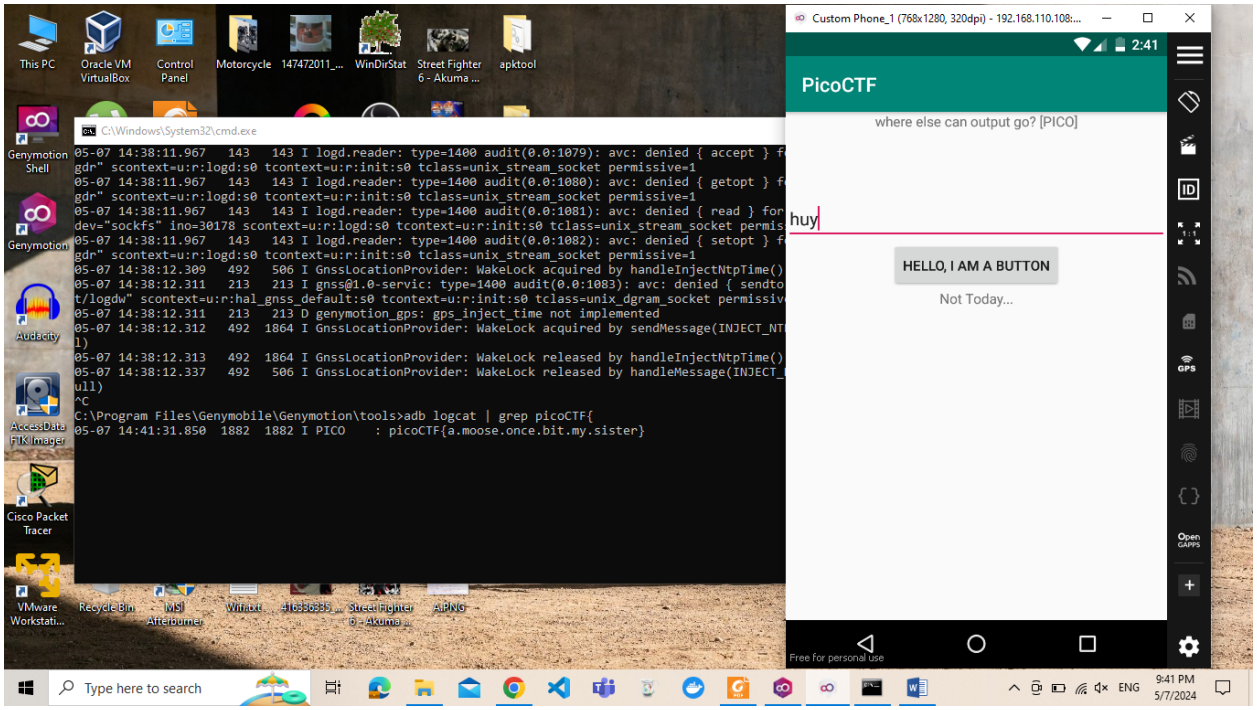
Flag1



Kiểm tra log của chương trình

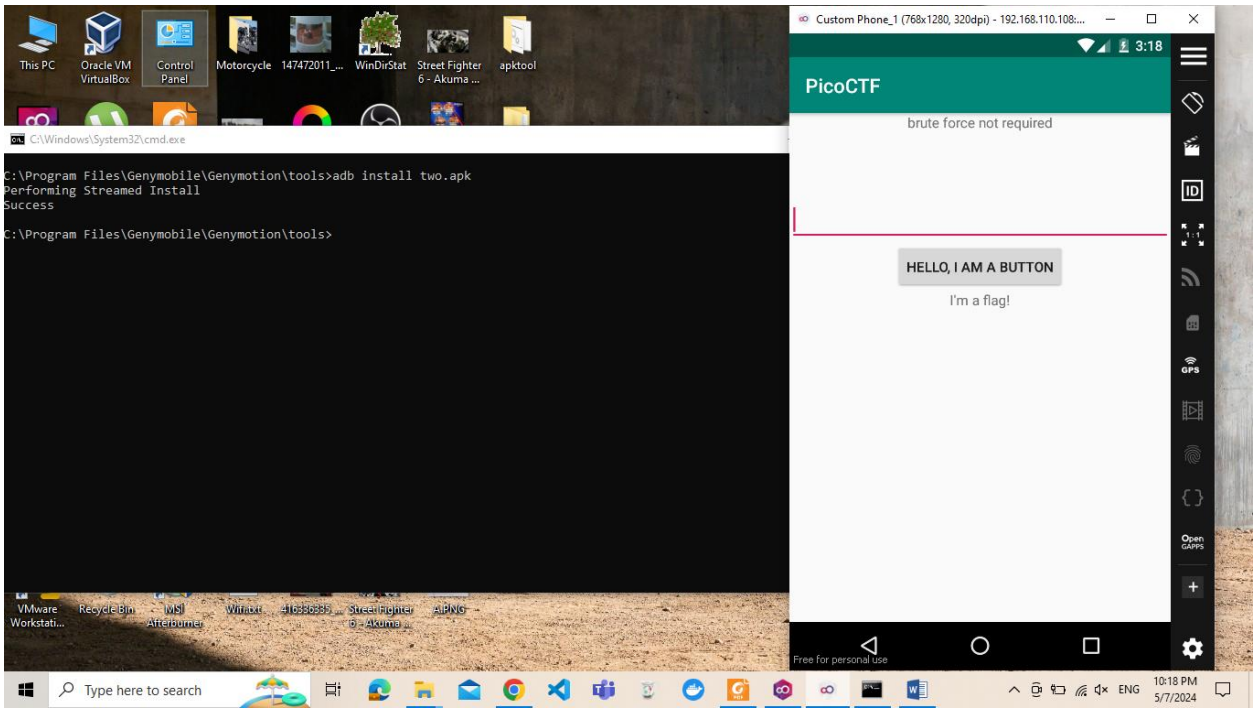


Tiến hành tìm flag

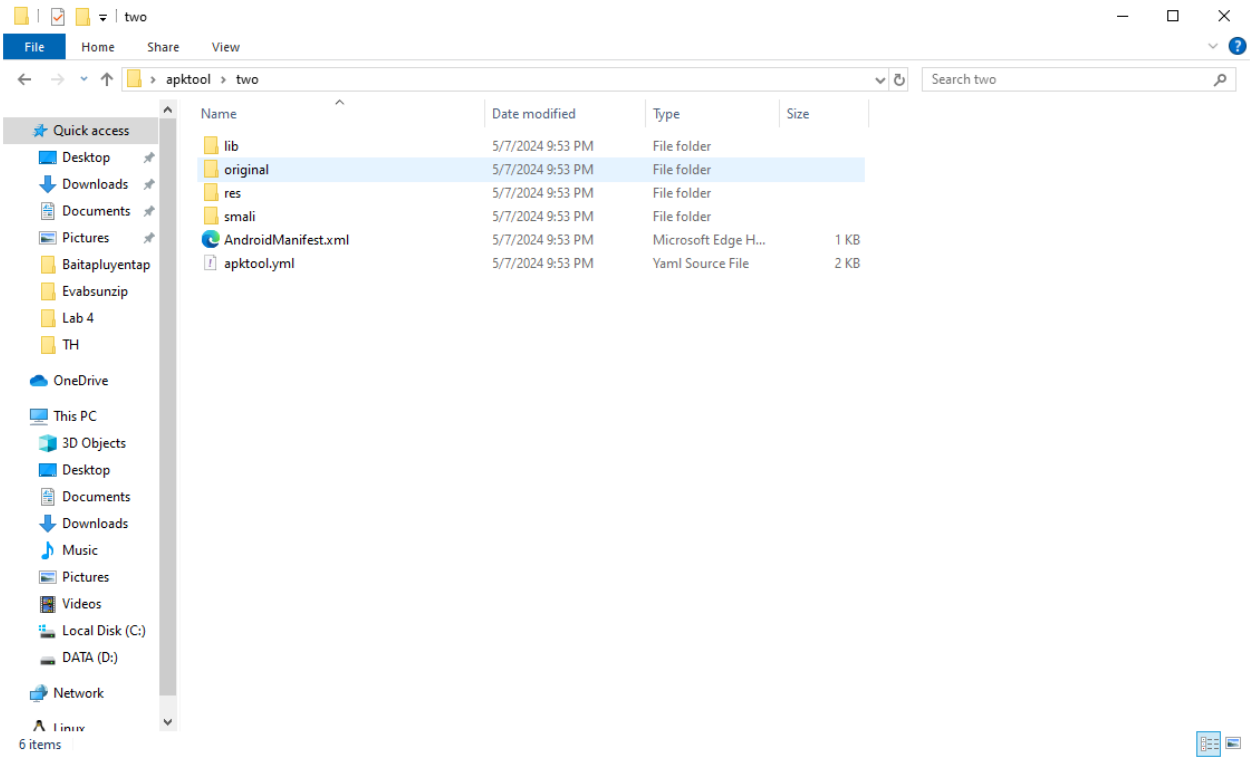


Flag: picoCTF{a.moose.once.bit.my.sister}

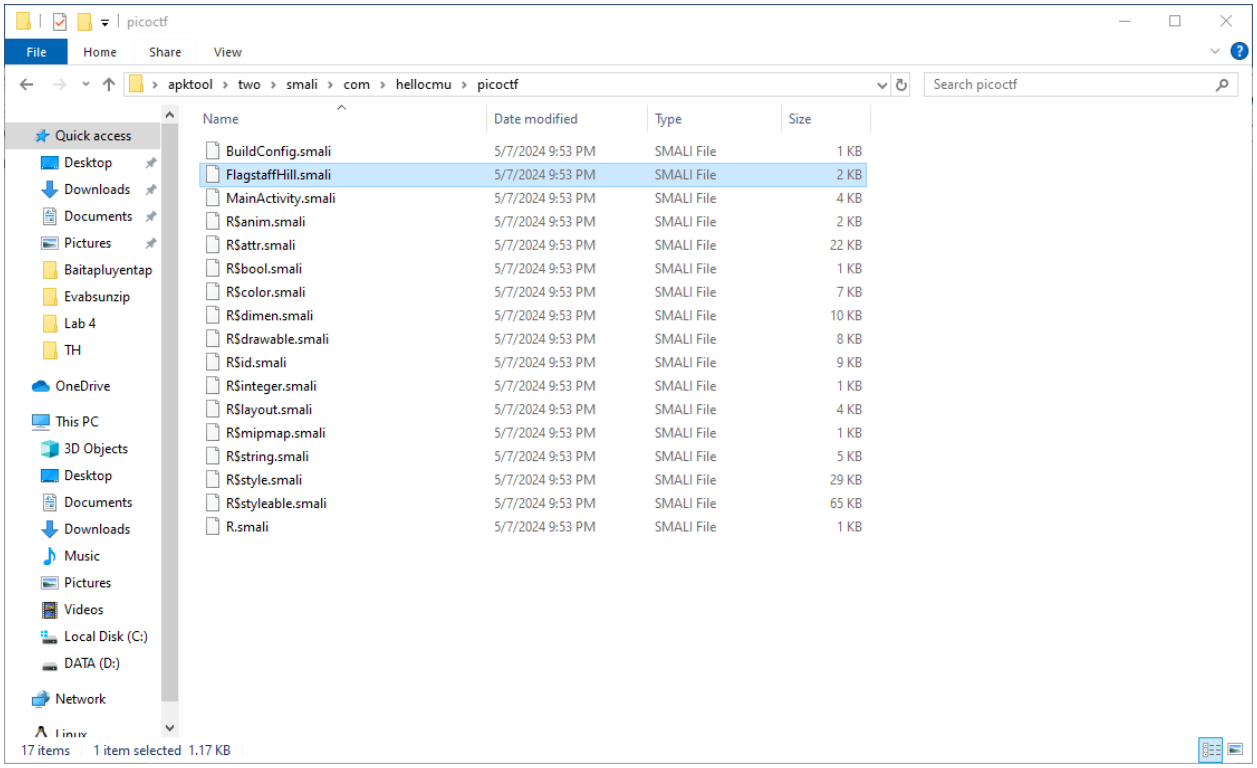
Flag2



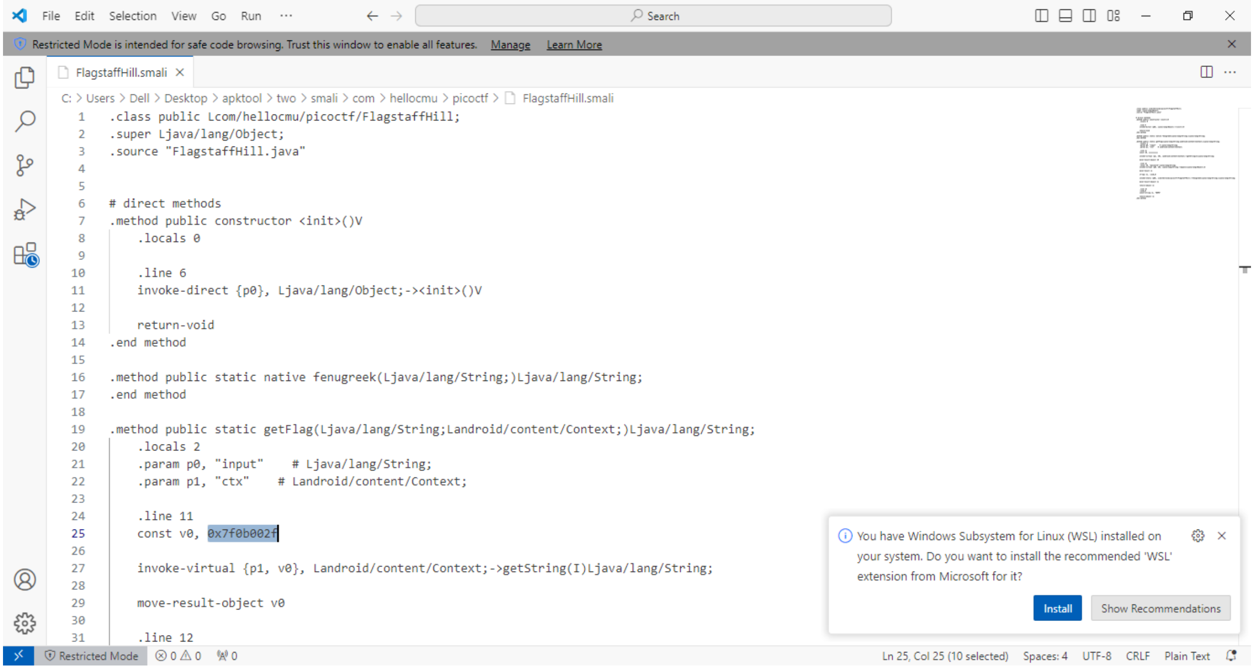
Tiến hành decompile file



Ta kiểm tra thử FlagstaffHill.smali

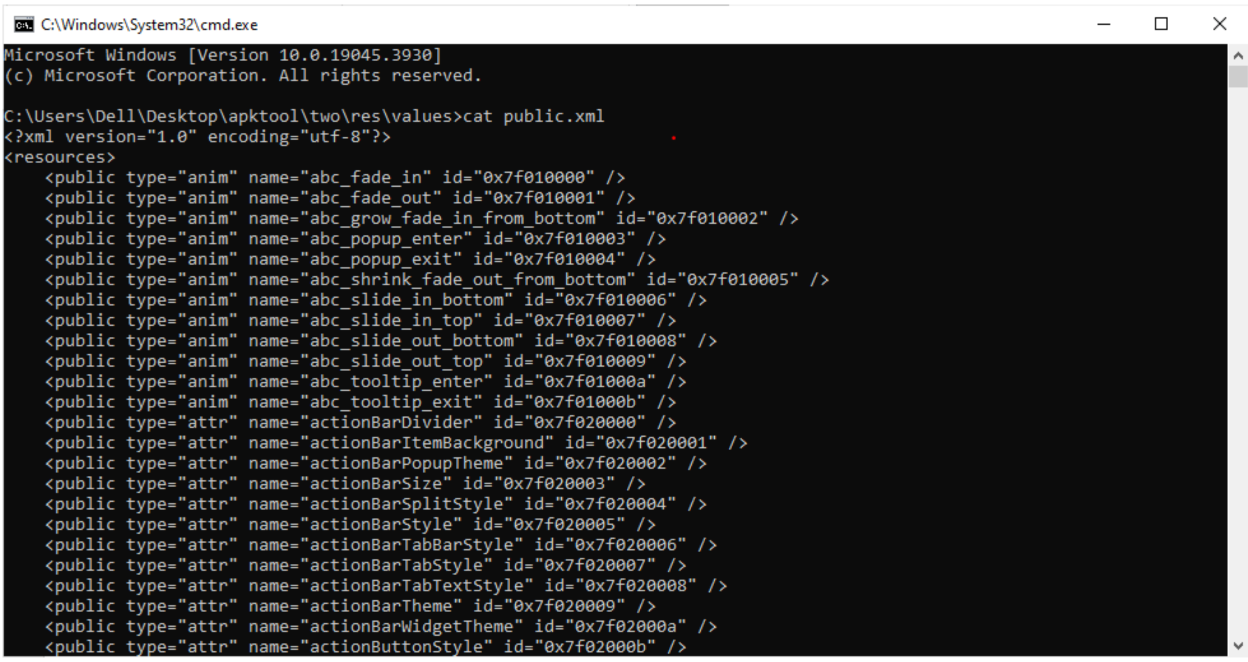


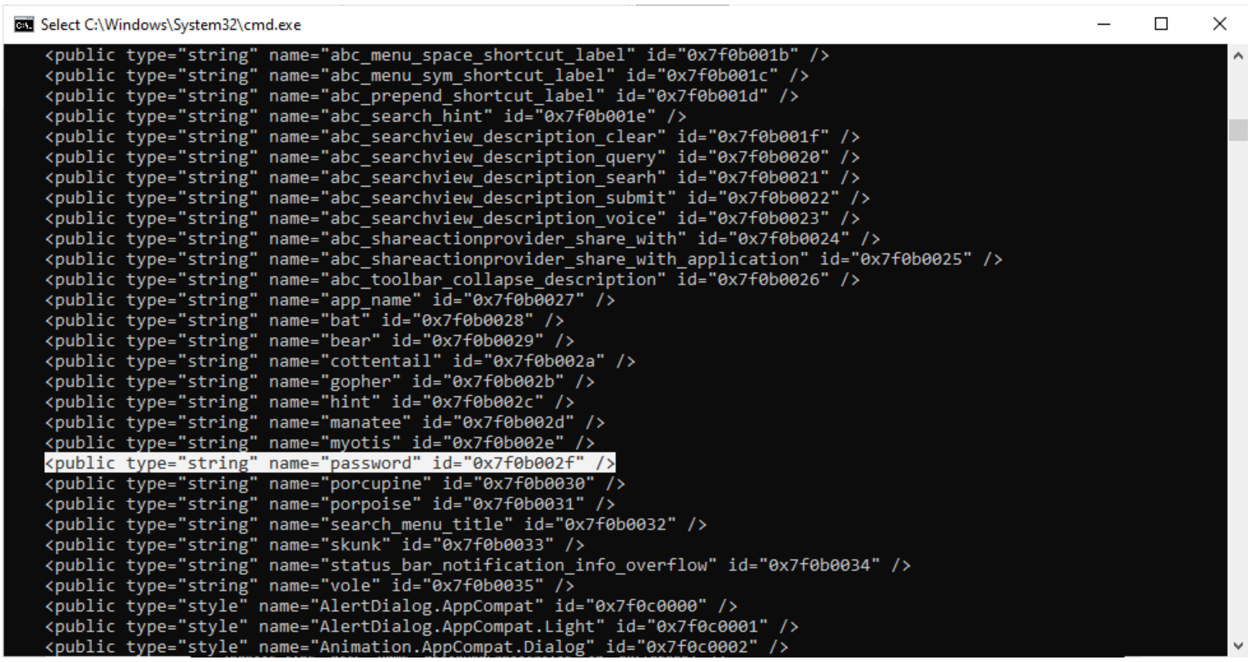
Ta thấy được thông tin



Giá trị: 0x7f0b002f

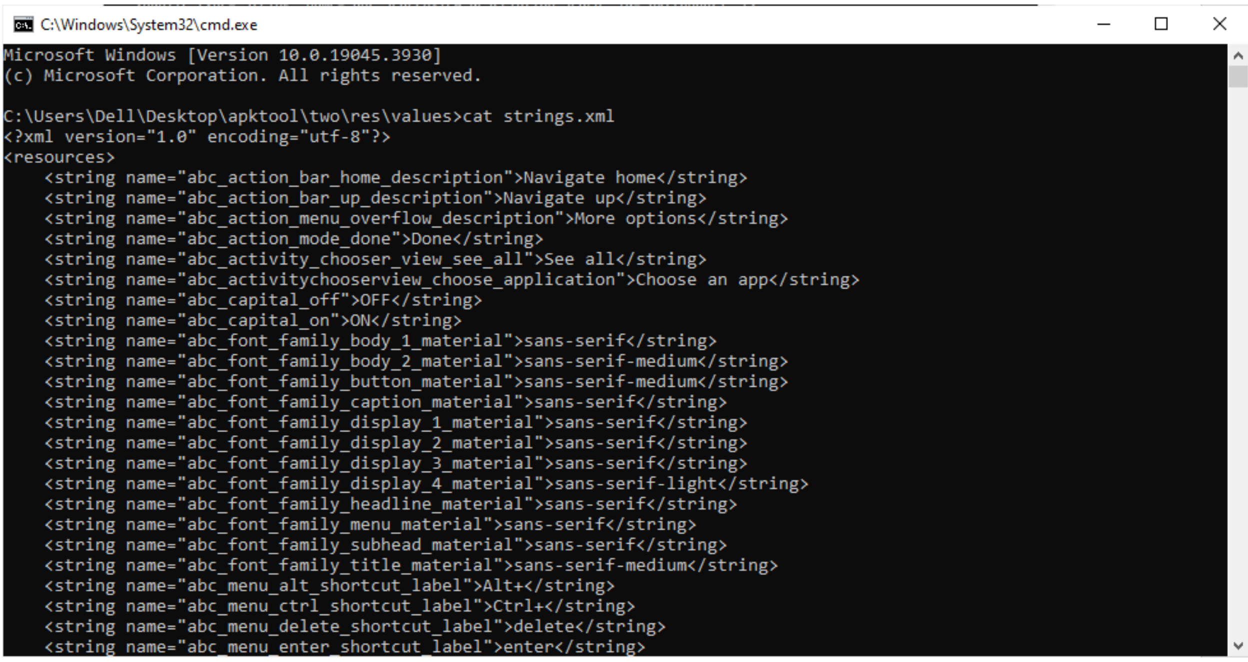
Tiến hành tìm kiếm giá trị ở file chứa

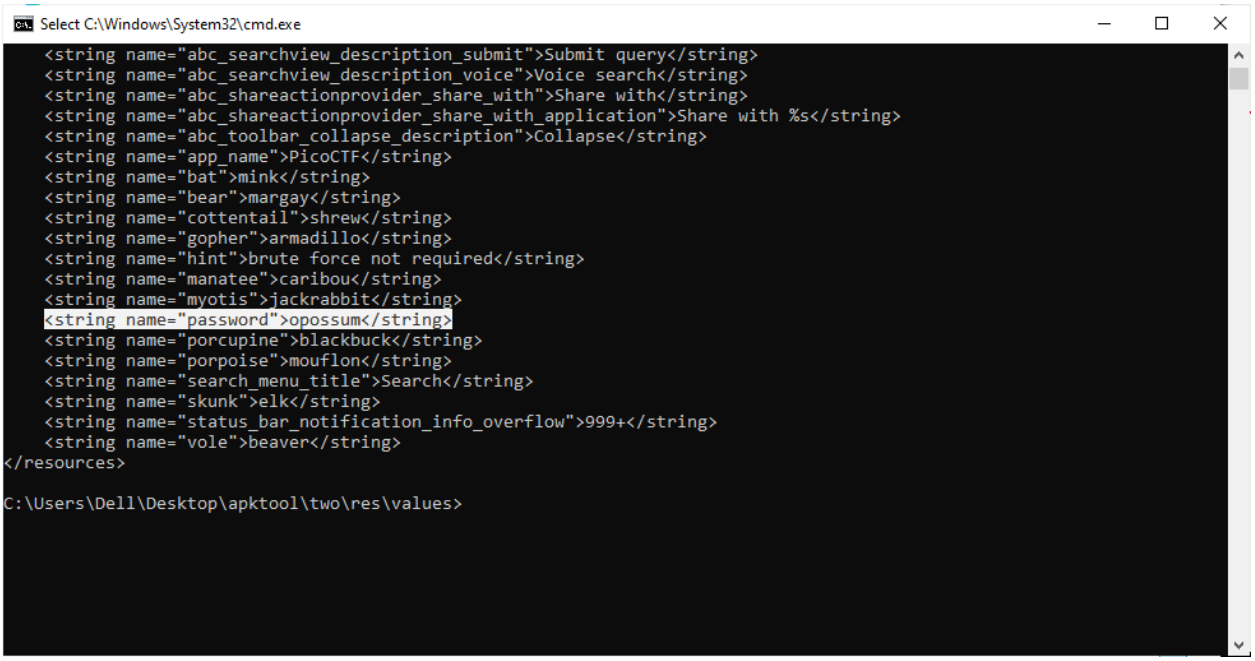




Ta thấy giá trị liên quan với thông tin name password

Đây là dữ liệu string, do đó ta tiếp tục tìm kiếm ở file strings.xml

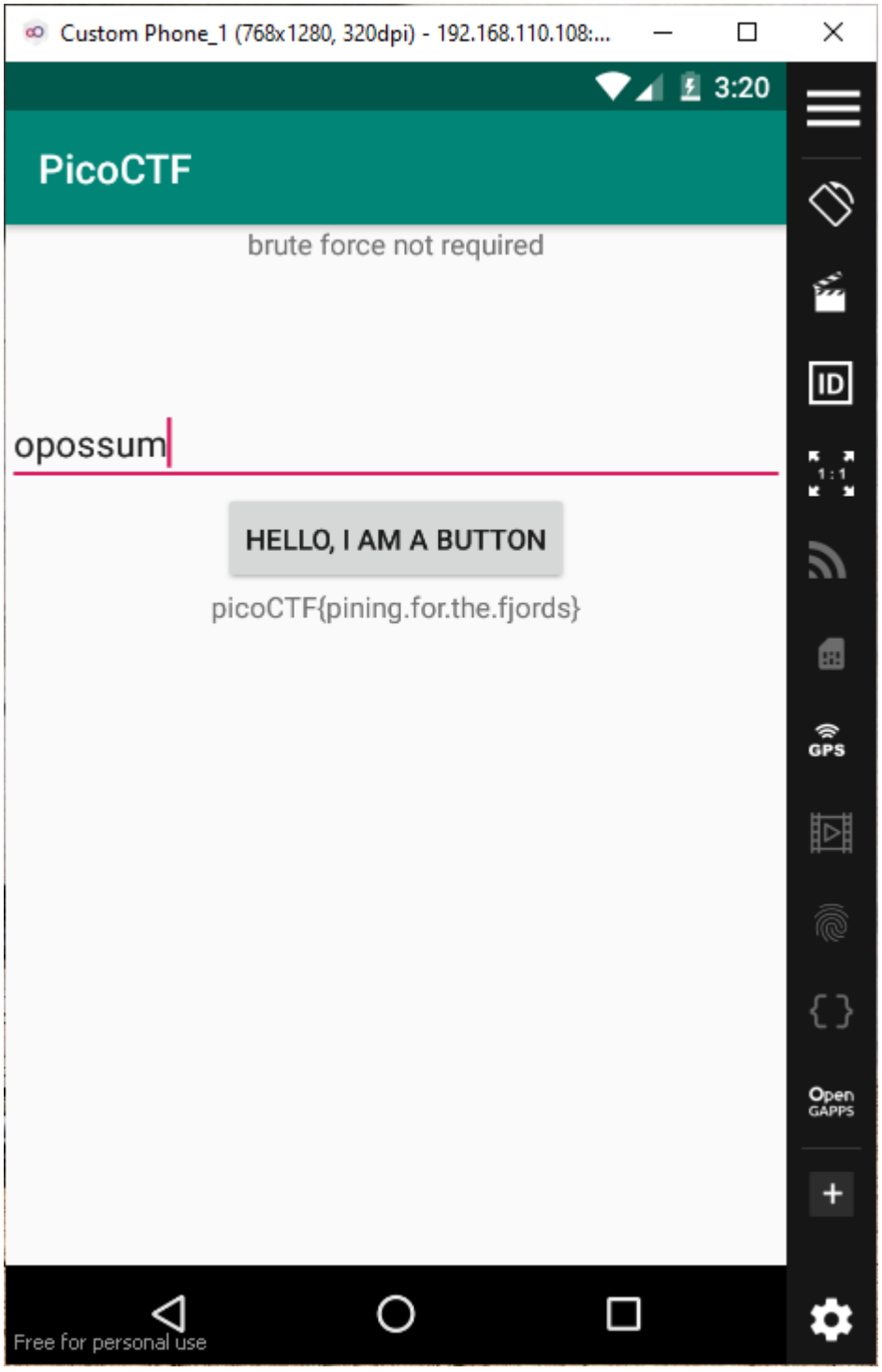




Ta thu được password

Password: opossum

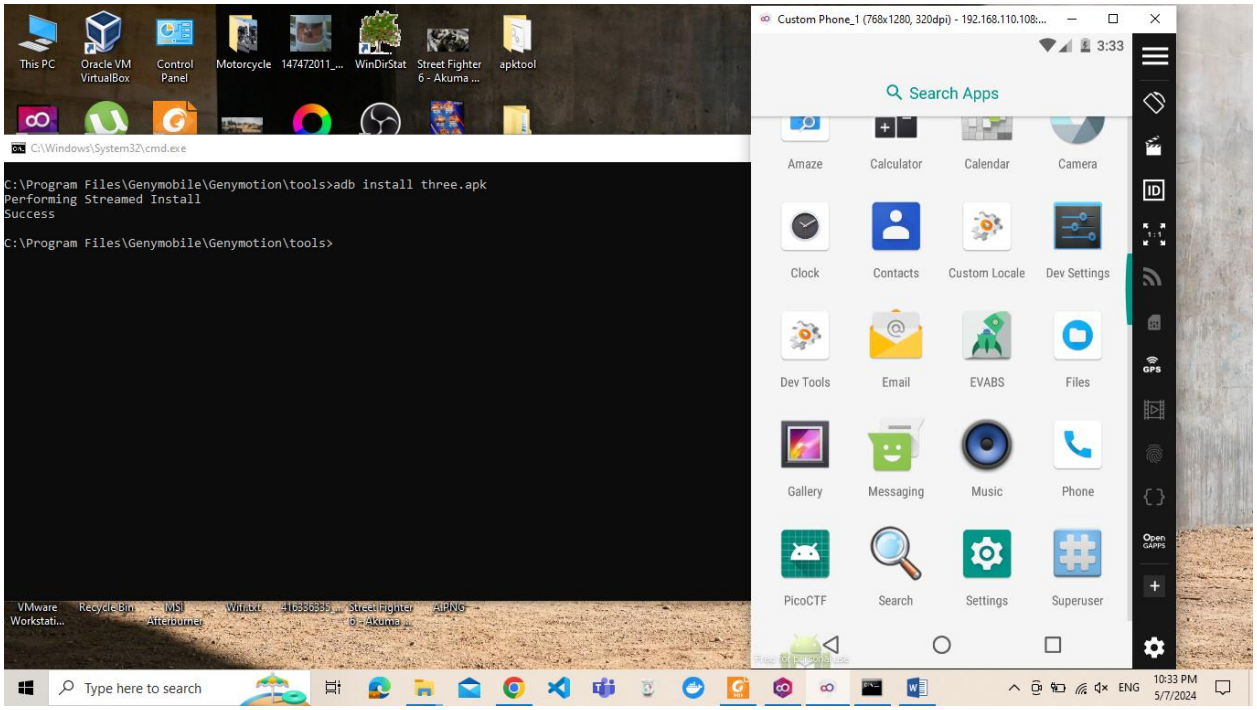
Nhập thử password



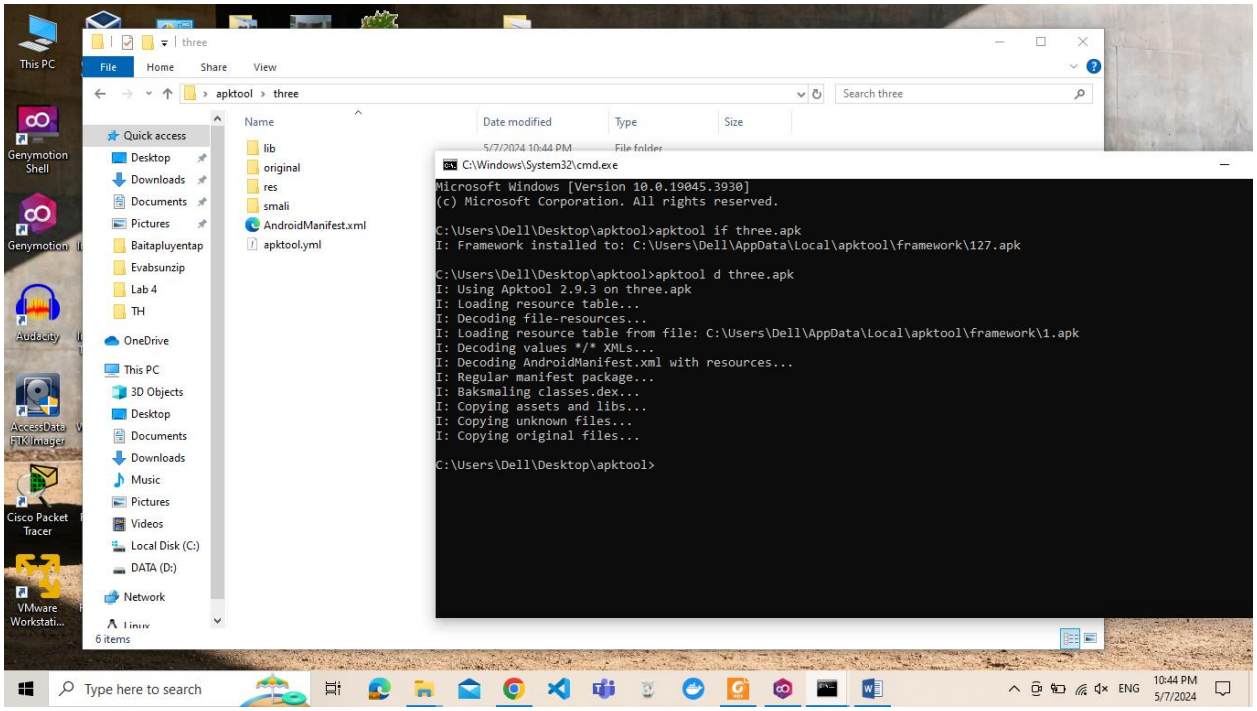
Ta thu được flag

Flag: picoCTF{pining.for.the.fjords}

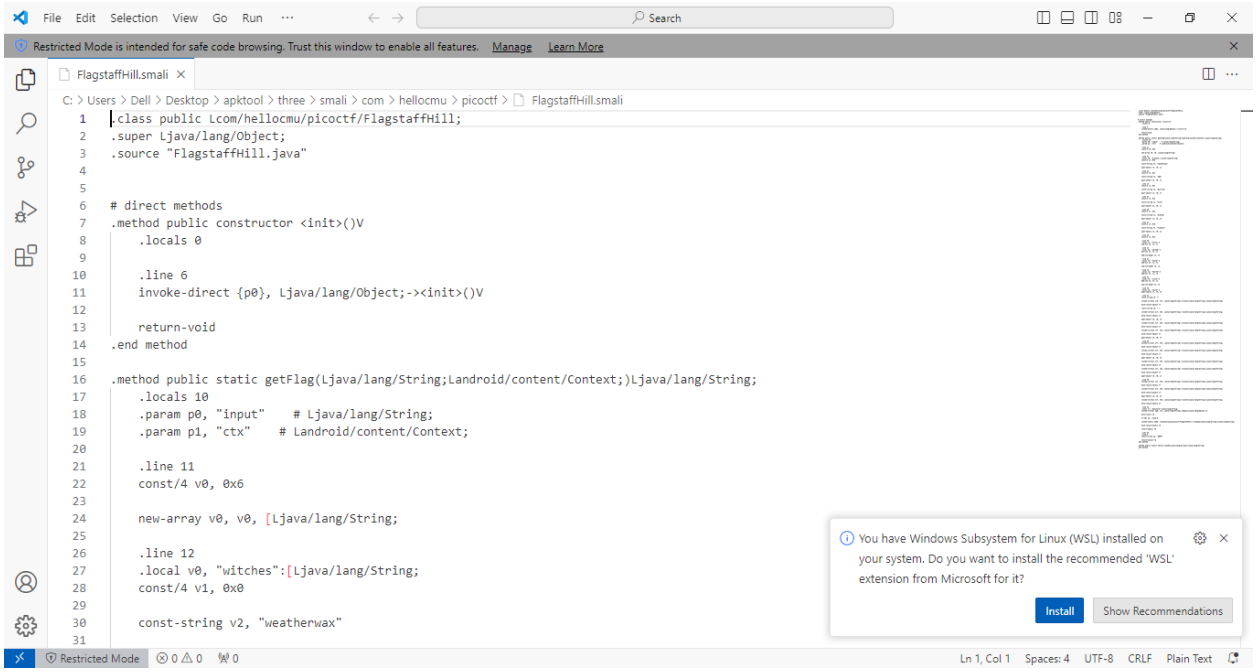
Flag3



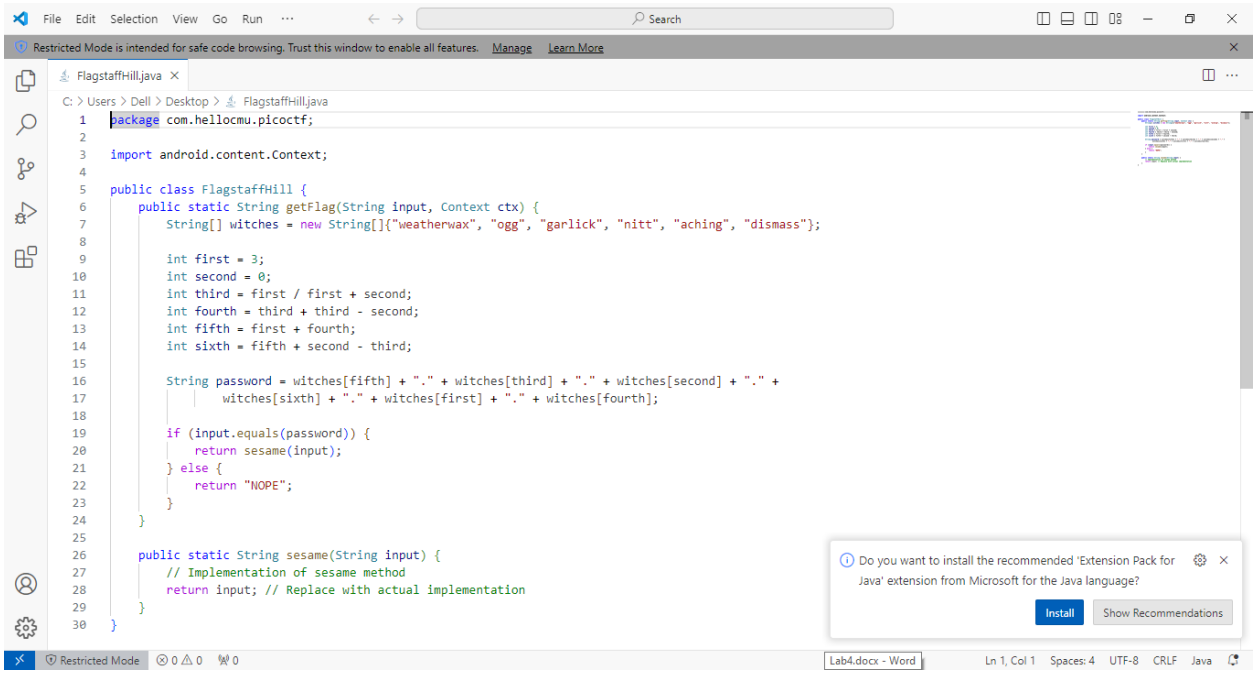
Tiến hành decompile file



Ta kiểm tra thử FlagstaffHill.smali

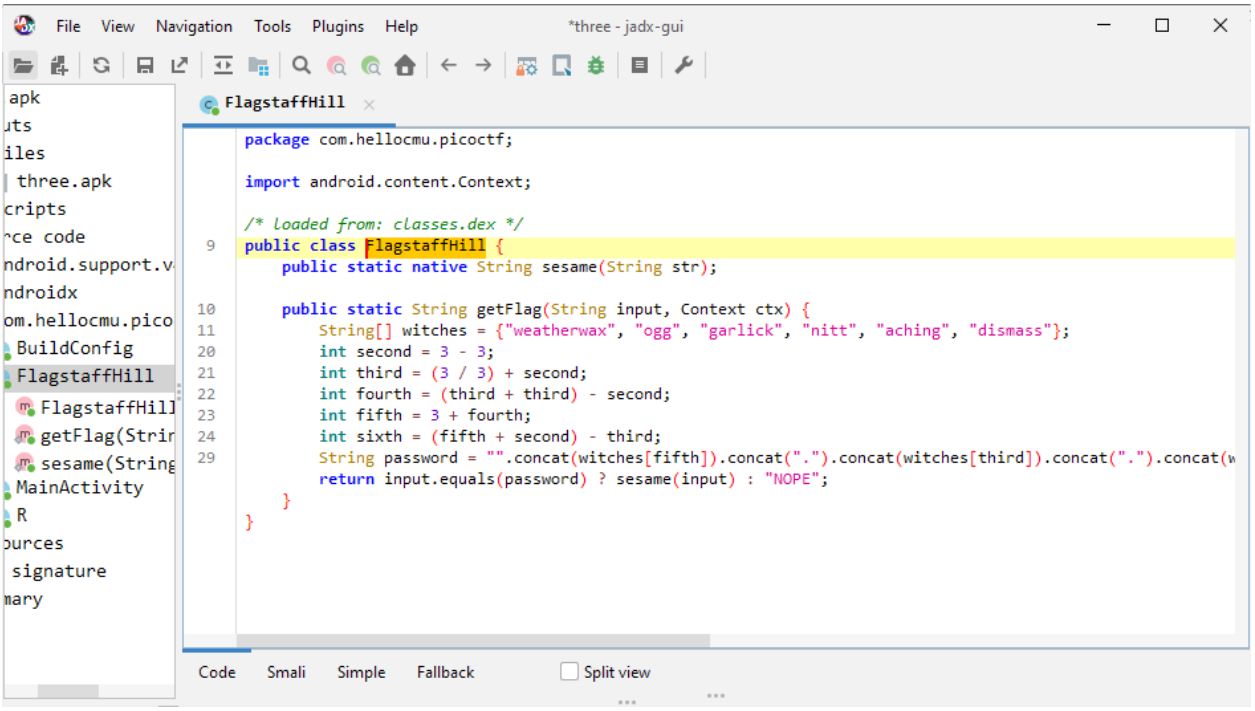


Ta thử tạo lại file FlagtaffHill.java từ thông tin trên

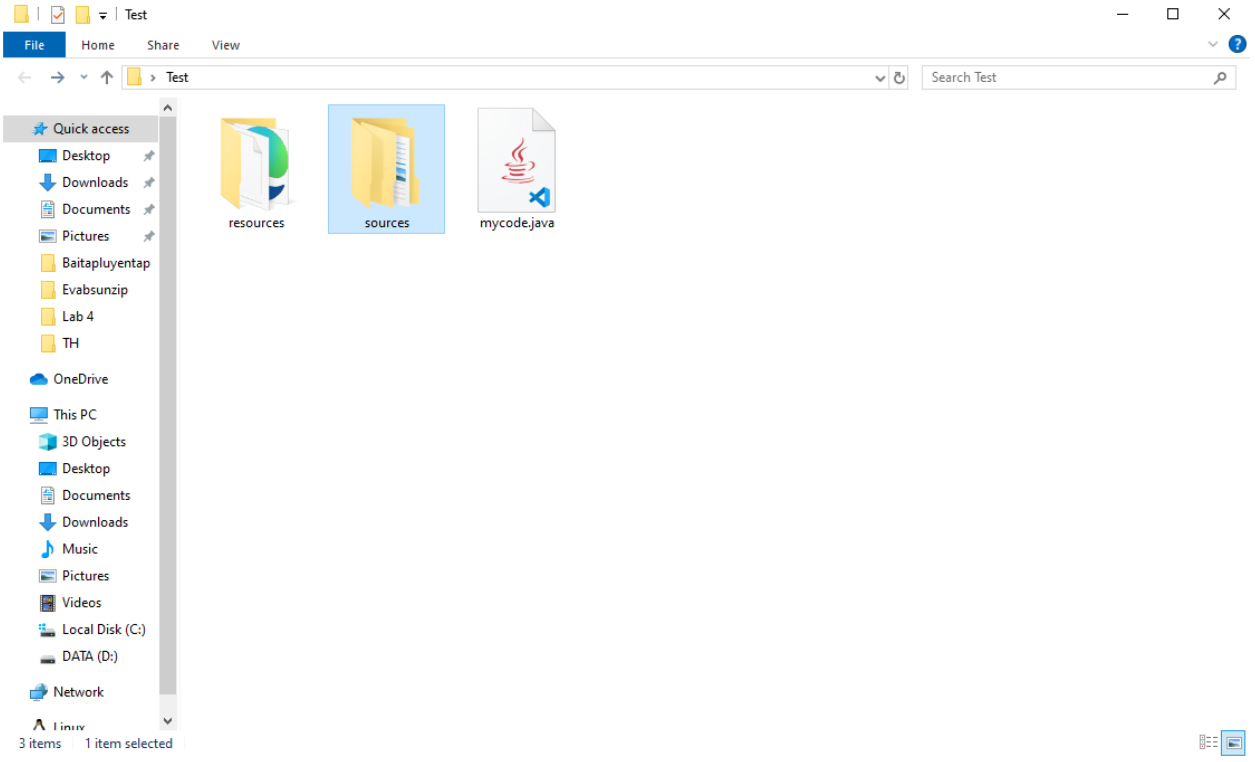


Ta nhận thấy cách làm trên không ra được kết quả

Sử dụng công cụ Jadx



Ta down code về



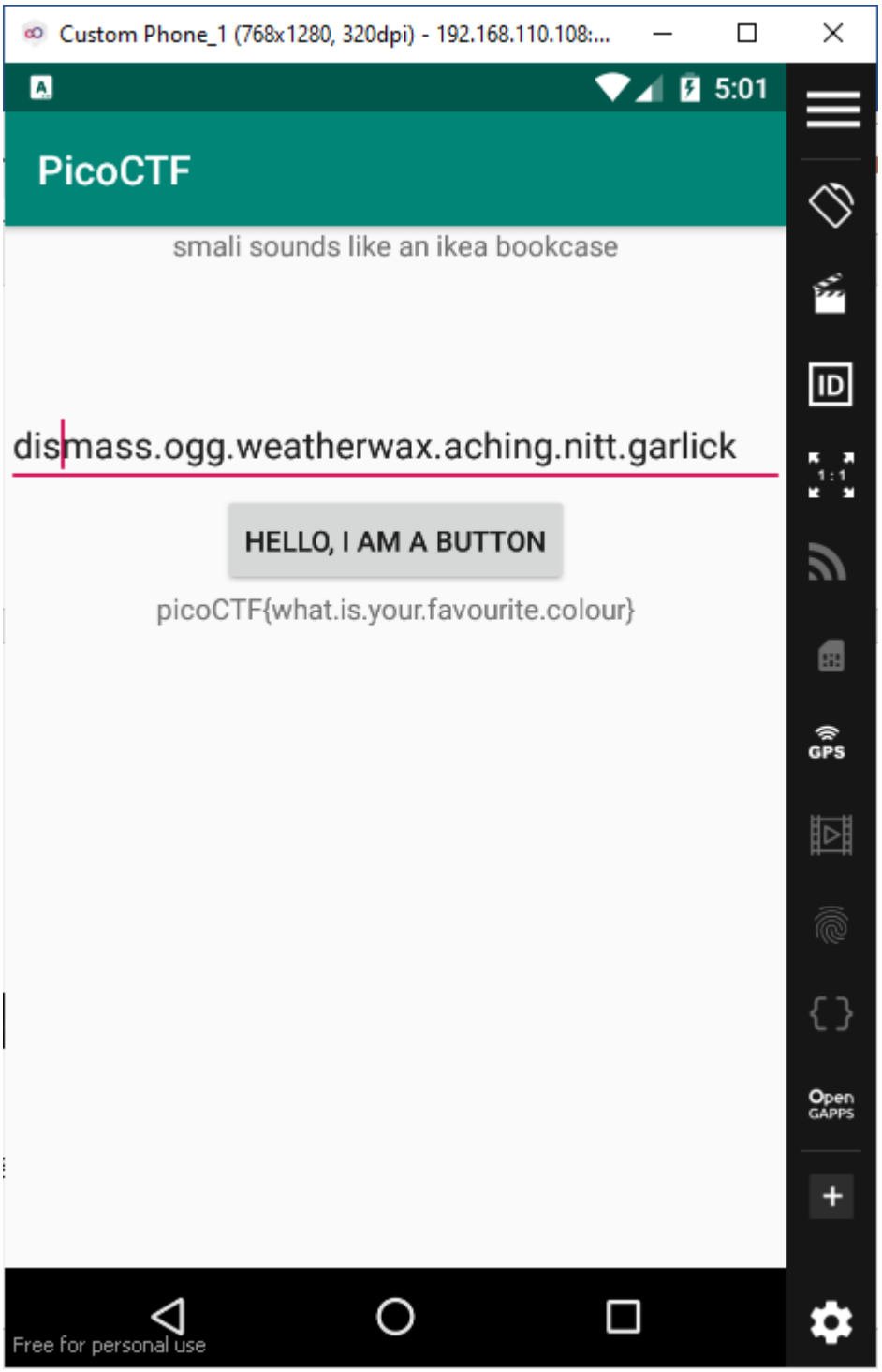
Tới đây, để chạy mycode.java cần thiết lập môi trường

Sau khi chạy thành công, thu được password

```
password: dismass.ogg.weatherwax.aching.nitt.garlick
```

password: dismass.ogg.weatherwax.aching.nitt.garlick

Nhập password vào



Ta thu được flag

Flag: picoCTF{what.is.your.favourite.colour}

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.K11.ATCL*]-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.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

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

HẾT