Forensics CTF 6

Platform: picoCTF 2024

Challenge Name: Mob Psycho

Category: Forensics

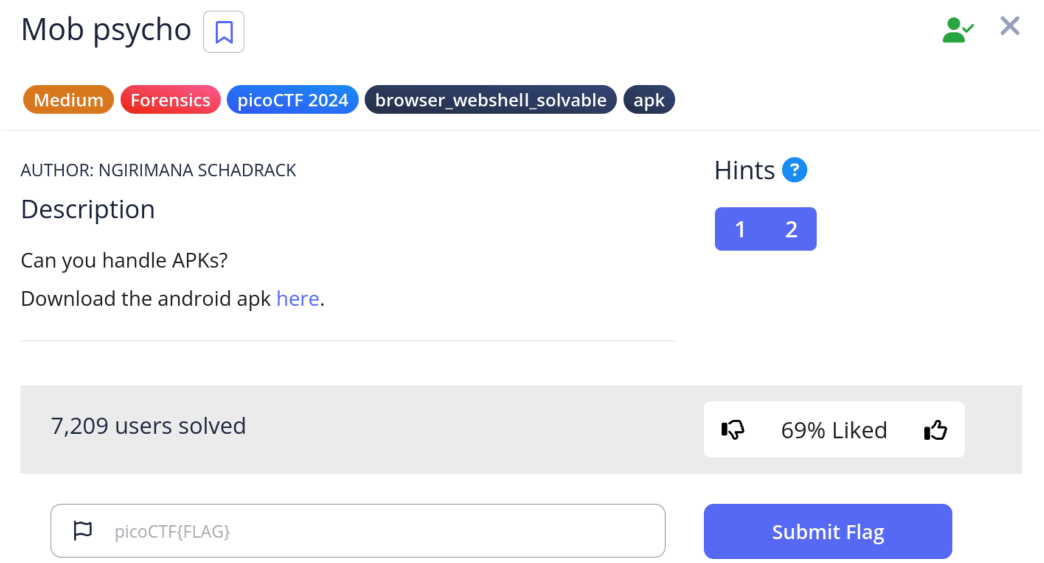
Difficulty: Medium

Submitted By: Gurleen Kaur Brar

Objective

The objective was to analyze an Android APK file and locate an embedded flag. This challenge tested the ability to inspect APK contents, locate suspicious files, and decode obfuscated strings.

Challenge Description



AUTHOR: NGIRIMANA SCHADRACK

Description

Can you handle APKs?

Download the android apk here.

7,209 users solved

Files and Tools Used

- **File Provided:** `mobpsycho.apk`
- **Tools Used:**

- Kali Linux Terminal
- APK extraction (automatically generates `_apk_FILES` folder)
- CyberChef (for decoding hex strings)

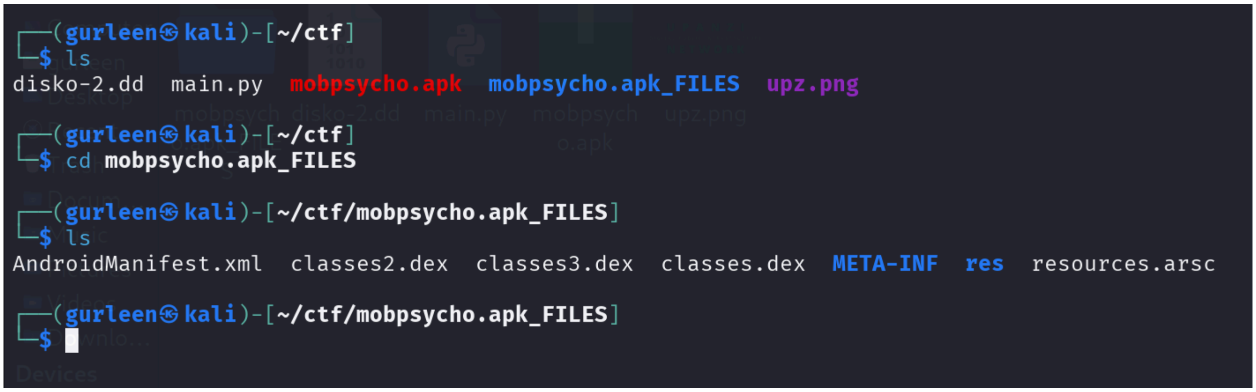
Step-by-Step Process

Step 1: Extract the APK

When the APK file was extracted (either using `apktool` or directly unzipped), a folder named `mobpsycho.apk_FILES` was created, containing several `.dex` files and resource directories.

Navigated into it:

```
cd mobpsycho.apk_FILES
```



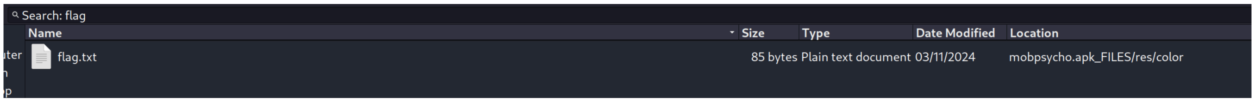
```
┌──(gurleen㉿kali)-[~/ctf]
└─$ ls
disko-2.dd  main.py  mobpsycho.apk  mobpsycho.apk_FILES  upz.png

┌──(gurleen㉿kali)-[~/ctf]
└─$ cd mobpsycho.apk_FILES

┌──(gurleen㉿kali)-[~/ctf/mobpsycho.apk_FILES]
└─$ ls
AndroidManifest.xml  classes2.dex  classes3.dex  classes.dex  META-INF  res  resources.arsc

┌──(gurleen㉿kali)-[~/ctf/mobpsycho.apk_FILES]
└─$ 
```

Located potential text data in flag.txt

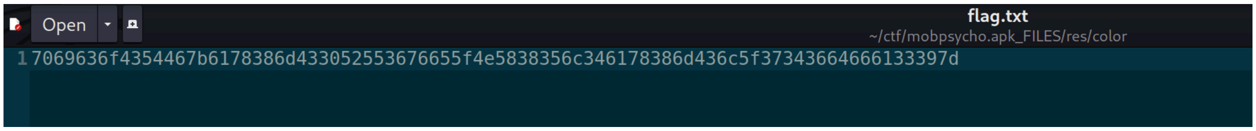


Search: flag

Name	Size	Type	Date Modified	Location
flag.txt	85 bytes	Plain text document	03/11/2024	mobpsycho.apk_FILES/res/color

Step 2: Inspect the Flag File

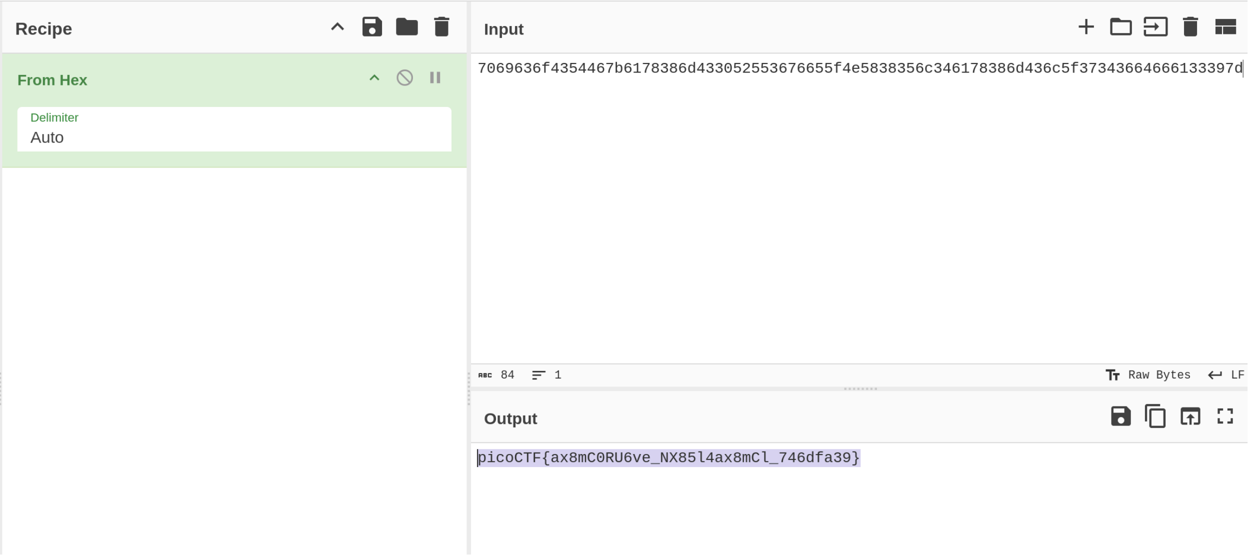
Opened `flag.txt` which contained a long hex string



```
7069636f4354467b6178386d433052553676655f4e5838356c346178386d436c5f37343664666133397d
```

Step 3: Decode Using CyberChef

Used CyberChef with the **From Hex** operation. This decoded the hex into a readable string:



Delimiter: Auto

```
7069636f4354467b6178386d433052553676655f4e5838356c346178386d436c5f37343664666133397d
```

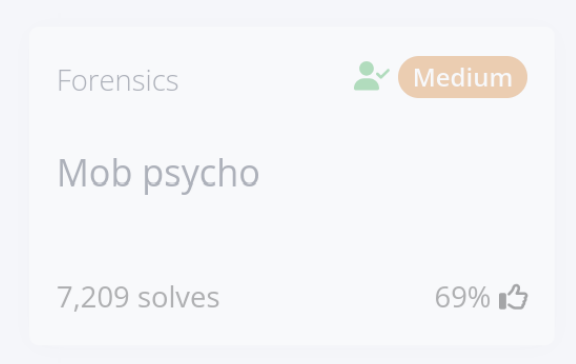
84 1

```
picoCTF{ax8mC0RU6ve_NX85l4ax8mCl_746dfa39}
```

Flag Submitted

```
picoCTF{ax8mC0RU6ve_NX85L4ax8mcL_746dfa39}
```

The decoded flag was correct and successfully submitted.



Forensics Medium

Mob psycho

7,209 solves 69%