AskFM-POC
AskFM OSINT Proof of concept

Introduction

While trying to find some fun way to use the app, I found out that the Add Friends option could be of some use.
In fact, it works in a way that I did not expect. While all your private information is "private" and should not be visible on your profile, somehow, you can do a research using an email and it will return you the linked profile. Pretty interesting.
I'm going to try to find a way to use this functionality outside the app and in a scalable way.
Also worth mentioning, you don't need to be registered to use this functionality.

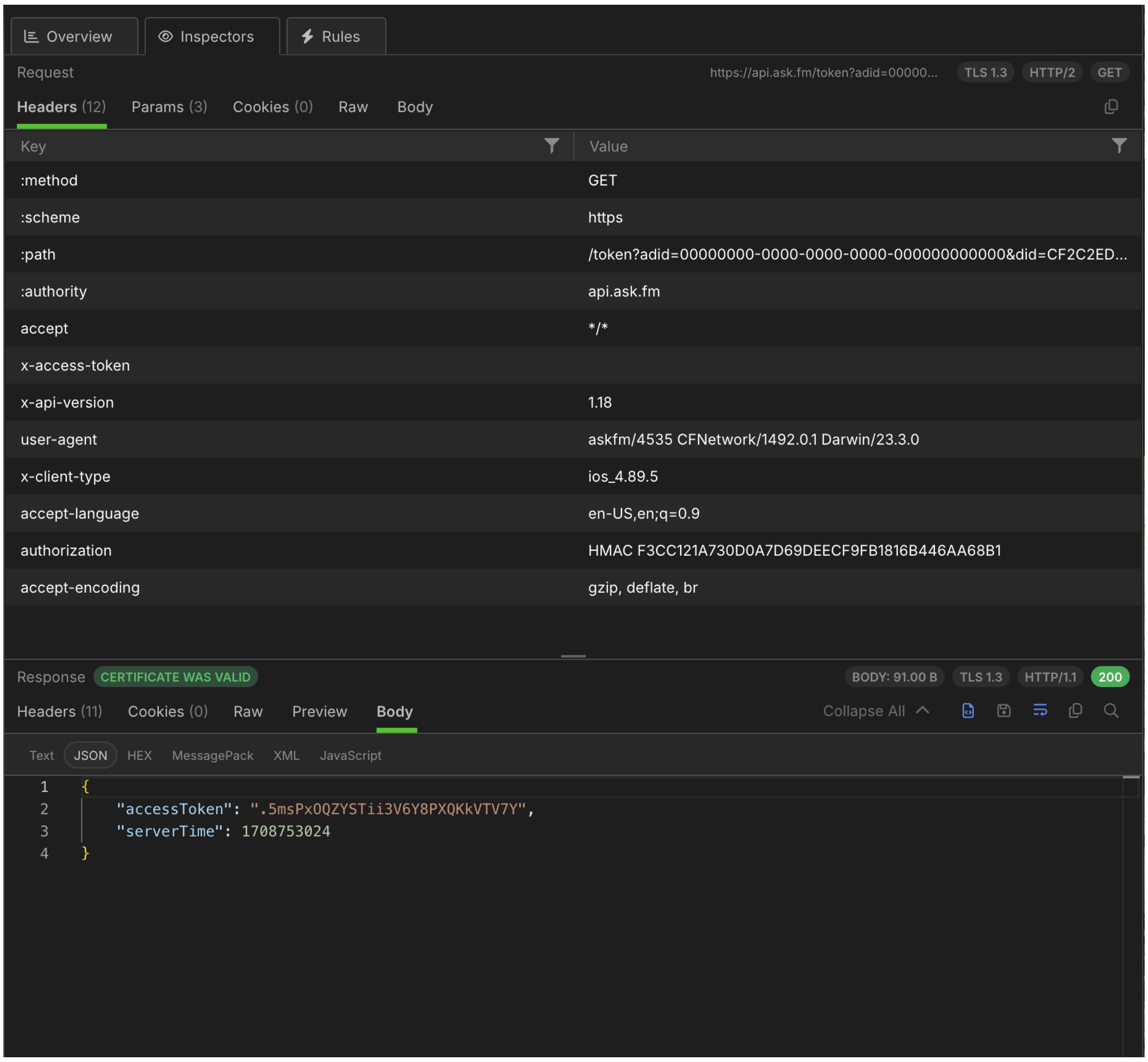
Network Analysis

So first of all, I wanted to find how the app communicates with the ASKFM server, so I started a network analysis. Here is what a regular request looks like

```
GET
https://api.ask.fm/search?bio=miaooo&limit=25&name=miaooo&offset=0&rt=29&ts=1709016
214 HTTP/1.1
Host: api.ask.fm
X-Access-Token: .3tzAQ2JtaZ2G5GKp77BQv7fJkOt2E
X-Api-Version: 1.18
Connection: keep-alive
X-Client-Type: ios_4.89.5
Accept: */*
Accept-Language: en-US,en;q=0.9
Authorization: HMAC FAC9BF579D474290AF2C67F6732688B805FD1897
Accept-Encoding: gzip, deflate, br
User-Agent: askfm/4535 CFNetwork/1492.0.1 Darwin/23.3.0
```

Most of the headers are not really important, and as long as we don't change them, everything will be fine.
The two interesting ones are the 'X-Access-Token' and the 'Authorization'

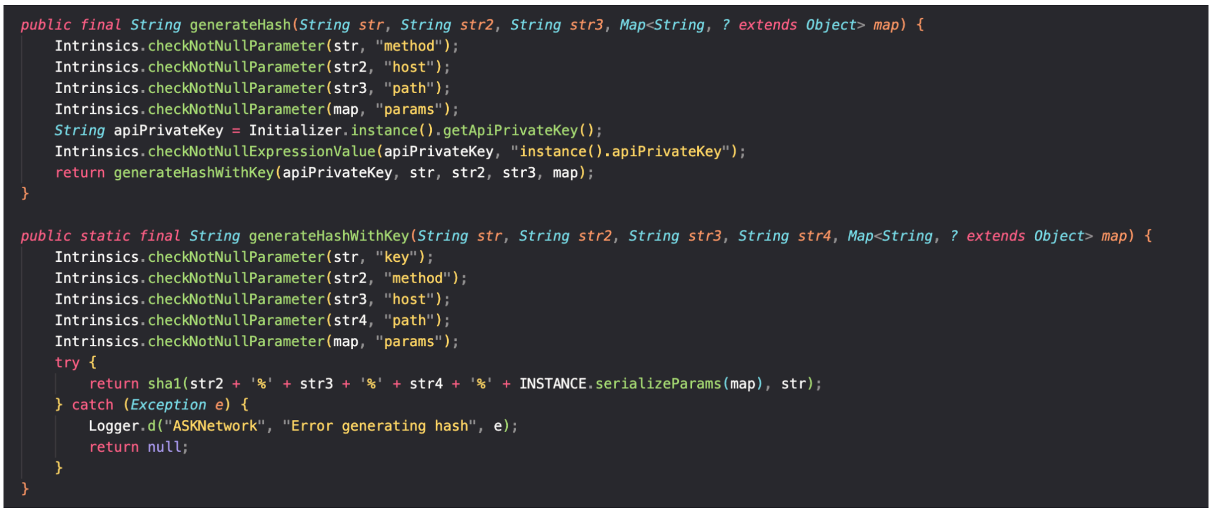
X-Access-Token
This access token seems to be related to a session with the server. This is the first thing we need. As soon as a connection is established with the server, the app send a GET request to api.ask.fm/token with some device related parameters, and a response will be returned with an accessToken that will be used in every request for this session.



Key	Value
:method	GET
:scheme	https
:path	/token?adid=00000000-0000-0000-0000-000000000000&did=CF2C2ED...
:authority	api.ask.fm
accept	*/*
x-access-token	
x-api-version	1.18
user-agent	askfm/4535 CFNetwork/1492.0.1 Darwin/23.3.0
x-client-type	ios_4.89.5
accept-language	en-US,en;q=0.9
authorization	HMAC F3CC121A730D0A7D69DEECF9FB1816B446AA68B1
accept-encoding	gzip, deflate, br

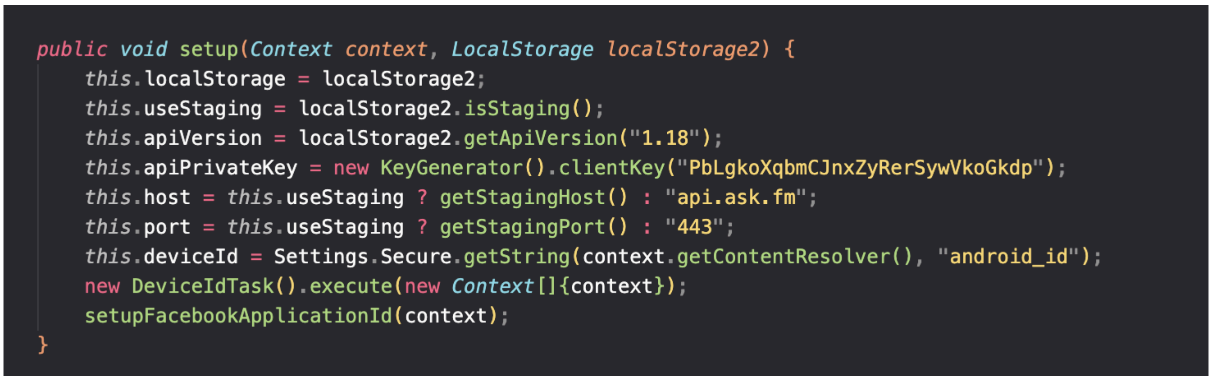
```json
{
    "accessToken": ".5msPxOQZYSTii3V6Y8PXQKkVTV7Y",
    "serverTime": 1708753024
}
```

Authorization
This authorization is a little more tricky, as it is constantly changing with every request. It seems like a hash of some sort. In order to understand this one, I found no other way than to start reversing the app.
After finding some interesting strings inside, I decompile the apk to start looking for this HMAC function. I quickly found this java file that does all the computation to calculate the hash for each request.
It uses the method, host, path, params and a key.



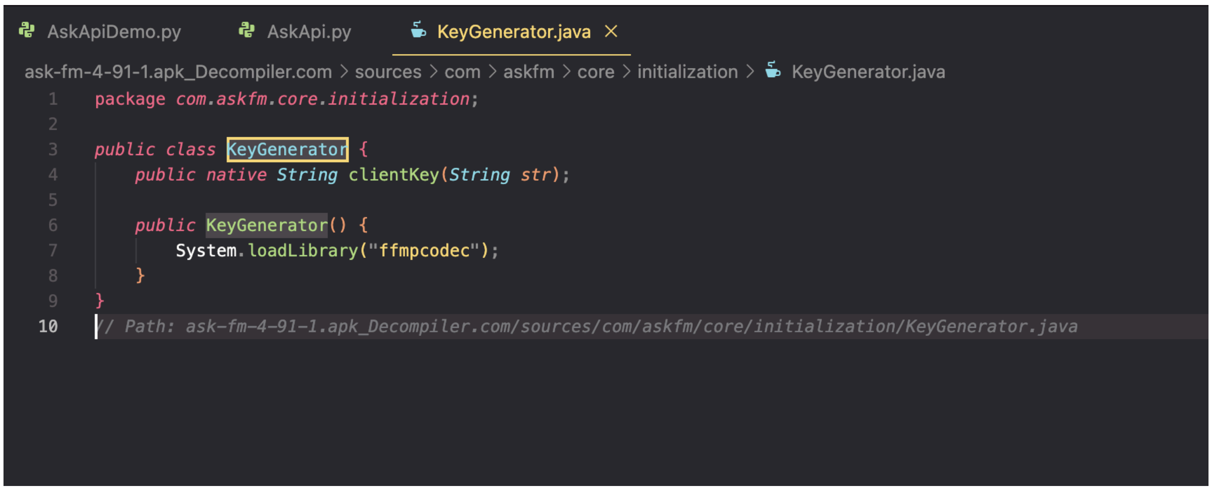
```java
public final String generateHash(String str, String str2, String str3, Map<String, ? extends Object> map) {
    Intrinsics.checkNotNullParameter(str, "method");
    Intrinsics.checkNotNullParameter(str2, "host");
    Intrinsics.checkNotNullParameter(str3, "path");
    Intrinsics.checkNotNullParameter(map, "params");
    String apiPrivateKey = Initializer.instance().getApiPrivateKey();
    Intrinsics.checkNotNullExpressionValue(apiPrivateKey, "instance().apiPrivateKey");
    return generateHashWithKey(apiPrivateKey, str, str2, str3, map);
}

public static final String generateHashWithKey(String str, String str2, String str3, String str4, Map<String, ? extends Object> map) {
    Intrinsics.checkNotNullParameter(str, "key");
    Intrinsics.checkNotNullParameter(str2, "method");
    Intrinsics.checkNotNullParameter(str3, "host");
    Intrinsics.checkNotNullParameter(str4, "path");
    Intrinsics.checkNotNullParameter(map, "params");
    try {
        return sha1(str2 + '%' + str3 + '%' + str4 + '%' + INSTANCE.serializeParams(map), str);
    } catch (Exception e) {
        Logger.d("ASKNetwork", "Error generating hash", e);
        return null;
    }
}
```

It calls some other functions to calculate the hash and uses an apiKey, so I started looking for the key. I found this line which looked like a key, and was really happy at first



```java
public void setup(Context context, LocalStorage localStorage2) {
    this.localStorage = localStorage2;
    this.useStaging = localStorage2.isStaging();
    this.apiVersion = localStorage2.getApiVersion("1.18");
    this.apiPrivateKey = new KeyGenerator().clientKey("PbLgkoXqbmCJnxZyRerSywVkoGkdp");
    this.host = this.useStaging ? getStagingHost() : "api.ask.fm";
    this.port = this.useStaging ? getStagingPort() : "443";
    this.deviceId = Settings.Secure.getString(context.getContentResolver(), "android_id");
    new DeviceIdTask().execute(new Context[]{context});
    setupFacebookApplicationId(context);
}
```

But after a better look, I found out the KeyGenerator class was implemented inside a shared library. Sadly, even after some time looking at the objdump of that library, I couldn't find what this clientKey function was doing exactly, as this library was calling some global variables from other libraries :(


AskApiDemo.py
AskApi.py
KeyGenerator.java
ask-fm-4-91-1.apk_Decompiler.com > sources > com > askfm > core > initialization > KeyGenerator.java

```java
package com.askfm.core.initialization;

public class KeyGenerator {
    public native String clientKey(String str);

    public KeyGenerator() {
        System.loadLibrary("ffmpcodec");
    }
}
// Path: ask-fm-4-91-1.apk_Decompiler.com/sources/com/askfm/core/initialization/KeyGenerator.java
```

```
❯ readelf -d libffmpcodec.so

Dynamic section at offset 0xbc8 contains 27 entries:
  Tag        Type                         Name/Value
 0x0000000000000001 (NEEDED)             Shared library: [liblog.so]
 0x0000000000000001 (NEEDED)             Shared library: [libm.so]
 0x0000000000000001 (NEEDED)             Shared library: [libdl.so]
 0x0000000000000001 (NEEDED)             Shared library: [libc.so]
 0x000000000000000e (SONAME)             Library soname: [libffmpcodec.so]
```

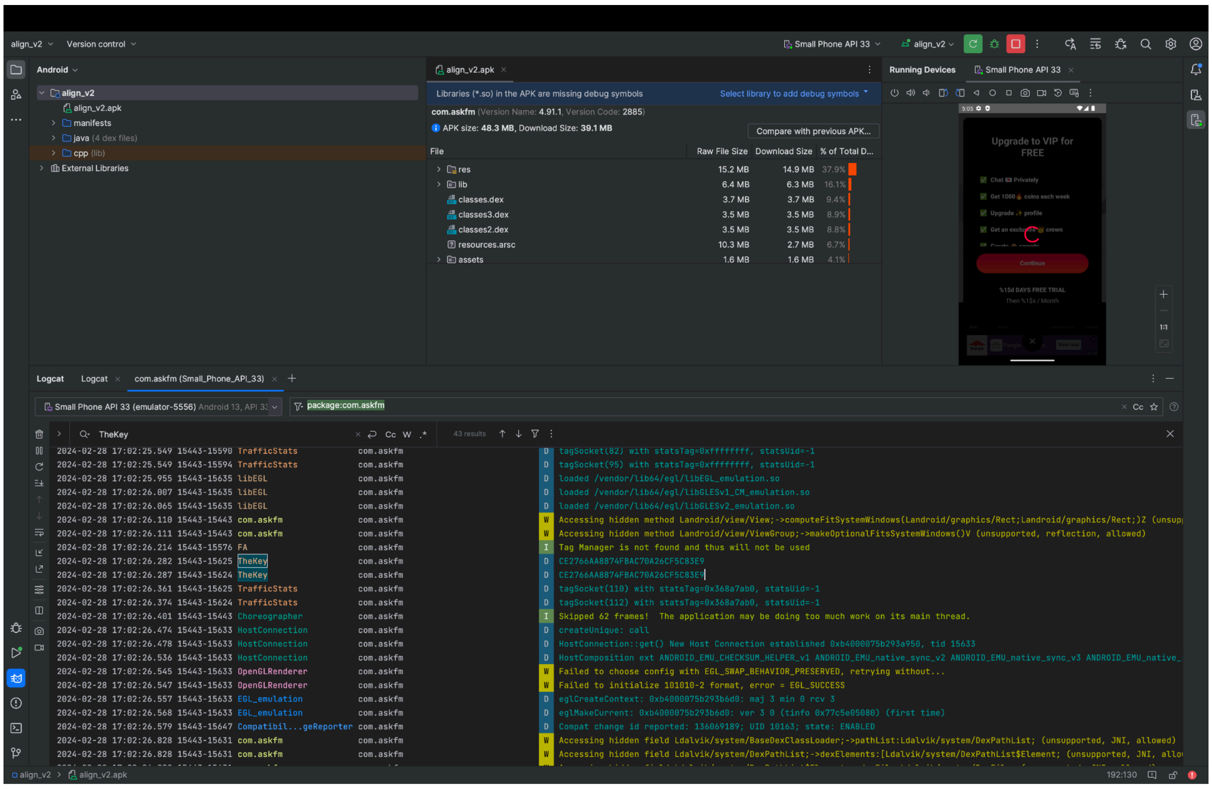
I also found out that those libraries are on Android, so i couldn't compile a simple Java program that called this function to find the behavior, it had to be in an app.
So at this point I just decided to decompile the app, add some logs just after the use of this function and then align, sign and recompile the app.
Was not an easy task but I managed to get a result

Added this line to the Signature.smali file just after the getApiPrivateKey call

```
const-string v2, "TheKey"

invoke-static {v2, v0}, Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I
```

Some commands to recompile the app
```
apktool d -f ask-fm-4-91-1.apk -o newapktest
code newapktest
apktool b -f -d newapktest
keytool -genkey -v -keystore my.keystore -keyalg RSA -keysize 2048 -validity 10000 -alias app\
~/Library/Android/sdk/build-tools/28.0.3/zipalign -p 4 newapktest/dist/ask-fm-4-91-1.apk newapktest/dist/aligned.apk
~/Library/Android/sdk/build-tools/28.0.3/zipalign -v -c 4 newapktest/dist/aligned.apk
~/Library/Android/sdk/build-tools/28.0.3/apksigner sign --ks-key-alias app --ks my.keystore newapktest/dist/aligned.apk
~/Library/Android/sdk/build-tools/28.0.3/apksigner verify newapktest/dist/aligned.apk
```

And we are ready to launch our new modified app. (Almost, after some android studio configuration to find the right SDK and emulated phone)

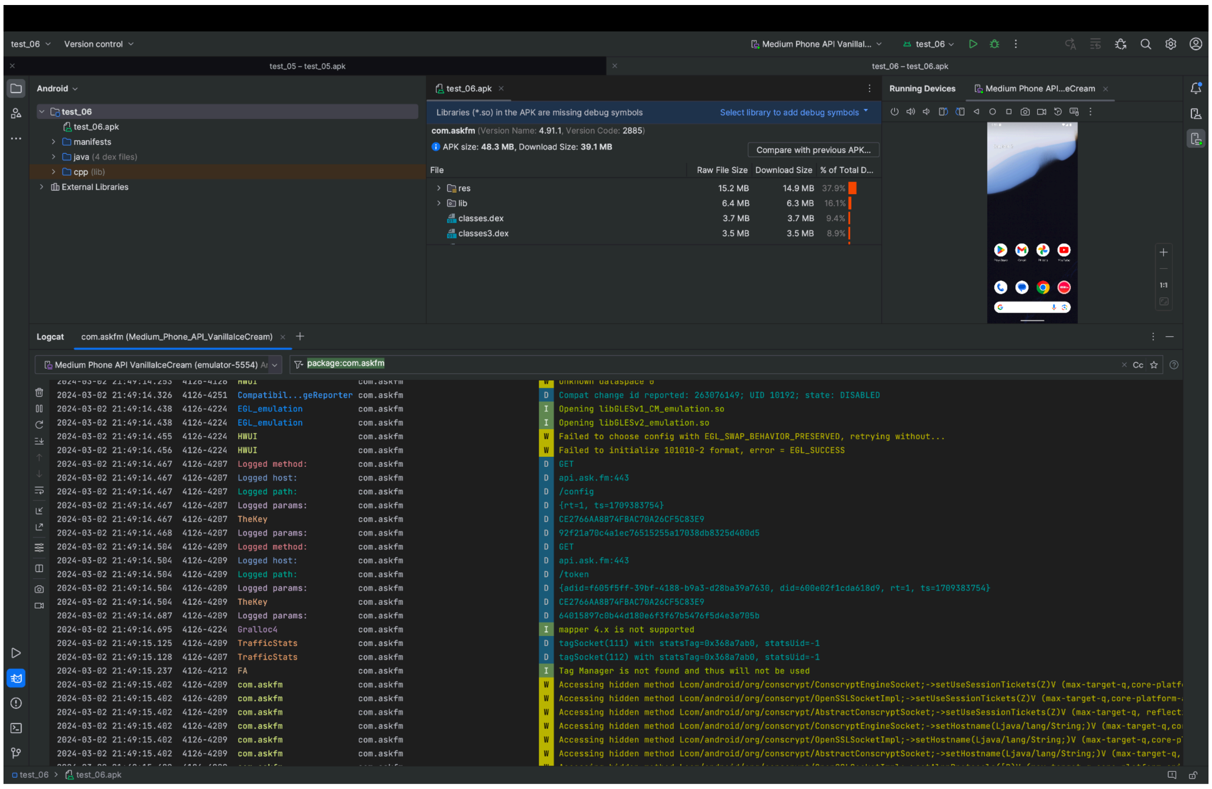


```
com.askfm (Version Name: 4.91.1, Version Code: 2885)
APK size: 48.3 MB, Download Size: 39.1 MB

File                Raw File Size  Download Size  % of Total D...
res                 15.2 MB        14.9 MB        37.9%
lib                 6.4 MB         6.3 MB         16.1%
classes.dex         3.7 MB         3.7 MB         9.4%
classes3.dex        3.5 MB         3.5 MB         8.9%
classes2.dex        3.5 MB         3.5 MB         8.8%
resources.arsc      10.3 MB        2.7 MB         6.7%
assets              1.6 MB         1.6 MB         4.1%
```

```
2024-02-28 17:02:25.549 15443-15590 TrafficStats            com.askfm  D  tagSocket(82) with statsTag=0xffffffff, statsUid=-1
2024-02-28 17:02:25.549 15443-15594 TrafficStats            com.askfm  D  tagSocket(95) with statsTag=0xffffffff, statsUid=-1
2024-02-28 17:02:25.955 15443-15635 libEGL                  com.askfm  D  loaded /vendor/lib64/egl/libEGL_emulation.so
2024-02-28 17:02:26.007 15443-15635 libEGL                  com.askfm  D  loaded /vendor/lib64/egl/libGLESv1_CM_emulation.so
2024-02-28 17:02:26.065 15443-15635 libEGL                  com.askfm  D  loaded /vendor/lib64/egl/libGLESv2_emulation.so
2024-02-28 17:02:26.110 15443-15443 com.askfm               com.askfm  W  Accessing hidden method Landroid/view/View;->computeFitSystemWindows(Landroid/graphics/Rect;Landroid/graphics/Rect;)Z (unsup
2024-02-28 17:02:26.111 15443-15443 com.askfm               com.askfm  W  Accessing hidden method Landroid/view/ViewGroup;->makeOptionalFitsSystemWindows()V (unsupported, reflection, allowed)
2024-02-28 17:02:26.214 15443-15576 FA                      com.askfm  I  Tag Manager is not found and thus will not be used
2024-02-28 17:02:26.282 15443-15625 TheKey                  com.askfm  D  CE2766AA8B74FBAC70A26CF5C83E9
2024-02-28 17:02:26.287 15443-15624 TheKey                  com.askfm  D  CE2766AA8B74FBAC70A26CF5C83E9
2024-02-28 17:02:26.361 15443-15625 TrafficStats            com.askfm  D  tagSocket(110) with statsTag=0x368a7ab0, statsUid=-1
2024-02-28 17:02:26.374 15443-15624 TrafficStats            com.askfm  D  tagSocket(112) with statsTag=0x368a7ab0, statsUid=-1
2024-02-28 17:02:26.401 15443-15443 Choreographer           com.askfm  I  Skipped 62 frames!  The application may be doing too much work on its main thread.
2024-02-28 17:02:26.474 15443-15633 HostConnection          com.askfm  D  createUnique: call
2024-02-28 17:02:26.478 15443-15633 HostConnection          com.askfm  D  HostConnection::get() New Host Connection established 0xb4000075b293a950, tid 15633
2024-02-28 17:02:26.536 15443-15633 HostConnection          com.askfm  D  HostComposition ext ANDROID_EMU_CHECKSUM_HELPER_v1 ANDROID_EMU_native_sync_v2 ANDROID_EMU_native_sync_v3 ANDROID_EMU_native_
2024-02-28 17:02:26.545 15443-15633 OpenGLRenderer          com.askfm  W  Failed to choose config with EGL_SWAP_BEHAVIOR_PRESERVED, retrying without...
2024-02-28 17:02:26.547 15443-15633 OpenGLRenderer          com.askfm  W  Failed to initialize 101010-2 format, error = EGL_SUCCESS
2024-02-28 17:02:26.557 15443-15633 EGL_emulation           com.askfm  D  eglCreateContext: 0xb4000075b293b6d0: maj 3 min 0 rcv 3
2024-02-28 17:02:26.568 15443-15633 EGL_emulation           com.askfm  D  eglMakeCurrent: 0xb4000075b293b6d0: ver 3 0 (tinfo 0x77c5e05080) (first time)
2024-02-28 17:02:26.579 15443-15647 Compatibil...geReporter com.askfm  D  Compat change id reported: 136069189; UID 10163; state: ENABLED
2024-02-28 17:02:26.828 15443-15631 com.askfm               com.askfm  W  Accessing hidden field Ldalvik/system/BaseDexClassLoader;->pathList:Ldalvik/system/DexPathList; (unsupported, JNI, allowed)
2024-02-28 17:02:26.828 15443-15631 com.askfm               com.askfm  W  Accessing hidden field Ldalvik/system/DexPathList;->dexElements:[Ldalvik/system/DexPathList$Element; (unsupported, JNI, allo
```

And here is our not so private apiPrivateKey.

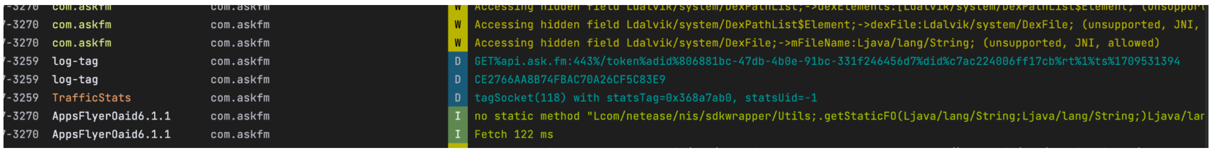
I also made some other logs in order to make sure of the parameters that are given to the hash function and the output hash



```
com.askfm (Version Name: 4.91.1, Version Code: 2885)
APK size: 48.3 MB, Download Size: 39.1 MB

File                Raw File Size  Download Size  % of Total D...
res                 15.2 MB        14.9 MB        37.9%
lib                 6.4 MB         6.3 MB         16.1%
classes.dex         3.7 MB         3.7 MB         9.4%
classes3.dex        3.5 MB         3.5 MB         8.9%
```

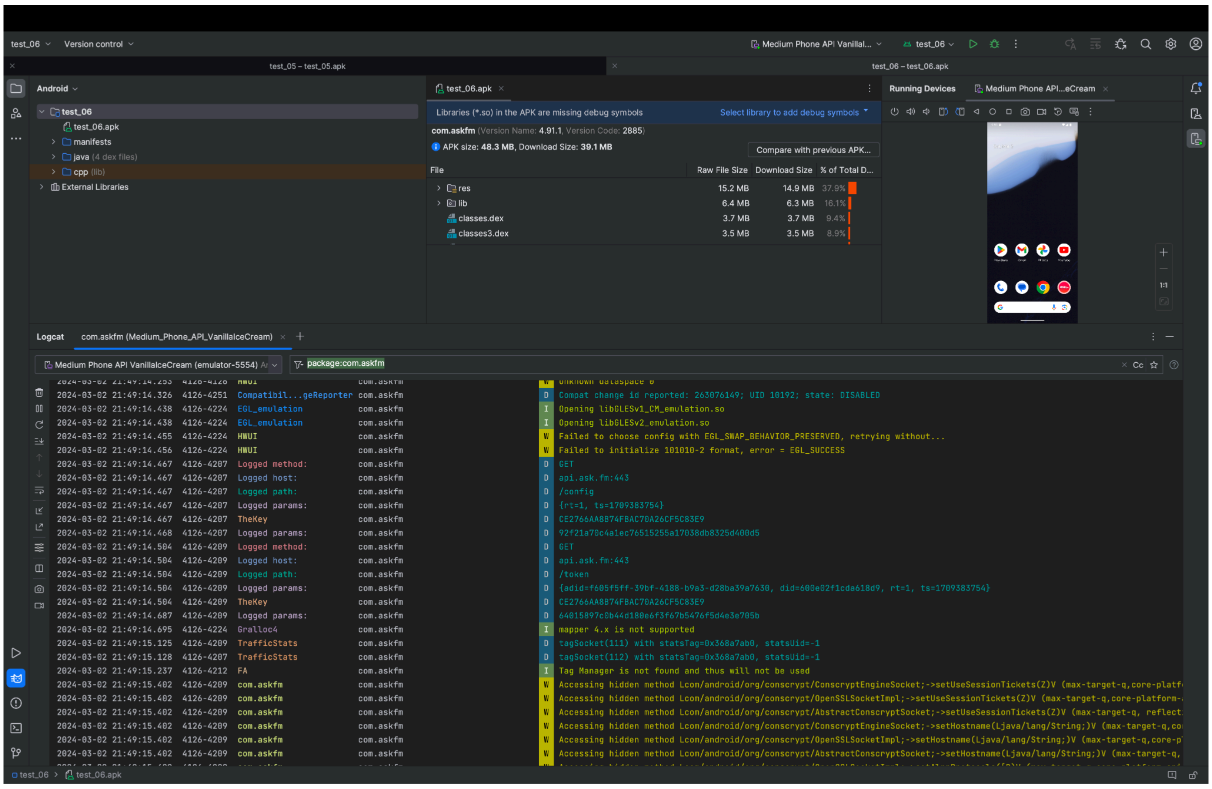
```
2024-03-02 21:49:14.326 4126-4251 Compatibil...geReporter com.askfm  D  Compat change id reported: 263076149; UID 10192; state: DISABLED
2024-03-02 21:49:14.438 4126-4224 EGL_emulation           com.askfm  I  Opening libGLESv1_CM_emulation.so
2024-03-02 21:49:14.438 4126-4224 EGL_emulation           com.askfm  I  Opening libGLESv2_emulation.so
2024-03-02 21:49:14.455 4126-4224 HWUI                    com.askfm  W  Failed to choose config with EGL_SWAP_BEHAVIOR_PRESERVED, retrying without...
2024-03-02 21:49:14.456 4126-4224 HWUI                    com.askfm  W  Failed to initialize 101010-2 format, error = EGL_SUCCESS
2024-03-02 21:49:14.467 4126-4207 Logged method:          com.askfm  D  GET
2024-03-02 21:49:14.467 4126-4207 Logged host:            com.askfm  D  api.ask.fm:443
2024-03-02 21:49:14.467 4126-4207 Logged path:            com.askfm  D  /config
2024-03-02 21:49:14.467 4126-4207 Logged params:          com.askfm  D  {rt=1, ts=1709383754}
2024-03-02 21:49:14.467 4126-4207 TheKey                  com.askfm  D  CE2766AA8B74FBAC70A26CF5C83E9
2024-03-02 21:49:14.468 4126-4207 Logged params:          com.askfm  D  92f21a70c4a1ec76515255a17038db8325d400d5
2024-03-02 21:49:14.504 4126-4209 Logged method:          com.askfm  D  GET
2024-03-02 21:49:14.504 4126-4209 Logged host:            com.askfm  D  api.ask.fm:443
2024-03-02 21:49:14.504 4126-4209 Logged path:            com.askfm  D  /token
2024-03-02 21:49:14.504 4126-4209 Logged params:          com.askfm  D  {adid=f605f5ff-39bf-4188-b9a3-d28ba39a7630, did=600e02f1cda618d9, rt=1, ts=1709383754}
2024-03-02 21:49:14.504 4126-4209 TheKey                  com.askfm  D  CE2766AA8B74FBAC70A26CF5C83E9
2024-03-02 21:49:14.687 4126-4209 Logged params:          com.askfm  D  64015897c0b44d180e6f3f67b5476f5d4e3e705b
2024-03-02 21:49:14.695 4126-4224 Gralloc4                com.askfm  I  mapper 4.x is not supported
2024-03-02 21:49:15.125 4126-4209 TrafficStats            com.askfm  D  tagSocket(111) with statsTag=0x368a7ab0, statsUid=-1
2024-03-02 21:49:15.128 4126-4207 TrafficStats            com.askfm  D  tagSocket(112) with statsTag=0x368a7ab0, statsUid=-1
2024-03-02 21:49:15.237 4126-4212 FA                      com.askfm  I  Tag Manager is not found and thus will not be used
2024-03-02 21:49:15.402 4126-4209 com.askfm               com.askfm  W  Accessing hidden method Lcom/android/org/conscrypt/ConscryptEngineSocket;->setUseSessionTickets(Z)V (max-target-q,core-platf
2024-03-02 21:49:15.402 4126-4209 com.askfm               com.askfm  W  Accessing hidden method Lcom/android/org/conscrypt/OpenSSLSocketImpl;->setUseSessionTickets(Z)V (max-target-q,core-platform-
2024-03-02 21:49:15.402 4126-4209 com.askfm               com.askfm  W  Accessing hidden method Lcom/android/org/conscrypt/AbstractConscryptSocket;->setUseSessionTickets(Z)V (max-target-q, reflect
2024-03-02 21:49:15.402 4126-4209 com.askfm               com.askfm  W  Accessing hidden method Lcom/android/org/conscrypt/ConscryptEngineSocket;->setHostname(Ljava/lang/String;)V (max-target-q,co
2024-03-02 21:49:15.402 4126-4209 com.askfm               com.askfm  W  Accessing hidden method Lcom/android/org/conscrypt/OpenSSLSocketImpl;->setHostname(Ljava/lang/String;)V (max-target-q,core-p
2024-03-02 21:49:15.402 4126-4209 com.askfm               com.askfm  W  Accessing hidden method Lcom/android/org/conscrypt/AbstractConscryptSocket;->setHostname(Ljava/lang/String;)V (max-target-q,
```

With that in mind, I started to make some python scripts to send requests to the server and implement the hash function



```
-3270  com.askfm              com.askfm   W  Accessing hidden field Ldalvik/system/DexPathList$Element;->dexFile:Ldalvik/system/DexFile; (unsupported, JNI,
-3270  com.askfm              com.askfm   W  Accessing hidden field Ldalvik/system/DexFile;->mFileName:Ljava/lang/String; (unsupported, JNI, allowed)
-3259  log-tag                com.askfm   D  GET%api.ask.fm:443%/token%adid%806881bc-47db-4b0e-91bc-331f246456d7%did%c7ac224006ff17cb%rt%1%ts%1709531394
-3259  log-tag                com.askfm   D  CE2766AA8B74FBAC70A26CF5C83E9
-3259  TrafficStats           com.askfm   D  tagSocket(118) with statsTag=0x368a7ab0, statsUid=-1
-3270  AppsFlyerOaid6.1.1     com.askfm   I  no static method "Lcom/netease/nis/sdkwrapper/Utils;.getStaticFO(Ljava/lang/String;Ljava/lang/String;)Ljava/lar
-3270  AppsFlyerOaid6.1.1     com.askfm   I  Fetch 122 ms
```

I made some tests with intercepted requests from the app to make sure this would work. After I got it right, I tried to understand the Hmac computation.



Logcat   com.askfm (Medium_Phone_API_VanillaIceCream)

Medium Phone API VanillaIceCream (emulator-5554)   package:com.askfm

```
2024-03-02 21:49:14.326  4126-4251  Compatibil...geReporter com.askfm  D  Compat change id reported: 263076149; UID 10192; state: DISABLED
2024-03-02 21:49:14.438  4126-4224  EGL_emulation           com.askfm  I  Opening libGLESv1_CM_emulation.so
2024-03-02 21:49:14.438  4126-4224  EGL_emulation           com.askfm  I  Opening libGLESv2_emulation.so
2024-03-02 21:49:14.455  4126-4224  HWUI                    com.askfm  W  Failed to choose config with EGL_SWAP_BEHAVIOR_PRESERVED, retrying without...
2024-03-02 21:49:14.456  4126-4224  HWUI                    com.askfm  W  Failed to initialize 101010-2 format, error = EGL_SUCCESS
2024-03-02 21:49:14.467  4126-4207  Logged method:          com.askfm  D  GET
2024-03-02 21:49:14.467  4126-4207  Logged host:            com.askfm  D  api.ask.fm:443
2024-03-02 21:49:14.467  4126-4207  Logged path:            com.askfm  D  /config
2024-03-02 21:49:14.467  4126-4207  Logged params:          com.askfm  D  {rt=1, ts=1709383754}
2024-03-02 21:49:14.467  4126-4207  TheKey                  com.askfm  D  CE2766AA8B74FBAC70A26CF5C83E9
2024-03-02 21:49:14.468  4126-4207  Logged params:          com.askfm  D  92f21a70c4a1ec76515255a17038db8325d400d5
2024-03-02 21:49:14.504  4126-4209  Logged method:          com.askfm  D  GET
2024-03-02 21:49:14.504  4126-4209  Logged host:            com.askfm  D  api.ask.fm:443
2024-03-02 21:49:14.504  4126-4209  Logged path:            com.askfm  D  /token
2024-03-02 21:49:14.504  4126-4209  Logged params:          com.askfm  D  {adid=f605f5ff-39bf-4188-b9a3-d28ba39a7630, did=600e02f1cda618d9, rt=1, ts=1709383754}
2024-03-02 21:49:14.504  4126-4209  TheKey                  com.askfm  D  CE2766AA8B74FBAC70A26CF5C83E9
2024-03-02 21:49:14.687  4126-4209  Logged params:          com.askfm  D  64015897c0b44d180e6f3f67b5476f5d4e3e705b
2024-03-02 21:49:14.695  4126-4224  Gralloc4                com.askfm  I  mapper 4.x is not supported
2024-03-02 21:49:15.125  4126-4209  TrafficStats            com.askfm  D  tagSocket(111) with statsTag=0x368a7ab0, statsUid=-1
2024-03-02 21:49:15.128  4126-4207  TrafficStats            com.askfm  D  tagSocket(112) with statsTag=0x368a7ab0, statsUid=-1
2024-03-02 21:49:15.237  4126-4212  FA                      com.askfm  I  Tag Manager is not found and thus will not be used
2024-03-02 21:49:15.402  4126-4209  com.askfm               com.askfm  W  Accessing hidden method Lcom/android/org/conscrypt/ConscryptEngineSocket;->setUseSessionTickets(Z)V (max-target-q,core-platf
2024-03-02 21:49:15.402  4126-4209  com.askfm               com.askfm  W  Accessing hidden method Lcom/android/org/conscrypt/OpenSSLSocketImpl;->setUseSessionTickets(Z)V (max-target-q,core-platform-
2024-03-02 21:49:15.402  4126-4209  com.askfm               com.askfm  W  Accessing hidden method Lcom/android/org/conscrypt/AbstractConscryptSocket;->setUseSessionTickets(Z)V (max-target-q, reflect
2024-03-02 21:49:15.402  4126-4209  com.askfm               com.askfm  W  Accessing hidden method Lcom/android/org/conscrypt/ConscryptEngineSocket;->setHostname(Ljava/lang/String;)V (max-target-q,co
2024-03-02 21:49:15.402  4126-4209  com.askfm               com.askfm  W  Accessing hidden method Lcom/android/org/conscrypt/OpenSSLSocketImpl;->setHostname(Ljava/lang/String;)V (max-target-q,core-p
2024-03-02 21:49:15.402  4126-4209  com.askfm               com.askfm  W  Accessing hidden method Lcom/android/org/conscrypt/AbstractConscryptSocket;->setHostname(Ljava/lang/String;)V (max-target-q,
```

Sadly this is where i got stuck. Even with all the information,I tried for days decompiling, rewriting, debugging and switching parameters.
I couldn't find a way to make this hmac function behave the same way it works in the app.
I feel like I'm very close but can't find it.

Thanks for reading until here.
I hope you can appreciate the work. I struggled a lot as it was my first time working on an Android app, I had to learn Android Studio and some Java/Android assembly the hard way. I had a lot of fun and learned a lot with this challenge, thanks for the opportunity.