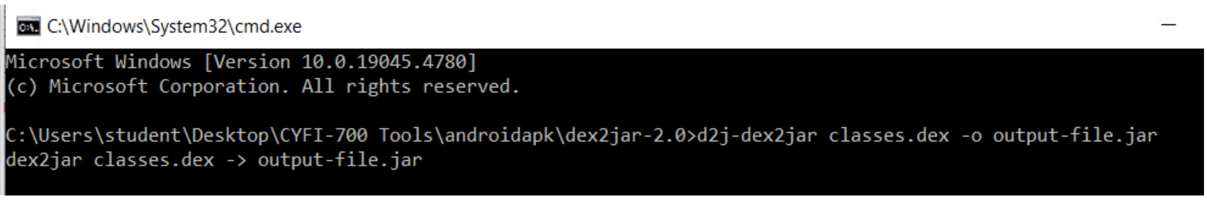
Name: Mohit Ajaykumar Dhabuwala

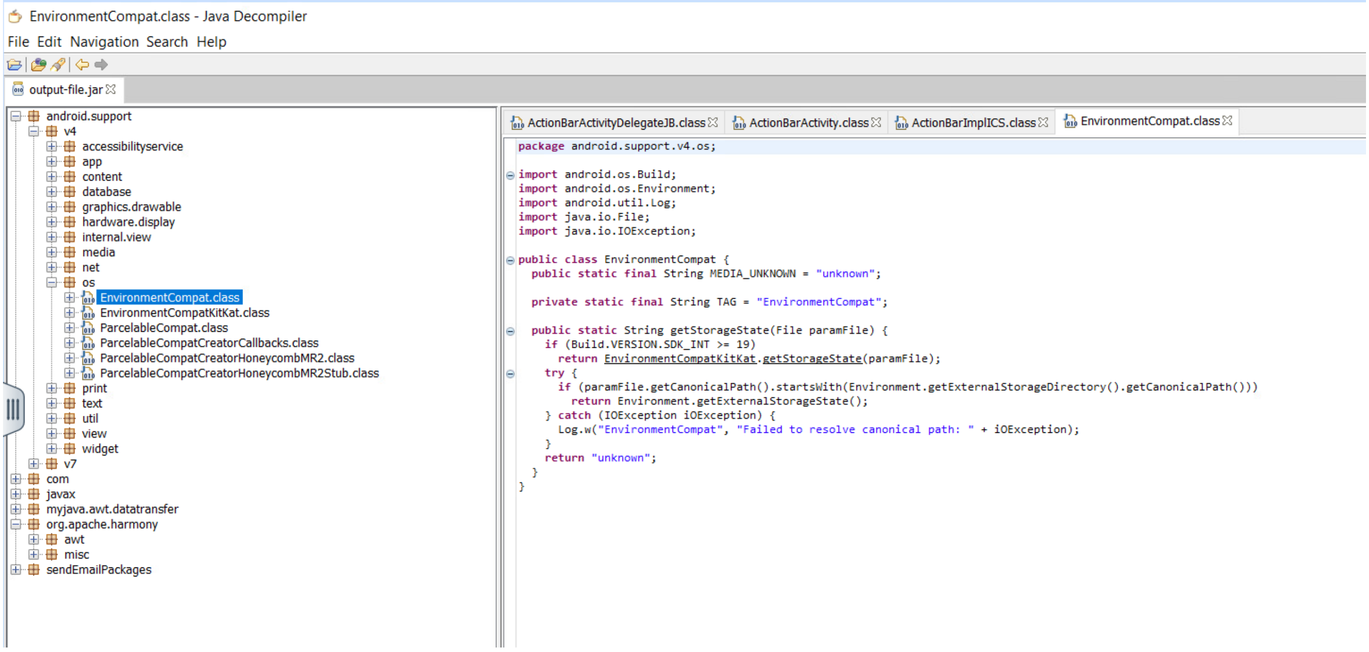
Assignment: Examination of a Suspicious .apk from an Android-based device.

- Extract the **classes.dex** file from **com.unknown.zip** file and place classes.dex in the dex2jar directory. And convert the file named "classes.dex" to a .jar file with the name "output-file.jar" with the command prompt using the command "**d2j-dex2jar classes.dex -o output-file.jar**"



```
Microsoft Windows [Version 10.0.19045.4780]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student\Desktop\CYFI-700 Tools\androidapk\dex2jar-2.0>d2j-dex2jar classes.dex -o output-file.jar
dex2jar classes.dex -> output-file.jar
```

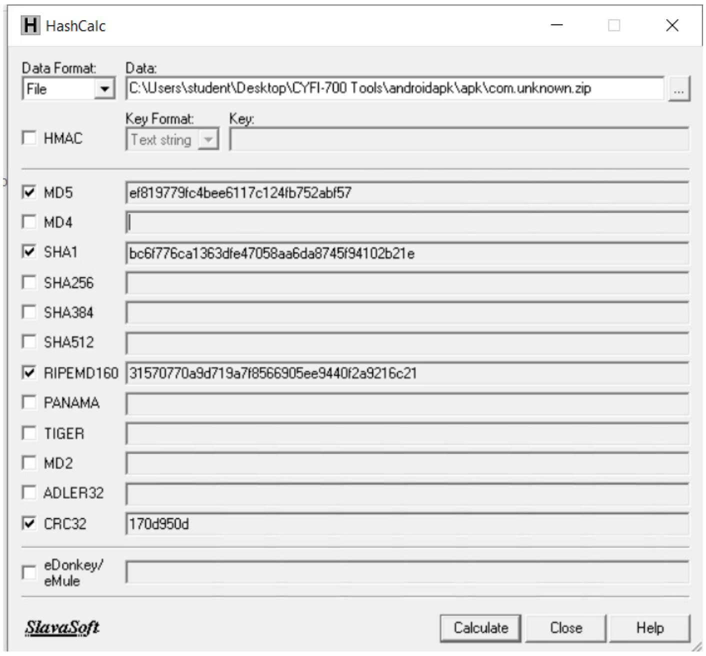
- Launch jd-gui and within jd-gui select "File: and then select "Open" and browse to **output-file.jar**. The file will appear as shown in below figure.



```java
package android.support.v4.os;

import android.os.Build;
import android.os.Environment;
import android.util.Log;
import java.io.File;
import java.io.IOException;

public class EnvironmentCompat {
  public static final String MEDIA_UNKNOWN = "unknown";

  private static final String TAG = "EnvironmentCompat";

  public static String getStorageState(File paramFile) {
    if (Build.VERSION.SDK_INT >= 19)
      return EnvironmentCompatKitKat.getStorageState(paramFile);
    try {
      if (paramFile.getCanonicalPath().startsWith(Environment.getExternalStorageDirectory().getCanonicalPath()))
        return Environment.getExternalStorageState();
    } catch (IOException iOException) {
      Log.w("EnvironmentCompat", "Failed to resolve canonical path: " + iOException);
    }
    return "unknown";
  }
}
```

- Use HashCalc tool to determine the MD5 hash of the .apk file. The MD5 hash value is:

ef819779fc4bee6117c124fb752abf57



Data Format: File

Data: C:\Users\student\Desktop\CYFI-700 Tools\androidapk\apk\com.unknown.zip

□ HMAC   Key Format: Text string   Key:

☑ MD5 ef819779fc4bee6117c124fb752abf57

□ MD4

☑ SHA1 bc6f776ca1363dfe47058aa6da8745f94102b21e

□ SHA256

□ SHA384

□ SHA512

☑ RIPEMD160 31570770a9d719a7f8566905ee9440f2a9216c21

□ PANAMA

□ TIGER

□ MD2

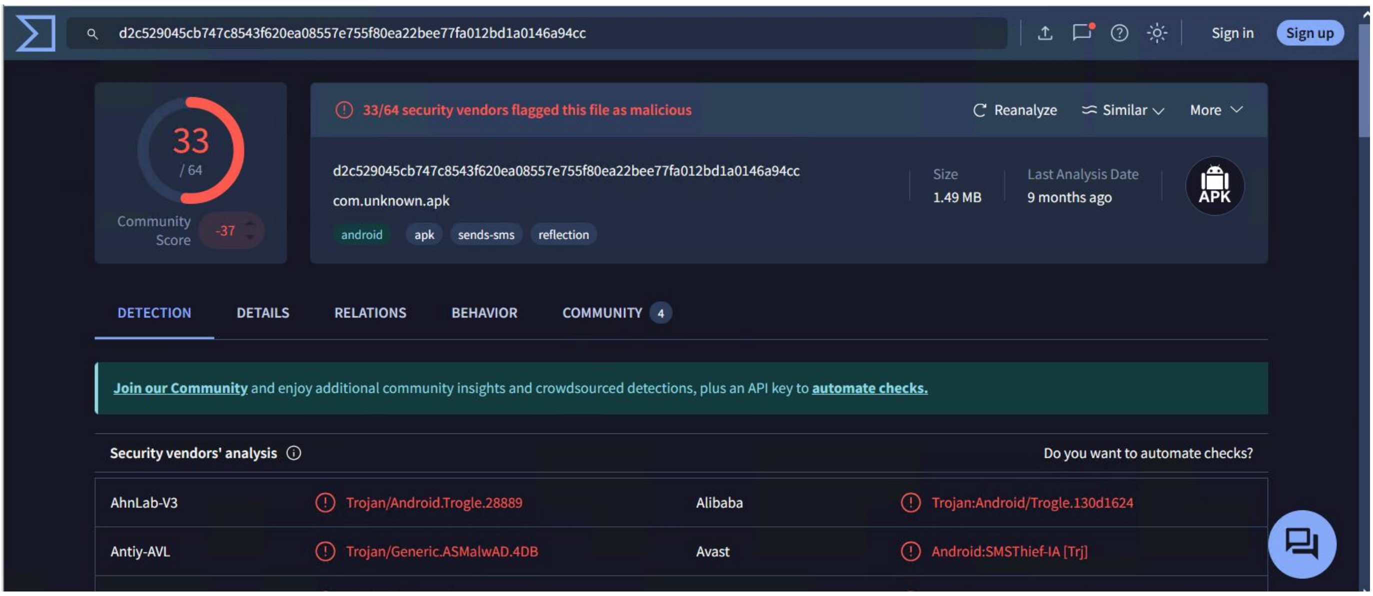
□ ADLER32

☑ CRC32 170d950d

□ eDonkey/ eMule

- Go to **VirusTotal (http://www.virustotal.com).** Click the “Search” tab (not the “Scan It” button). Paste the MD5 hash of the .apk file into the text box and click the “Search It” button.

- What results were returned: Over half of the anti-virus companies identified this as a Trojan or SMS-sender.



d2c529045cb747c8543f620ea08557e755f80ea22bee77fa012bd1a0146a94cc

33 / 64

Community Score -37

33/64 security vendors flagged this file as malicious

d2c529045cb747c8543f620ea08557e755f80ea22bee77fa012bd1a0146a94cc

com.unknown.apk

android apk sends-sms reflection

Size 1.49 MB

Last Analysis Date 9 months ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Android.Trogle.28889	Alibaba	Trojan:Android/Trogle.130d1624
Antiy-AVL	Trojan/Generic.ASMalwAD.4DB	Avast	Android:SMSThief-IA [Trj]