Hunting Malware in Clone Iphone

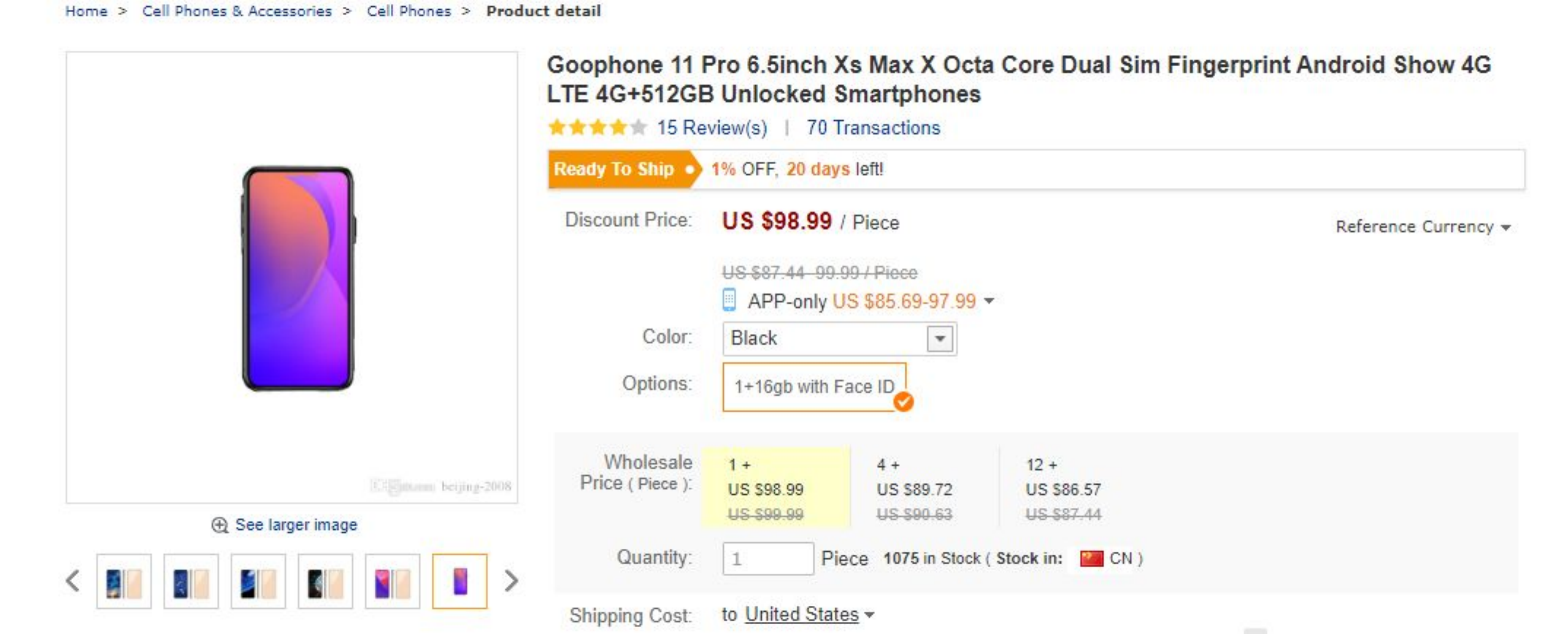
Clone phones doesn’t hurts your health only...

WHOAMI

#! FenriScan

#! Malware.ninja

#! Flag4beer



Home > Cell Phones & Accessories > Cell Phones > Product detail

Goophone 11 Pro 6.5inch Xs Max X Octa Core Dual Sim Fingerprint Android Show 4G LTE 4G+512GB Unlocked Smartphones

★★★★☆ 15 Review(s) | 70 Transactions

Ready To Ship • 1% OFF, 20 days left!

Discount Price: US $98.99 / Piece

Reference Currency

~~US $87.44 - 99.99 / Piece~~

APP-only US $85.69-97.99

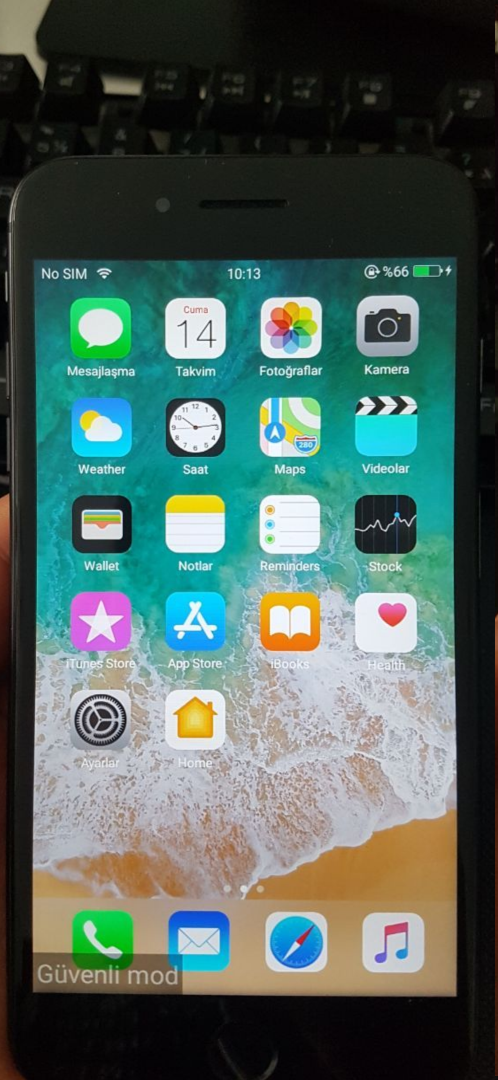
Color: Black

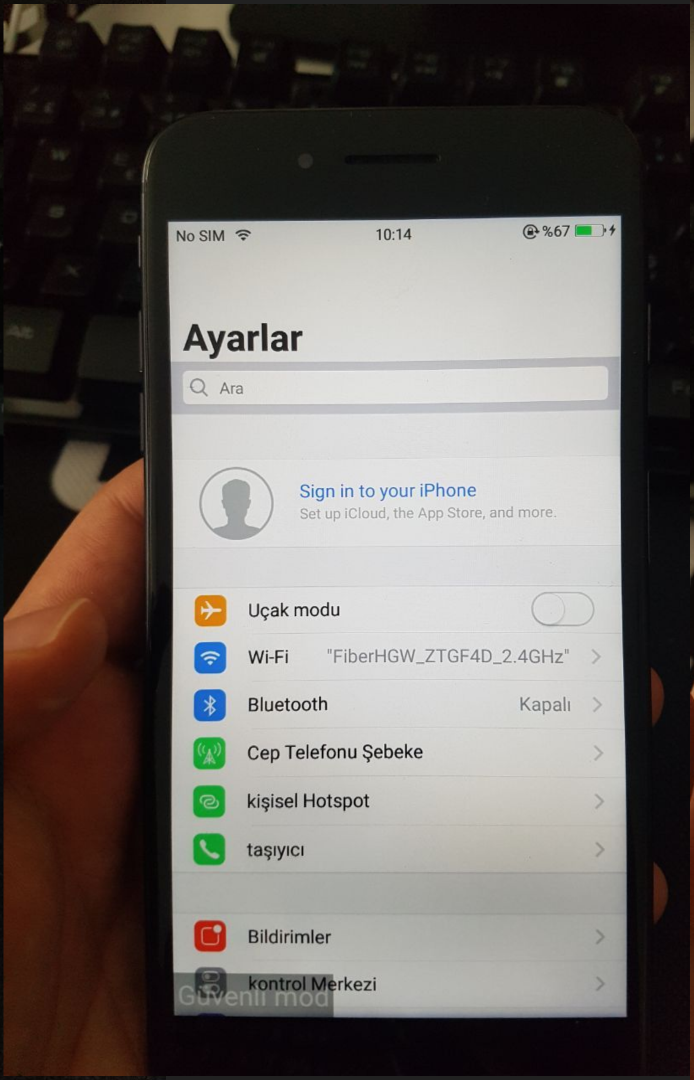
Options: 1+16gb with Face ID ✓

Wholesale Price (Piece):	1 +	4 +	12 +
	US $98.99	US $89.72	US $86.57
	~~US $99.99~~	~~US $90.63~~	~~US $87.44~~

Quantity: 1 Piece 1075 in Stock (**Stock in:** CN)

Shipping Cost: to United States





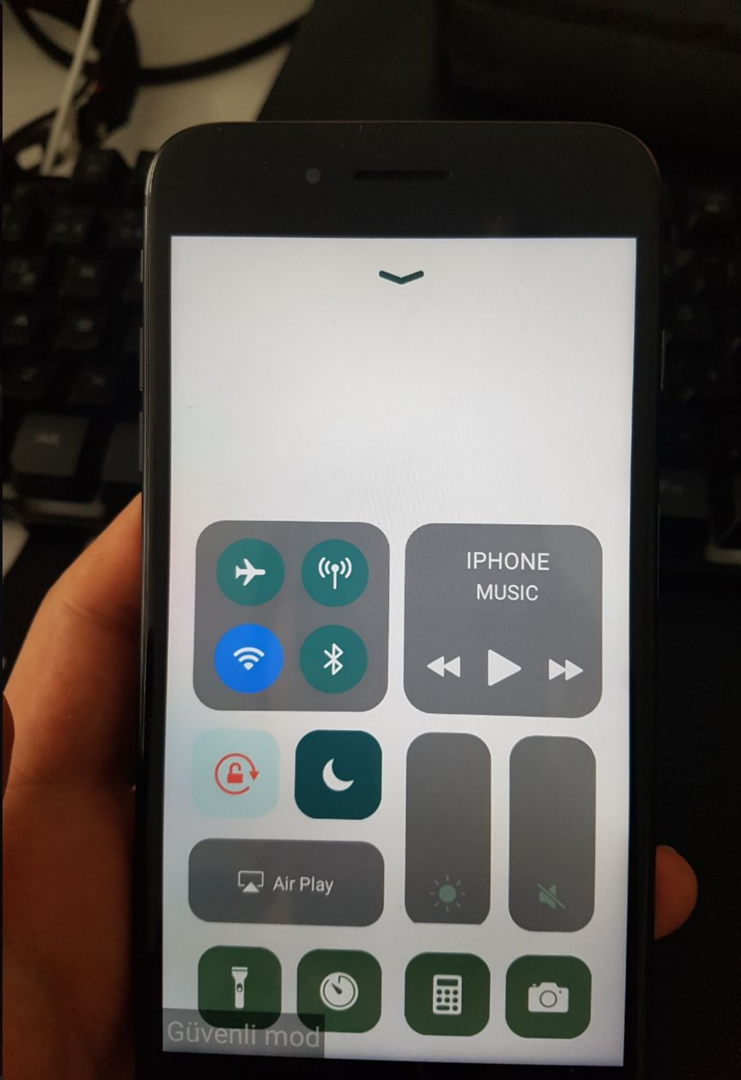
Ayarlar

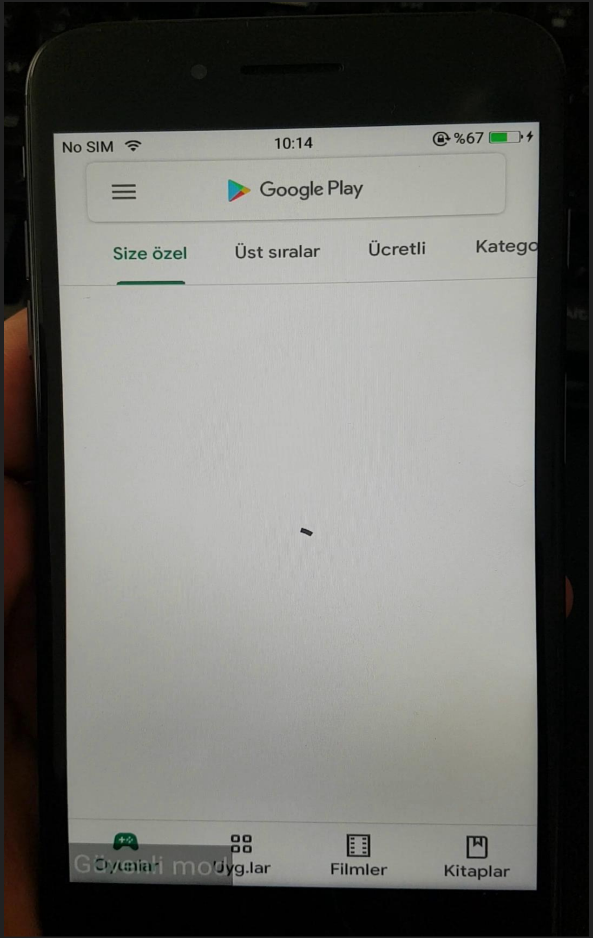
Ara

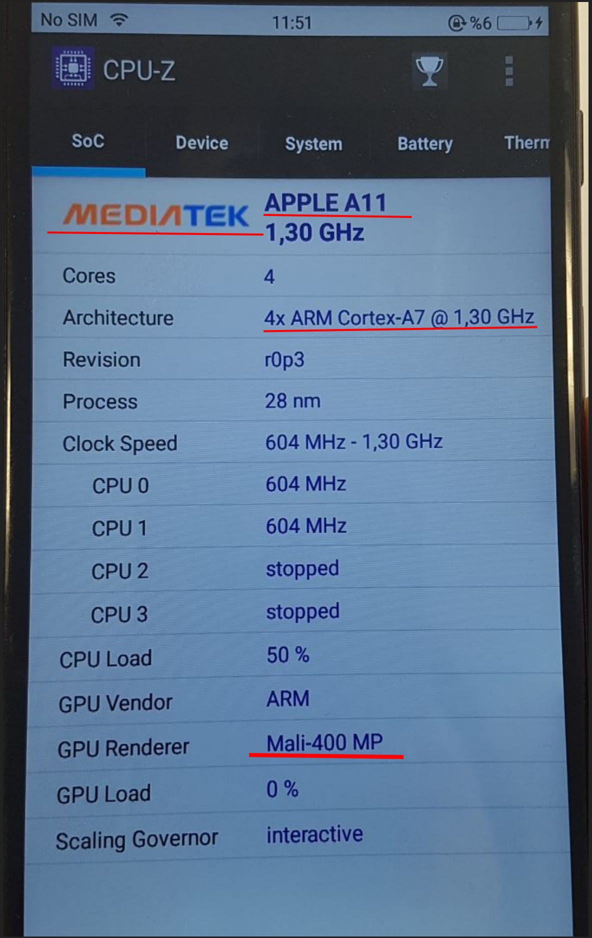
Sign in to your iPhone
Set up iCloud, the App Store, and more.

Uçak modu
Wi-Fi "FiberHGW_ZTGF4D_2.4GHz"
Bluetooth Kapalı
Cep Telefonu Şebeke
kişisel Hotspot
taşıyıcı

Bildirimler
kontrol Merkezi

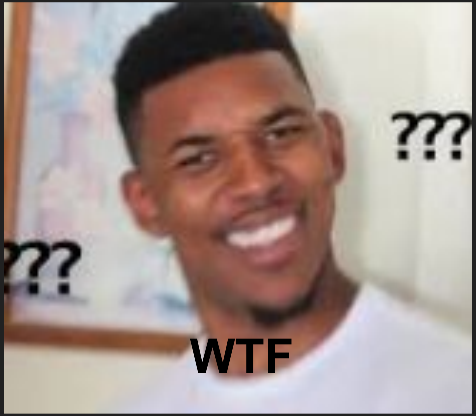




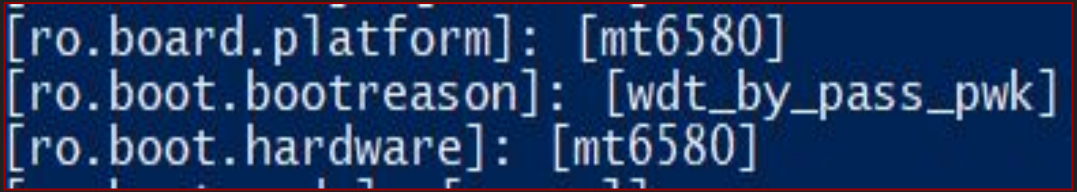


APPLE A11
1,30 GHz

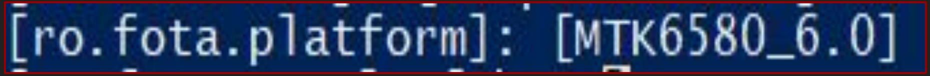
Cores	4
Architecture	4x ARM Cortex-A7 @ 1,30 GHz
Revision	r0p3
Process	28 nm
Clock Speed	604 MHz - 1,30 GHz
CPU 0	604 MHz
CPU 1	604 MHz
CPU 2	stopped
CPU 3	stopped
CPU Load	50 %
GPU Vendor	ARM
GPU Renderer	Mali-400 MP
GPU Load	0 %
Scaling Governor	interactive



```
> adb shell getprop
```



```
[ro.board.platform]: [mt6580]
[ro.boot.bootreason]: [wdt_by_pass_pwk]
[ro.boot.hardware]: [mt6580]
```



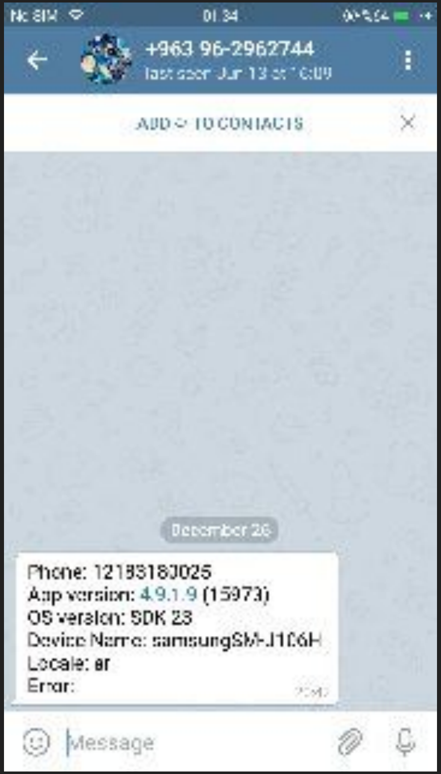
```
[ro.fota.platform]: [MTK6580_6.0]
```

MEDIATEK MT6580 SoC

4x ARM Cortex-A7 MPcore

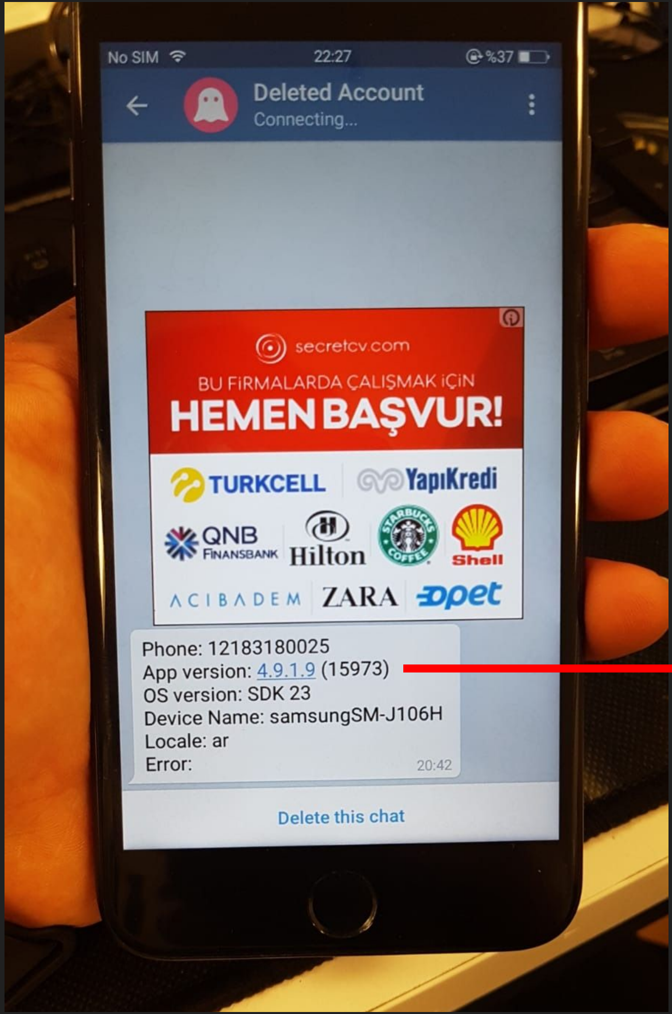
Mali 400 MP GPU

4x ARM Cortex-A7 MPcore



Phone: 12183180025
App version: 4.9.1.9 (15973)
OS version: SDK 23
Device Name: samsungSM-J106H
Locale: ar
Error:

20:42



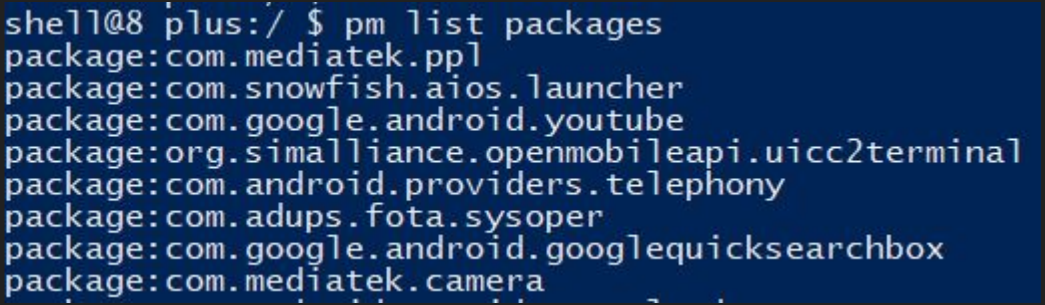
Phone: 12183180025
App version: 4.9.1.9 (15973)
OS version: SDK 23
Device Name: samsungSM-J106H
Locale: ar
Error:

20:42

backdoor app ?

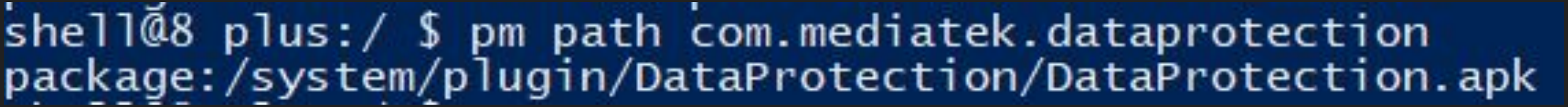
> Adb shell

> pm list packages

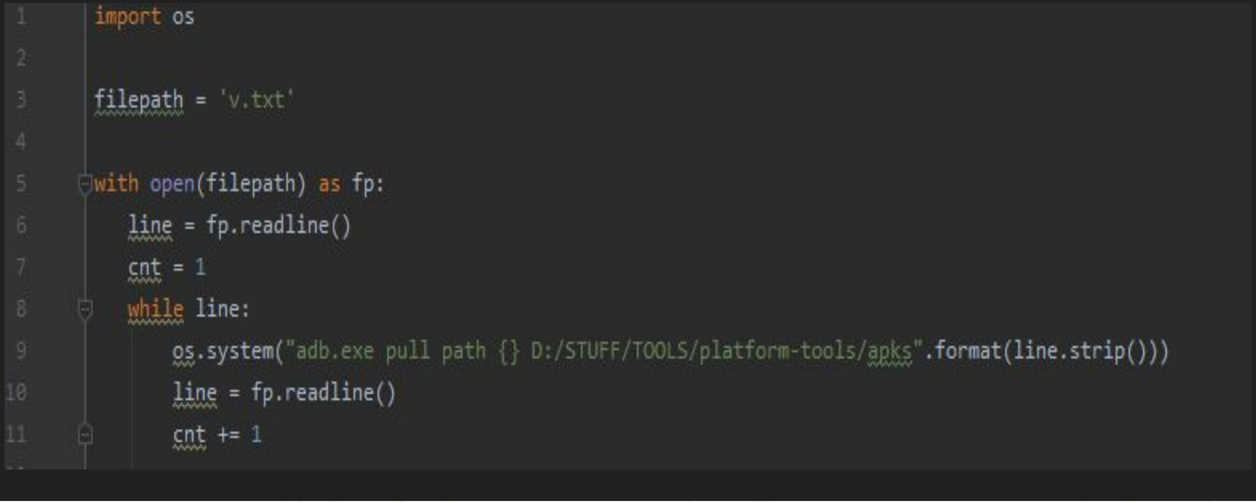


```
shell@8 plus:/ $ pm list packages
package:com.mediatek.ppl
package:com.snowfish.aios.launcher
package:com.google.android.youtube
package:org.simalliance.openmobileapi.uicc2terminal
package:com.android.providers.telephony
package:com.adups.fota.sysoper
package:com.google.android.googlequicksearchbox
package:com.mediatek.camera
```

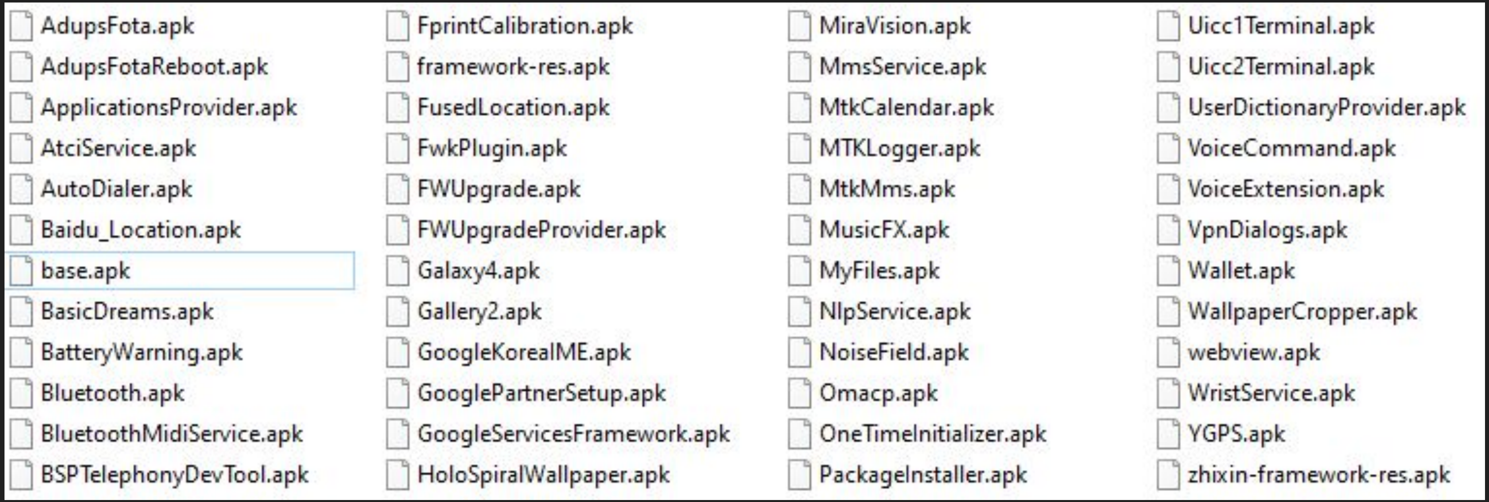
> pm path %package%



```
shell@8 plus:/ $ pm path com.mediatek.dataprotection
package:/system/plugin/DataProtection/DataProtection.apk
```

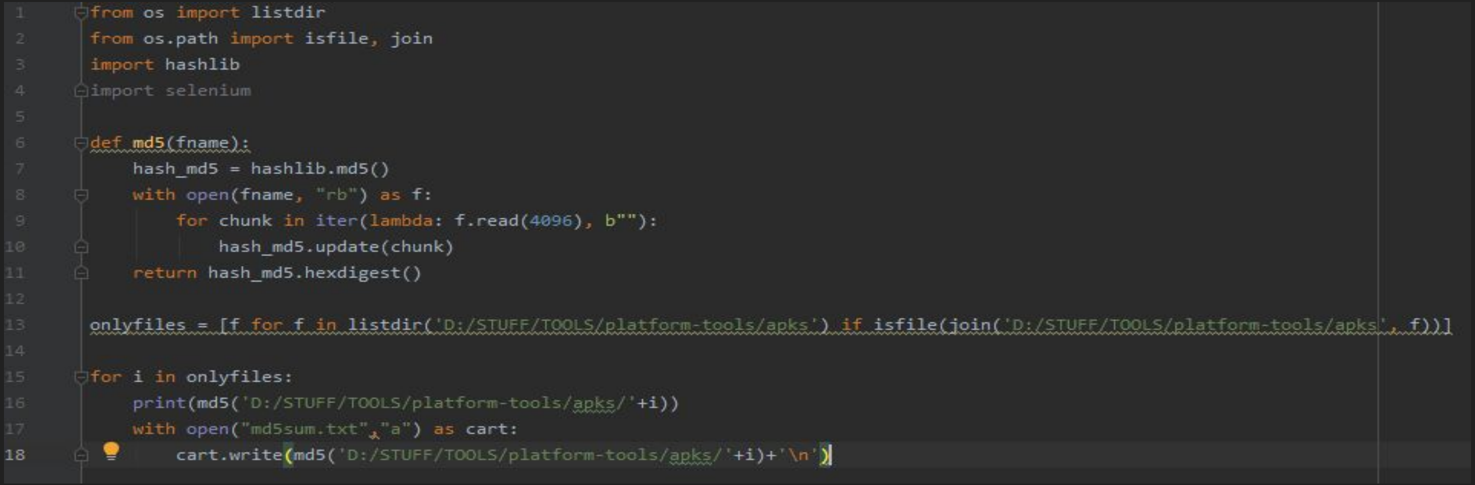


```python
import os

filepath = 'v.txt'

with open(filepath) as fp:
    line = fp.readline()
    cnt = 1
    while line:
        os.system("adb.exe pull path {} D:/STUFF/TOOLS/platform-tools/apks".format(line.strip()))
        line = fp.readline()
        cnt += 1
```

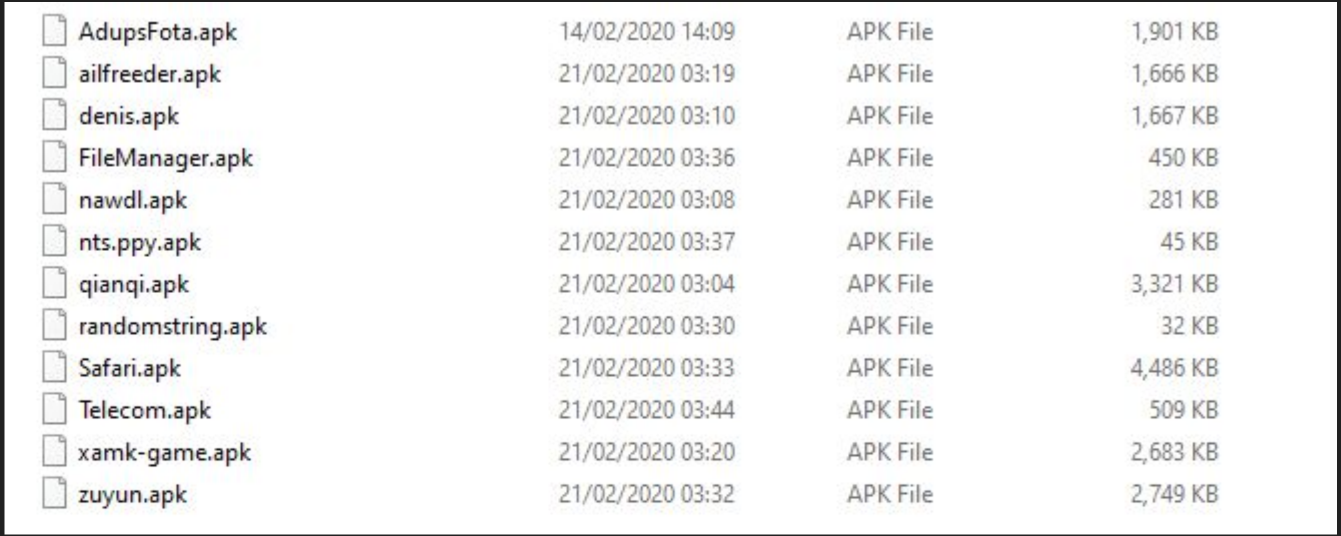


```
AdupsFota.apk
AdupsFotaReboot.apk
ApplicationsProvider.apk
AtciService.apk
AutoDialer.apk
Baidu_Location.apk
base.apk
BasicDreams.apk
BatteryWarning.apk
Bluetooth.apk
BluetoothMidiService.apk
BSPTelephonyDevTool.apk
FprintCalibration.apk
framework-res.apk
FusedLocation.apk
FwkPlugin.apk
FWUpgrade.apk
FWUpgradeProvider.apk
Galaxy4.apk
Gallery2.apk
GoogleKoreaIME.apk
GooglePartnerSetup.apk
GoogleServicesFramework.apk
HoloSpiralWallpaper.apk
MiraVision.apk
MmsService.apk
MtkCalendar.apk
MTKLogger.apk
MtkMms.apk
MusicFX.apk
MyFiles.apk
NlpService.apk
NoiseField.apk
Omacp.apk
OneTimeInitializer.apk
PackageInstaller.apk
Uicc1Terminal.apk
Uicc2Terminal.apk
UserDictionaryProvider.apk
VoiceCommand.apk
VoiceExtension.apk
VpnDialogs.apk
Wallet.apk
WallpaperCropper.apk
webview.apk
WristService.apk
YGPS.apk
zhixin-framework-res.apk
```

HASH DUMP



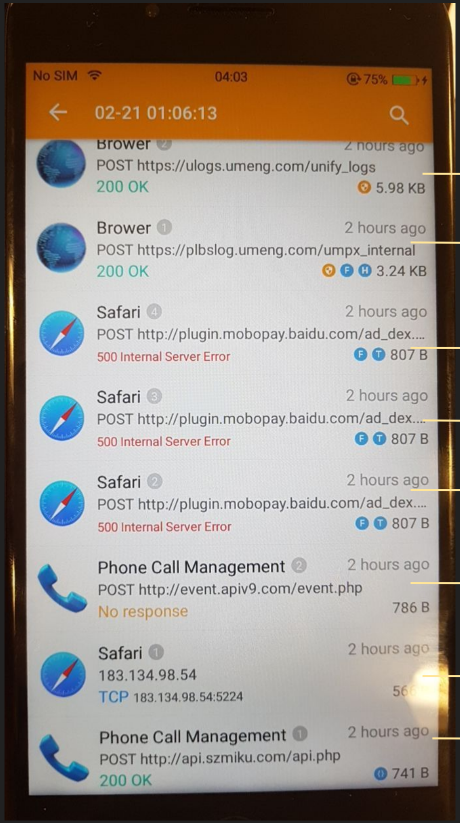
```python
from os import listdir
from os.path import isfile, join
import hashlib
import selenium

def md5(fname):
    hash_md5 = hashlib.md5()
    with open(fname, "rb") as f:
        for chunk in iter(lambda: f.read(4096), b""):
            hash_md5.update(chunk)
    return hash_md5.hexdigest()

onlyfiles = [f for f in listdir('D:/STUFF/TOOLS/platform-tools/apks') if isfile(join('D:/STUFF/TOOLS/platform-tools/apks', f))]

for i in onlyfiles:
    print(md5('D:/STUFF/TOOLS/platform-tools/apks/'+i))
    with open("md5sum.txt","a") as cart:
        cart.write(md5('D:/STUFF/TOOLS/platform-tools/apks/'+i)+'\n')
```



AdupsFota.apk	14/02/2020 14:09	APK File	1,901 KB
ailfreeder.apk	21/02/2020 03:19	APK File	1,666 KB
denis.apk	21/02/2020 03:10	APK File	1,667 KB
FileManager.apk	21/02/2020 03:36	APK File	450 KB
nawdl.apk	21/02/2020 03:08	APK File	281 KB
nts.ppy.apk	21/02/2020 03:37	APK File	45 KB
qianqi.apk	21/02/2020 03:04	APK File	3,321 KB
randomstring.apk	21/02/2020 03:30	APK File	32 KB
Safari.apk	21/02/2020 03:33	APK File	4,486 KB
Telecom.apk	21/02/2020 03:44	APK File	509 KB
xamk-game.apk	21/02/2020 03:20	APK File	2,683 KB
zuyun.apk	21/02/2020 03:32	APK File	2,749 KB

TO STATIC CODE ANALYSIS

NOW TIME SNIFF NETWORK ;)



No SIM 04:03 75%

02-21 01:06:13

Brower 2 2 hours ago
POST https://ulogs.umeng.com/unify_logs
200 OK 5.98 KB

Brower 1 2 hours ago
POST https://plbslog.umeng.com/umpx_internal
200 OK F H 3.24 KB

Safari 4 2 hours ago
POST http://plugin.mobopay.baidu.com/ad_dex....
500 Internal Server Error F T 807 B

Safari 3 2 hours ago
POST http://plugin.mobopay.baidu.com/ad_dex....
500 Internal Server Error F T 807 B

Safari 2 2 hours ago
POST http://plugin.mobopay.baidu.com/ad_dex....
500 Internal Server Error F T 807 B

Phone Call Management 2 2 hours ago
POST http://event.apiv9.com/event.php
No response 786 B

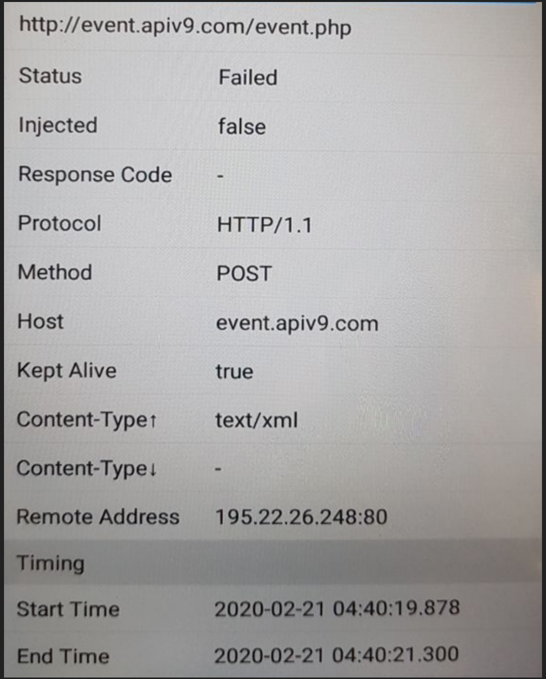
Safari 1 2 hours ago
183.134.98.54
TCP 183.134.98.54:5224 56

Phone Call Management 1 2 hours ago
POST http://api.szmiku.com/api.php
200 OK 741 B

TOOL : HTTPCANARY

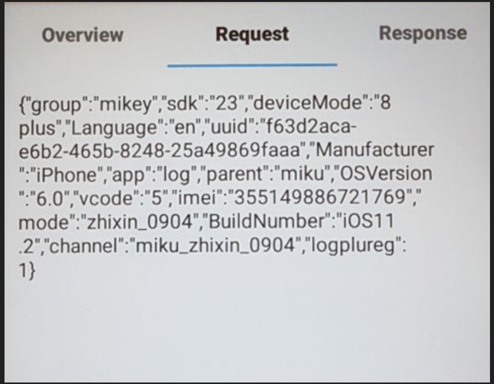
WE'VE GOT SOME WEIRD TRAFFIC

EXAMPLE REQUEST

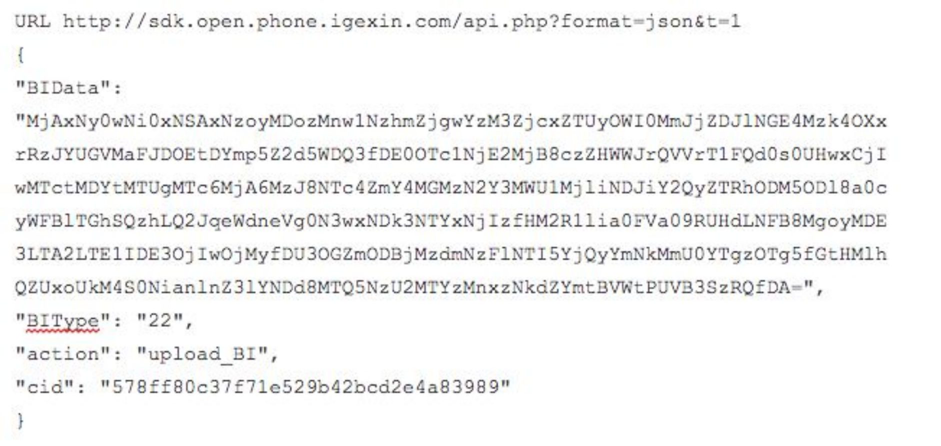


http://event.apiv9.com/event.php

Status	Failed
Injected	false
Response Code	-
Protocol	HTTP/1.1
Method	POST
Host	event.apiv9.com
Kept Alive	true
Content-Type↑	text/xml
Content-Type↓	-
Remote Address	195.22.26.248:80
Timing	
Start Time	2020-02-21 04:40:19.878
End Time	2020-02-21 04:40:21.300



```
{"group":"mikey","sdk":"23","deviceMode":"8
plus","Language":"en","uuid":"f63d2aca-
e6b2-465b-8248-25a49869faaa","Manufacturer
":"iPhone","app":"log","parent":"miku","OSVersion
":"6.0","vcode":"5","imei":"355149886721769","
mode":"zhixin_0904","BuildNumber":"iOS11
.2","channel":"miku_zhixin_0904","logplureg":
1}
```



URL http://sdk.open.phone.igexin.com/api.php?format=json&t=1

```
{
"BIData":
"MjAxNy0wNi0xNSAxNzoyMDozMnw1NzhmZjgwYzM3ZjcxZTUyOWI0MmJjZDJlNGE4Mzk4OXx
rRzJYUGVMaFJDOEtDYmp5Z2d5WDQ3fDE0OTc1NjE2MjB8czZHWWJrQVVrT1FQd0s0UHwxCjI
wMTctMDYtMTUgMTc6MjA6MzJ8NTc4ZmY4MGMzN2Y3MWU1MjliNDJiY2QyZTRhODM5ODl8a0c
yWFBlTGhSQzhLQ2JqeWdneVg0N3wxNDk3NTYxNjIzfHM2R1lia0FVa09RUHdLNFB8MgoyMDE
3LTA2LTE1IDE3OjIwOjMyfDU3OGZmODBjMzdmNzFlNTI5YjQyYmNkMmU0YTgzOTg5fGtHMlh
QZUxoUkM4S0NianlnZ3lYNDd8MTQ5NzU2MTYzMnxzNkdZYmtBVWtPUVB3SzRQfDA=",
"BIType": "22",
"action": "upload_BI",
"cid": "578ff80c37f71e529b42bcd2e4a83989"
}
```

http://sdk.open.lbs.igexin.com/api.htm

http://sdk.open.amp.igexin.com/

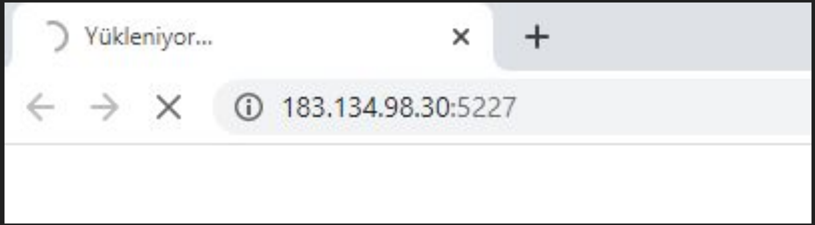
http://d.gt.igexin.com/api.htm

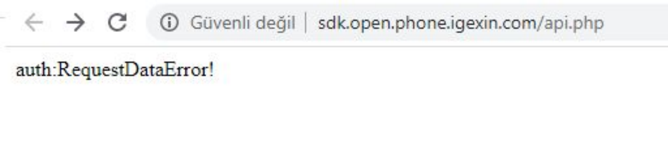
http://s-gt.getui.com/api.php

http://c-hzgt2.getui.com/

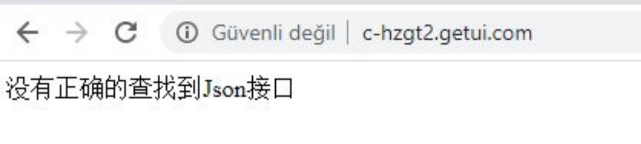
http://sdk.open.phone.igexin.com/api.php

http://sj54.nnmwm.com:90//upload/google_c.action

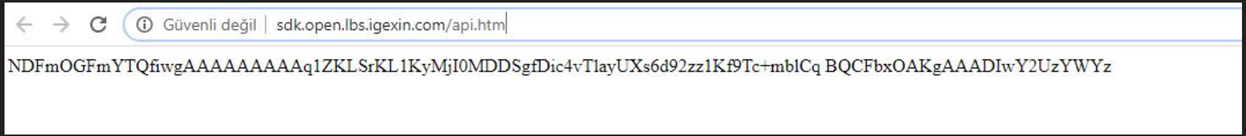




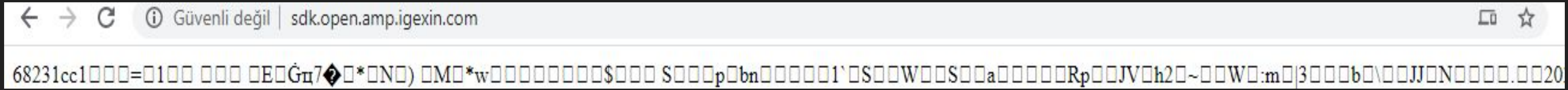
auth:RequestDataError!



没有正确的查找到Json接口



NDFmOGFmYTQfiwgAAAAAAAAAq1ZKLSrKL1KyMjI0MDDSgfDic4vTlayUXs6d92zz1Kf9Tc+mblCq BQCFbxOAKgAAADIwY2UzYWYz



```
68231cc1□□□=□1□□ □□□ □E□Ġπ7�□*□N□) □M□*w□□□□□□□□$□□□ S□□□p□bn□□□□□1`□S□□W□□S□□a□□□□□Rp□□JV□h2□~□□W□:m□|3□□□b□\□□JJ□N□□□□.□□20
```

Igexin SDK **(software development kit)** ?

Not all igexin sdk versions has malicious functionality

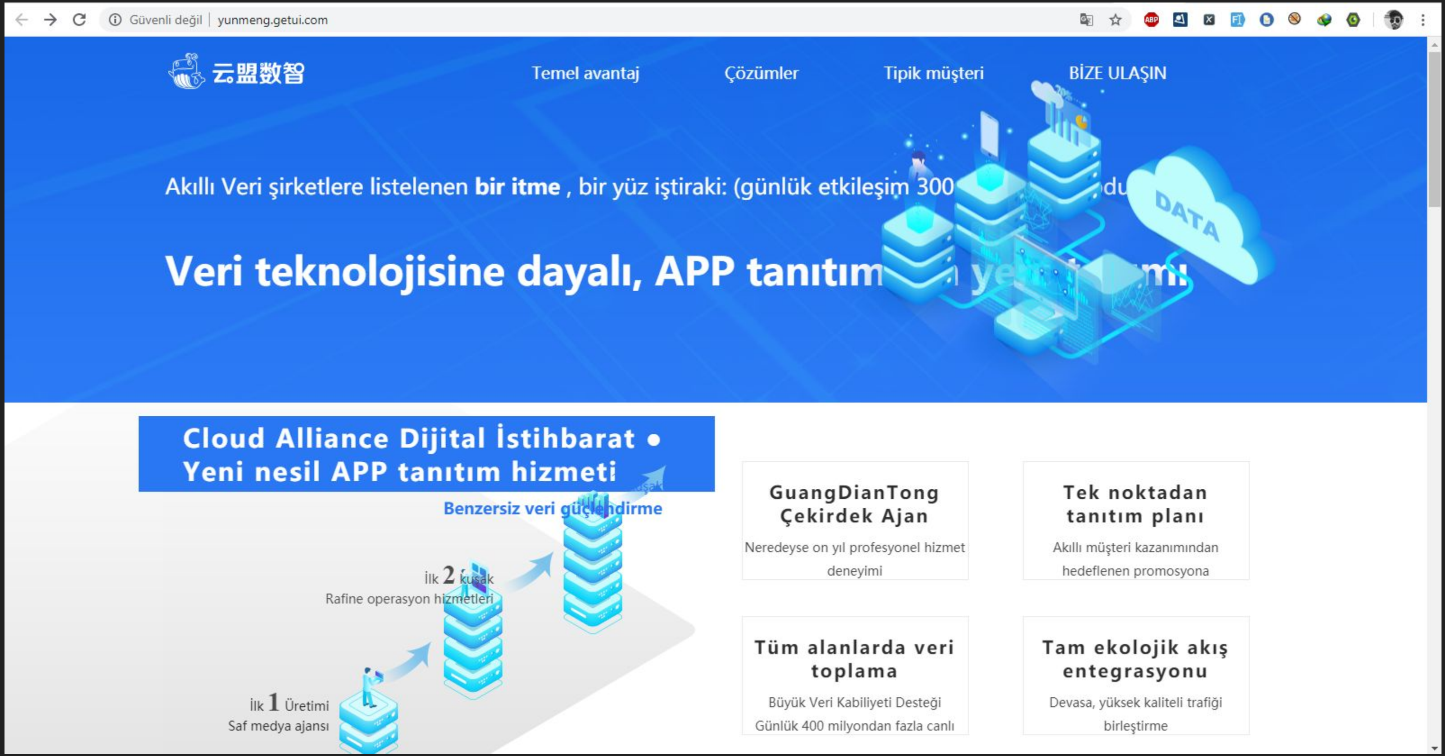
http: // sdk [.] Open [.] Phone [.] İgexin [.] com / api.php

ADVERTISING SDK

data collected about people such as their interests, occupation, income, and location.

http://c-hzgt2.getui.com/

http://s-gt.getui.com/api.php



Akıllı Veri şirketlere listelenen **bir itme** , bir yüz iştiraki: (günlük etkileşim 300 du

Veri teknolojisine dayalı, APP tanıtım n ye mı

Cloud Alliance Dijital İstihbarat •
Yeni nesil APP tanıtım hizmeti

Benzersiz veri güçlendirme

İlk 2 kuşak
Rafine operasyon hizmetleri

İlk 1 Üretimi
Saf medya ajansı

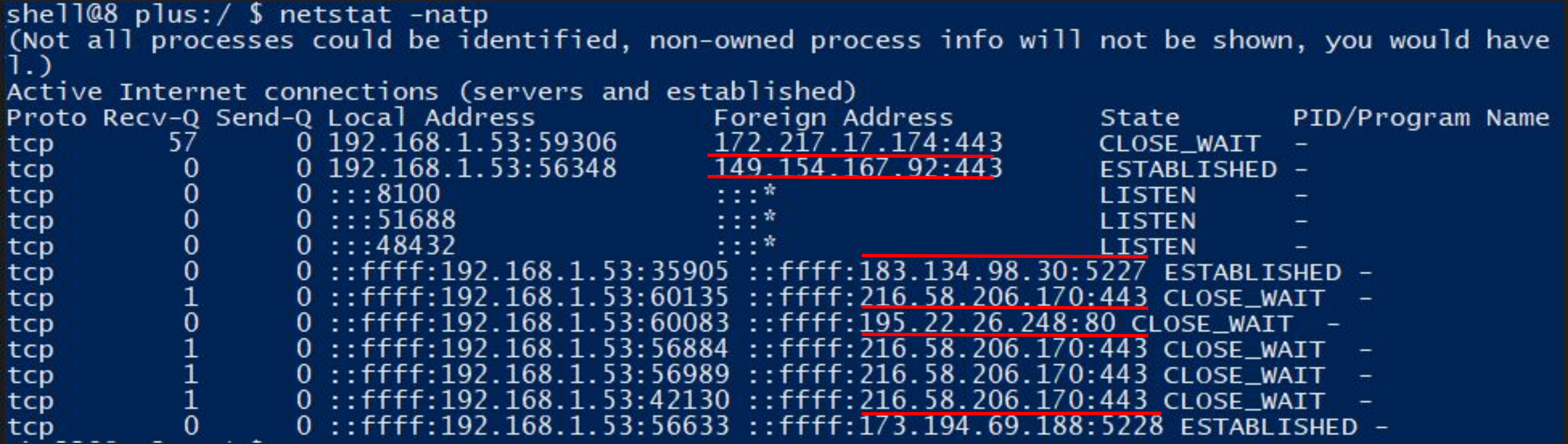
GuangDianTong Çekirdek Ajan
Neredeyse on yıl profesyonel hizmet deneyimi

Tek noktadan tanıtım planı
Akıllı müşteri kazanımından hedeflenen promosyona

Tüm alanlarda veri toplama
Büyük Veri Kabiliyeti Desteği
Günlük 400 milyondan fazla canlı

Tam ekolojik akış entegrasyonu
Devasa, yüksek kaliteli trafiği birleştirme

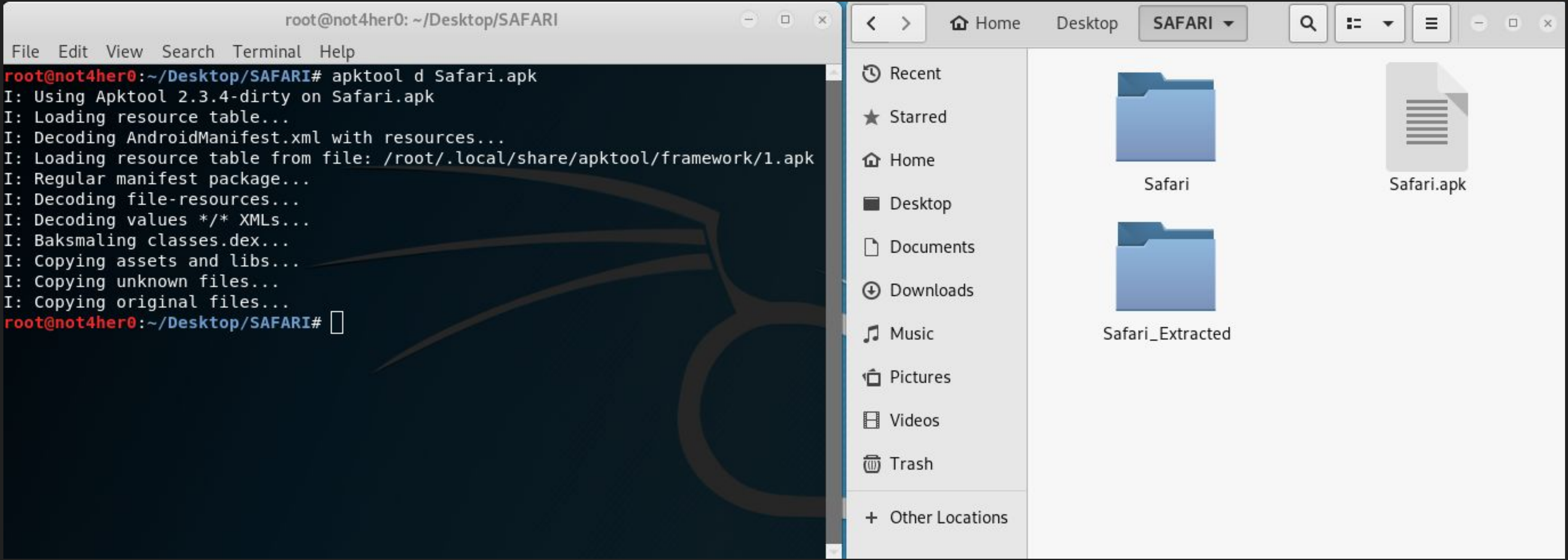
Connections



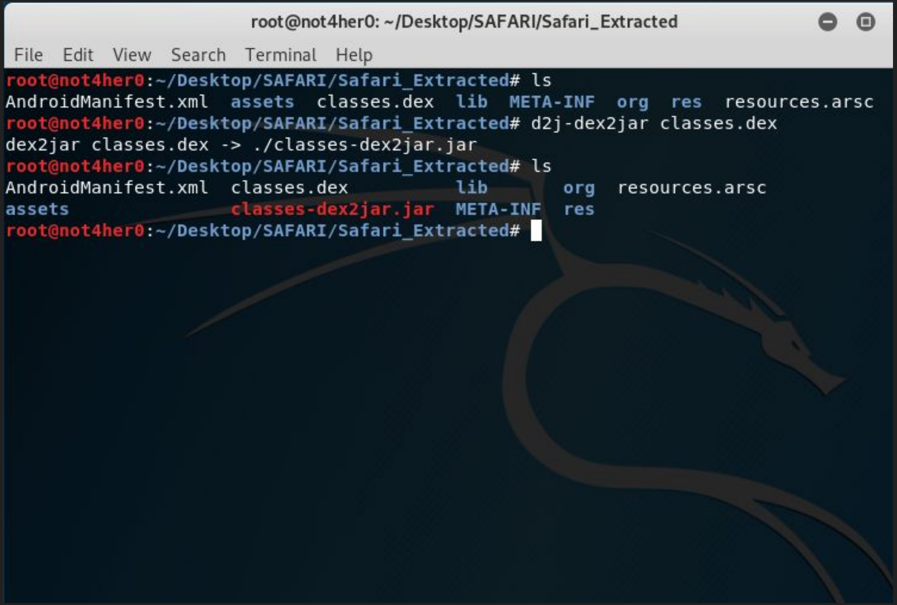
```
shell@8 plus:/ $ netstat -natp
(Not all processes could be identified, non-owned process info will not be shown, you would have
l.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program Name
tcp       57      0 192.168.1.53:59306      172.217.17.174:443      CLOSE_WAIT  -
tcp        0      0 192.168.1.53:56348      149.154.167.92:443      ESTABLISHED -
tcp        0      0 :::8100                 :::*                    LISTEN      -
tcp        0      0 :::51688                :::*                    LISTEN      -
tcp        0      0 :::48432                :::*                    LISTEN      -
tcp        0      0 ::ffff:192.168.1.53:35905 ::ffff:183.134.98.30:5227 ESTABLISHED -
tcp        1      0 ::ffff:192.168.1.53:60135 ::ffff:216.58.206.170:443 CLOSE_WAIT  -
tcp        0      0 ::ffff:192.168.1.53:60083 ::ffff:195.22.26.248:80 CLOSE_WAIT  -
tcp        1      0 ::ffff:192.168.1.53:56884 ::ffff:216.58.206.170:443 CLOSE_WAIT  -
tcp        1      0 ::ffff:192.168.1.53:56989 ::ffff:216.58.206.170:443 CLOSE_WAIT  -
tcp        1      0 ::ffff:192.168.1.53:42130 ::ffff:216.58.206.170:443 CLOSE_WAIT  -
tcp        0      0 ::ffff:192.168.1.53:56633 ::ffff:173.194.69.188:5228 ESTABLISHED -
```

172.217.17.174 : 443 -> google
149.154.167.92 : 443 -> telegram
183.134.98.30 : 5227 -> cm-10-39.igexin.com
195.22.26.248 : 80 -> CnC Server TCP group 61
173.194.69.188 : 5228 -> google
183.131.24.149 : 5226 -> cm-10-47.igexin.com
183.134.98.101 : 5224 -> talk.nz.igexin.com

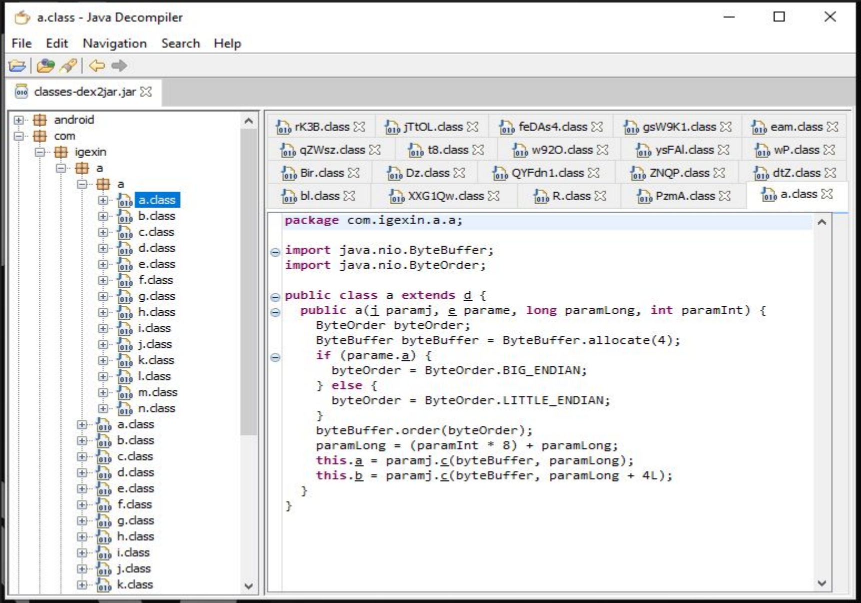
SAFARI BROWSER STATIC CODE ANALYSIS



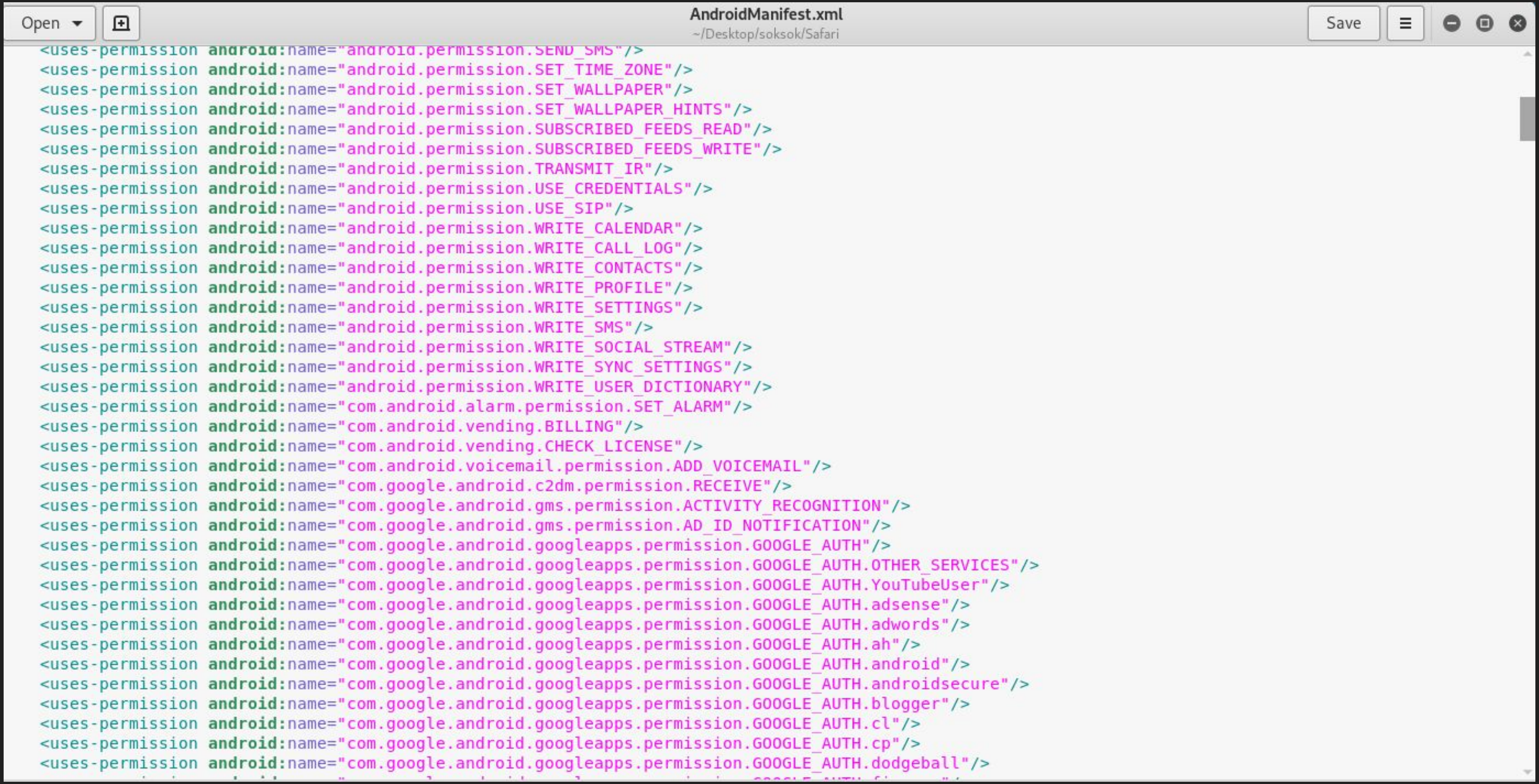
```
root@not4her0:~/Desktop/SAFARI# apktool d Safari.apk
I: Using Apktool 2.3.4-dirty on Safari.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
root@not4her0:~/Desktop/SAFARI# 
```


root@not4her0: ~/Desktop/SAFARI/Safari_Extracted
File Edit View Search Terminal Help

```
root@not4her0:~/Desktop/SAFARI/Safari_Extracted# ls
AndroidManifest.xml  assets  classes.dex  lib  META-INF  org  res  resources.arsc
root@not4her0:~/Desktop/SAFARI/Safari_Extracted# d2j-dex2jar classes.dex
dex2jar classes.dex -> ./classes-dex2jar.jar
root@not4her0:~/Desktop/SAFARI/Safari_Extracted# ls
AndroidManifest.xml  classes.dex          lib       org  resources.arsc
assets               classes-dex2jar.jar  META-INF  res
root@not4her0:~/Desktop/SAFARI/Safari_Extracted# 
```

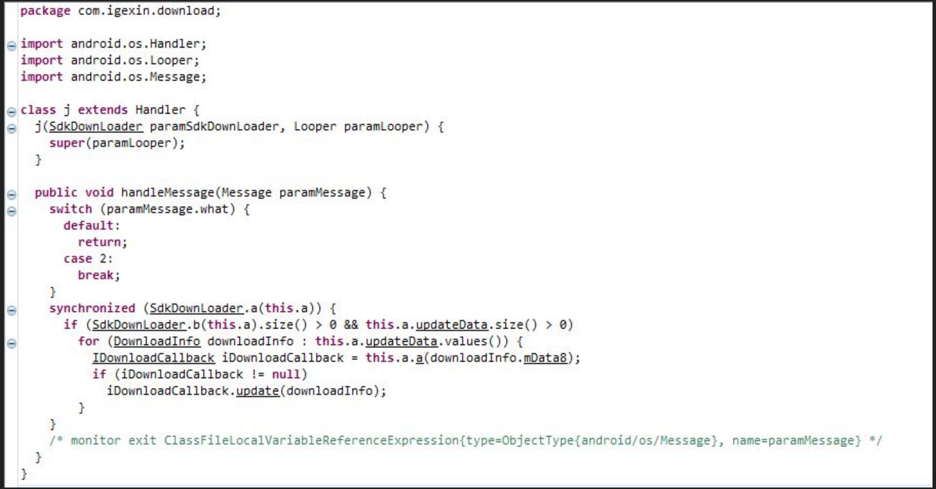


```java
package com.igexin.a.a;

import java.nio.ByteBuffer;
import java.nio.ByteOrder;

public class a extends d {
  public a(j paramj, e parame, long paramLong, int paramInt) {
    ByteOrder byteOrder;
    ByteBuffer byteBuffer = ByteBuffer.allocate(4);
    if (parame.a) {
      byteOrder = ByteOrder.BIG_ENDIAN;
    } else {
      byteOrder = ByteOrder.LITTLE_ENDIAN;
    }
    byteBuffer.order(byteOrder);
    paramLong = (paramInt * 8) + paramLong;
    this.a = paramj.c(byteBuffer, paramLong);
    this.b = paramj.c(byteBuffer, paramLong + 4L);
  }
}
```

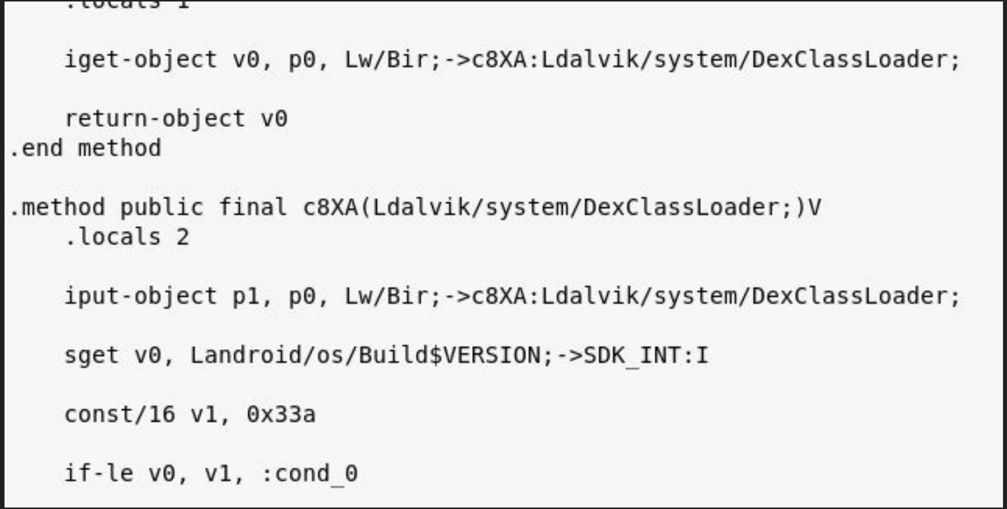


Open
AndroidManifest.xml
~/Desktop/soksok/Safari
Save

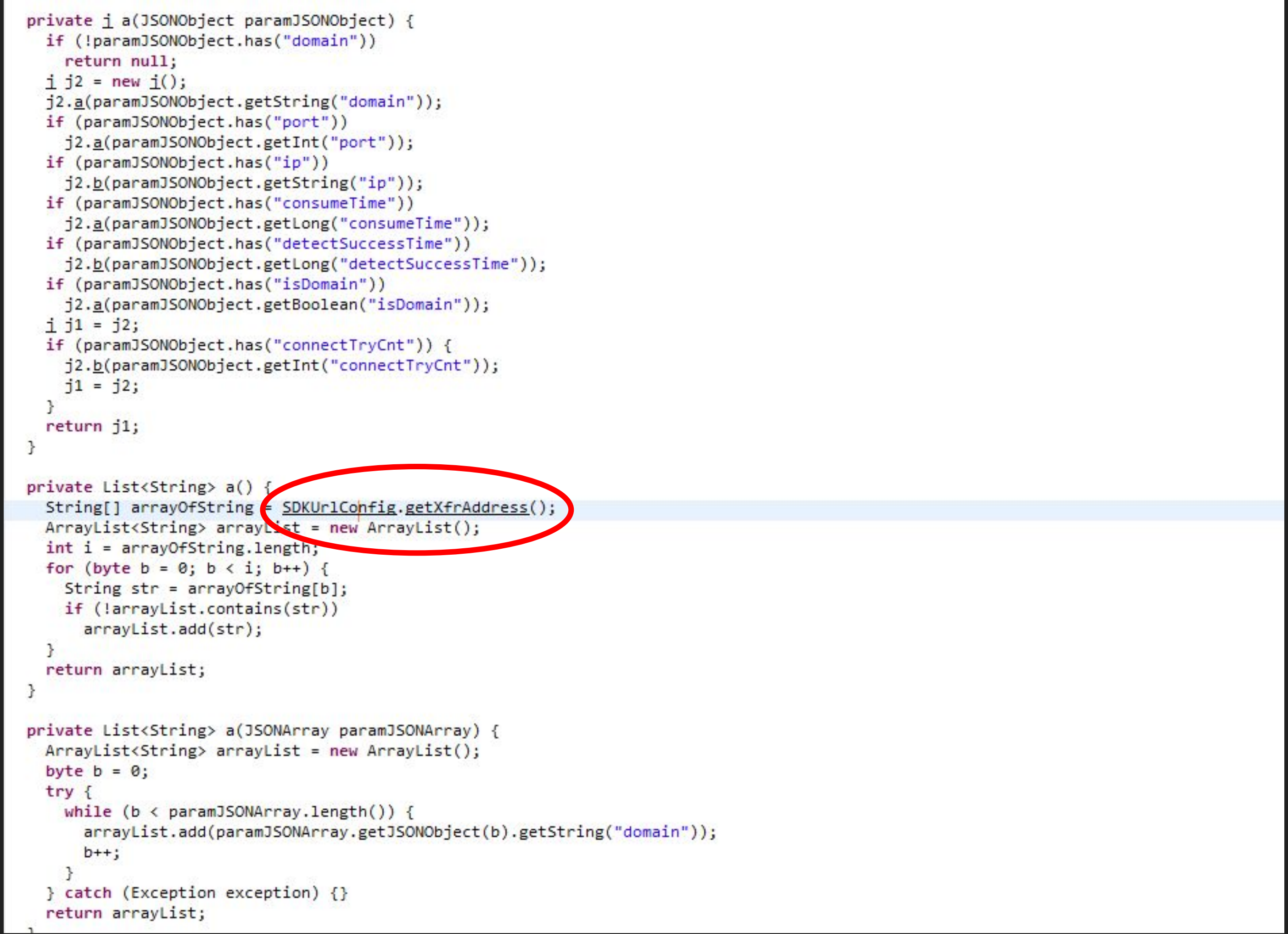
```
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-permission android:name="android.permission.SET_TIME_ZONE"/>
    <uses-permission android:name="android.permission.SET_WALLPAPER"/>
    <uses-permission android:name="android.permission.SET_WALLPAPER_HINTS"/>
    <uses-permission android:name="android.permission.SUBSCRIBED_FEEDS_READ"/>
    <uses-permission android:name="android.permission.SUBSCRIBED_FEEDS_WRITE"/>
    <uses-permission android:name="android.permission.TRANSMIT_IR"/>
    <uses-permission android:name="android.permission.USE_CREDENTIALS"/>
    <uses-permission android:name="android.permission.USE_SIP"/>
    <uses-permission android:name="android.permission.WRITE_CALENDAR"/>
    <uses-permission android:name="android.permission.WRITE_CALL_LOG"/>
    <uses-permission android:name="android.permission.WRITE_CONTACTS"/>
    <uses-permission android:name="android.permission.WRITE_PROFILE"/>
    <uses-permission android:name="android.permission.WRITE_SETTINGS"/>
    <uses-permission android:name="android.permission.WRITE_SMS"/>
    <uses-permission android:name="android.permission.WRITE_SOCIAL_STREAM"/>
    <uses-permission android:name="android.permission.WRITE_SYNC_SETTINGS"/>
    <uses-permission android:name="android.permission.WRITE_USER_DICTIONARY"/>
    <uses-permission android:name="com.android.alarm.permission.SET_ALARM"/>
    <uses-permission android:name="com.android.vending.BILLING"/>
    <uses-permission android:name="com.android.vending.CHECK_LICENSE"/>
    <uses-permission android:name="com.android.voicemail.permission.ADD_VOICEMAIL"/>
    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
    <uses-permission android:name="com.google.android.gms.permission.ACTIVITY_RECOGNITION"/>
    <uses-permission android:name="com.google.android.gms.permission.AD_ID_NOTIFICATION"/>
    <uses-permission android:name="com.google.android.googleapps.permission.GOOGLE_AUTH"/>
    <uses-permission android:name="com.google.android.googleapps.permission.GOOGLE_AUTH.OTHER_SERVICES"/>
    <uses-permission android:name="com.google.android.googleapps.permission.GOOGLE_AUTH.YouTubeUser"/>
    <uses-permission android:name="com.google.android.googleapps.permission.GOOGLE_AUTH.adsense"/>
    <uses-permission android:name="com.google.android.googleapps.permission.GOOGLE_AUTH.adwords"/>
    <uses-permission android:name="com.google.android.googleapps.permission.GOOGLE_AUTH.ah"/>
    <uses-permission android:name="com.google.android.googleapps.permission.GOOGLE_AUTH.android"/>
    <uses-permission android:name="com.google.android.googleapps.permission.GOOGLE_AUTH.androidsecure"/>
    <uses-permission android:name="com.google.android.googleapps.permission.GOOGLE_AUTH.blogger"/>
    <uses-permission android:name="com.google.android.googleapps.permission.GOOGLE_AUTH.cl"/>
    <uses-permission android:name="com.google.android.googleapps.permission.GOOGLE_AUTH.cp"/>
    <uses-permission android:name="com.google.android.googleapps.permission.GOOGLE_AUTH.dodgeball"/>
```



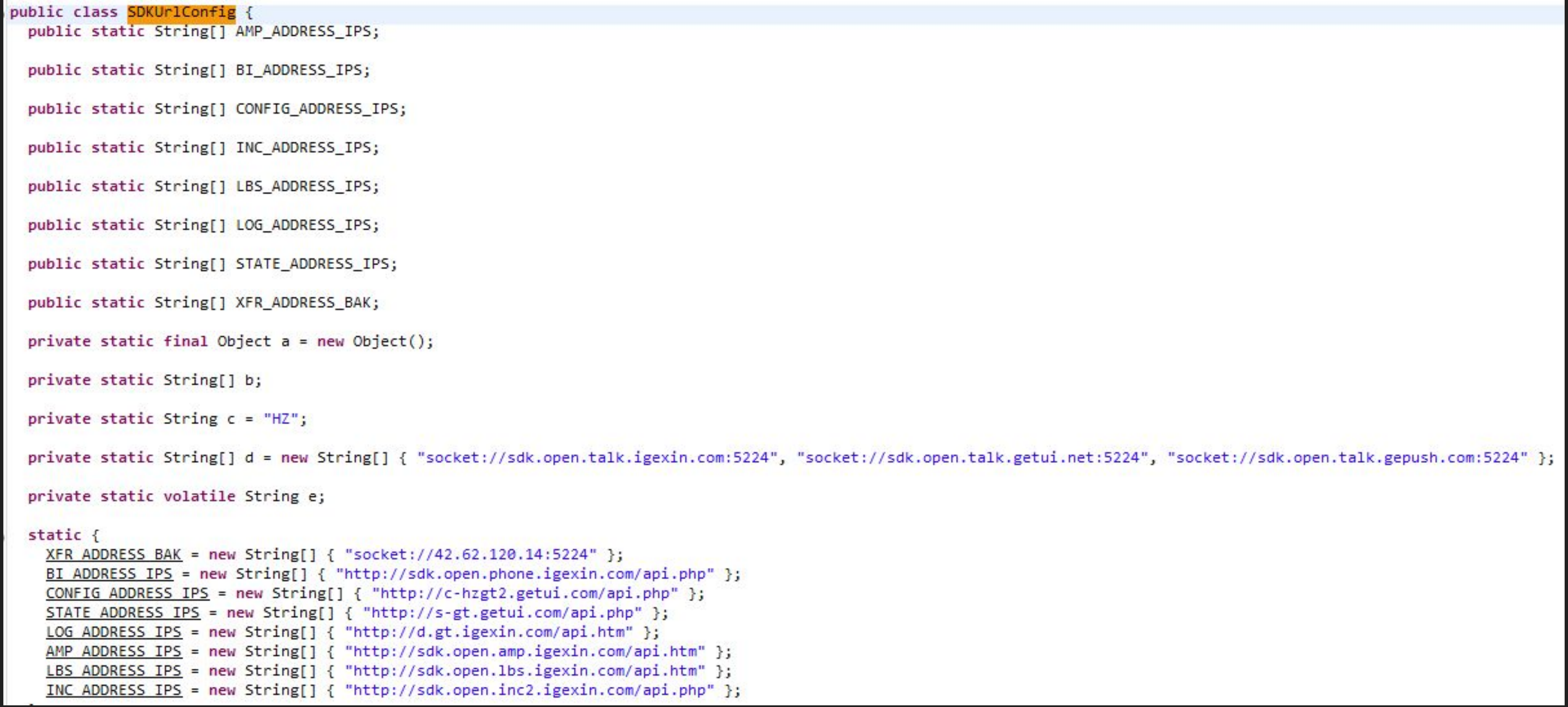
```java
package com.igexin.download;

import android.os.Handler;
import android.os.Looper;
import android.os.Message;

class j extends Handler {
  j(SdkDownLoader paramSdkDownLoader, Looper paramLooper) {
    super(paramLooper);
  }

  public void handleMessage(Message paramMessage) {
    switch (paramMessage.what) {
      default:
        return;
      case 2:
        break;
    }
    synchronized (SdkDownLoader.a(this.a)) {
      if (SdkDownLoader.b(this.a).size() > 0 && this.a.updateData.size() > 0)
        for (DownloadInfo downloadInfo : this.a.updateData.values()) {
          IDownloadCallback iDownloadCallback = this.a.a(downloadInfo.mData8);
          if (iDownloadCallback != null)
            iDownloadCallback.update(downloadInfo);
        }
    }
    /* monitor exit ClassFileLocalVariableReferenceExpression{type=ObjectType{android/os/Message}, name=paramMessage} */
  }
}
```



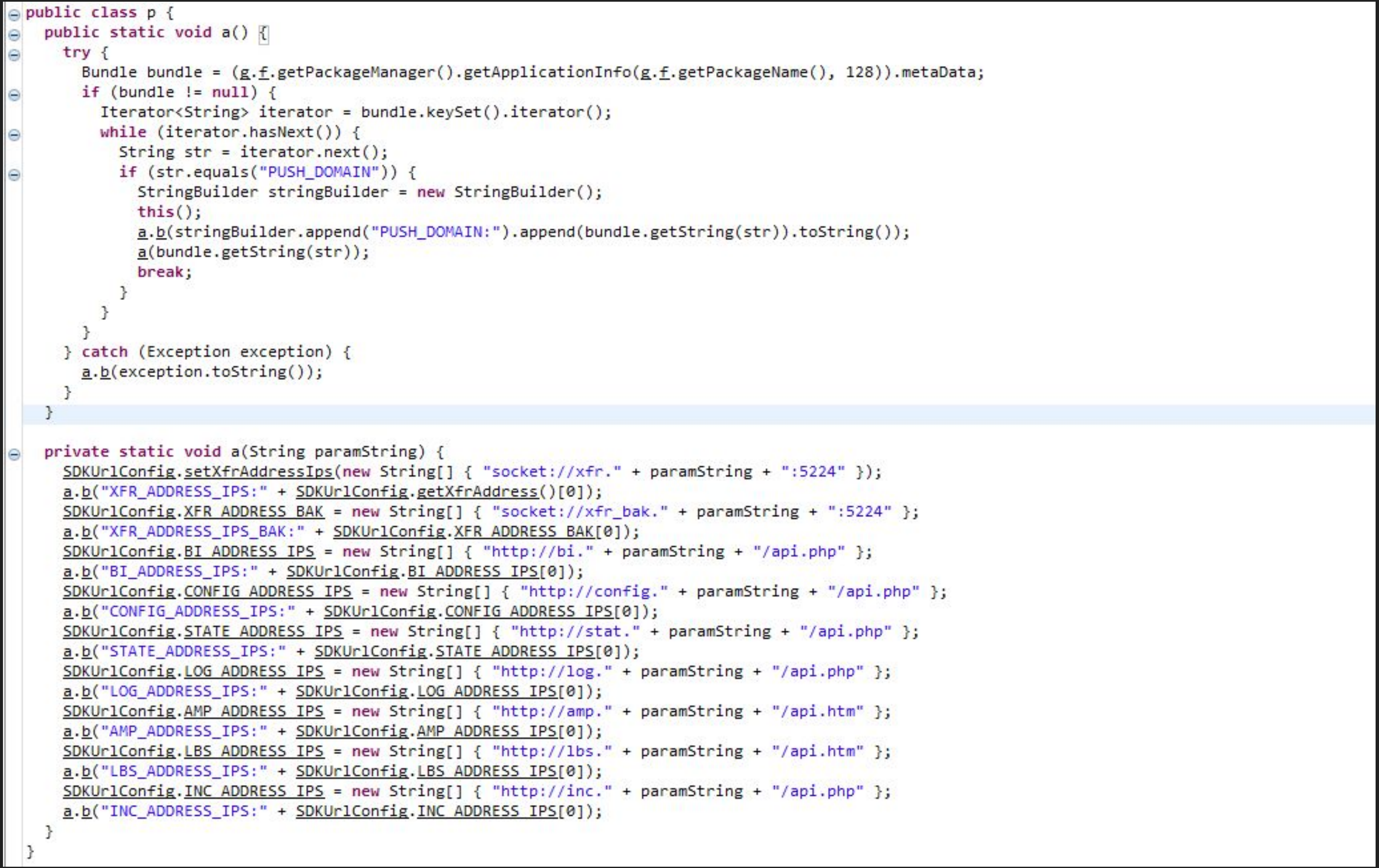
```
    .locals 1

    iget-object v0, p0, Lw/Bir;->c8XA:Ldalvik/system/DexClassLoader;

    return-object v0
.end method

.method public final c8XA(Ldalvik/system/DexClassLoader;)V
    .locals 2

    iput-object p1, p0, Lw/Bir;->c8XA:Ldalvik/system/DexClassLoader;

    sget v0, Landroid/os/Build$VERSION;->SDK_INT:I

    const/16 v1, 0x33a

    if-le v0, v1, :cond_0
```



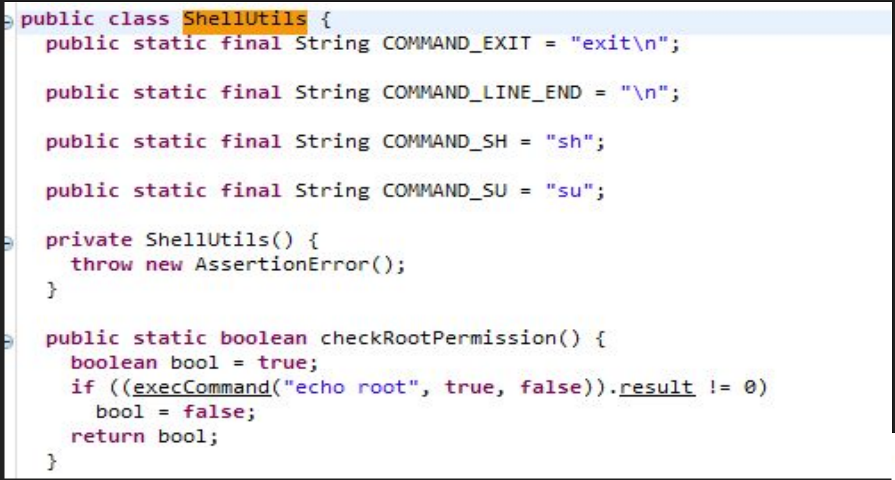
```
private j a(JSONObject paramJSONObject) {
  if (!paramJSONObject.has("domain"))
    return null;
  j j2 = new j();
  j2.a(paramJSONObject.getString("domain"));
  if (paramJSONObject.has("port"))
    j2.a(paramJSONObject.getInt("port"));
  if (paramJSONObject.has("ip"))
    j2.b(paramJSONObject.getString("ip"));
  if (paramJSONObject.has("consumeTime"))
    j2.a(paramJSONObject.getLong("consumeTime"));
  if (paramJSONObject.has("detectSuccessTime"))
    j2.b(paramJSONObject.getLong("detectSuccessTime"));
  if (paramJSONObject.has("isDomain"))
    j2.a(paramJSONObject.getBoolean("isDomain"));
  j j1 = j2;
  if (paramJSONObject.has("connectTryCnt")) {
    j2.b(paramJSONObject.getInt("connectTryCnt"));
    j1 = j2;
  }
  return j1;
}

private List<String> a() {
  String[] arrayOfString = SDKUrlConfig.getXfrAddress();
  ArrayList<String> arrayList = new ArrayList();
  int i = arrayOfString.length;
  for (byte b = 0; b < i; b++) {
    String str = arrayOfString[b];
    if (!arrayList.contains(str))
      arrayList.add(str);
  }
  return arrayList;
}

private List<String> a(JSONArray paramJSONArray) {
  ArrayList<String> arrayList = new ArrayList();
  byte b = 0;
  try {
    while (b < paramJSONArray.length()) {
      arrayList.add(paramJSONArray.getJSONObject(b).getString("domain"));
      b++;
    }
  } catch (Exception exception) {}
  return arrayList;
}
```



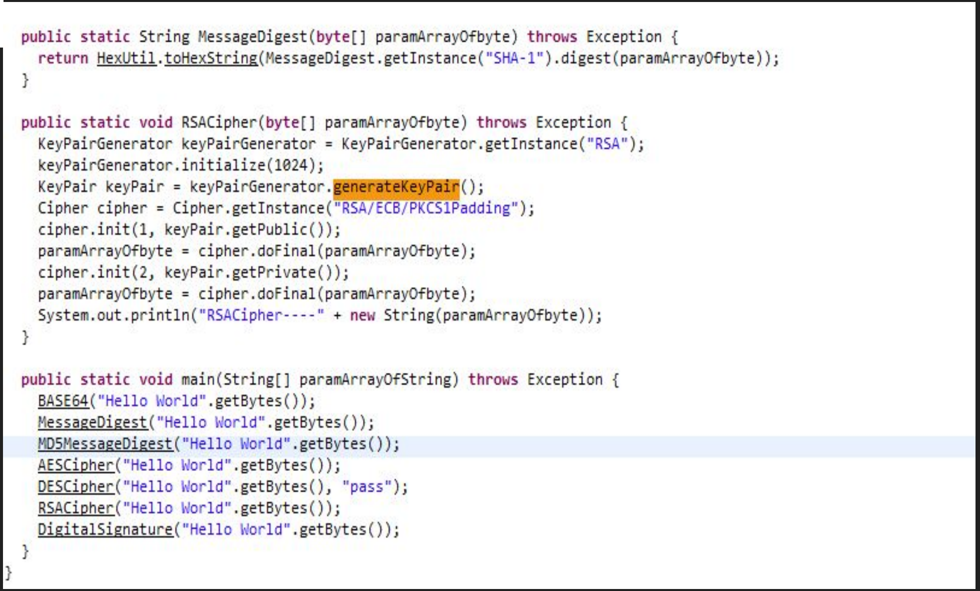
```java
public class SDKUrlConfig {
  public static String[] AMP_ADDRESS_IPS;

  public static String[] BI_ADDRESS_IPS;

  public static String[] CONFIG_ADDRESS_IPS;

  public static String[] INC_ADDRESS_IPS;

  public static String[] LBS_ADDRESS_IPS;

  public static String[] LOG_ADDRESS_IPS;

  public static String[] STATE_ADDRESS_IPS;

  public static String[] XFR_ADDRESS_BAK;

  private static final Object a = new Object();

  private static String[] b;

  private static String c = "HZ";

  private static String[] d = new String[] { "socket://sdk.open.talk.igexin.com:5224", "socket://sdk.open.talk.getui.net:5224", "socket://sdk.open.talk.gepush.com:5224" };

  private static volatile String e;

  static {
    XFR_ADDRESS_BAK = new String[] { "socket://42.62.120.14:5224" };
    BI_ADDRESS_IPS = new String[] { "http://sdk.open.phone.igexin.com/api.php" };
    CONFIG_ADDRESS_IPS = new String[] { "http://c-hzgt2.getui.com/api.php" };
    STATE_ADDRESS_IPS = new String[] { "http://s-gt.getui.com/api.php" };
    LOG_ADDRESS_IPS = new String[] { "http://d.gt.igexin.com/api.htm" };
    AMP_ADDRESS_IPS = new String[] { "http://sdk.open.amp.igexin.com/api.htm" };
    LBS_ADDRESS_IPS = new String[] { "http://sdk.open.lbs.igexin.com/api.htm" };
    INC_ADDRESS_IPS = new String[] { "http://sdk.open.inc2.igexin.com/api.php" };
```



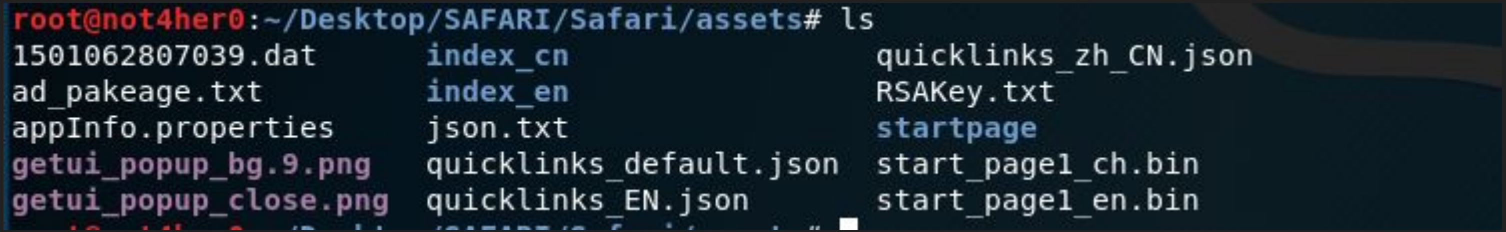
```
public class p {
  public static void a() {
    try {
      Bundle bundle = (g.f.getPackageManager().getApplicationInfo(g.f.getPackageName(), 128)).metaData;
      if (bundle != null) {
        Iterator<String> iterator = bundle.keySet().iterator();
        while (iterator.hasNext()) {
          String str = iterator.next();
          if (str.equals("PUSH_DOMAIN")) {
            StringBuilder stringBuilder = new StringBuilder();
            this();
            a.b(stringBuilder.append("PUSH_DOMAIN:").append(bundle.getString(str)).toString());
            a(bundle.getString(str));
            break;
          }
        }
      }
    } catch (Exception exception) {
      a.b(exception.toString());
    }
  }

  private static void a(String paramString) {
    SDKUrlConfig.setXfrAddressIps(new String[] { "socket://xfr." + paramString + ":5224" });
    a.b("XFR_ADDRESS_IPS:" + SDKUrlConfig.getXfrAddress()[0]);
    SDKUrlConfig.XFR_ADDRESS_BAK = new String[] { "socket://xfr_bak." + paramString + ":5224" };
    a.b("XFR_ADDRESS_IPS_BAK:" + SDKUrlConfig.XFR_ADDRESS_BAK[0]);
    SDKUrlConfig.BI_ADDRESS_IPS = new String[] { "http://bi." + paramString + "/api.php" };
    a.b("BI_ADDRESS_IPS:" + SDKUrlConfig.BI_ADDRESS_IPS[0]);
    SDKUrlConfig.CONFIG_ADDRESS_IPS = new String[] { "http://config." + paramString + "/api.php" };
    a.b("CONFIG_ADDRESS_IPS:" + SDKUrlConfig.CONFIG_ADDRESS_IPS[0]);
    SDKUrlConfig.STATE_ADDRESS_IPS = new String[] { "http://stat." + paramString + "/api.php" };
    a.b("STATE_ADDRESS_IPS:" + SDKUrlConfig.STATE_ADDRESS_IPS[0]);
    SDKUrlConfig.LOG_ADDRESS_IPS = new String[] { "http://log." + paramString + "/api.php" };
    a.b("LOG_ADDRESS_IPS:" + SDKUrlConfig.LOG_ADDRESS_IPS[0]);
    SDKUrlConfig.AMP_ADDRESS_IPS = new String[] { "http://amp." + paramString + "/api.htm" };
    a.b("AMP_ADDRESS_IPS:" + SDKUrlConfig.AMP_ADDRESS_IPS[0]);
    SDKUrlConfig.LBS_ADDRESS_IPS = new String[] { "http://lbs." + paramString + "/api.htm" };
    a.b("LBS_ADDRESS_IPS:" + SDKUrlConfig.LBS_ADDRESS_IPS[0]);
    SDKUrlConfig.INC_ADDRESS_IPS = new String[] { "http://inc." + paramString + "/api.php" };
    a.b("INC_ADDRESS_IPS:" + SDKUrlConfig.INC_ADDRESS_IPS[0]);
  }
}
```



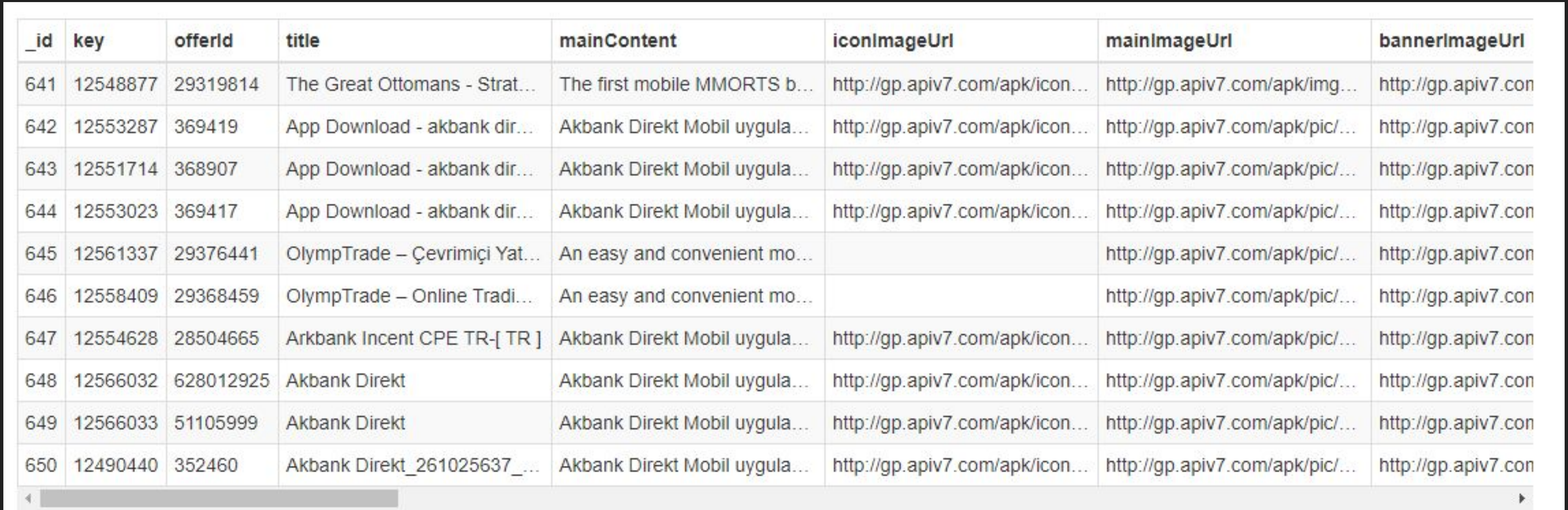
```java
public class ShellUtils {
  public static final String COMMAND_EXIT = "exit\n";

  public static final String COMMAND_LINE_END = "\n";

  public static final String COMMAND_SH = "sh";

  public static final String COMMAND_SU = "su";

  private ShellUtils() {
    throw new AssertionError();
  }

  public static boolean checkRootPermission() {
    boolean bool = true;
    if ((execCommand("echo root", true, false)).result != 0)
      bool = false;
    return bool;
  }
```



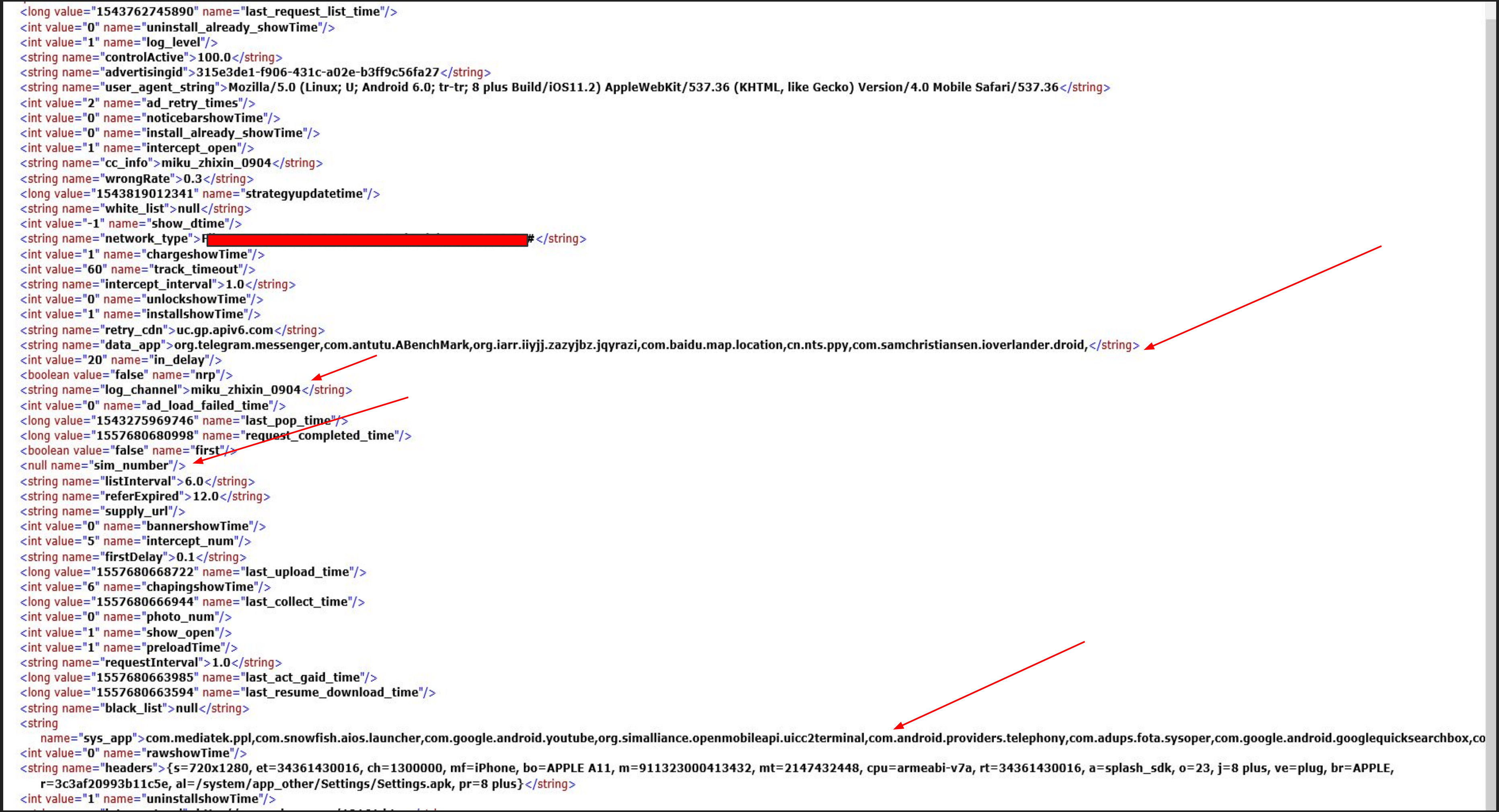
```java
  public static String MessageDigest(byte[] paramArrayOfbyte) throws Exception {
    return HexUtil.toHexString(MessageDigest.getInstance("SHA-1").digest(paramArrayOfbyte));
  }

  public static void RSACipher(byte[] paramArrayOfbyte) throws Exception {
    KeyPairGenerator keyPairGenerator = KeyPairGenerator.getInstance("RSA");
    keyPairGenerator.initialize(1024);
    KeyPair keyPair = keyPairGenerator.generateKeyPair();
    Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");
    cipher.init(1, keyPair.getPublic());
    paramArrayOfbyte = cipher.doFinal(paramArrayOfbyte);
    cipher.init(2, keyPair.getPrivate());
    paramArrayOfbyte = cipher.doFinal(paramArrayOfbyte);
    System.out.println("RSACipher----" + new String(paramArrayOfbyte));
  }

  public static void main(String[] paramArrayOfString) throws Exception {
    BASE64("Hello World".getBytes());
    MessageDigest("Hello World".getBytes());
    MD5MessageDigest("Hello World".getBytes());
    AESCipher("Hello World".getBytes());
    DESCipher("Hello World".getBytes(), "pass");
    RSACipher("Hello World".getBytes());
    DigitalSignature("Hello World".getBytes());
  }
}
```



```
root@not4her0:~/Desktop/SAFARI/Safari/assets# ls
1501062807039.dat      index_cn                  quicklinks_zh_CN.json
ad_pakeage.txt         index_en                  RSAKey.txt
appInfo.properties     json.txt                  startpage
getui_popup_bg.9.png   quicklinks_default.json   start_page1_ch.bin
getui_popup_close.png  quicklinks_EN.json        start_page1_en.bin
```

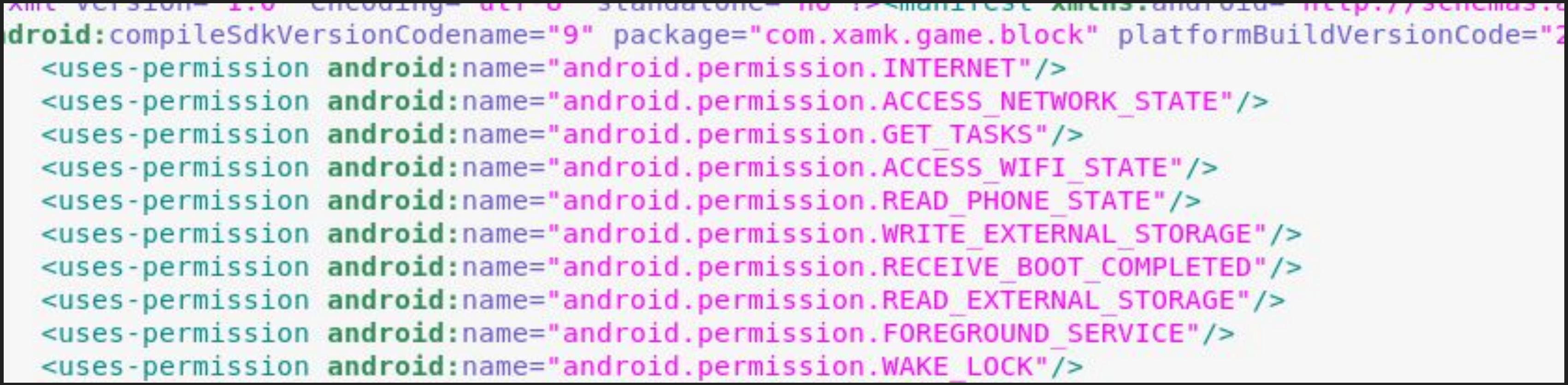


_id	key	offerId	title	mainContent	iconImageUrl	mainImageUrl	bannerImageUrl
641	12548877	29319814	The Great Ottomans - Strat...	The first mobile MMORTS b...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/img...	http://gp.apiv7.con
642	12553287	369419	App Download - akbank dir...	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
643	12551714	368907	App Download - akbank dir...	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
644	12553023	369417	App Download - akbank dir...	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
645	12561337	29376441	OlympTrade – Çevrimiçi Yat...	An easy and convenient mo...		http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
646	12558409	29368459	OlympTrade – Online Tradi...	An easy and convenient mo...		http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
647	12554628	28504665	Arkbank Incent CPE TR-[TR]	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
648	12566032	628012925	Akbank Direkt	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
649	12566033	51105999	Akbank Direkt	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con
650	12490440	352460	Akbank Direkt_261025637_...	Akbank Direkt Mobil uygula...	http://gp.apiv7.com/apk/icon...	http://gp.apiv7.com/apk/pic/...	http://gp.apiv7.con



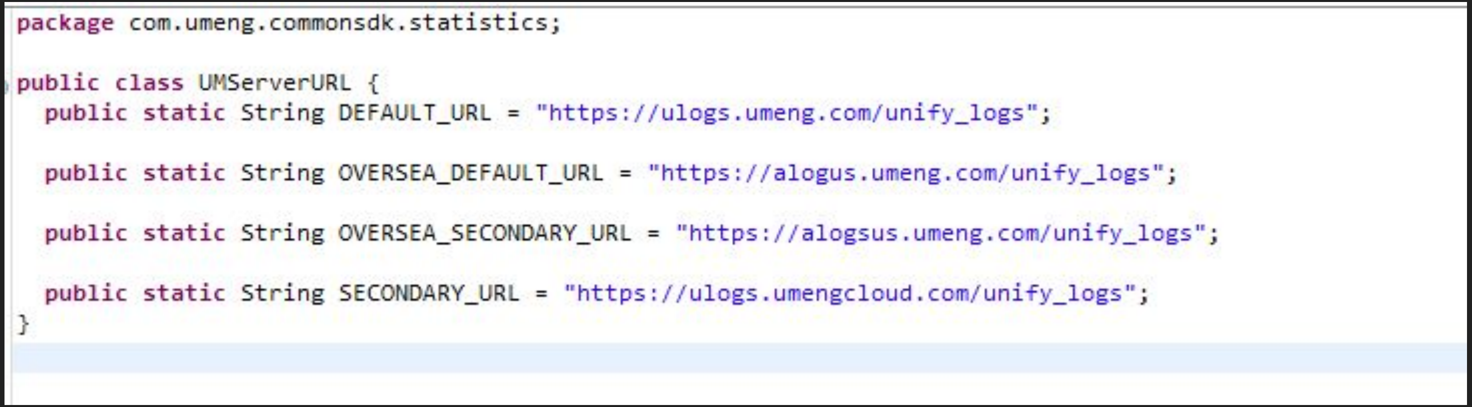
```
<long value="1543762745890" name="last_request_list_time"/>
<int value="0" name="uninstall_already_showTime"/>
<int value="1" name="log_level"/>
<string name="controlActive">100.0</string>
<string name="advertisingid">315e3de1-f906-431c-a02e-b3ff9c56fa27</string>
<string name="user_agent_string">Mozilla/5.0 (Linux; U; Android 6.0; tr-tr; 8 plus Build/iOS11.2) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Mobile Safari/537.36</string>
<int value="2" name="ad_retry_times"/>
<int value="0" name="noticebarshowTime"/>
<int value="0" name="install_already_showTime"/>
<int value="1" name="intercept_open"/>
<string name="cc_info">miku_zhixin_0904</string>
<string name="wrongRate">0.3</string>
<long value="1543819012341" name="strategyupdatetime"/>
<string name="white_list">null</string>
<int value="-1" name="show_dtime"/>
<string name="network_type">[redacted]</string>
<int value="1" name="chargeshowTime"/>
<int value="60" name="track_timeout"/>
<string name="intercept_interval">1.0</string>
<int value="0" name="unlockshowTime"/>
<int value="1" name="installshowTime"/>
<string name="retry_cdn">uc.gp.apiv6.com</string>
<string name="data_app">org.telegram.messenger,com.antutu.ABenchMark,org.iarr.iiyjj.zazyjbz.jqyrazi,com.baidu.map.location,cn.nts.ppy,com.samchristiansen.ioverlander.droid,</string>
<int value="20" name="in_delay"/>
<boolean value="false" name="nrp"/>
<string name="log_channel">miku_zhixin_0904</string>
<int value="0" name="ad_load_failed_time"/>
<long value="1543275969746" name="last_pop_time"/>
<long value="1557680680998" name="request_completed_time"/>
<boolean value="false" name="first"/>
<null name="sim_number"/>
<string name="listInterval">6.0</string>
<string name="referExpired">12.0</string>
<string name="supply_url"/>
<int value="0" name="bannershowTime"/>
<int value="5" name="intercept_num"/>
<string name="firstDelay">0.1</string>
<long value="1557680668722" name="last_upload_time"/>
<int value="6" name="chapingshowTime"/>
<long value="1557680666944" name="last_collect_time"/>
<int value="0" name="photo_num"/>
<int value="1" name="show_open"/>
<int value="1" name="preloadTime"/>
<string name="requestInterval">1.0</string>
<long value="1557680663985" name="last_act_gaid_time"/>
<long value="1557680663594" name="last_resume_download_time"/>
<string name="black_list">null</string>
<string
    name="sys_app">com.mediatek.ppl,com.snowfish.aios.launcher,com.google.android.youtube,org.simalliance.openmobileapi.uicc2terminal,com.android.providers.telephony,com.adups.fota.sysoper,com.google.android.googlequicksearchbox,co
<int value="0" name="rawshowTime"/>
<string name="headers">{s=720x1280, et=34361430016, ch=1300000, mf=iPhone, bo=APPLE A11, m=911323000413432, mt=2147432448, cpu=armeabi-v7a, rt=34361430016, a=splash_sdk, o=23, j=8 plus, ve=plug, br=APPLE,
    r=3c3af20993b11c5e, al=/system/app_other/Settings/Settings.apk, pr=8 plus}</string>
<int value="1" name="uninstallshowTime"/>
```

XAMK-GAME.apk ??



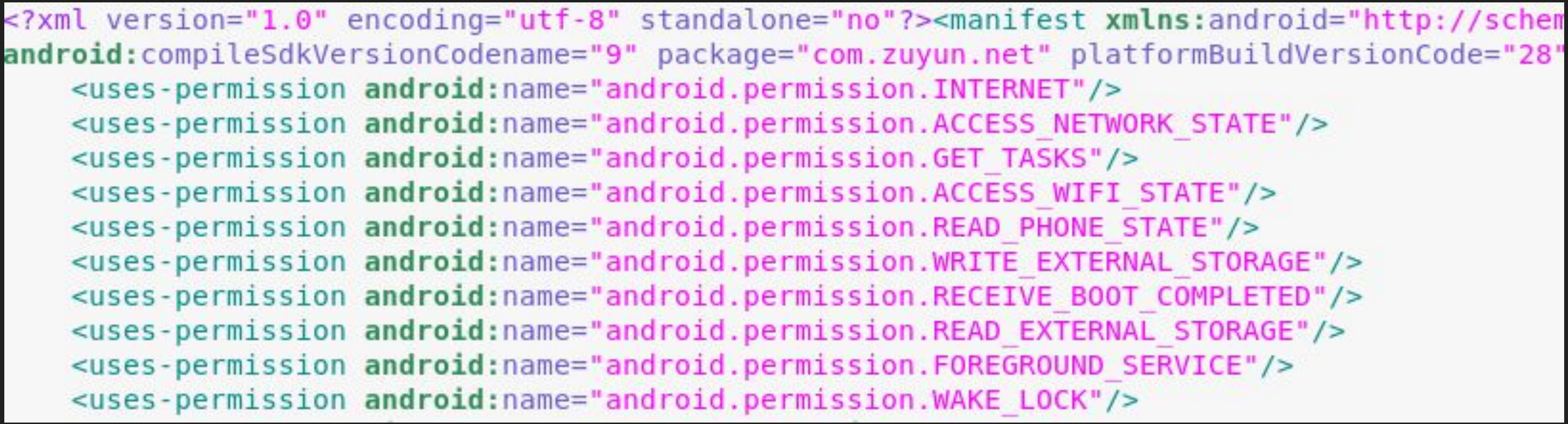
```
xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.a
droid:compileSdkVersionCodename="9" package="com.xamk.game.block" platformBuildVersionCode="2
  <uses-permission android:name="android.permission.INTERNET"/>
  <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
  <uses-permission android:name="android.permission.GET_TASKS"/>
  <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
  <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
  <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
  <uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
  <uses-permission android:name="android.permission.WAKE_LOCK"/>
```

https://www.virustotal.com/gui/file/032fba0c177443a53c8d51fe8c58b0fb51ad71019567de6c480e25d77d5a57d6/behavior/Tencent%20HABO

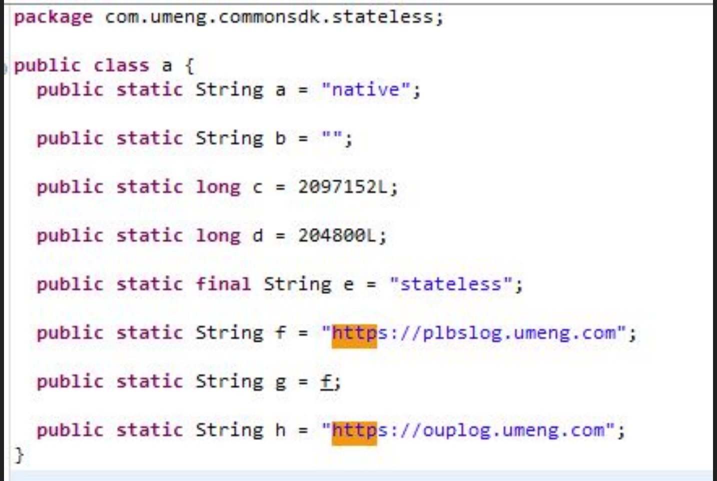


```
package com.umeng.commonsdk.statistics;

public class UMServerURL {
  public static String DEFAULT_URL = "https://ulogs.umeng.com/unify_logs";

  public static String OVERSEA_DEFAULT_URL = "https://alogus.umeng.com/unify_logs";

  public static String OVERSEA_SECONDARY_URL = "https://alogsus.umeng.com/unify_logs";

  public static String SECONDARY_URL = "https://ulogs.umengcloud.com/unify_logs";
}
```

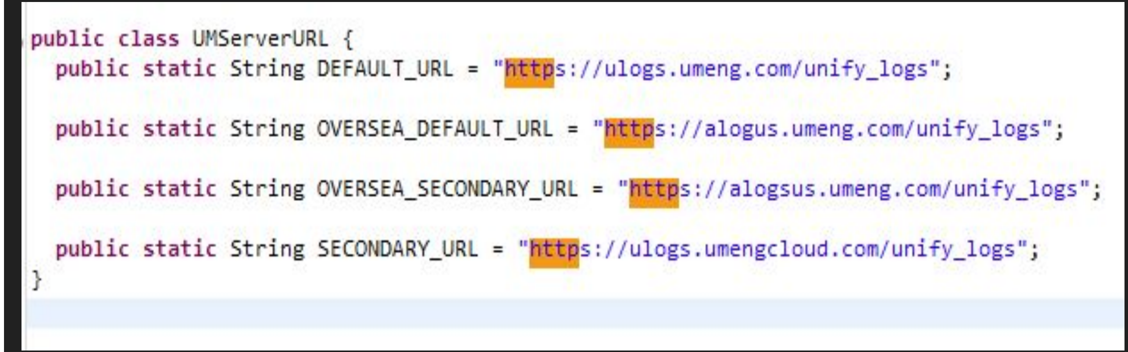
zuyun.apk ??



```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schem
android:compileSdkVersionCodename="9" package="com.zuyun.net" platformBuildVersionCode="28"
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.GET_TASKS"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
```



```java
package com.umeng.commonsdk.stateless;

public class a {
  public static String a = "native";

  public static String b = "";

  public static long c = 2097152L;

  public static long d = 204800L;

  public static final String e = "stateless";

  public static String f = "https://plbslog.umeng.com";

  public static String g = f;

  public static String h = "https://ouplog.umeng.com";
}
```



```java
public class UMServerURL {
  public static String DEFAULT_URL = "https://ulogs.umeng.com/unify_logs";

  public static String OVERSEA_DEFAULT_URL = "https://alogus.umeng.com/unify_logs";

  public static String OVERSEA_SECONDARY_URL = "https://alogsus.umeng.com/unify_logs";

  public static String SECONDARY_URL = "https://ulogs.umengcloud.com/unify_logs";
}
```

QUESTIONS ?

Mail > dogusyalcin@outlook.com

Twitter > not4her0