

# Android Uygulamalarında



## Güvenlik Testi



# İÇERİK

**Android üzerine**

**Penetrasyon testi üzerine**

**Penetrasyon testi adımları**

**Örnek Zafiyetler**

**Sonuç**



# BEN KİMİM?

**Ahlaklı Korsan**

**Mesai saatlerinde...**

**Blog Yazarı**

**<http://www.mertsarica.com>**

**Python Programcısı**

**[http://www.mertsarica.com/?page\\_id=893](http://www.mertsarica.com/?page_id=893)**

**Zararlı Yazılım Analisti**

**Boş zamanlarımda...**

**Sertifika Koleksiyoncusu**

**CISSP , SSCP , OSCP , OPST , CREA**



# MESLEĞİM ?

Finans sektörünün ihtiyaçlarına ve günün teknolojilerine uygun hizmetler sunan, ürünler meydana getiren, NBG Grup şirketlerinden Finansbank'ın Bilgi Teknolojileri iştiraki olan IBTech firmasında Bilişim Güvenliği Uzmanı (Senior Penetration Tester / Ethical Hacker) olarak çalışmaktayım.

<http://www.ibtech.com.tr>



# KONU ?

Open Handset Alliance liderliğinde Google firması tarafından akıllı telefonlar ve tablet bilgisayarlar gibi mobil cihazlar için geliştirilmiş linux tabanlı işletim sistemi olan Android işletim sistemi için geliştirilen uygulamalarda penetrasyon testi gerçekleştirme.



# NEDİR/NEDEN PENTEST ?

**Bilişim Sistemler'ini oluşturan altyapılarda, sistemlerde ve/veya uygulamalarda art niyetli kişilerden önce istismar edilebilir güvenlik zafiyetlerini tespit etmek ve raporlamak için gerçekleştirilen teste penetrasyon testi denir.**

**Kendi güvenliğiniz için**

**Müşterilerinizin güvenliği, itibarınız, marka değeriniz için**

**Kurum içi güvenlik farkındalığını arttırmak için**



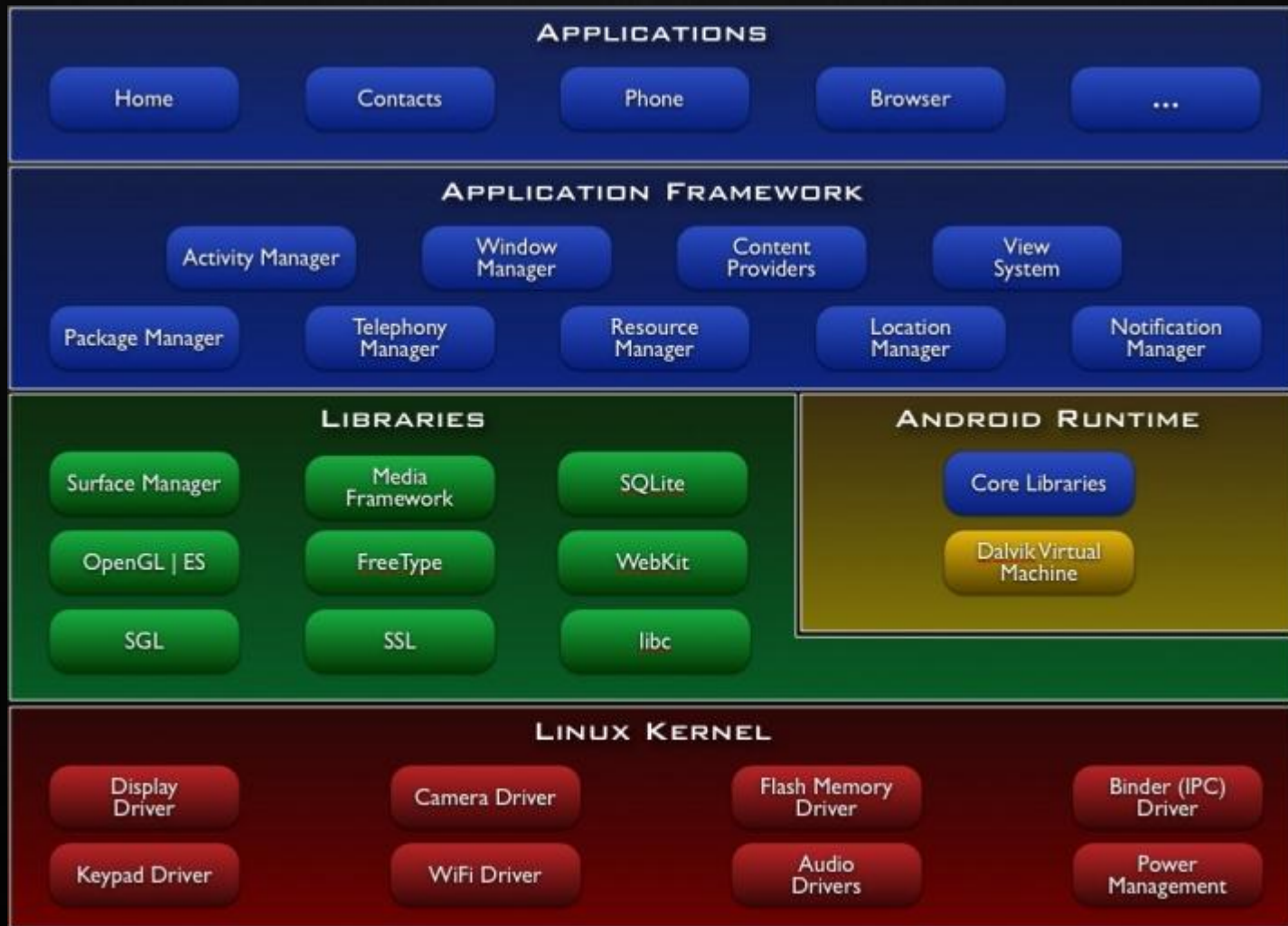
# İSTATİSTİKİ BİLGİ

**Table 3**  
**Worldwide Smartphone Sales to End Users by Operating System in 4Q11**  
**(Thousands of Units)**

Operating System	4Q11 Units	4Q11 Market Share (%)	4Q10 Units	4Q10 Market Share (%)
Android	75,906.1	50.9	30,801.2	30.5
iOS	35,456.0	23.8	16,011.1	15.8
Symbian	17,458.4	11.7	32,642.1	32.3
Research In Motion	13,184.5	8.8	14,762.0	14.6
Bada	3,111.3	2.1	2,026.8	2.0
Microsoft	2,759.0	1.9	3,419.3	3.4
Others	1,166.5	0.8	1,487.9	1.5
<b>Total</b>	<b>149,041.8</b>	<b>100.0</b>	<b>101,150.3</b>	<b>100.0</b>

Source: Gartner (February 2012)

# ANDROID MİMARISI





# ANDROID GÜVENLİK MODELİ

**Linux Güvenlik Modeli baz alınmıştır. (UID/GUID)**

**Uygulama bazlı izinler kullanılmaktadır.**

**İzinler, AndroidManifest.xml dosyasında tanımlanmaktadır.**

**Kurulum için uygulamanın sertifika ile imzalanmış olması gerekmektedir.**

**Her bir uygulama farklı bir Dalvik Sanal Makinesi içinde çalışmaktadır.**

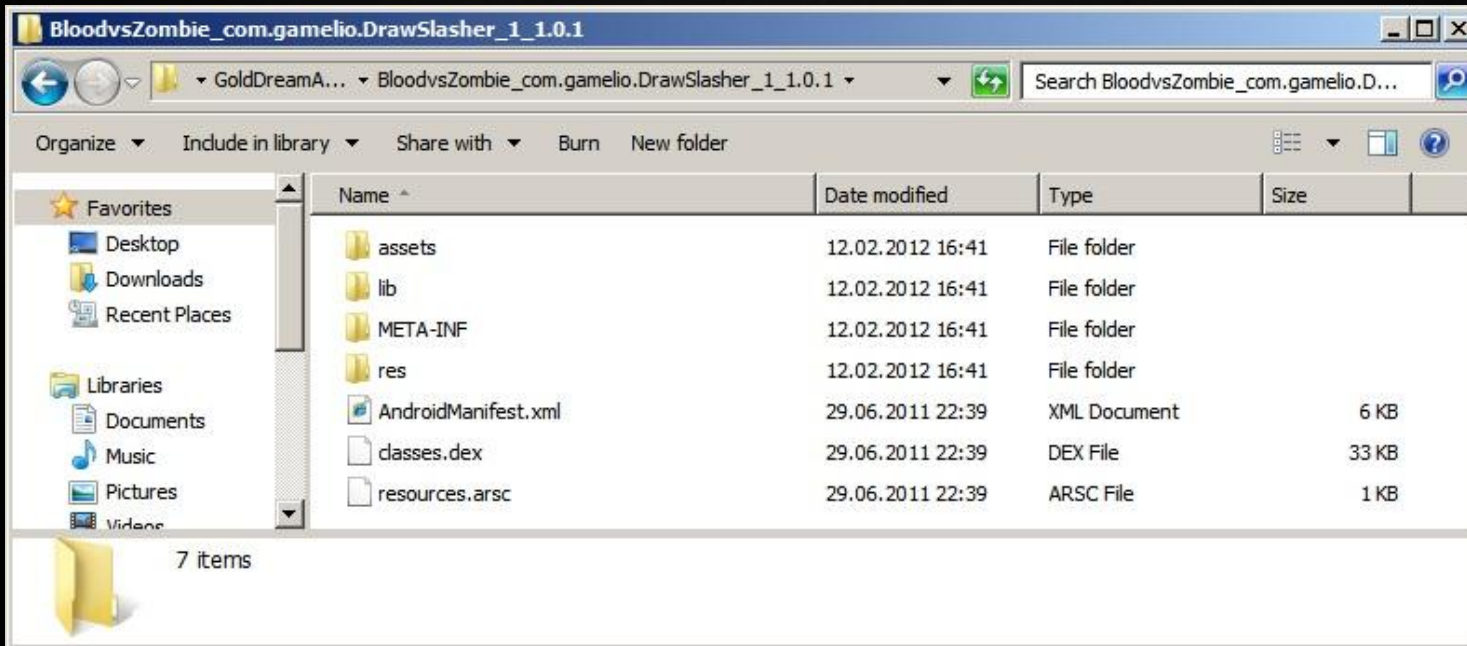
**Sistem güvenliğinde kullanıcı kilit rol oynamaktadır.**



# APK NEDİR ?

Android application package file (APK) dosyası, zip dosya formatına sahip .apk uzantılı dosyalardır.

APK dosyası, uzantısı .zip olarak değiştirildikten sonra Winzip, Winrar gibi araçlar ile açılabilir.



# APK NEDİR ?

**META-INF klasöründe MANIFEST dosyası, uygulamanın sertifikası ve dosyaların SHA-1 hash bilgileri yer almaktadır.**

**res klasöründe resources.arsc dosyasında yer almayan ses dosyaları, grafik dosyaları vb. dosyalar bulunur.**

**Android Manifest dosyasında uygulama izinleri, paket adı, sürümü vb. bilgiler yer alır.**

**Classes.dex dosyası Dalvik sanal makinesi tarafından çalıştırılabilen derlenmiş sınıfları içerir.**



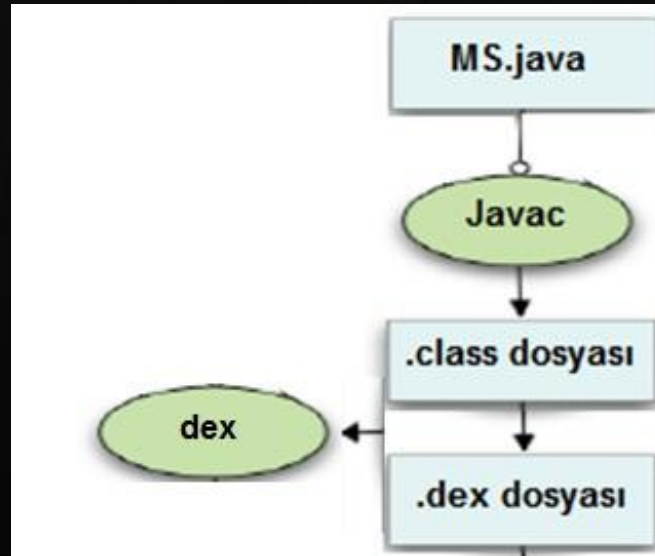
# DEX NEDİR ?

Dalvik sanal makinesinde çalıştırılabilen derlenmiş Android uygulamasıdır.

Dex dosyasını class dosyasına çevirebilirsek kaynak koduna da çevirebiliriz.

**Komut:** `d2j-dex2jar.bat classes.dex`

**URL:** <http://code.google.com/p/dex2jar/downloads/list>



# ANDROID SDK NEDİR ?

**Android Software Development Kit (SDK), uygulama geliřtirmek için kullanılan ve içinde birçok aracı bulunduran bir araç takımıdır.**

**Hata ayıklayıcı (debugger)**

**Öykünücü (emulator)**

**Kütüphaneler**

**API belgeleri, örnek kaynak kodları, özel dersler (tutorial) vs.**

**URL: <http://developer.android.com/sdk/index.html>**



# ANDROID SDK NEDİR ?



# ANDROID SDK NEDİR ?

**ADB (Android Debug Bridge), Android cihaz/emülatör ile iletişim kurmayı sağlayan terminal tabanlı bir arabirimdir.**

**ADB push (cihaza dosya gönderir) -- adb push uygulama.apk /sdcard/uygulama.apk**

**ADB pull (cihazdan dosya alır) -- adb pull /system/app/uygulama.apk**

**ADB install (cihaza uygulama yükler) -- adb install uygulama.apk**

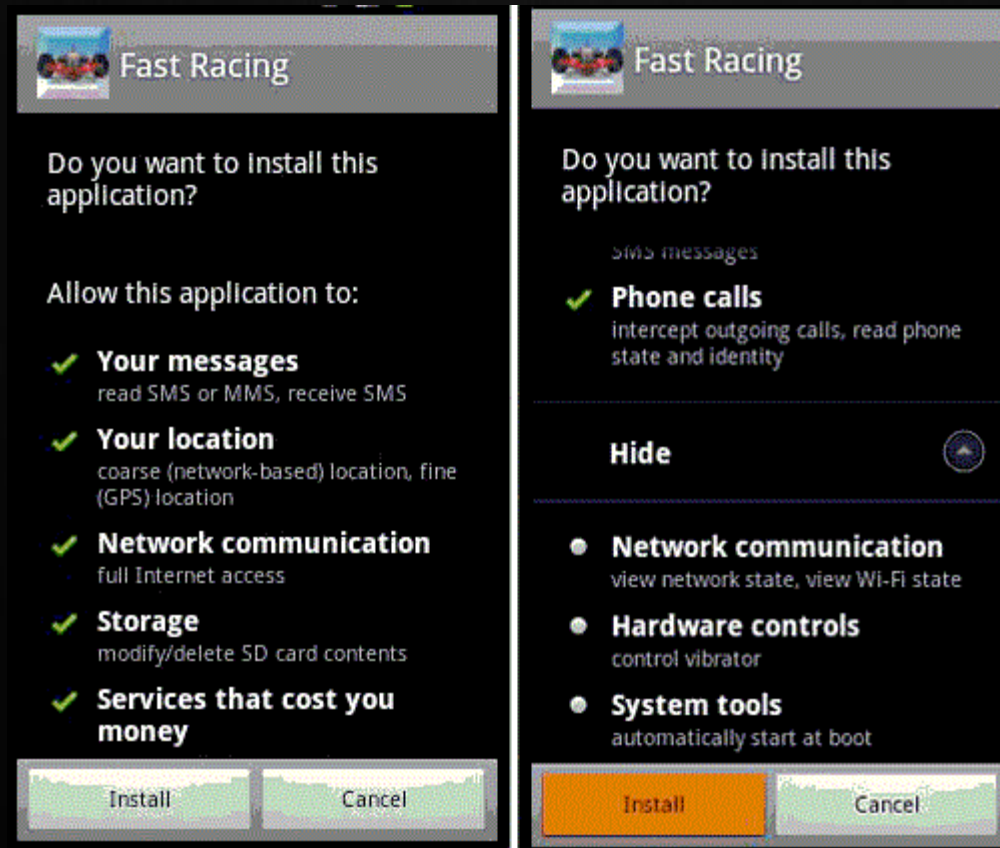
**ADB shell (cihazın komut satırına bağlanır)**

**ADB remount (dosya sistemine yazma izni verir)**



# İZINLER

İzinler, `AndroidManifest.xml` dosyasında tanımlanmaktadır.





# PENTEST ADIMLARI

**Ağ trafiği analizi/manipülasyonu**

**Kaynak kodu incelemesi**

**Tersine çevirme/yamama**

**Dosya sistemi incelemesi**

**İzinler**



# Ağ Trafiği Analizi



# AĞ TRAFİĞİ ANALİZİ

**Haberleşme güvenli kanaldan mı gerçekleştiriliyor ? (SSL)**

**Hassas, kişisel bilgiler sunucuya gönderiliyor mu ?**

**Şifreler açık (clear text) olarak mı sunucuya gönderiliyor ?**

**Araçlar:** Android Emulator, App Player & Wireshark

**URL:** <http://bluestacks.com/app-player/>

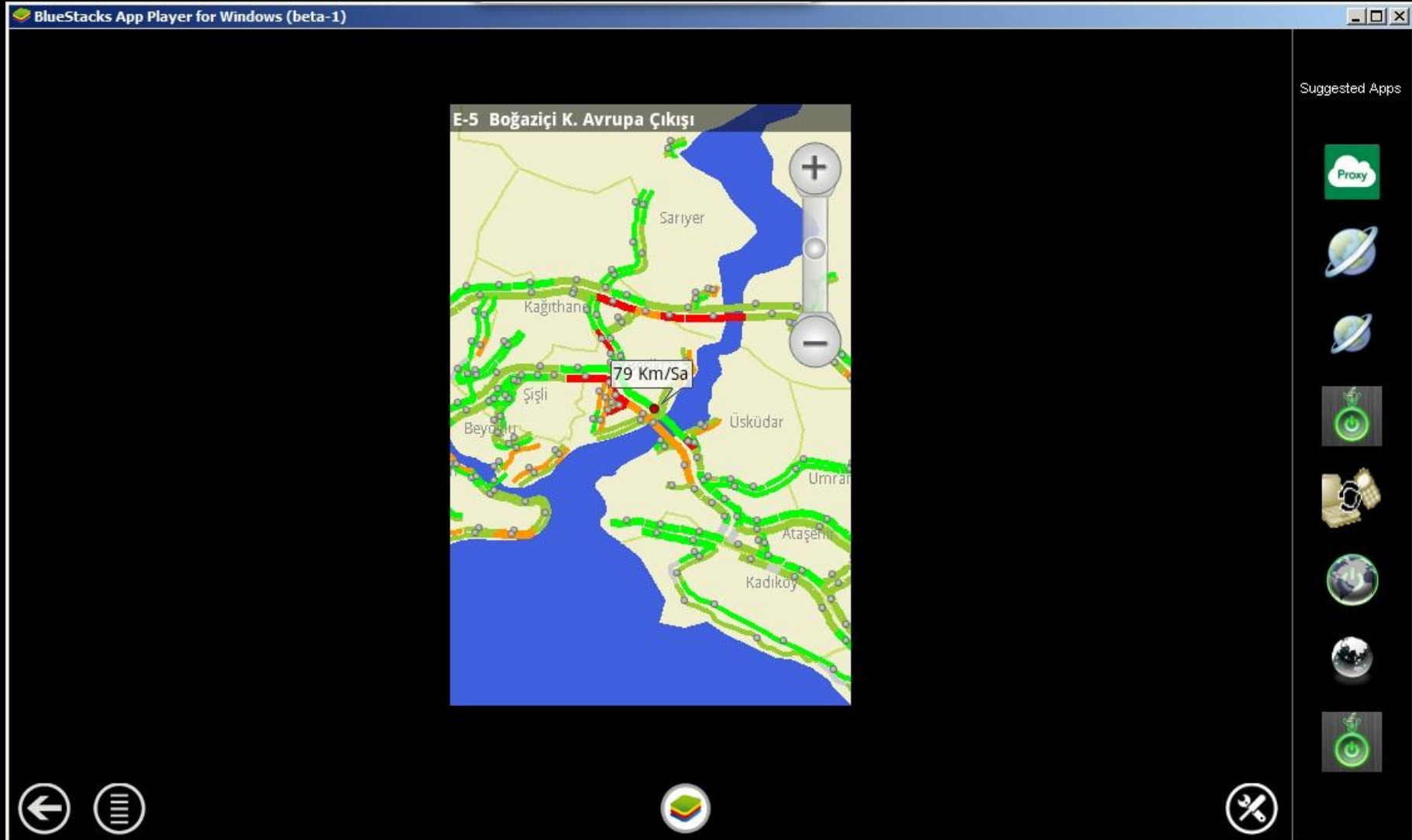
**URL:** <http://www.wireshark.org/>



# AĞ TRAFİĞİ ANALİZİ



# AĞ TRAFİĞİ ANALİZİ



# AĞ TRAFİĞİ ANALİZİ

IMEI ?

Microsoft [Wireshark 1.6.6 (SVN Rev 41803 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 42

No.	Time	Source	Destination	Length	Info
6236	38.689220	192.168.1.36	[REDACTED]	60	[SYN] Seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1
6244	38.698187	[REDACTED]	192.168.1.36	60	[SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MSS=1452 SACK_PERM=1
6245	38.698264	192.168.1.36	[REDACTED]	60	[ACK] Seq=1 Ack=1 win=65536 Len=0
6249	38.708098	192.168.1.36	[REDACTED]	426	GET /ct21/mobil/getser...aspx?platform=android&uAgent=Bluestacks-b0daa9f3-88b3-11e1-88bf-e5700337f244&imei=1334685043806&version=3.1&msisdn=null&memorylimited=0&q=SENSOR HTTP/1.1
6303	38.783137	[REDACTED]	[REDACTED]	60	[ACK] Seq=1 Ack=1 win=65536 Len=0
6304	38.783830	[REDACTED]	[REDACTED]	60	[ACK] Seq=1 Ack=1 win=65536 Len=0
6305	38.783855	192.168.1.36	[REDACTED]	60	[ACK] Seq=1 Ack=1 win=65536 Len=0
6316	38.800806	[REDACTED]	[REDACTED]	60	[ACK] Seq=1 Ack=1 win=65536 Len=0
6318	38.801664	[REDACTED]	[REDACTED]	60	[ACK] Seq=1 Ack=1 win=65536 Len=0
6319	38.801690	192.168.1.36	[REDACTED]	60	[ACK] Seq=1 Ack=1 win=65536 Len=0
6320	38.802647	[REDACTED]	[REDACTED]	60	[ACK] Seq=1 Ack=1 win=65536 Len=0
6343	38.838077	[REDACTED]	[REDACTED]	60	[ACK] Seq=1 Ack=1 win=65536 Len=0
6344	38.838104	192.168.1.36	[REDACTED]	60	[ACK] Seq=1 Ack=1 win=65536 Len=0
6345	38.839006	[REDACTED]	[REDACTED]	60	[ACK] Seq=1 Ack=1 win=65536 Len=0
6470	39.041603	192.168.1.36	[REDACTED]	426	HTTP/1.1 200 OK

Follow TCP Stream

Stream Content

```

GET /ct21/mobil/getser...aspx?platform=android&uAgent=Bluestacks-
b0daa9f3-88b3-11e1-88bf-e5700337f244&imei=1334685043806&version=3.1&msisdn=null&memorylimited=0&q=SENSOR
HTTP/1.1
User-Agent: Dalvik/1.4.0 (Linux; u; Android 2.3.4; Bluestacks-b0daa9f3-88b3-11e1-88bf-
e5700337f244 Build/GRJ22)
Host: [REDACTED]
Connection: Keep-Alive
Accept-Encoding: gzip

HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Length: 3439
Date: Tue, 17 Apr 2012 17:50:49 GMT
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-version: 2.0.50727
Cache-Control: private

00003431<SYSTEM. MSISDN=null.>...</SYSTEM.>...<SENSOR.>...<F. L=2496./
>.....X.....M.....a.....L.....J
.....K.....<
.....B.....O.....4#.....c.....Q.....j.....^.....
.....).....P.....E2.....1$.....1&.....Q6'.....P).....P'.....d
+.....K.....O.....Q3.....e4.....Z6.....8.....C.....W.....TK.....K<.....=.....w?.....VA.....J
B.....!D.....BE.....>F.....YH.....II.....hy'.....ik.....XL.....M.....QN.....LP.....6R.....
\S.....T.....EU.....ZV.....LW.....Pg'.....X.....XY.....wZ.....Y
\.....K.....Sm'.....O^.....Y.....T.....Ha.....Ub.....dc.....Cd.....de.....
\F.....Yg.....Uh.....Kj.....Lk.....Hl.....On.....No.....?.....=p.....P.....Sq.....=.....'.....
$S.....]......Mt.....Fu.....=v.....-w.....N.....DX.....7.....<y.....L.....?Z.....E
  
```

Frame 6249: 426 bytes on wire (Ethernet II, Src: AskeyCom\_ca:1, Destination: Internet Protocol Version 4, Src: 192.168.1.36, Destination port: http (80), [Stream index: 42], Sequence number: 1 (relative to stream sequence number 373))

0000 c8 6c 87 94 37 cc 00 24 d2  
0010 01 9c 0c f7 40 00 80 06 43  
0020 12 b6 c1 9d 00 50 97 8e 6d  
0030 ff 3c 0e ab 00 00 47 45 54  
0040 6d 6f 62 69 6c 2f 67 65 74  
0050 2e 61 73 70 78 3f 70 6c 61  
0060 6e 64 72 6f 69 64 26 75 41  
0070 75 65 53 74 61 63 6b 73 2d  
0080 33 2d 38 38 62 33 2d 31 31  
0090 2d 65 35 37 30 30 33 33 37  
00a0 65 69 3d 31 33 33 34 36 38  
00b0 26 76 65 72 73 69 6f 6e 3d  
00c0 73 64 6e 3d 6e 75 6c 6c 26  
00d0 69 6d 69 74 65 64 3d 30 26

File: C:\Users\Mert\AppData\Local\Temp\wiresh...



# AĞ TRAFİĞİ ANALİZİ

```
IbbTrafik.class x
public void init()
{
    instance = this;
    parser = new Parser();
    parser.start();
    http = new Http();
    http.start();
    imei = getDate();
    url = "http://[REDACTED].tr/ct21/";
    version = "3.1";
    uAgent = Build.MODEL;
}

public void onError(Exception paramException, boolean paramBoolean)
{
    try
    {
        ((Activities)ActivityManager.instance.getActiveActivity()).startErrorAlertDialog();
        System.out.print("nete baglanmada hata var");
        ActivityManager.instance.setActiveOpenCamera(false);
        ActivityManager.instance.createErrorMessage(paramException, paramBoolean);
        return;
    }
    catch (Exception localException)
    {
        while (true)
        {
            if (!PreferencesActivity.waitingFlag)
                continue;
            PreferencesActivity.deActiveLoading();
        }
    }
}
```


# AĞ TRAFİĞİ ANALİZİ

www.mcks.gov.tr/tr/imeisorgu.php?

Hack 4 Career. Infor... LinkedIn Mert SARICA (mertsarica) Google Reader (1000+)

Other bookmarks

Ana Sayfa İletişim

Select language:  Ara

**BTK**  
BİLGİ TEKNOLOJİLERİ  
VE İLETİŞİM KURUMU

**MCKS**  
Mobil Cihaz Kayıt Sistemi

**SORGULAMALAR**

- IMEI Sorgulama
- IMEI-MSISDN Sorgulama
- Bireysel Başvuru Sorgulama
- İhbar Sorgulama

**GENEL BİLGİLER VE MEVZUAT**

- MCKS Hakkında
- Tanımlar
- Kanunlar
- Yönetmelikler
- Usul ve Esaslar
- Dış Ticaret Mevzuatı
- Gümrük Mevzuatı

**KAYIT VE EŞLEŞTİRME İŞLEMLERİ**

- Toplu İthalat
- Bireysel İthalat
- İthalatçı Eşleştirmeleri
- Geçici Süre İle Ülkede Bulunma

**KAPATILAN CİHAZLAR**

- Kaçak Cihazlar

**IMEI Sorgulama :**

**IMEI SORGULAMA**

IMEI :	[REDACTED]
Durumu :	<b>IMEI numarası kayıtlı</b>
Kaynak :	İthalat yoluyla kaydedilen IMEI
Üretici :	Üretici: Samsung Korea Pazar Adı: Samsung GT-19100 Model Bilgileri: Samsung GT-19100
Sorgulama Tarihi 12.05.12	

[Yeni Sorgu](#)

Bu sorgulama bilgilendirme amaçlıdır, kesinleşmiş kayıt anlamına gelmemekte olup ispat hukuku açısından geçerliliği bulunmamaktadır.

\* Üretici Bilgisi sorgulama GSM Association dan alınan veriler üzerinden yapılmakta olup sadece bilgilendirme amaçlıdır,





# AĞ TRAFİĞİ ANALİZİ

**Peki ya SSL trafik nasıl analiz edilir ? - MITM**

**Uygulama Native ise ve sertifika hatası alırsa iletişim kurmaz.**

**CA sertifikamızı güvenilir kök sertifikalara eklememiz gerekir.**

**Araçlar:** Android Emulator, Charles Proxy & Bouncy Castle

**URL:** <http://www.charlesproxy.com/>

**URL:** <http://bouncycastle.org/download/bcprov-jdk16-141.jar>



# AĞ TRAFİĞİ ANALİZİ

**Edit Android Virtual Device (AVD)**

Name:

Target:

CPU/ABI:

SD Card:

Size:

File:

Snapshot:

Enabled

Skin:

Built-in:

Resolution:  x

Hardware:

Property	Value	
Abstracted LCD density	160	
Max VM application heap size	24	
Device ram size	512	

Override the existing AVD with the same name

# AĞ TRAFİĞİ ANALİZİ

5554:Hack4Career

Charles 3.6.4 - Session 1 \*

File Edit View Proxy Tools Window Help

Structure Sequence

Overview Request Response Summary Chart Notes

Name Value

Name	Value
URL	https://[redacted]
Status	Failed
Failure	No request was made. Possibly the certificate was rejected.
Response Code	-
Protocol	HTTP/1.1
Method	CONNECT
Content-Type	-
Client Address	/192.168.1.34
Remote Address	[redacted]
<b>Timing</b>	
Request Start Time	29.04.2012 11:35:58
Request End Time	-
Response Start Time	-
Response End Time	-
Duration	-
Request Duration	-
Response Duration	-
Latency	-
Speed	0,00 KB/s
Response Speed	-
<b>Size</b>	

Structure

- http://api.[redacted].net
  - V3.5/
    - tools/
    - notification/
  - http://www.google-analytics.com
  - https://[redacted]
  - <default>

Copy URL  
Copy Response  
Save Response...  
Repeat  
Repeat Advanced...  
Edit  
Validate  
Sort By Name  
Ignore  
Clear  
Clear Others  
SSL Proxying  
Breakpoints  
No Caching

GET http://www.google

ma&utm=158847643&utmcs=UTF-8&utmsr=320x480&utmul=en-US&utmp=%2Flogin&utmcc=UA-3905012-8&utmcc=\_\_utma%3

mert

....

Giriş Yap

q w e r t y u i o p  
a s d f g h j k l  
z x c v b n m  
?123



# AĞ TRAFİĞİ ANALİZİ

```

komutlar.txt - Notepad
File Edit Format View Help
Yarat: AVD
İndir: http://bouncycastle.org/download/bcprov-jdk16-141.jar
Kopyala: C:\Program Files\Java\jre6\lib\ext\bcprov-jdk16-141.jar
İndir: http://www.charlesproxy.com/ssl.zip
Çalıştır:
emulator -avd Hack4Career

adb pull /system/etc/security/cacerts.bks cacerts.bks
keytool -keystore cacerts.bks -storetype BKS -provider
org.bouncycastle.jce.provider.BouncyCastleProvider
-storepass changeit -importcert -trustcacerts -alias somealias -file
charles-proxy-ssl-proxying-certificate.crt
-noprompt

adb remount

adb shell chmod 777 /system/etc/security/cacerts.bks

adb push cacerts.bks /system/etc/security/

İndir: http://android-group-korea.googlecode.com/files/mkfs.yaffs2.arm
Çalıştır:
adb push mkfs.yaffs2.arm /data/data/temp/mkfs.yaffs2
adb shell chmod 777 /data/data/temp/mkfs.yaffs2
adb shell

# /data/data/temp/mkfs.yaffs2 /system /sdcard/system.img
/data/data/temp/mkfs.yaffs2 /system /sdcard/system.img
mkfs.yaffs2: Android YAFFS2 Tool, Build by PowerGUI
at http://www.openhandsetalliance.org.cn
Building...
Build ok.
# exit
exit

adb pull /sdcard/system.img system.img
Kopyala: system.img -> C:\Users\Mert\.android\avd\Hack4Career.avd
emulator -avd Hack4Career -http-proxy http://192.168.1.34:8888

```



# AĞ TRAFİĞİ ANALİZİ

The image displays a mobile application interface on the left and the Charles proxy tool on the right. The app screen shows a login form with the name 'mert' and a 'Giriş Yap' button. Below the form, there is a link for users who are not yet members and buttons for registration and Facebook login. The Charles tool interface shows a captured request to a login endpoint with various parameters.

**Charles 3.6.4 - Session 1 \***

File Edit View Proxy Tools Window Help

Structure Sequence

- http://api.████████.net
- http://www.google-analytics.com
- https://████████.████████
- v3.5/
  - login?e=mert&p=mert&apikey=add2c3bf-b5

Overview Request Response Summary Chart Notes

e	mert
p	mert
apikey	████████-8011a8638b43
code	████████2f515068fc
ts	
lat	
lon	
aac	0.0
did	0000000000000000
ios	2.3.4
dtid	generic
isAndroid	true
ver	2.5
apiVer	3.5

Headers Query String Raw



# Kaynak Kodu İncelemelesi



# KAYNAK KODU İNCELEMESİ

**Native uygulamaların çoğu Java ile geliştirilmektedir.**

**Kaynak kodu incelemesi sayesinde birçok bilgi elde edinilebilir.**

**Gömülü şifreleme anahtarları, hatalı loglama, webservisler vs.**

**Dex2jar aracı ile class dosyasına dönüştürülmüş olan Android uygulaması, JD-GUI aracı ile kaynak koduna (decompile) geri çevrilebilir.**

**Kaynak koduna geri çeviren araçlar kimi zaman hatalı sonuçlar üretebilirler bu nedenle uygulamayı tersine çevirmek (disassembling) gerekebilir.**

**Araç: JD-GUI**

**URL: <http://java.decompiler.free.fr/?q=jdgui>**



# KAYNAK KODU İNCELEMESİ

```

UtilityClass.class X
public static String connectUpdate()
    throws XmlPullParserException, IOException
{
    dling = true;
    DefaultHttpClient localDefaultHttpClient = new DefaultHttpClient();
    Object localObject1 = new HttpGet("http://[REDACTED].appspot.com/[REDACTED]/getversion");
    Object localObject2 = "1";
    try
    {
        localObject1 = convertStreamToString(localDefaultHttpClient.execute((HttpRequest) localObject1).getEntity().getContent());
        localObject2 = localObject1;
        label150: return localObject2;
    }
    catch (Exception localException)
    {
        break label150;
    }
}

// ERROR //
private static String convertStreamToString(InputStream paramInputStream)
{
    // Byte code:
    // 0: new 274 java/io/BufferedReader
    // 3: dup
    // 4: new 276 java/io/InputStreamReader
    // 7: dup
    // 8: aload_0
    // 9: invokespecial 279 java/io/InputStreamReader:<init> (Ljava/io/InputStream;)V
    // 12: invokespecial 281 java/io/BufferedReader:<init> (Ljava/io/Reader;)V
    // 15: astore_2
    // 16: new 152 java/lang/StringBuilder
    // 19: dup
    // 20: invokespecial 282 java/lang/StringBuilder:<init> ()V

```





# KAYNAK KODU İNCELEMESİ



# KAYNAK KODU İNCELEMESİ



# KAYNAK KODU İNCELEMESİ

```
UtilityClass.class x
public static ArrayList<ImkbObject> getHisseList()
{
    dling = true;
    Object localObject1 = new DefaultHttpClient();
    Object localObject2 = new HttpGet("http://iphone. [REDACTED].com.tr/[REDACTED]_push/Service.asmx/getHisseList");
    ArrayList localArrayList = new ArrayList();
    try
    {
        localObject1 = ((HttpClient)localObject1).execute((HttpRequest)localObject2).getEntity();
        int i;
        if (localObject1 != null)
        {
            localObject1 = convertStreamToString(((HttpEntity)localObject1).getContent());
            localObject1 = ((String)localObject1).substring(((String)localObject1).indexOf('A'));
            localObject2 = ((String)localObject1).substring(0, ((String)localObject1).indexOf('<')).split(";");
            i = 0;
            int j = localObject2.length;
            if (i < j);
        }
        else
        {
            label197: dling = false;
            return localArrayList;
        }
        ImkbObject localImkbObject = new ImkbObject();
        String str = localObject2[i].replace('|', ';');
        String[] arrayOfString = str.split(";");
        for (int k = 0; ; k++)
        {
            if (k >= arrayOfString.length)
            {
```



# KAYNAK KODU İNCELEMESİ

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```

<?xml version="1.0" encoding="utf-8" ?>
<wsdl:definitions xmlns:s="http://www.w3.org/2001/XMLSchema" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/" xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
xmlns:tns="http://tempuri.org/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:tm="http://microsoft.com/wsdl/mime/textMatching/"
xmlns:http="http://schemas.xmlsoap.org/wsdl/http/" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
targetNamespace="http://tempuri.org/">
  <wsdl:types>
    <s:schema elementFormDefault="qualified" targetNamespace="http://tempuri.org/">
      <s:element name="getDovizHisseDetay">
        <s:complexType>
          <s:sequence>
            <s:element minOccurs="0" maxOccurs="1" name="abbr" type="s:string"/>
          </s:sequence>
        </s:complexType>
      </s:element>
      <s:element name="getDovizHisseDetayResponse">
        <s:complexType>
          <s:sequence>
            <s:element minOccurs="0" maxOccurs="1" name="getDovizHisseDetayResult" type="s:string"/>
          </s:sequence>
        </s:complexType>
      </s:element>
      <s:element name="getDovizList">
        <s:complexType/>
      </s:element>
      <s:element name="getDovizListResponse">
        <s:complexType>
          <s:sequence>
            <s:element minOccurs="0" maxOccurs="1" name="getDovizListResult" type="s:string"/>
          </s:sequence>
        </s:complexType>
      </s:element>
      <s:element name="getHisseList">
        <s:complexType/>
      </s:element>
      <s:element name="getHisseListResponse">
        <s:complexType>
  
```



# Tersine Çevirme (Disassembling)



# TERSİNE ÇEVİRME

**Kaynak koduna çevirmenin yeterli/ başarılı olmadığı durumlarda dex dosyası tersine çevrilerek (disassembling) analiz edilebilir.**

**Uygulamanın akışını değiştirmek, yamamak (patch) için de kullanılır.**

**Araç:** android-apktool

**URL:** <http://code.google.com/p/android-apktool/downloads/list>

**Komut (Disassemble):** java -jar apktool.jar d Uygulama.apk

**Komut (Assemble):** java -jar apktool.jar b Uygulama Uygulama.apk



# TERSİNE ÇEVİRME

```
297 # virtual methods
298 .method public ZamanNeAlemde (LProb/GeriGel_Prob;Landroid/content/Context;)Ljava/lang/Boolean;
299     .locals 7
300     .parameter "gerici"
301     .parameter "con"
302
303     .prologue
304     const/4 v6, 0x1
305
306     const/4 v4, 0x0
307
308     .line 135
309     :try_start_0
310
311     invoke-static {}, Ljava/util/Calendar;-->getInstance()Ljava/util/Calendar;
312
313     move-result-object v0
314
315     .line 138
316     .local v0, cc:Ljava/util/Calendar;
317     invoke-virtual {v0}, Ljava/util/Calendar;-->getTime()Ljava/util/Date;
318
319     move-result-object v3
320
321     .line 139
322     .local v3, simdiki:Ljava/util/Date;
323     new-instance v2, Ljava/util/Date;
324
325     invoke-virtual {p1}, LProb/GeriGel_Prob;-->getNezamanCozum()Ljava/lang/String;
326
327     move-result-object v5
328
329     invoke-direct {v2, v5}, Ljava/util/Date;--><init>(Ljava/lang/String;)V
330
```



# TERSİNE ÇEVİRME

**URL:** [http://pallergabor.uw.hu/androidblog/dalvik\\_opcodes.html](http://pallergabor.uw.hu/androidblog/dalvik_opcodes.html)

## Dalvik opcodes

Author: [Gabor Paller](#)

Vx values in the table denote a Dalvik register. Depending on the instruction, 16, 256 or 64k registers can be accessed. Operations on long and double values use two registers, e.g. a double value addressed in the V0 register occupies the V0 and V1 registers.

Boolean values are stored as 1 for true and 0 for false. Operations on booleans are translated into integer operations.

All the examples are in big-endian format, e.g. 0F00 0A00 is coded as 0F, 00, 0A, 00 sequence.

Note there are no explanation/example at some instructions. This means that I have not seen that instruction "in the wild" and its presence/name is only known from [Android opcode constant list](#).

Opcode (hex)	Opcode name	Explanation	Example
00	nop	No operation	0000 - nop
01	move vx,vy	Moves the content of vy into vx. Both registers must be in the first 256 register range.	0110 - move v0, v1 Moves v1 into v0.
02	move/from16 vx,vy	Moves the content of vy into vx. vy may be in the 64k register range while vx is one of the first 256 registers.	0200 1900 - move/from16 v0, v25 Moves v25 into v0.
03	move/16		
04	move-wide		
05	move-wide/from16 vx,vy	Moves a long/double value from vy to vx. vy may be in the 64k register range while vx is one of the first 256 registers.	0516 0000 - move-wide/from16 v22, v0 Moves v0 into v22.
06	move-wide/16		
07	move-object vx,vy	Moves the object reference from vy to vx.	0781 - move-object v1, v8 Moves the object reference in v8 to v1.
08	move-object/from16 vx,vy	Moves the object reference from vy to vx, vy can address 64k registers and vx can address 256 registers.	0801 1500 - move-object/from16 v1, v21 Move the object reference in v21 to v1.
09	move-object/16		
0A	move-result vx	Move the result value of the previous method invocation into vx.	0A00 - move-result v0 Move the return value of a previous method invocation into v0.
0B	move-result-wide vx	Move the long/double result value of the previous method invocation into vx,vx+1.	0B02 - move-result-wide v2





# Dosya Sistemi İncelemesi



# DOSYA SİSTEMİ İNCELEMESİ

Android, uygulamalara verilerini saklamak için 4 seçenek sunmaktadır; Dahili depolama, Harici depolama, Veritabanı (SQLite) ve Shared Preferences

**Veritabanı:** Yapısal depolama için kullanılır.

**Shared Preferences:** Basit depolama için kullanılır.

**Harici Depolama:** Özel olmayan büyük veri setlerini saklamak için kullanılır.

**Dahili Depolama:** Özel verileri saklamak için kullanılır.

**Araçlar:** adb ve Sqlite

**URL:** <http://www.sqlite.org/download.html>



# DOSYA SİSTEMİ İNCELEMESİ

```
C:\Windows\system32\cmd.exe - adb shell

C:\Users\Mert>adb shell
# cd data/data/com.██████████/shared_prefs
cd data/data/com.██████████/shared_prefs
# cat GeriGel.xml
cat GeriGel.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<boolean name="isAkdif" value="false" />
<string name="Nezaman">4713DDA0D000F2C5AF3C78EB4DA473EC9E67597C7A0C30AC33ACAFE3D
22CE935514709C927710FB379771B60E82BE892</string>
<int name="Nerden" value="7" />
<string name="BelkiLazimOlur">8EE2B284310D25297D5389438C8DD68A</string>
<int name="KatKey" value="1" />
</map>
#
```

# DOSYA SİSTEMİ İNCELEMESİ

```
C:\Windows\system32\cmd.exe - sqlite [REDACTED].AS

C:\Users\Mert\Desktop\NOPcon>sqlite [REDACTED].AS
SQLite version 3.7.11 2012-03-20 11:35:50
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
EkAlan          [REDACTED] Table          android_metadata
Kategori        [REDACTED] Table          android_metadata
Kullanici       [REDACTED] Table          android_metadata
sqlite> select * from [REDACTED] Table;
1|1|Hack4Career|Hack4Career|http://mertsarica|65195E82A27897F01C4E1A10030D58E1|FA4ABFEAF248393D2A58756506DCAA33
sqlite> select * from Kullanici;
1|916834009920CC19DE6E61C3F9E21439|2|
sqlite> select * from Kategori;
1|Hack4Career
sqlite> select * from EkAlan;
sqlite> ■
```

# İzinler



# İZİNLER

AndroidManifest.xml dosyası AXMLPrinter2.jar aracı ile okunabilir.

**Komut:** java -jar AXMLPrinter2.jar AndroidManifest.xml

**URL:** <http://code.google.com/p/android4me/downloads/list>

```
<uses-permission android:name="android.permission INTERNET" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission RECEIVE_SMS" />
<uses-permission android:name="android.permission SEND_SMS" />
<uses-permission android:name="android.permission READ_SMS" />
<uses-permission android:name="android.permission CALL_PHONE" />
<uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS" />
<uses-permission android:name="android.permission.DELETE_PACKAGES" />
<uses-permission android:name="android.permission.INSTALL_PACKAGES" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
```



# İZINLER

OVERVIEW
USER REVIEWS
WHAT'S NEW
PERMISSIONS

## Permissions

**THIS APPLICATION HAS ACCESS TO THE FOLLOWING:**

**SERVICES THAT COST YOU MONEY**

**DIRECTLY CALL PHONE NUMBERS**  
 Allows the app to call phone numbers without your intervention. Malicious apps may cause unexpected calls on your phone bill. Note that this doesn't allow the app to call emergency numbers.

**YOUR LOCATION**

**FINE (GPS) LOCATION**  
 Access fine location sources such as the Global Positioning System on the tablet, where available. Malicious apps may use this to determine where you are, and may consume additional battery power. Access fine location sources such as the Global Positioning System on the phone, where available. Malicious apps may use this to determine where you are, and may consume additional battery power.

**COARSE (NETWORK-BASED) LOCATION**  
 Access coarse location sources such as the cellular network database to determine an approximate tablet location, where available. Malicious apps may use this to determine approximately where you are. Access coarse location sources such as the cellular network database to determine an approximate phone location, where available. Malicious apps may use this to determine approximately where you are.

**NETWORK COMMUNICATION**

**FULL INTERNET ACCESS**  
 Allows the app to create network sockets.

**YOUR PERSONAL INFORMATION**



# İZINLER

OVERVIEW USER REVIEWS WHAT'S NEW PERMISSIONS

## Permissions

**THIS APPLICATION HAS ACCESS TO THE FOLLOWING:**

**SERVICES THAT COST YOU MONEY**

**DIRECTLY CALL PHONE NUMBERS**  
 Allows the app to call phone numbers without your intervention. Malicious apps may cause unexpected calls on your phone bill. Note that this doesn't allow the app to call emergency numbers.

**SEND SMS MESSAGES**  
 Allows the app to send SMS messages. Malicious apps may cost you money by sending messages without your confirmation.


**HARDWARE CONTROLS**

**TAKE PICTURES AND VIDEOS**  
 Allows the app to take pictures and videos with the camera. This allows the app at any time to collect images the camera is seeing.

**YOUR LOCATION**

**FINE (GPS) LOCATION**  
 Access fine location sources such as the Global Positioning System on the tablet, where available. Malicious apps may use this to determine where you are, and may consume additional battery power. Access fine location sources such as the Global Positioning System on the phone, where available. Malicious apps may use this to determine where you are, and may consume additional battery power.

**COARSE (NETWORK-BASED) LOCATION**  
 Access coarse location sources such as the cellular network database to determine an approximate tablet location, where available. Malicious apps may use this to determine approximately where you are. Access coarse location



18 İzin



# İZİNLER

OVERVIEW
USER REVIEWS
WHAT'S NEW
PERMISSIONS

## User Ratings

5 star	19
4 star	5
3 star	1
2 star	4
1 star	8

Average rating:

## 3.6

★★★★☆  
37

## User Reviews

[Write a Review >](#)

All Versions ▾
All Devices ▾
Sort by Helpfulness ▾

**gry** on March 26, 2012 (Samsung Galaxy S with version 1.0.0) [↔](#)

★★★★★ **Cok basarili hakikaten nasil dusunmusler boyle birseyi. Guven veren bir ...**

Cok basarili hakikaten nasil dusunmusler boyle birseyi. Guven veren bir uygulama.artik hayat mobilde:)

[👍](#) [👎](#) [Spam](#)

---

**ulysses** on July 9, 2011 (Samsung Galaxy S with version 1.0.0) [↔](#)

★★★★★ **asiri derecede gereksiz [REDACTED] kartin son 4 hanesi nedir. ibinternet subene son 4 hane ...**

asiri derecede gereksiz. [REDACTED] kartin son 4 hanesi nedir. ibinternet subene son 4 hane ile mi aliyosun. **bi de uygulamanin izinleri nedir oyle.**

[👍](#) [👎](#) [Spam](#)

# Örnek Zafiyetler



# #1



# ÖRNEK ZAFİYET

5554:Hack4Career

Charles 3.6.4 - Session 1 \*

File Edit View Proxy Tools Window Help

Structure Sequence

Overview Request Response Summary Chart Notes

username mert

password A7-71-DA-5D-CC-62-18-16-09-05-31-1D-9D-38-50-3E

headers Text Hex Form Raw

POST http://webservicess[redacted].com/[redacted]CatalogWebService/CatalogExportMobile.asmx/Mobile\_Login2

No Caching Recording

Kullanıcı Girişi Yeni Üye

üyesiyseniz:

Kullanıcı Adı mert

Şifre .....

Beni Hatırla Hayır

Giriş yapılamadı. Lütfen şifre ve kullanıcı adınızı kontrol ediniz.

26 ESKİŞEHİR 27 GAZİANTEP 31 HATAY

Giriş Yap

md5

replay

http



# #2



# ÖRNEK ZAFİYET

```
PrefHelper.class  Helper.class  User.class  UserAreas.class  Activity.class x
    Activity.this.startApp();
    paramDialogInterface.dismiss();
    }
    });
    localObject = ((AlertDialog.Builder)localObject).create();
    }
    return (Dialog)localObject;
    }

    public void onLoginClick(View paramView)
    {
        this.name = this.user_name.getText().toString();
        this.pass = this.password.getText().toString();
        Log.i("v", "user name:" + this.name + " şifre:" + this.pass);
        this.pass = WebServis.convetoMd5(this.pass);
        this.remember = this.remBtn.isChecked();
        if ((!this.name.equals("")) && (!this.pass.equals("")))
        {
            this.pb.setVisibility(0);
            new LoginTask(null).execute(new Object[0]);
        }
        else
        {
            InovelUtils.showToastError(getApplicationContext(), getString(2131034114));
        }
    }

    public void startApp()
    {
        if (!PrefHelper.getRemember(this))
        {
            new CityTask(null).execute(new Object[0]);
        }
        else
        {
            this.name = PrefHelper.getUserName(this);
        }
    }
}
```



# ÖRNEK ZAFİYET

The image shows a mobile application login screen on the left and a Charles proxy tool interface on the right. The mobile app screen displays a login form with the following fields and options:

- Kullanıcı Girişi** (User Login) with a **Yeni Üye** (New User) button.
- üyesiyseniz:** (If you are a member:)
- Kullanıcı Adı** (Username): mert
- Şifre** (Password): masked with dots
- Beni Hatırla** (Remember me) checkbox, currently unchecked, with a **Hayır** (No) button.
- Şehir Seçimi :** (City Selection): 26 ESKİŞEHİR, 27 GAZİANTEP, 31 HATAY
- Giriş Yap** (Login) button.

The Charles proxy tool interface shows a session titled "Charles 3.6.4 - Session 1". The Structure pane displays the request path: `http://webservices[redacted].com/CatalogWebService/CatalogExportMobile.asmx/Mobile_Login2`. The Overview pane shows the request details:

- username:** mert
- password:** A7-71-DA-5D-CC-62-18-16-09-05-31-ID-9D-38-50-3E

A command prompt window is open, showing the following commands and output:

```
C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\NOPcon>adb logcat -d -v time > log.txt
C:\Users\Mert\Desktop\NOPcon>cat log.txt | grep mert
04-29 12:09:03.991 I/v      < 320>: user name:mert &vifre:mert
04-29 12:09:04.080 I/v      < 320>: 0-mert
C:\Users\Mert\Desktop\NOPcon>
```

The bottom status bar of the Charles interface shows the request details: `POST http://webservices[redacted].com/[redacted]CatalogWebService/CatalogExportMobile.asmx/Mobile_Login2` with `No Caching` and `Recording` options.



# #3





# ÖRNEK ZAFİYET

OVERVIEW
USER REVIEWS
WHAT'S NEW
PERMISSIONS

## Description

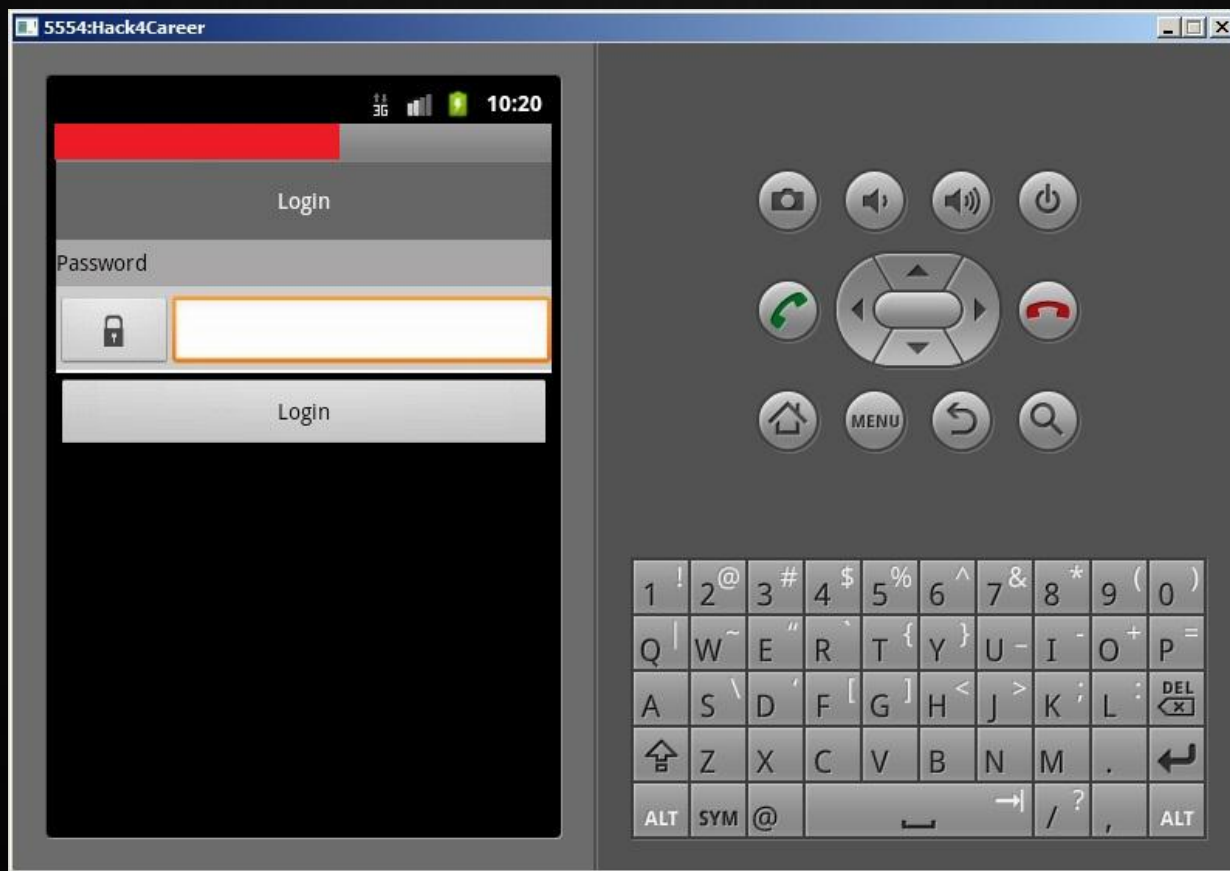
██████████ stores your passwords securely. All passwords protected by master password and access them all with single password. It has user friendly interface and easy to use. It uses the AES encryption for store your passwords. You can copy and paste your password wherever you want.

██████████ tüm şifrelerinizi güvenli bir şekilde saklar. Tüm şifrelerinize sadece bir ana şifre ile erişirsiniz. Kullanıcı dostu bir arayüze sahiptir ve kullanımı kolaydır. Gelişmiş bir şifreleme yöntemi olan AES şifreleme sistemini kullanır. Şifrelerinizi ve diğer bilgileri kopyalayıp istediğiniz uygulamaya yapıştırabilirsiniz.

[Visit Developer's Website >](#)    [Email Developer >](#)

## App Screenshots

# ÖRNEK ZAFİYET



# ÖRNEK ZAFİYET



# ÖRNEK ZAFİYET

```
Gerigel.class  GeriGel_Prob.class  Login.class  X
public void Kaydet(View paramView)
{
    Statix.Criptorix = this.Sifre.getText().toString();
    if (!this.KayitVar.booleanValue())
        if (this.Sifre.getText().toString().length() > 5)
        {
            Statix.ZamaniDurdur(2, 2);
            User_Prob localUser_Prob = new User_Prob(Integer.valueOf(0), this.Sifre.getText().toSt
            InsertS localInsertS = new InsertS(this);
            localInsertS.insert(localUser_Prob);
            KayitSornarsi(getString(2130968595) + " : " + this.Sifre.getText().toString(), this);
            localInsertS.Close();
            UserMainMetot.Giris(this, this.Sifre.getText().toString());
            this.gu.setSifre(this.Sifre.getText().toString());
            this.edt.putString("BelkiLazimOlur", this.gu.getSifreSifreli());
            this.edt.commit();
            this.Sifre.setText("");
        }
    while (true)
    {
```



# ÖRNEK ZAFİYET

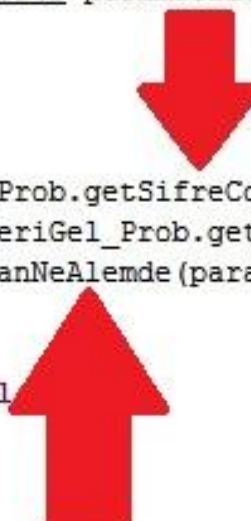
```

Gerigel.class  GeriGel_Prob.class  Login.class  X
public void onCreate(Bundle paramBundle)
{
    setTitle("Mobile");
    super.onCreate(paramBundle);
    setContentView(2130903050);
    .logcu();
    this.gerikayit = getSharedPreferences("GeriGel", 0);
    this.edt = this.gerikayit.edit();
    this.ger = new GeriGel_Prob(this.gerikayit.getString("Nezaman", Gerigel.tarih(Boolean.valueOf(false)
try
{
    this.v = nerdekaldik(this.ger);
    if (this.v != null)
    {
        C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\NOPcon>adb shell cat /data/data/com. /shared_prefs/GeriGel.xml
1 <?xml version='1.0' encoding='utf-8' standalone='yes' ?>
t <map>
t <boolean name="isAkdif" value="false" />
t <string name="Nezaman">4713DDA0D000F2C5AF3C78EB4DA473EC9E67597C7A0C30AC33ACAFE3D
t 22CE935514709C9227710FB379771B60F52BE892</string>
t <int name="Nerden" value="7" />
t <string name="BelkiLazimOlur">8EE2B284310D25297D5389438C8DD68A</string>
t <int name="KatKey" value="1" />
t </map>
C:\Users\Mert\Desktop\NOPcon>
    }
    }
}

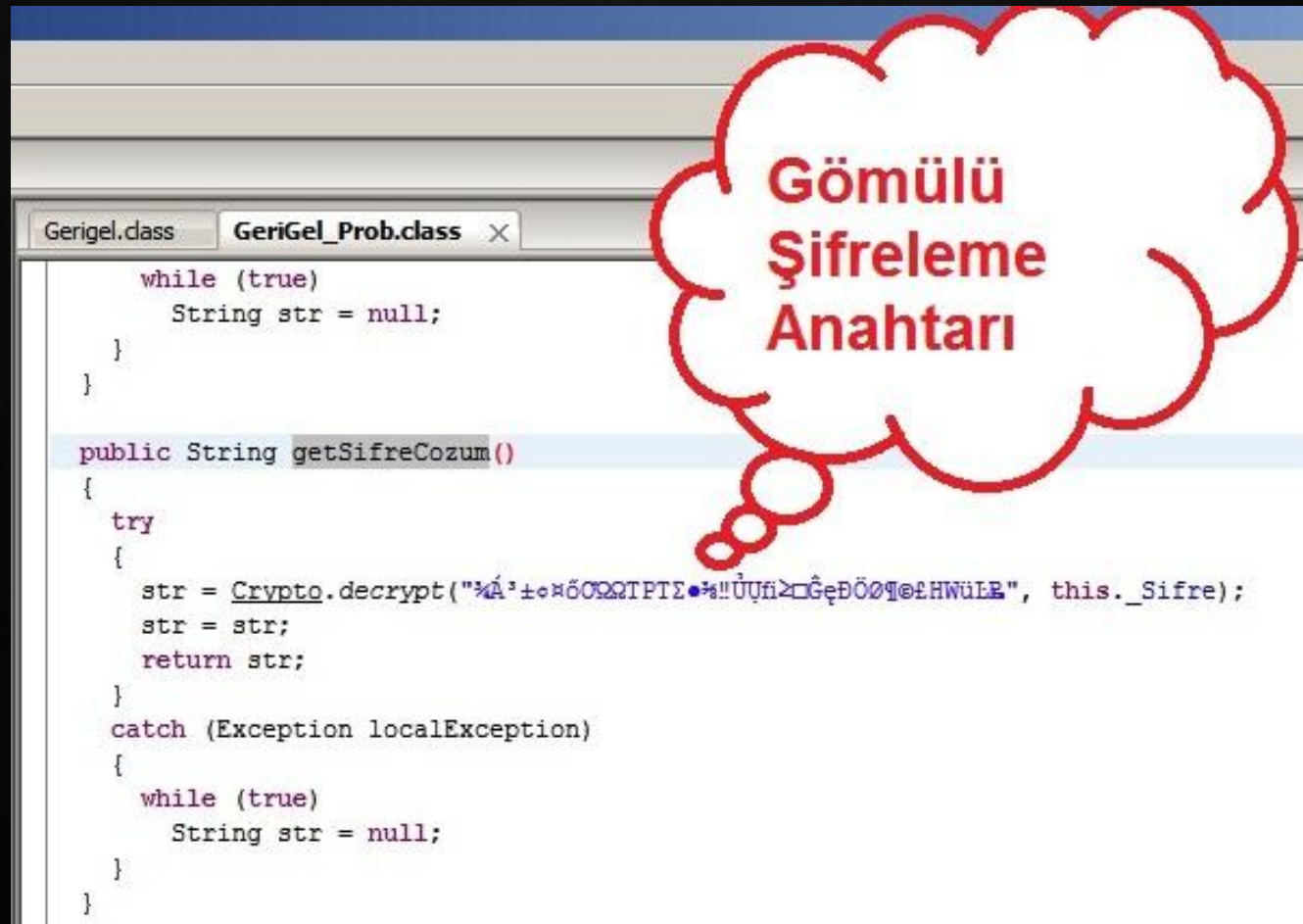
```

# ÖRNEK ZAFİYET

```
Gerigel.class  GeriGel_Prob.class  Login.class X
private Boolean nerdekaldik(GeriGel_Prob paramGeriGel_Prob)
{
    Boolean localBoolean;
    try
    {
        Statix.Criptorix = paramGeriGel_Prob.getSifreCozum();
        UserMainMetot.Giris(this, paramGeriGel_Prob.getSifreCozum());
        localBoolean = new Gerigel().ZamanNeAlemde(paramGeriGel_Prob, this);
        if (localBoolean == null)
        {
            UserMainMetot.GirisYapti = null;
            localBoolean = null;
        }
    }
    catch (Exception localException)
    {
        UserMainMetot.GirisYapti = null;
        localBoolean = null;
    }
    return localBoolean;
}
```



# ÖRNEK ZAFİYET



```
Gerigel.class  GeriGel_Prob.class X
while (true)
    String str = null;
}
}

public String getSifreCozum()
{
    try
    {
        str = Crypto.decrypt("%Á'±ø*8002TPTΣ•*!úfi>□GēĐ0Q@lHWuLE", this._Sifre);
        str = str;
        return str;
    }
    catch (Exception localException)
    {
        while (true)
            String str = null;
    }
}
}
```

Gömülü  
Şifreleme  
Anahtarı

# ÖRNEK ZAFİYET

```

GeriGel.class  x  GeriGel_Prob.class  KeyBoxLogin.class
public Boolean ZamanNeAlemde(GeriGel_Prob paramGeriGel_Prob, Context paramContext)
{
    Boolean localBoolean = null;
    try
    {
        if (Calendar.getInstance().getTime().compareTo(new Date(paramGeriGel_Prob.getNezamanCozum())) >= 0)
        {
            Statix.setKategori_Prob(null);
            Statix.ikizamnıdadurdur();
            UserMainMetot.GirisYapti = null;
            Statix.setKeyBox_Prob(null);
            Statix.eDegerss = null;
            Statix.eTanimss = null;
            if (Copy.copyx != null)
            {
                Copy.copyx.setText("");
                Statix.Criptorix = "";
            }
        }
        else if (paramGeriGel_Prob.getNerde() > 1)
        {
            if (paramGeriGel_Prob.getKatKey() != 0)
            {
                if (paramGeriGel_Prob.getisAktif().booleanValue())
                {
                    kategoriyukel(paramGeriGel_Prob.getKatKey(), paramContext);
                    while (true)
                    {
                        Statix.k = paramGeriGel_Prob.getNerde();
                        localBoolean = Boolean.valueOf(true);
                        break;
                        keyboxyukle(paramGeriGel_Prob.getKatKey(), paramContext);
                    }
                }
                Statix.k = paramGeriGel_Prob.getNerde();
                localBoolean = Boolean.valueOf(false);
            }
        }
        else if (paramGeriGel_Prob.getNerde() == 1)
        {
            Statix.k = 1;
            localBoolean = Boolean.valueOf(true);
            localBoolean = localBoolean;
        }
        label165: return localBoolean;
    }
    catch (Exception localException)
    {
        break label165;
    }
}

```





# ÖRNEK ZAFİYET

```
Login.smali  Gerigel.smali
297 # virtual methods
298 .method public ZamanNeAlemde (LProb/GeriGel_Prob;Landroid/content/Context;)Ljava/lang/Boolean;
299   .locals 7
300   .parameter "gerici"
301   .parameter "con"
302
303   .prologue
304   const/4 v6, 0x1
305
306   const/4 v4, 0x0
307
308   .line 135
309   :try_start_0
310
311   # M.S
312   goto :cond_10
313
314   invoke-static {}, Ljava/util/Calendar;->getInstance()Ljava/util/Calendar;
315
316   move-result-object v0
317
318   .line 138
319   .local v0, cc:Ljava/util/Calendar;
320   invoke-virtual {v0}, Ljava/util/Calendar;->getTime()Ljava/util/Date;
321
322   move-result-object v3
323
324   .line 139
325   .local v3, simdiki:Ljava/util/Date;
326   new-instance v2, Ljava/util/Date;
327
328   invoke-virtual {p1}, LProb/GeriGel_Prob;->getNezamanCozum()Ljava/lang/String;
329
330   move-result-object v5
331
332   invoke-direct {v2, v5}, Ljava/util/Date;-><init>(Ljava/lang/String;)V
333
334   .line 140
```



# ÖRNEK ZAFİYET



# SONUÇ

**Gizlilik ile sağlanmaya çalışılan güvenlik (Security Through Obscurity) faydadan çok zarar getirir.**

**Google Play'e yüklenen her uygulama art niyetli kişiler tarafından indirilebilir ve analiz edilebilir.**

**Güvenliğiniz, müşterilerinizin güvenliği, itibarınız ve/veya marka değeriniz için uygulamalarınızı test edin veya ettirin!**

**Uygulamalarınızın en az yetki ile çalışmasına , sadece ve sadece ihtiyacı olan izinler ile çalışmasına özen gösterin.**

**Harici diskin tüm uygulamalar tarafından okunabildiğini unutmayın.**



# SORULAR?



# TEŞEKKÜRLER

