
	<h1>INGENIERÍA DE SISTEMAS</h1>	 INICIAL APELLIDO PATERNO
	<h2>AUDITORIA DE SISTEMAS</h2>	
<h3>EXAMEN FINAL</h3>		
NOMBRES	APELLIDO PATERNO	APELLIDO MATERNO
EDSON JAVIER	PACO	LIMACHI
CI.	CEL.	FECHA
5972576	73734591	02/07/2023

TABLA DE CONTENIDO

examen final.....	2
Pregunta.....	2
PROCESO DE DESCARGA DE LA primera aplicación	2
Análisis del archivo AndroidManifest	5
Proceso de descarga de la segunda aplicación	10
Análisis del archivo AndroidManifest	14
Conclusiones	16

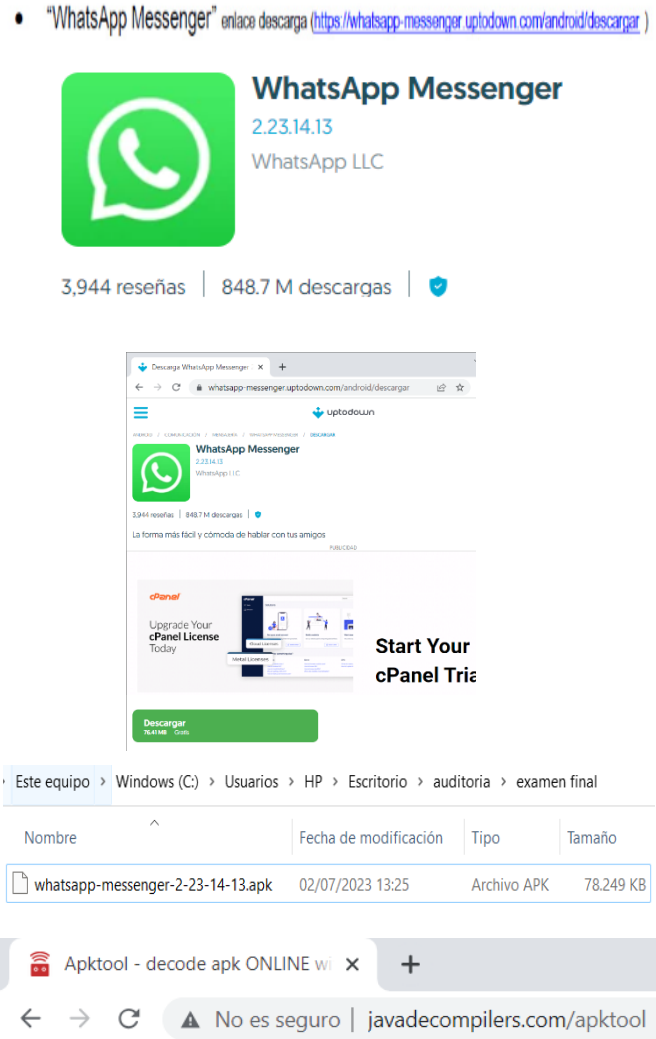
EXAMEN FINAL

PREGUNTA

2.2. LABORATORIO 2 (Auditoria informática de una Aplicación Móvil - APP).

Para este laboratorio debe realizar paso a paso y con capturas de pantalla de todo el procedimiento realizado en función de los siguientes puntos:

- De las siguientes App:
 - "WhatsApp Messenger" enlace descarga (<https://whatsapp-messenger.uptodown.com/android/descargar>)
 - "TikTok" enlace descarga (<https://tiktok.uptodown.com/android/descargar>)
- Debe realizar de ambas App el procedimiento de "De compilación" y buscar la mayor cantidad de códigos maliciosos y/o permisos innecesarios (Sobre este punto debe describir e investigar minuciosamente los permisos descubiertos y/o códigos maliciosos encontrados...)
- A parte de descubrir los códigos maliciosos y/o permisos innecesarios de las Aplicaciones puestas a prueba en función a la "De compilación" (IMPRESINDIBLE), debe tratar de descubrir los malwares maliciosos que tienen las APP en función a códigos extraños que encuentren, si descubre una mayor cantidad de software malicioso, la asignación de la nota será mayor.

CAPTURAS	EXPLICACION
<p>• "WhatsApp Messenger" enlace descarga (https://whatsapp-messenger.uptodown.com/android/descargar)</p> 	<p>PROCESO DE DESCARGA DE LA PRIMERA APLICACIÓN</p> <ol style="list-style-type: none">1. Ingresamos al link que nos proporciona2. Podemos apreciar que no es una pagina oficial3. Procedemos a descargar el archivo APK4. Podemos ver que tiene 8487M de descargas y mas de 3000 reseñas5. En la imagen podemos ver la imagen de la aplicación y del botón de descarga6. Damos clic al botón de descarga7. Podemos apreciar que se realizo la descarga cabe destacar que debe ser con la extensión .APK8. Procedemos abrir la herramienta a utilizar que es el software online APKTOOLS que es desarrollada por JAVA para realizar la reingeniería a las aplicaciones móviles

Decompilers online

Apktool - Reverse engineer Android apk files

Decode resources from the apk file to its original form

Seleccionar archivo Ninguno archivo selec.

Upload and Decompile

Select a decompiler

Apktool - decoding assets

APK decompiler

ApkTool online

Knowledge base

Selecciónar archivo Ninguno archivo selec.

Upload and Decompile

whatsapp-messenger-2-23-14-13.apk 02/07/2023 13:25 Archivo APK 78.249

whatsapp-messenger-2-23-14-13.apk Archivo APK

Abrir Cancelar

Selecciónar archivo Ninguno archivo selec.

Selecciónar archivo whatsapp...-14-13.apk

Upload and Decompile

Apktool - decode apk ONLINE wi

No es seguro | ja

Decompilers online

Decompilation Results

File Name: whatsapp-messenger-2-23-14-13.apk

Decompiler: apktool

Job status: Done.

Save

whatsapp-messenger-2-23-14-13.apk		
res	folder	
unknown	folder	
lib	folder	
META-INF	folder	
kotlin	folder	
assets	folder	
original	folder	
classes3.dex	.dex	7.81 MB
classes5.dex	.dex	2.29 MB
classes2.dex	.dex	11.7 MB
classes4.dex	.dex	2.44 MB
AndroidManifest.xml	.xml	162 KB
apktool.yml	.yml	125 KB

9. Apreciamos la pantalla de inicio de la aplicación

10. Nos debemos ir la opción que indica en la imagen

11. Procedemos a cargar el archivo

12. Indicamos la ubicación

13. Una vez cargada damos al clic al botón de **upload**

14. Procedemos a ver que empieza a cargar la aplicación por lo cual significa que esta cargando el archivo

15. Una vez finalizado nos da la siguiente opción

16. Nos muestra los archivos de compilados de la aplicación



Nombre: whatsapp-messenger-2-23-14-13_decoded_by_apktool

Tipo: Archivo WinRAR ZIP

whatsapp-messenger-2-23-14-13_decod... 02/07/2023 13:54

whatsapp-messenger-2-23-14-13_decod...

whatsapp-messenger-2-23-14-13_decod...

assets	02/07/2023 13:42	Carpeta de archivos	
kotlin	02/07/2023 13:42	Carpeta de archivos	
lib	02/07/2023 13:42	Carpeta de archivos	
META-INF	02/07/2023 13:42	Carpeta de archivos	
original	02/07/2023 13:42	Carpeta de archivos	
res	02/07/2023 13:42	Carpeta de archivos	
unknown	02/07/2023 13:42	Carpeta de archivos	
AndroidManifest	02/07/2023 13:42	Microsoft Edge HT...	163 KB
apktool.yml	02/07/2023 13:42	Archivo YML	126 KB
classes2.dex	02/07/2023 13:42	Archivo DEX	12.009 KB
classes3.dex	02/07/2023 13:42	Archivo DEX	8.002 KB
classes4.dex	02/07/2023 13:42	Archivo DEX	2.500 KB
classes5.dex	02/07/2023 13:42	Archivo DEX	2.349 KB

AndroidManifest 02/07/2023 13:42

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" android:compileSdkVersion="33"
android:compileSdkVersionCode="13" package="com.whatsapp" platformBuildVersionName="13">
  <uses-feature android:name="android.hardware.bluetooth" android:required="false"/>
  <uses-feature android:name="android.hardware.location" android:required="false"/>
  <uses-feature android:name="android.hardware.location.network" android:required="false"/>
  <uses-feature android:name="android.hardware.location.gps" android:required="false"/>
  <uses-feature android:name="android.hardware.camera" android:required="false"/>
  <uses-feature android:name="android.hardware.nfc" android:required="false"/>
  <uses-feature android:name="android.hardware.wifi" android:required="false"/>
  <uses-feature android:name="android.hardware.telephony" android:required="false"/>
  <queries>
    <queryes>
      <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
      <uses-permission android:name="android.permission.VIBRATE"/>
      <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
      <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
      <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
      <uses-permission android:name="android.permission.READ_PHONE_NUMBERS"/>
      <uses-permission android:name="android.permission.RECEIVE_SMS"/>
      <uses-permission android:name="android.permission.USE_BIOMETRIC"/>
      <uses-permission android:name="android.permission.USE_FINGERPRINT"/>
      <uses-permission android:name="android.permission.AUTHENTICATE_ACCOUNTS"/>
      <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
      <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
      <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
      <uses-permission android:name="android.permission.INTERNET"/>
      <uses-permission android:name="android.permission.NEARBY_WIFI_DEVICES" android:usesPermissionFlags="android.permission.ACCESS_WIFI_STATE"/>
      <uses-permission android:name="android.permission.CAMERA"/>
      <uses-permission android:name="android.permission.RECORD_AUDIO"/>
      <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
      <uses-permission android:name="android.permission.MANAGE_OWN_CALLS"/>
      <uses-permission android:name="android.permission.CALL_PHONE"/>
      <uses-permission android:name="android.permission.ACCESS_MEDIA_LOCATION"/>
    </queryes>
  </queries>
</xml>
```

17. Procedemos a descargar los archivos
18. Damos clic a la opción que nos indica SAVE

19. Damos la ruta donde se guardara los archivos
20. Podemos apreciar que es en formato comprimido .ZIP

21. Podemos apreciar el archivo
22. Procedemos a realizar la extracción de los archivos

23. Una vez finalizado este proceso podemos ver los documentos de compilados del archivo .APK

24. Podemos ver que hay un archivo llamado AndroidManifest
25. Este es el archivo que realizaremos la auditoria

26. Podemos apreciar el archivo .XML que debemos analizar

ANÁLISIS DEL ARCHIVO ANDROIDMANIFEST

```
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
```

Permite el acceder al estado de la conexión de red del móvil

```
<uses-permission android:name="android.permission.VIBRATE"/>
```

Permite controlar vibración del dispositivo

```
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
```

Permite acceder a la ubicación aproximada del dispositivo

```
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
```

Permite acceder a la ubicación precisa del dispositivo

```
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
```

Permite leer el estado del teléfono como el IMEI y el número de teléfono

```
<uses-permission android:name="android.permission.READ_PHONE_NUMBERS"/>
```

Permite leer los números de teléfono asociados

```
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
```

Permite leer y recibir sms

```
<uses-permission android:name="android.permission.USE_BIOMETRIC"/>
```

permite usar funciones biométricas como huella o reconocimiento facial

```
<uses-permission android:name="android.permission.USE_FINGERPRINT"/>
```

Permite la autenticación de huella

```
<uses-permission android:name="android.permission.AUTHENTICATE_ACCOUNTS"/>
```

permite autenticar cuentas de usuario

```
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
```

Permite acceder a cuentas configuradas del dispositivo

```
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
```

Permite acceder al estado de conexión wifi

```
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
```

Permite cambiar al estado de conexión wifi

```
<uses-permission android:name="android.permission.INTERNET"/>
```

Permite el acceso a internet

```
Usespermission android:name="android.permission.NEARBY_WIFI_DEVICES" android:usesPermis  
sionFlags="0x00010000"/>
```

Permit el acceso a dispositivos wifi cercanos

```
<uses-permission android:name="android.permission.CAMERA"/>
```

Permite acceso a la camara del dispositivo

```
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
```

Permite al uso del microfono y grabar audio

```
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
```

Permite leer archivos almacenados externamente al dispositivo

```
<uses-permission android:name="android.permission.MANAGE_OWN_CALLS"/>
```

Permite accionar llamadas telefonicos entrants y salidas

```
<uses-permission-sdk-23 android:name="android.permission.CALL_PHONE"/>
```

permite realizar llamadas desde la aplicación

```
<uses-permission android:name="android.permission.ACCESS_MEDIA_LOCATION"/>
```

Permite acceder a la ubicacion de los medios FOTOS VIDEOS ETC (ACTIVIDAD SOSPECHOSA E INNECESARIA)

```
<uses-permission android:name="android.permission.BLUETOOTH"/>
```

Permite usar funciones de bluetooth (ACTIVIDAD SOSPECHOSA E INNECESARIA)

```
<uses-permission android:name="android.permission.BROADCAST_STICKY"/>
```

Permite enviar transmisiones Sticky que se mantiene en el sistema (peligroso)

```
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
```

Permite cambiar el estado de la conexión de red

```
<uses-permission android:name="android.permission.FOREGROUND_SERVICE_DATA_SYNC"/>
```

Permite sincronizar datos en segundo plano utilizando un servicio en primer plano.

```
<uses-permission android:name="android.permission.GET_TASKS"/>
```

Permite acceder a la lista de tareas y actividades en ejecución.

```
<uses-permission android:name="android.permission.INSTALL_SHORTCUT"/>
```

Permite instalar accesos directos en la pantalla de inicio.

```
<uses-permission android:name="android.permission.MANAGE_ACCOUNTS"/>
```

Permite administrar cuentas de usuario en el dispositivo.

```
<uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
```

Permite modificar la configuración de audio del dispositivo.

```
<uses-permission android:name="android.permission.READ_PROFILE"/>
```

Permite leer el perfil de usuario del dispositivo.(SOSPECHOSO)

```
<uses-permission android:name="android.permission.READ_SYNC_SETTINGS"/>
```

Permite leer la configuración de sincronización del dispositivo.

```
<uses-permission android:name="android.permission.READ_SYNC_STATS"/>
```

Permite leer las estadísticas de sincronización del dispositivo.

```
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
```

Permite recibir la notificación de que el dispositivo ha terminado de arrancar.

```
<uses-permission android:name="android.permission.SCHEDULE_EXACT_ALARM"/>
```

Permite programar alarmas exactas en el tiempo.

```
<uses-permission android:name="android.permission.SEND_SMS"/>
```

Permite envío de SMS

```
<uses-permission android:name="android.permission.USE_CREDENTIALS"/>
```

Permite utilizar las credenciales almacenadas en el dispositivo.

```
<uses-permission android:name="android.permission.WAKE_LOCK"/>
```

Permite mantener el dispositivo despierto para evitar que entre en suspensión.

```
<uses-permission android:name="android.permission.WRITE_CONTACTS"/>
```

Permite modificar o agregar contactos en el dispositivo.

```
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
```

Permite escribir en el almacenamiento externo del dispositivo.

```
<uses-permission android:name="android.permission.READ_MEDIA_AUDIO"/>
```

Permite leer archivos de audio almacenados en el dispositivo.

```
<uses-permission android:name="android.permission.READ_MEDIA_IMAGES"/>
```

Permite leer archivos de imágenes almacenados en el dispositivo.

```
<uses-permission android:name="android.permission.READ_MEDIA_VIDEO"/>
```

: Permite leer archivos de video almacenados en el dispositivo.

```
<uses-permission android:name="android.permission.READ_MEDIA_VISUAL_USER_SELECTED"/>
```

Permite leer archivos visuales seleccionados por el usuario almacenados en el dispositivo.

```
<uses-permission android:name="android.permission.POST_NOTIFICATIONS"/>
```

```
<uses-permission android:name="android.permission.WRITE_SYNC_SETTINGS"/>
```

```
<uses-permission android:name="android.permission.REQUEST_INSTALL_PACKAGES"/>
```

Permite solicitar la instalación de paquetes en el dispositivo.

```
<uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
```

Permite ejecutar un servicio en primer plano

```
<uses-permission android:name="android.permission.USE_FULL_SCREEN_INTENT"/>
```

Permite utilizar ventanas de intento de pantalla completa.

```
<uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
```

Permiso de instalación de accesos directos específico para el lanzador de Android.(SOSPECHOSO Y PELIGROSO)

```
<uses-permission android:name="com.android.launcher.permission.UNINSTALL_SHORTCUT"/>
```

Permiso de desinstalación de accesos directos específico para el lanzador de Android.

```
<uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
```

Permite recibir mensajes de Google Cloud Messaging.

```
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>
```

Permite acceder al ID de publicidad de Google.

```
<uses-
```

```
permission android:name="com.google.android.providers.gsf.permission.READ_GSERVICES"/
```

```
>
```

Permite leer servicios de Google Play.

```
<uses-permission android:name="com.sec.android.provider.badge.permission.READ"/>
```

Permiso de lectura de insignias específico para dispositivos Samsung.

```
<uses-permission android:name="com.sec.android.provider.badge.permission.WRITE"/>
```

Permiso de escritura de insignias específico para dispositivos Samsung.

```
<uses-permission android:name="com.htc.launcher.permission.READ_SETTINGS"/>
```

Permiso de lectura de configuración específico para dispositivos HTC.

```
<uses-permission android:name="com.htc.launcher.permission.UPDATE_SHORTCUT"/>
```

Permiso de actualización de accesos directos específico para dispositivos HTC.

```
<uses-permission android:name="com.sonyericsson.home.permission.BROADCAST_BADGE"/>
```


Permiso de transmisión de insignias específico para dispositivos Sony Ericsson.

```
permission android:name="com.sonymobile.home.permission.PROVIDER_INSERT_BADGE"/>
```

Permiso de inserción de insignias específico para dispositivos Sony Mobile.

```
<uses-
```

```
permission android:name="com.huawei.android.launcher.permission.READ_SETTINGS"/>
```

Permiso de lectura de configuración específico para dispositivos Huawei.

```
<uses-
```

```
permission android:name="com.huawei.android.launcher.permission.WRITE_SETTINGS"/>
```

Permiso de escritura de configuración específico para dispositivos Huawei.

```
<uses-
```

```
permission android:name="com.huawei.android.launcher.permission.CHANGE_BADGE"/>
```

Permiso de cambio de insignias específico para dispositivos Huawei.

```
<uses-permission android:name="com.whatsapp.permission.BROADCAST"/>
```

Permiso de transmisión específico para la aplicación WhatsApp.

```
<uses-permission android:name="com.whatsapp.permission.MAPS_RECEIVE"/>
```

Permiso para recibir mapas específico para la aplicación WhatsApp.

```
<uses-permission android:name="com.whatsapp.permission.REGISTRATION"/>
```

Permiso de registro específico para la aplicación WhatsApp.

```
<uses-permission android:name="com.whatsapp.sticker.READ"/>
```

Permiso de lectura específico para la aplicación WhatsApp para leer pegatinas.

```
<uses-permission-sdk-23 android:name="android.permission.ANSWER_PHONE_CALLS"/>
```

versión SDK 23): Permite responder llamadas telefónicas desde la aplicación.

```
<uses-permission-sdk-23 android:name="android.permission.READ_CALL_LOG"/>
```

versión SDK 23): Permite leer el registro de llamadas del dispositivo.

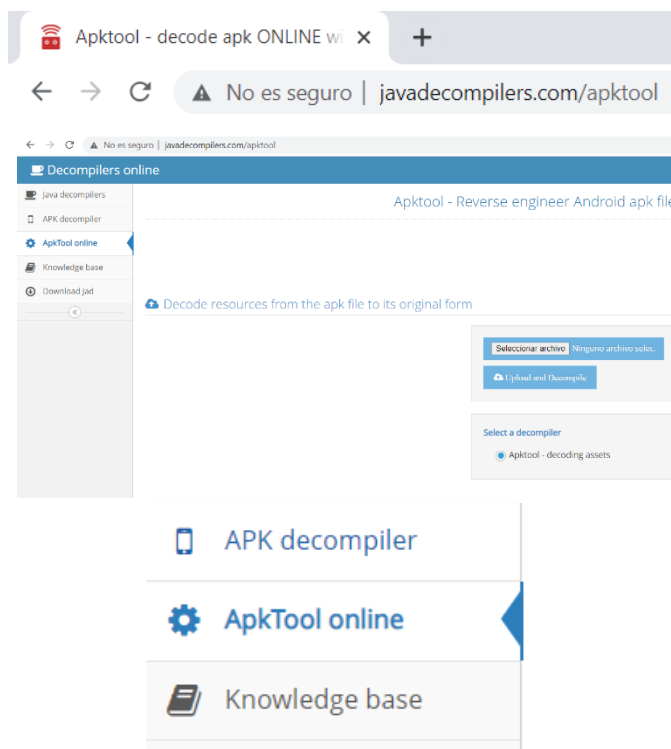
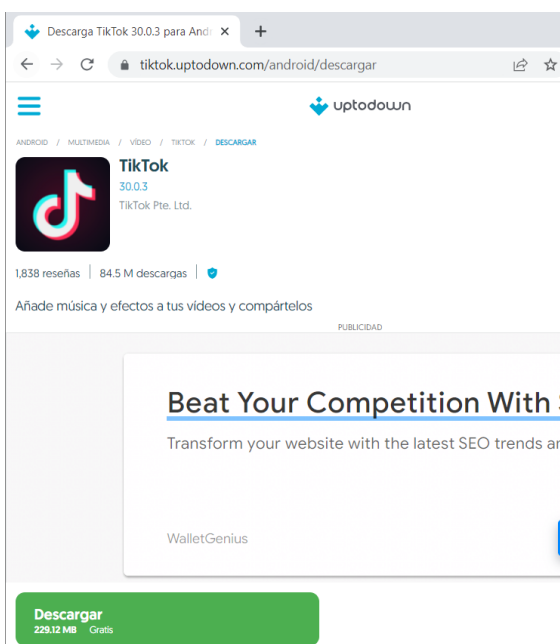
Capturas

"TikTok" enlace descarga (<https://tiktok.uptodown.com/android/descargar>)



TikTok
30.0.3
TikTok Pte. Ltd.

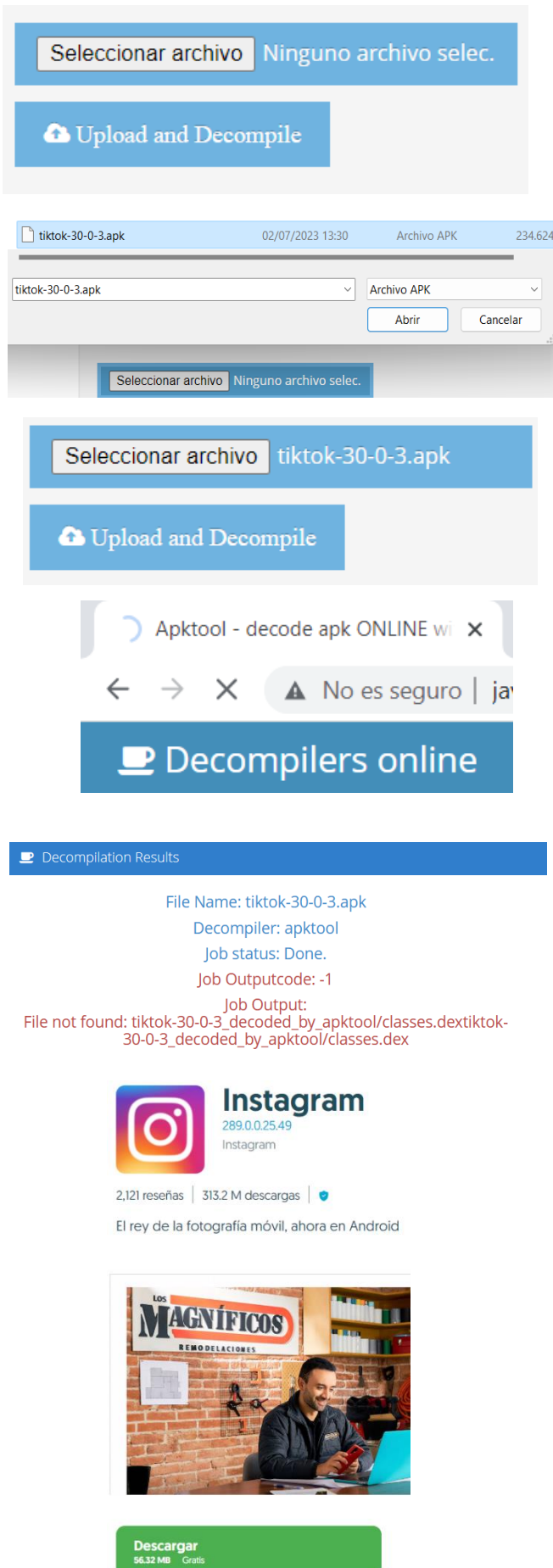
1,838 reseñas | 84.5 M descargas |



Explicación

PROCESO DE DESCARGA DE LA SEGUNDA APLICACIÓN

1. Procedemos a realizar el ingreso al link proporcionado
2. Podemos ver el 84.5M descargas que se le realizo y 1838 reseñas que tiene la aplicación
3. Procedemos a ver la pagina de descarga
4. Procedemos a dar clic al botón de descarga
5. Procedemos abrir la herramienta web utilizada para la auditoria
6. Procedemos a ingresar a esta opción es muy importante



7. Cargamos el archivo .APK descargado

8. Damos a la ruta del archivo

9. Esperamos a que cargue

10. Damos a la opción de upload y empezara el trabajo

11. Procedemos a ver que la aplicación se recarga la aplicación

12. Esto indica que está procesando la operación

13. Al finaliza la operación podemos ver que nos da un erro indicando que la ruta este mal del archivo, pero ante verificaciones estaba todo normal y se realizo los pasos indicados para le laboratorio

14. Se realizo el intento con una versión más antigua y non indica el mismo error por los cual se optó por otra aplicación

15. Se realizo la descarga del mismo sitio web indicado por la pregunta

16. Ingresamos a la opción para realizar la descarga de la aplicación INSTAGRAM

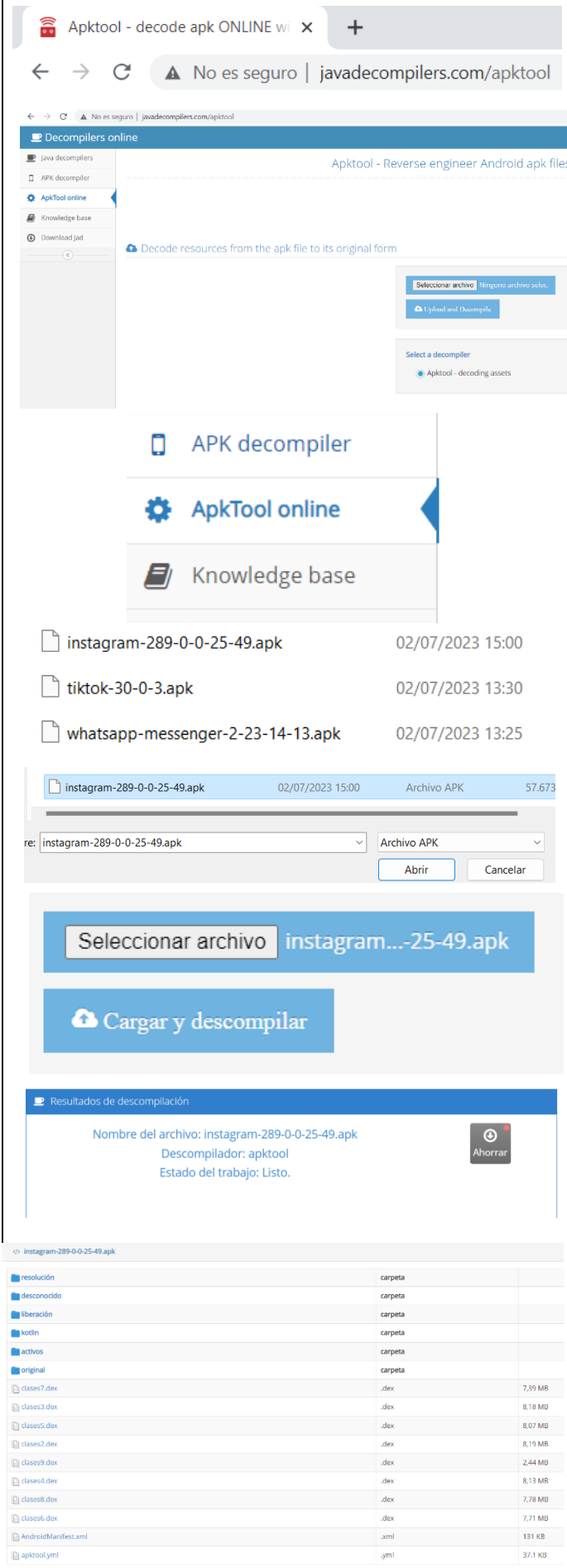
17. Podemos apreciar que no es una página oficial

18. Procedemos a descargar el archivo APK

19. Podemos ver que tiene 3132M de descargas y más de 2121 reseñas

20. En la imagen podemos ver la imagen de la aplicación y del botón de descarga

21. Damos clic al botón de descarga



22. Podemos apreciar que se realizó la descarga cabe destacar que debe ser con la extensión .APK
23. Procedemos a abrir la herramienta a utilizar que es el software online APKTOOLS que es desarrollada por JAVA para realizar la reingeniería a las aplicaciones móviles
24. Apreciamos la pantalla de inicio de la aplicación
25. Nos debemos ir la opción que indica en la imagen
26. Procedemos a cargar el archivo
27. Indicamos la ubicación
28. Una vez cargada damos al clic al botón de **upload**
29. Procedemos a ver que empieza a cargar la aplicación por lo cual significa que está cargando el archivo
30. Una vez finalizado nos da la siguiente opción
31. Nos muestra los archivos de compilados de la aplicación
32. Procedemos a descargar los archivos
33. Damos clic a la opción que nos indica SAVE
34. Damos la ruta donde se guardará los archivos

instagram-289-0-0-25-49_decoded_by_a...

instagram-289-0-0-25-49_decoded_by_a... 02/07/2023 15:04

assets	02/07/2023 15:04	Carpeta de archivos	
kotlin	02/07/2023 15:04	Carpeta de archivos	
lib	02/07/2023 15:04	Carpeta de archivos	
original	02/07/2023 15:04	Carpeta de archivos	
res	02/07/2023 15:04	Carpeta de archivos	
unknown	02/07/2023 15:04	Carpeta de archivos	
AndroidManifest	02/07/2023 15:04	Microsoft Edge HT...	132 KB
apktool.yml	02/07/2023 15:04	Archivo YML	38 KB
classes2.dex	02/07/2023 15:04	Archivo DEX	8.384 KB
classes3.dex	02/07/2023 15:04	Archivo DEX	8.378 KB
classes4.dex	02/07/2023 15:04	Archivo DEX	8.327 KB
classes5.dex	02/07/2023 15:04	Archivo DEX	8.260 KB
classes6.dex	02/07/2023 15:04	Archivo DEX	7.894 KB
classes7.dex	02/07/2023 15:04	Archivo DEX	7.573 KB
classes8.dex	02/07/2023 15:04	Archivo DEX	7.965 KB
classes9.dex	02/07/2023 15:04	Archivo DEX	2.500 KB

AndroidManifest 02/07/2023 15:04 Microsoft Edge HT... 132 KB

```
*manifest xmlns:android="http://schemas.android.com/apk/res/android" xmlns:android="http://schemas.android.com/apk/res/android" android:installLocation="auto" package="com.instagram.android" platformBuildVersionCode="33" platformBuildVersionName="13"
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.WAKE_LOCK" violationExplanation="Need wake lock when user using SUR" violationTyp<
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="android.permission.USE_CREDENTIALS"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
<uses-permission android:name="android.permission.USE_FULL_SCREEN_INTENT"/>
<uses-permission android:name="com.google.android.cdm.permission.RECEIVE"/>
<uses-permission android:name="android.permission.BLUETOOTH"/>
<uses-permission android:name="android.permission.CAMERA"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.READ_PROFILE"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_MEDIA_IMAGES"/>
<uses-permission android:name="android.permission.READ_MEDIA_VIDEO"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.ACCESS_MEDIA_LOCATION"/>
<uses-permission android:name="android.permission.POST_NOTIFICATIONS"/>
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.READ_PHONE_NUMBERS"/>
<uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
<uses-permission android:name="com.android.launcher.permission.UNINSTALL_SHORTCUT"/>
<uses-permission android:name="com.instagram.direct.permission.PROTECTED_STREAMING"/>
<uses-permission android:name="com.instagram.direct.permission.DIRECT_APP_THREAD_STORE_SERVICE"/>
<uses-permission android:name="com.facebook.services.identity.FEQ"/>
<uses-permission android:name="com.htc.launcher.permission.READ_SETTINGS"/>
<uses-permission android:name="com.htc.launcher.permission.UPDATE_SHORTCUT"/>
<uses-permission android:name="com.huawei.android.launcher.permission.CHANGE_BADGE"/>
<uses-permission android:name="com.sonyericsson.home.permission.BROADCAST_BADGE"/>
<uses-permission android:name="com.sonymobile.home.permission.PROVIDER_INSERT_BADGE"/>
<uses-permission-sd-23 android:name="android.permission.UPDATE_APP_BADGE"/>
<uses-permission-sd-23 android:name="android.permission.CALL_PHONE"/>
<uses-permission-sd-23 android:name="android.permission.BLUETOOTH_ADORN"/>
<uses-permission-sd-23 android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission-sd-23 android:name="android.permission.WRITE_CALENDAR"/>
```

35. Podemos apreciar que es en formato comprimido .ZIP

36. Podemos apreciar el archivo

37. Procedemos a realizar la extracción de los archivos

38. Una vez finalizado este proceso podemos ver los documentos de compilados del archivo .APK

39. Podemos ver que hay un archivo llamado AndroidManifest

40. Este es el archivo que realizaremos la auditoria

ANÁLISIS DEL ARCHIVO ANDROIDMANIFEST

Estos son algunos de los permisos que el APK requiere por lo cual analizaremos los más importantes y peligrosas

```
<uses-permission-sdk-23 android:name="android.permission.ACCESS_WIFI_STATE"/>
```

Permiso de acceso al estado de la conexión wifi

```
<uses-permission android:name="android.permission.INTERNET"/>
```

Permiso de conexión a internet

```
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
```

Permiso a estado de la red

```
<uses-permission android:name="android.permission.WAKE_LOCK" violationExplanation="Need wake lock when user using SUP" violationType="MOS_BLOCKED_PERMISSION_WAKE_LOCK"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
```

Obtener cuentas almacenadas en el dispositivo

```
<uses-permission android:name="android.permission.USE_CREDENTIALS"/>
```

Usar credenciales almacenadas en el dispositivo

```
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
```

Recibir notificación al reinicio del dispositivo

```
<uses-permission android:name="android.permission.VIBRATE"/>
```

Control de la vibración del dispositivo

```
<uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
```

Ejecutar un servicio en Segundo plano

```
<uses-permission android:name="android.permission.USE_FULL_SCREEN_INTENT"/>
```

Mostrar ventanas emergentes en la pantalla completa

```
<uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
```

Recibir mensajes de Google Cloud Messaging.

```
<uses-permission android:name="android.permission.BLUETOOTH"/>
```

Funciones de bluetooth

```
<uses-permission android:name="android.permission.CAMERA"/>
```

Acceder a la cámara

```
<uses-permission android:name="android.permission.READ_CONTACTS"/>
```

Leer información de los contactos

<uses-permission android:name="android.permission.READ_PROFILE"/>

Leer perfil de usuario

<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>

Acceder a la ubicación del dispositivo

<uses-permission android:name="android.permission.RECORD_AUDIO"/>

Graba audio con el microfono

<uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>

Modificar configuración de audio

<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>

Leer contenido de almacenamiento externo

<uses-permission android:name="android.permission.READ_MEDIA_IMAGES"/>

Lee imágenes almacenadas en el dispositivo

<uses-permission android:name="android.permission.READ_MEDIA_VIDEO"/>

Leer videos almacenados

<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>

Escribe en el almacenamiento externo

<uses-permission android:name="android.permission.ACCESS_MEDIA_LOCATION"/>

Acceder a la ubicación de los archivos de multimedia

<uses-permission android:name="android.permission.POST_NOTIFICATIONS"/>

Permite publicar notificaciones en el dispositivos

<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>

Permite ID de publicaciones de Google

<uses-permission android:name="android.permission.READ_PHONE_STATE"/>

Lee estado del telefono

<uses-permission android:name="android.permission.READ_PHONE_NUMBERS"/>

Lee números almacenados en el dispositivo

<uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>

Instalador acceso directos en el lanzador de android

<uses-permission android:name="com.android.launcher.permission.UNINSTALL_SHORTCUT"/>

desinstala acceso directos en el lanzador de android

<uses-permission android:name="com.instagram.direct.permission.PROTECTED_DEEPLINKING"/>

Permiso de acceso a enlaces profundos protegidos de Instagram Direct.

```
<uses-permission android:name="com.instagram.direct.permission.DIRECT_APP_THREAD_STORE_SERVICE"/>
```

Permiso de acceso al servicio de almacenamiento de hilos de la aplicación Direct de Instagram.

```
<uses-permission android:name="com.facebook.services.identity.FEO2"/>
```

Permiso de identidad de servicios de Facebook.

```
<uses-permission android:name="com.htc.launcher.permission.READ_SETTINGS"/>
```

Permiso de lectura de configuración específico para dispositivos HTC.

```
<uses-permission android:name="com.htc.launcher.permission.UPDATE_SHORTCUT"/>
```

Permiso de actualización de accesos directos específico para dispositivos HTC.

```
<uses-permission android:name="com.huawei.android.launcher.permission.CHANGE_BADGE"/>
```

Permiso de cambio de insignias específico para dispositivos Huawei.

```
<uses-permission android:name="com.sonyericsson.home.permission.BROADCAST_BADGE"/>
```

Permiso de transmisión de insignias específico para dispositivos Sony Ericsson.

```
<uses-permission android:name="com.sonymobile.home.permission.PROVIDER_INSERT_BADGE"/>
```

```
<uses-permission-sdk-23 android:name="android.permission.UPDATE_APP_BADGE"/>
```

Actualizar insignias de aplicaciones (requiere SDK 23 o superior).

```
<uses-permission-sdk-23 android:name="android.permission.CALL_PHONE"/>
```

Realizar llamadas telefónicas (requiere SDK 23 o superior).

CONCLUSIONES

Como conclusión a la auditoria de las dos aplicaciones llegamos a que hay muchos permisos extraños e innecesario para el funcionamiento por lo cual es muy importa tener el control de los permisos que se le da en las aplicaciones con el dispositivo y tener actualizado las versiones de Android ya que vienen en conjunto de actualizaciones de parches de seguridad.

La segunda conclusión llega es que siempre es mas seguro realizar la descarga e instalación de las aplicaciones de una fuente oficial ya que de fuente de terceros pueden venir con una reingeniería realizada e implementado código malicioso. Cabe recalcar que no siempre es necesario que el código malicioso este en la versión descargada si no puede ver con alguna actualización del APK