ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 9 Issue 4 July 2021

International Manuscript ID : 23482001V9I4072021-139

(Approved and Registered with Govt. of India)

Android APK Analytics with Monitoring Apps and Forensic Aspects

Ekta Srivastava

Research Scholar

Shri Venkateshwara University

Gajraula, Uttar Pradesh

Dr. Vishal Bhatnagar

Assistant Professor

Shri Venkateshwara University

Gajraula, Uttar Pradesh

Abstract

The activities on a mobile phone are one of the aspects related to personal privacy and integrity. Still, there are number of reasons by which a mobile phone and its activities is required to be monitored. Whenever a crime or negative incident happens anywhere, the security agencies attempts to access the mobile devices in use by the criminals or suspects. This manuscript focuses on the development and use of a unique and effective mobile app which can be used to monitor the remote activities of the mobile phone users. An Android App can be developed and installed in the Android based mobile phones which can be easily monitored remotely.

Keywords: Android Forensic, Cyber Forensic, Real Time Monitoring

ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 9 Issue 4 July 2021
International Manuscript ID : 23482001V9I4072021-139
(Approved and Registered with Govt. of India)

Introduction

Digital forensic investigation on mobile devices requires an investigator to follow step by step procedure to collect, extract and analyze digital evidence [1]. To accomplish complete extraction of digital evidence, the primary step is data collection or device acquisition [2]. Android forensics depends on the level of access a device provides which further determines the level or depth of the data which an investigator can extract. Generally, an Android operating system provides two layers of user access control which are rooted or non-rooted access. Primarily Android OS does not provide user administrative or root access hence devices are manufactured with non-root access [3].

For parents, it is useful many times to monitor the activities of their children. For this domain, the remote app can be useful. In this manuscript, the development of a background app will be covered to take the screenshots automatically from Mobile Handset and sending to a particular E-mail ID [4]. This app is useful for the monitoring of users about their activities (For Parents, Security Agencies) on the mobile phone. The same screenshots can be uploaded to a cloud platform so that the logs can be checked.

Real Time Monitoring Apps

There are number of Android apps available which can be used for real time monitoring for cyber security and digital forensic.

Following are the key Android apps for parental control and cyber security based implementations

- Realtime-spy
- Real Time GPS Tracker

ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 9 Issue 4 July 2021
International Manuscript ID : 23482001V9I4072021-139
(Approved and Registered with Govt. of India)

- WebSafety
- Kids Place
- MMGuardian
- Famingo
- Net Nanny
- Funamo
- Screen Time
- Norton Family
- Safe Browser
- AppLock
- Toddler Lock

Developing Mobile App for Auto Screenshots

As there are number of apps developed for the remote monitoring and observations, still there is huge scope of research and innovations [5].

Following is the code is to fetch a series of screenshots based on a particular time mentioned in the script and regular E-mail to a particular account [6].

The code of MainActivity.java is to create the front-end of app in which there is a button. On click of this button, the timer will start to take the serial screenshots and email.

MainActivity.java

```
public class MainActivity extends Activity {
    private MyIntent pendingIntent;
```

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 9 Issue 4 July 2021

International Manuscript ID : 23482001V9I4072021-139

(Approved and Registered with Govt. of India)

```
Intent myIntent;
AlarmManager alarmManager;
int delay = 25;
Button Start_service;
@Override
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity_main);
    Start_service = (Button) findViewById(R.id.buttonStartTimer);
    Start_service.setOnClickListener(new View.OnClickListener() {
        @Override
        public void onClick(View v) {
            startService(new Intent(MainActivity.this,myService.class));
        }       }); }
@Override
protected void onResume() {
    super.onResume();
    Start_service.setOnClickListener(new View.OnClickListener() {
        public void onClick(View v) {
            AlarmManager alarmManager =
(AlarmManager)getSystemService(ALARM_SERVICE);
            Calendar calendar = Calendar.getInstance();
            calendar.setTimeInMillis(System.currentTimeMillis());
            calendar.add(Calendar.SECOND, 20);
pendingIntent);
```

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 9 Issue 4 July 2021

International Manuscript ID : 23482001V9I4072021-139

(Approved and Registered with Govt. of India)

```
            Toast.makeText(MainActivity.this, "Service Started",
Toast.LENGTH_LONG).show();*/
            /*String Interval = editText.getText().toString();
            startService(intent);*/
            startService(new Intent(MainActivity.this,myService.class));
        }
    });
  }
}
```

The code for background activity which is used to take the screenshots automatically and then email. This service is executed at the back-end without any user intervention and sends the screenshots to a particular email id.

Following is the XML file that is required in the Android Project.

ActivityMain.xml

```
<?xml version="1.0" encoding="utf-8"?>
<LinearLayout xmlns:android="http://schemas.android.com/apk/res/android"
  xmlns:tools="http://schemas.android.com/tools"
  android:layout_width="match_parent"
  android:layout_height="match_parent"
  android:paddingBottom="@dimen/activity_vertical_margin"
  android:paddingLeft="@dimen/activity_horizontal_margin"
  android:paddingRight="@dimen/activity_horizontal_margin"
  android:paddingTop="@dimen/activity_vertical_margin"
```

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 9 Issue 4 July 2021

International Manuscript ID : 23482001V9I4072021-139

(Approved and Registered with Govt. of India)

```
   android:orientation="vertical"
   tools:context="com.myname.domain.screenshot.MainActivity">
   <LinearLayout
      android:layout_width="match_parent"
      android:layout_height="wrap_content"
      android:orientation="horizontal">
      <Button
      android:id="@+id/buttonStartTimer"
     android:layout_width="match_parent"
      android:layout_height="wrap_content"
      android:text="Start Timer"
      android:onClick="startTimer" />
   </LinearLayout>
</LinearLayout>
```

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
   package="com.myname.domain.screenshot">

   <uses-feature android:name="android.hardware.camera" />
   <uses-feature android:name="android.hardware.camera.front"
      android:required="false" />
   <uses-permission android:name="android.permission.CAMERA" />
   <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
   <uses-permission android:name="android.permission.INTERNET"/>
```

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 9 Issue 4 July 2021

International Manuscript ID : 23482001V9I4072021-139

(Approved and Registered with Govt. of India)

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

<application
    android:allowBackup="true"
    android:icon="@mipmap/ic_launcher"
    android:label="@string/app_name"
    android:supportsRtl="true"
    android:theme="@style/AppTheme">
    <activity android:name=".MainActivity">
        <intent-filter>
            <action android:name="android.intent.action.MAIN" />
            <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>
    </activity>
    <service android:name=".myService"></service>
</application>
</manifest>
```

SENDING GPS LOCATION WITH THE SCREENSHOT

Following code can be integrated with the application to fetch the dynamic [7] GPS location and then sending to particular mail id or cloud storage

```
public class GPSLocationTracker extends Service implements LocationListener {
    private final Context mContext;
    boolean isGPSServiceEnabled = false;
```

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 9 Issue 4 July 2021

International Manuscript ID : 23482001V9I4072021-139

(Approved and Registered with Govt. of India)

```
boolean isNetworkServiceEnabled = false;
 boolean GetLocation = false;
Location MyLocation;
double CurrentLatitude;
double CurrentLongitude;
 private static final long MIN_DISTANCE_CHANGE_FOR_UPDATES = 50;
private static final long MIN_TIME_BW_UPDATES = 1000 * 60 * 1;
protected MylocationManager locationManager;
public MyGPSTracker(Context mycontext) {
   this.mContext = mycontext;
   getLocation();
}
public Location geMytLocation() {
    try {
       MylocationManager = (LocationManager) mContext
             .getSystemService(LOCATION_SERVICE);
       isGPSServiceEnabled = locationManager
             .isProviderEnabled(LocationManager.GPS_PROVIDER);
       isNetworkServiceEnabled = locationManager
             .isProviderEnabled(LocationManager.NETWORK_PROVIDER);
       if (!isGPSServiceEnabled && !isNetworkEnabled) {
       } else {
          this.GetLocation = true;
          if (isNetworkEnabled) {
             locationManager.requestLocationUpdates(
                   LocationManager.NETWORK_PROVIDER,
```

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 9 Issue 4 July 2021

International Manuscript ID : 23482001V9I4072021-139

(Approved and Registered with Govt. of India)

```
            MIN_TIME_BW_UPDATES,
            MIN_DISTANCE_CHANGE_FOR_UPDATES, this);
      Log.d("Network", "Network");
       if (MylocationManager != null) {
          MyLocation = locationManager
                .getLastKnownLocation(LocationManager.NETWORK_PROVIDER);
          if (MyLocation != null) {
            CurrentLatitude = location.getCurrentLatitude();
            CurrentLongitude = location.getCurrentLongitude();
          }
       }
    }
    if (isGPSEnabled) {
       if (MyLocation == null) {
          locationManager.requestLocationUpdates(
                LocationManager.GPS_PROVIDER,
                MIN_TIME_BW_UPDATES,
                MIN_DISTANCE_CHANGE_FOR_UPDATES, this);
          Log.d("GPS Service is Enabled", "GPS Service is Enabled");
          if (MylocationManager != null) {
            MyLocation = locationManager
                  .getLastKnownLocation(LocationManager.GPS_PROVIDER);
            if (MyLocation != null) {
              CurrentLatitude = MyLocation.getCurrentLatitude();
              CurrentLongitude = MyLocation.getCurrentLongitude();
            }
```

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 9 Issue 4 July 2021

International Manuscript ID : 23482001V9I4072021-139

(Approved and Registered with Govt. of India)

```
                }
            }
        }
    }

    } catch (Exception e1) {
        e1.printStackTrace();
    }
    return location;
}
@Override
public void onMyLocationChanged(Location MyLocation) {
}
@Override
public void onMyProviderDisabled(String provider) {
}
@Override
public void onMyProviderEnabled(String provider) {
}
@Override
public void onStatusChanged(String provider, int status, Bundle extras) {
}
@Override
public IBinder onMyBind(Intent arg0) {
    return null;
}
```

ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 9 Issue 4 July 2021
International Manuscript ID : 23482001V9I4072021-139
(Approved and Registered with Govt. of India)

Generally manufacturer and Android do not provide root access to the device owner by default. Non-rooted devices provide access to the internal and external memory storage medium which enables an investigator to perform Logical Acquisition of the device [8]. The system, memory and internal partitions won't be visible or accessible. However, full device backup or adb backup can be utilized to perform logical acquisition of the device [9]. A device with complete administrative access is what you get after rooting the device. Access to device system, memory and internal partitions are granted to the super user or the root user. For rooted devices a complete device acquisition can be performed using dd command or automated tools [10]. Root access also allows an investigator to perform data recovery and carving which uncovers deleted evidence stored in the device.

Conclusion

Forensic Investigation requires in-depth recovery of artifacts for complete analysis. A rooted device provides complete extraction of user data and access to the system partition. The system partition stores complete application data, ROM and system files. For a non-rooted user, the partitions and system folders are kept hidden with no access. Android Package (APK) is the Android application package file format used by the Android operating system, and a number of other Android-based operating systems for distribution and installation of mobile apps, mobile games and middleware. Google has announced new Android App Bundle will replace APK in Google Play. Android Forensic Investigation requires an investigator to be proficient regarding acquisition, extraction and analysis of evidence. The methods involved and the amount of data collected while performing device acquisition, can become a crucial pointer determining extraction of artifacts leading towards discovering an evidence. Android is a rapid evolving operating system, hence the methods and acquisition methods will keep changing on the basis of device & data access it is providing. Google timely releases patches for security enhancement

and authorized device access. The acquisition methods are also affected by the custom ROMs being developed by individual device manufacturers which causes an investigator to customize acquisition methods every time. However, the basic device acquisition & data collection practices mentioned in the paper will remain constant for Android devices.

References

[1] "Inside the Android Application Framework" (video). Google Sites. 2008.

[2] Hatem Ben Yacoub (20 April 2018). "Tips: How to install apk files on Android Emulator". Open Ha Magazine. Archived from the original on 2012-05-26. Retrieved 2021-07-17.

[3] "The Structure of Android Package (APK) Files". OPhone SDN. OPhone Software Developer Network. 17 November 2010. Archived from the original on 8 February 2011.

[4] Eagleapk (2 January 2021). "Your one step shop for all app!". SDX-Developers Forum. Eagle APK. Archived from the original on 5 January 2021.

[5] "Unknown Sources: Everything you need to know!". Android Central. 27 July 2018.

[6] "How to Downgrade an App on Android - No Root Needed". xda-developers. 25 August 2017.

[7] Parmar, Mayank (2021-06-27). "Microsoft confirms Android apps will run on all Windows 11 PCs". Windows Latest. Retrieved 2021-06-28.

[8] "ABI Management | Android Developers". developer.android.com. Retrieved 16 June 2018.

[9] "Android ABIs | Android NDK". Android Developers. Retrieved 2020-08-14. Note: Historically the NDK supported ARMv5 (armeabi), and 32-bit and 64-bit MIPS, but support for these ABIs was removed in NDK r17.

[10] Dan, Albert (Sep 5, 2018). "Changelog r17". GitHub. Retrieved 2020-08-14. Support for ARMv5 (armeabi), MIPS, and MIPS64 has been removed. in an error.