LIFS
LEGAL INFORMATICS AND FORENSIC SCIENCE

App Inventor 2: Mobile Forensic Toolkit

20166405 박성미
20146425 정연석

INDEX

01.
해쉬란?

02.
앱인벤터 확장기능

03.
Mobile Tool Kit

1. Hash란?

무결성의 원칙

- 수집 증거가 위·변조 되지 않았음을 증명
  - 수집 당시의 데이터 hash 값과 법정 제출 시점 데이터의 hash 값이 같다면 hash 함수의 특성에 따라 무결성을 입증

디지털 포렌식 개관, 박종혁 (2013)

2. 앱인벤터 확장기능

http://my.bryanqiang.com/createext.html

Tools you will need:
1.Git Bash(a software for download git code sources)
2.JDK(java 7)
3.a java code editor(Jedit,EditPlus,etc)
4.basic java programming experience
5.Apache ant(a software for complie extensions)

https://docs.google.com/document/d/1xk9dMfczvjbbwD-wMsr-ffqkTlE3ga0ocCE1KOb2wvw/pub#h.3kn0fmfydnq1

1b. The Class Hierarchy

All components fit within a class/interface hierarchy, a subset of which is shown in Figure 2. All components implemer
`Component` interface, which consists mostly of useful constants. Every component extends either the `VisibleComp`
`AndroidNonvisibleComponent` abstract classes, and some also implement the `ComponentContainer` interface.
`Form` (displayed to the user as "Screen"), which holds zero or more instances of `AndroidViewComponent`, the supe
components. Exceptions include `Sprite`, which can only be contained in a `Canvas`.

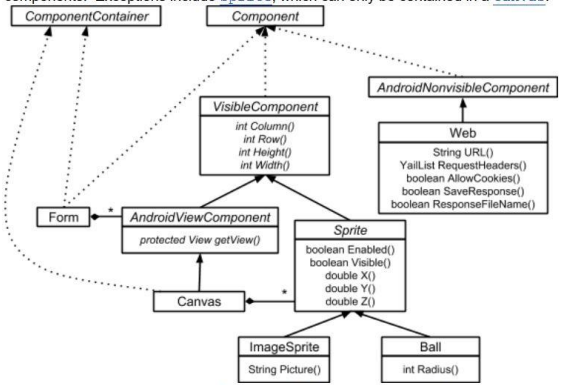


Figure 2: An incomplete subset of the component class/interface hierarchy. Interfaces and abstract methods are shown in italics.

CERTIFICATE

SOLOLEARN
DISCOVER YOUR POTENTIAL

Issued 15 November, 2018

This is to certify that

tansanapple

has successfully completed the

Java Tutorial course

Yeva Hyusyan
Chief Executive Officer

Certificate #1068-1008753

ıngmi › appinventor-sources › appinventor › components › build › extensions

Name	Date modified	Type
com.sungmi.binaryConverter.aix	11/25/2018 6:22 PM	AIX Fil
com.sungmi.runtimeLogs.aix	11/25/2018 6:22 PM	AIX Fil
com.sungmi.sungmiHasher.aix	11/25/2018 6:22 PM	AIX Fil

ngmi › appinventor-sources › appinventor › components ›

Name
binaryConverter
runtimeLogs
sungmiHasher

ngmi › appinventor-sources › appinventor › lib

Name	Date modified	Type
gwt_incubator	11/15/2018 8:45 PM	File folder
gwt_query	11/15/2018 8:45 PM	File folder
gwt_svg	11/15/2018 8:45 PM	File folder
jdk5	11/15/2018 8:45 PM	File folder
jedis	11/15/2018 8:45 PM	File folder
json	11/15/2018 8:45 PM	File folder
jts	11/15/2018 8:45 PM	File folder
junit	11/15/2018 8:45 PM	File folder
junit4	11/15/2018 8:45 PM	File folder
junit-addons	11/15/2018 8:45 PM	File folder
kawa	11/15/2018 8:45 PM	File folder
keyczar	11/15/2018 8:45 PM	File folder
leaflet	11/15/2018 8:45 PM	File folder
log4j	11/15/2018 8:45 PM	File folder
oauth	11/15/2018 8:45 PM	File folder
objectify-3.1	11/15/2018 8:45 PM	File folder
org-apache-commons-codec	11/22/2018 4:53 AM	File folder
org-apache-commons-io	11/20/2018 10:48 PM	File folder

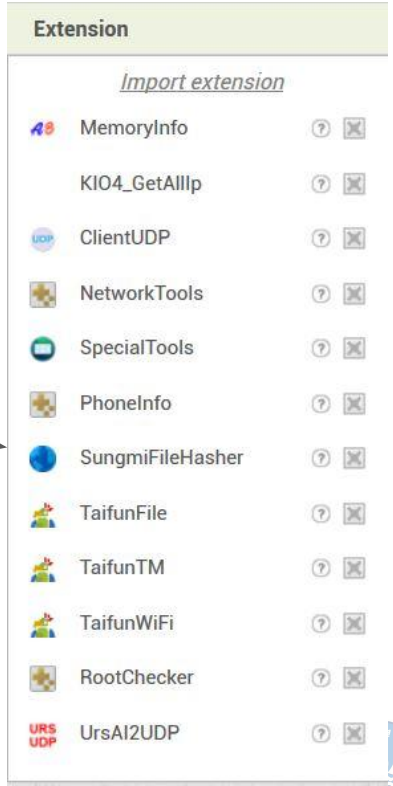
SungmiFileHasher.java

```
package com.sungmi.sungmiHasher;

//import libraries

import android.content.Context;
import android.util.Log;
//import android.app.Activity;
//import android.os.Environment;

import com.google.appinventor.components.annotations.*;
import com.google.appinventor.components.common.ComponentCategory;
import com.google.appinventor.components.runtime.*;
import com.google.appinventor.components.runtime.collect.Sets;
import com.google.appinventor.components.runtime.util.BoundingBox;
import com.google.appinventor.components.runtime.util.ErrorMessages;
import com.google.appinventor.components.runtime.util.FileUtil;
import com.google.appinventor.components.runtime.util.MediaUtil;
import com.google.appinventor.components.runtime.util.PaintUtil;
import com.google.appinventor.components.common.ComponentConstants;
import com.google.appinventor.components.common.PropertyTypeConstants;
import com.google.appinventor.components.common.YaVersion;
import org.apache.commons.codec.DecoderException;
import org.apache.commons.codec.binary.Hex;
import org.apache.commons.codec.digest.DigestUtils;

import java.io.FileNotFoundException;
import java.io.FileInputStream;
import java.io.InputStream;
import java.io.IOException;


//////////////////////////annotations for basic initialization/////////////////////////////////////

@DesignerComponent(version = YaVersion.SUNGMI_TEST_VERSION,
    description = "my testings",                                        //this is your extension's description
    category = ComponentCategory.EXTENSION,     //the category is extension
    nonVisible = true,                                                  //only can be nonvisible
    iconName = "images/web.png")                                        //picture path

@SimpleObject(external = true)
@UsesLibraries(libraries = "org-apache-commons-codec.jar")
@UsesPermissions(permissionNames = "android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE")

```

```
public class SungmiFileHasher extends AndroidNonvisibleComponent    //set your class name in XXX for replacement.
implements Component {

    public static final int VERSION = 0;    //version number
    private ComponentContainer container;                                   //define the component
    private Context context;                                                          //define the context
    private static final String LOG_TAG = "sungmi EXTENSION STARTS!!!!";
    private DigestUtils DigestUtils;
    private Hex Hex;
    private DecoderException DecoderException;
    //private final Activity activity;
    //private boolean isRepl = false;


   public SungmiFileHasher (ComponentContainer container) {
        super(container.$form());
        this.container = container;
        context = (Context) container.$context();                       //define the context
        Log.d(LOG_TAG, "sungmiHasher created" );                                  //record
    }

////////////////////////////////////////////add your code here/////////////////////////////////////////////////////////


 @SimpleFunction(description = "reads file as binary and hashes with md5")

 public String SungmiMD5(String fileName) {
    String md5String = null;

    //String md5String = null;
     try {
         //md5String = DigestUtils.md5Hex(new FileInputStream(fileName));
         md5String = new String(Hex.encodeHex(DigestUtils.md5(new FileInputStream(fileName))));

         //String s = new String(Hex.encodeHex(DigestUtils.md5(data)));
     } catch (IOException e){
         Log.d(LOG_TAG, "IO exception");
     }
     Log.d(LOG_TAG, "md5String");
     return md5String;
```

```
Sungmi@DESKTOP-FQTSSLM MINGW64 ~/appinventor-sources/appinventor (master)
$ ant extensions
Buildfile: C:\Users\Sungmi\appinventor-sources\appinventor\build.xml

extensions:
```

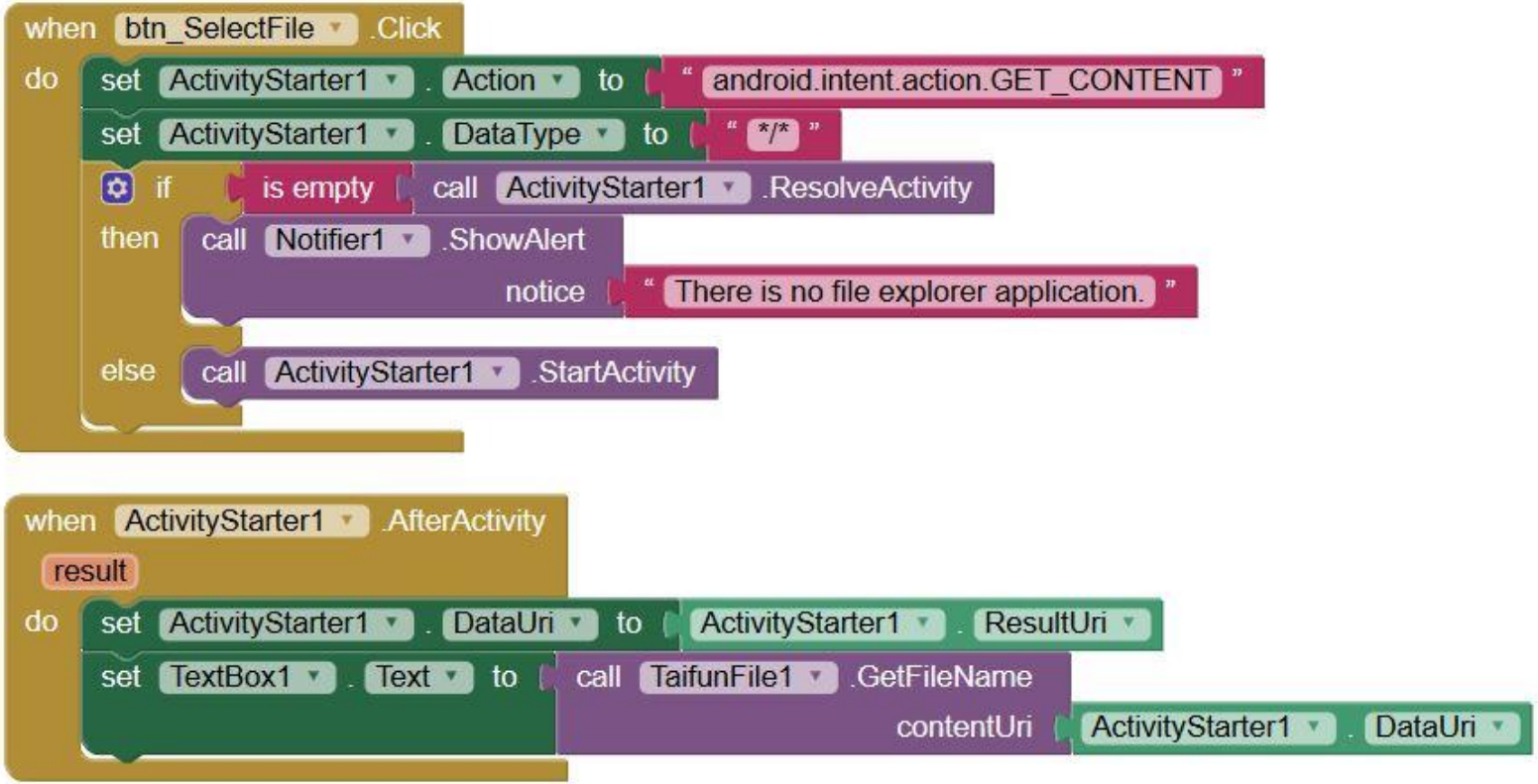
```
BUILD SUCCESSFUL
Total time: 3 minutes 3 seconds
Picked up _JAVA_OPTIONS: -Xmx1024m
```

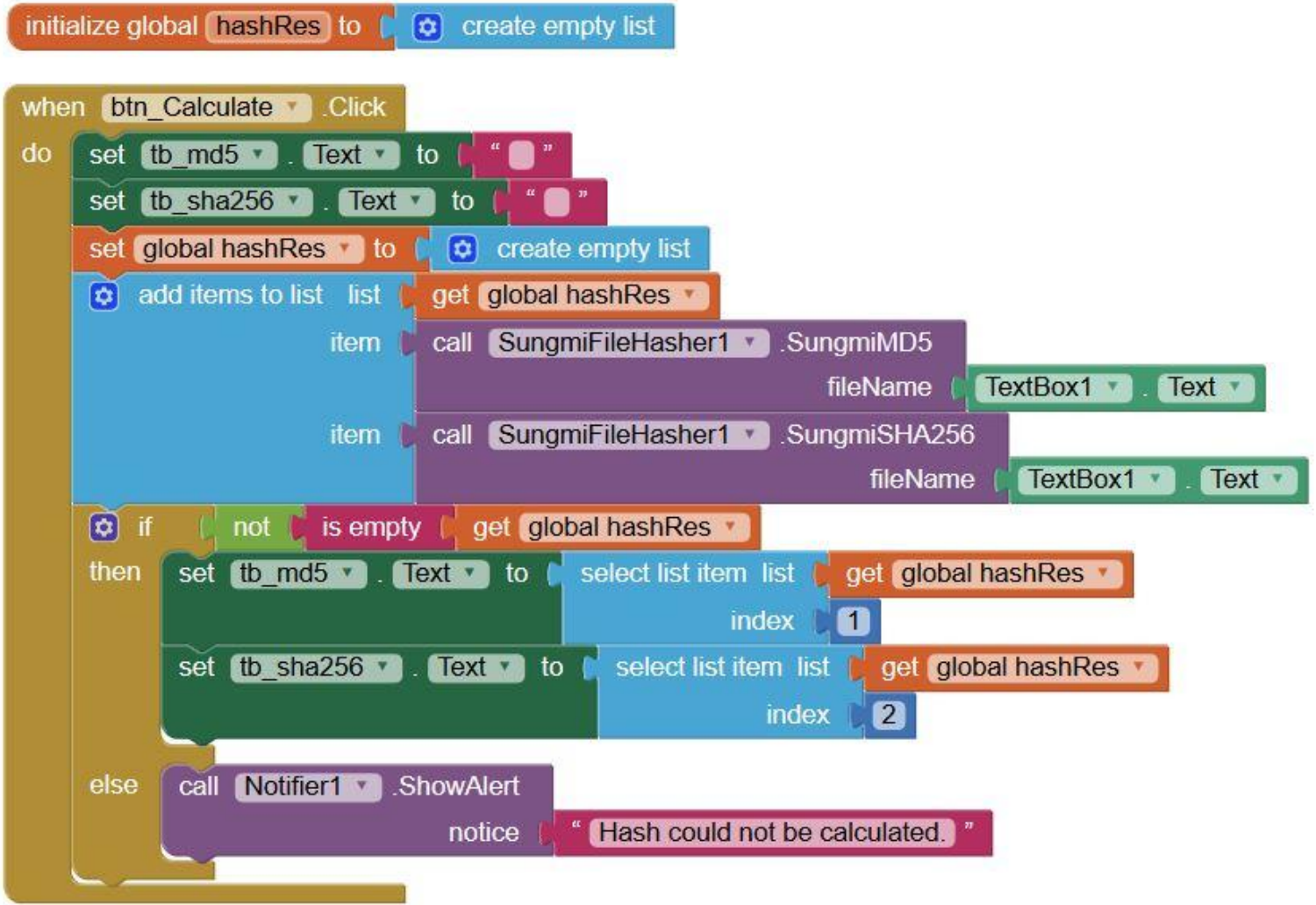


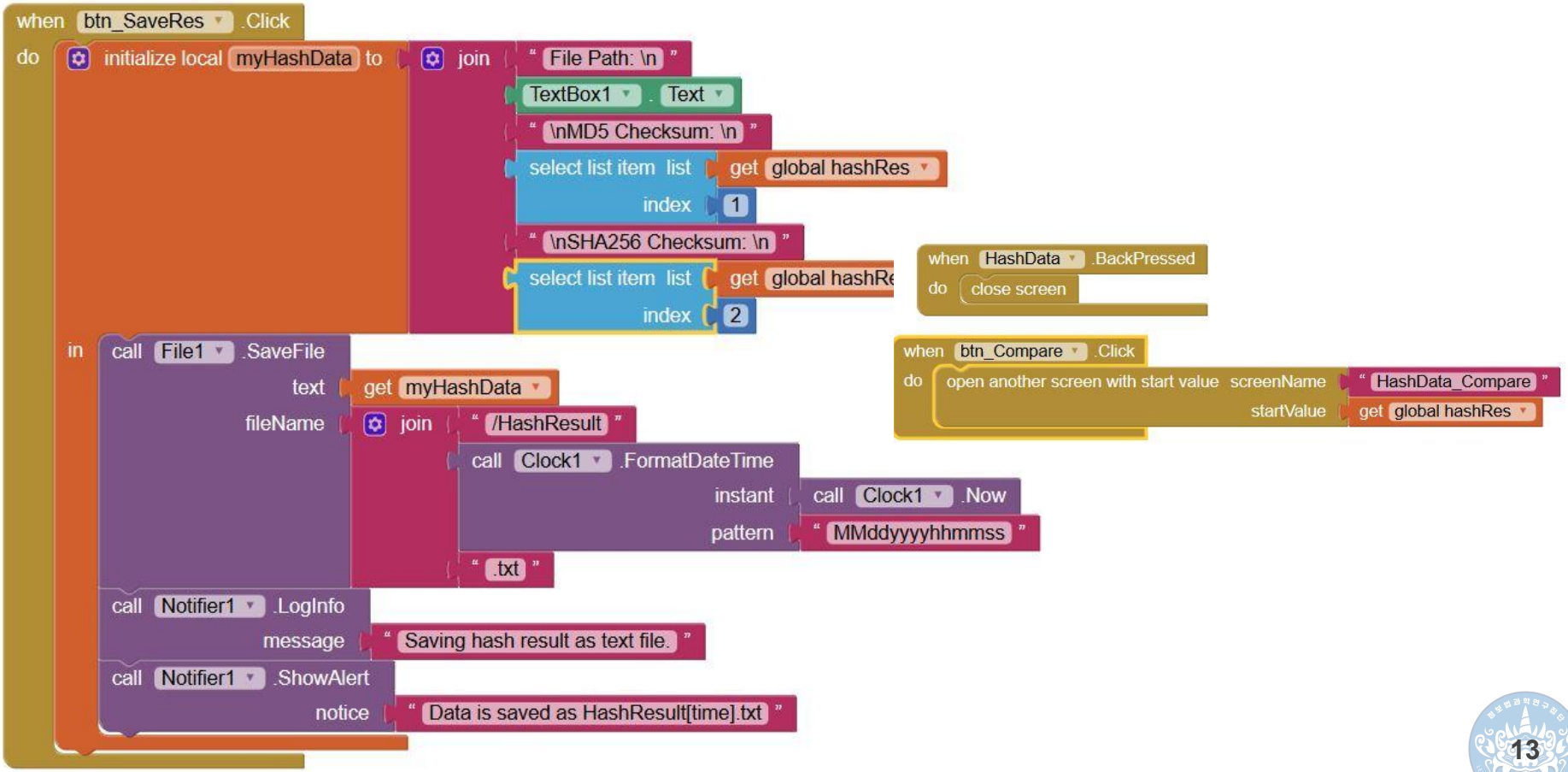
해쉬 기능 구동 영상

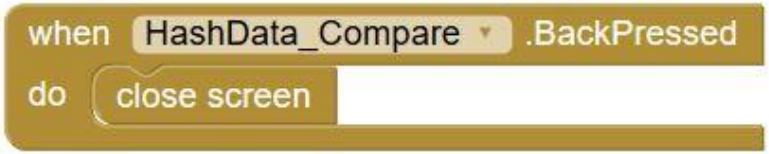
https://youtu.be/yF4ff1giKoA

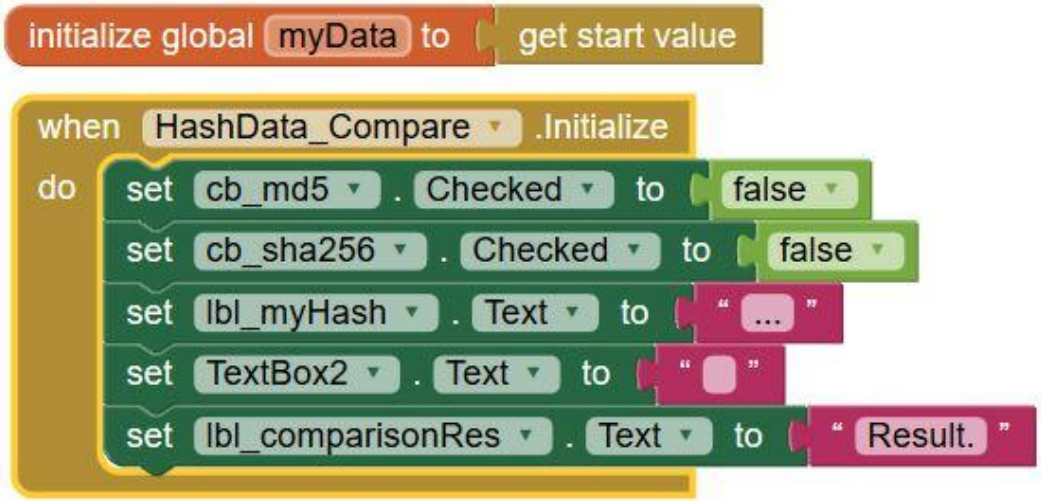
3. Mobile Forensic Kit

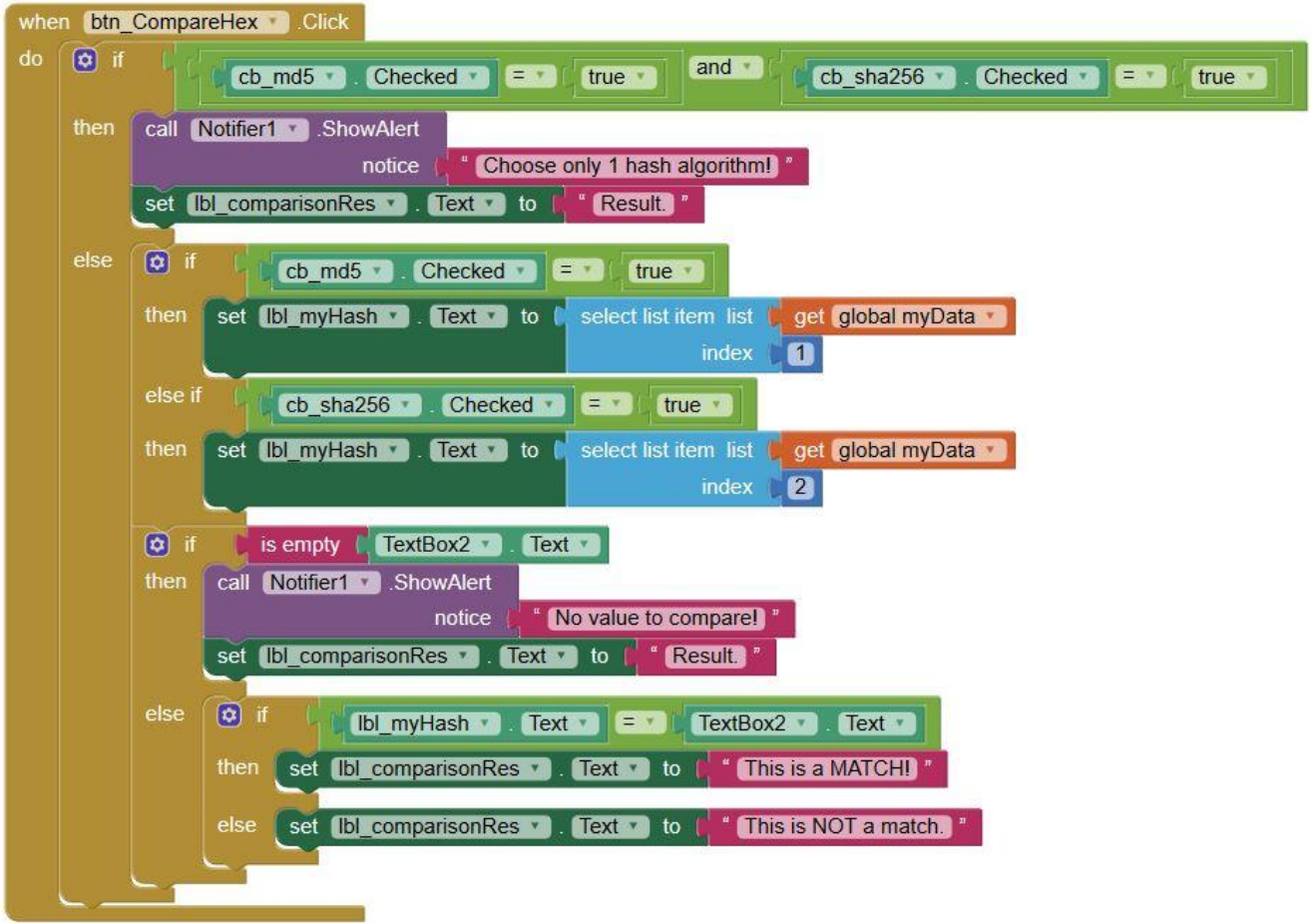



initialize global hashRes to create empty list
when btn_Calculate .Click
do set tb_md5 . Text to ""
set tb_sha256 . Text to ""
set global hashRes to create empty list
add items to list list get global hashRes
item call SungmiFileHasher1 .SungmiMD5
fileName TextBox1 . Text
item call SungmiFileHasher1 .SungmiSHA256
fileName TextBox1 . Text
if not is empty get global hashRes
then set tb_md5 . Text to select list item list get global hashRes
index 1
set tb_sha256 . Text to select list item list get global hashRes
index 2
else call Notifier1 .ShowAlert
notice "Hash could not be calculated."


when btn_SaveRes .Click
do initialize local myHashData to join " File Path: \n "
TextBox1 . Text
" \nMD5 Checksum: \n "
select list item list get global hashRes
index 1
" \nSHA256 Checksum: \n "
select list item list get global hashRe
index 2
in call File1 .SaveFile
text get myHashData
fileName join " /HashResult "
call Clock1 .FormatDateTime
instant call Clock1 .Now
pattern " MMddyyyyhhmmss "
" .txt "
call Notifier1 .LogInfo
message " Saving hash result as text file. "
call Notifier1 .ShowAlert
notice " Data is saved as HashResult[time].txt "
when HashData .BackPressed
do close screen
when btn_Compare .Click
do open another screen with start value screenName " HashData_Compare "
startValue get global hashRes


when HashData_Compare .BackPressed
do close screen


initialize global myData to get start value
when HashData_Compare .Initialize
do set cb_md5 . Checked to false
set cb_sha256 . Checked to false
set lbl_myHash . Text to " ... "
set TextBox2 . Text to " "
set lbl_comparisonRes . Text to " Result. "


when btn_CompareHex .Click
do
if cb_md5 . Checked = true and cb_sha256 . Checked = true
then call Notifier1 .ShowAlert
notice " Choose only 1 hash algorithm! "
set lbl_comparisonRes . Text to " Result. "
else if cb_md5 . Checked = true
then set lbl_myHash . Text to select list item list get global myData
index 1
else if cb_sha256 . Checked = true
then set lbl_myHash . Text to select list item list get global myData
index 2
if is empty TextBox2 . Text
then call Notifier1 .ShowAlert
notice " No value to compare! "
set lbl_comparisonRes . Text to " Result. "
else if lbl_myHash . Text = TextBox2 . Text
then set lbl_comparisonRes . Text to " This is a MATCH! "
else set lbl_comparisonRes . Text to " This is NOT a match. "

THANK YOU!

2ricecake@hallym.ac.kr

네트워크 포렌식

- **기기의 연결 상태 및 상세 정보를 제공**

  자동으로 연결되는 AP와 AP의 맥주소를 찾고,

  추후 AP에 대한 로그 감식을 할 수 있다.

  호스트 스캐닝을 통해 지정한 아이피 대역에 있는 호스트를 검색한다.

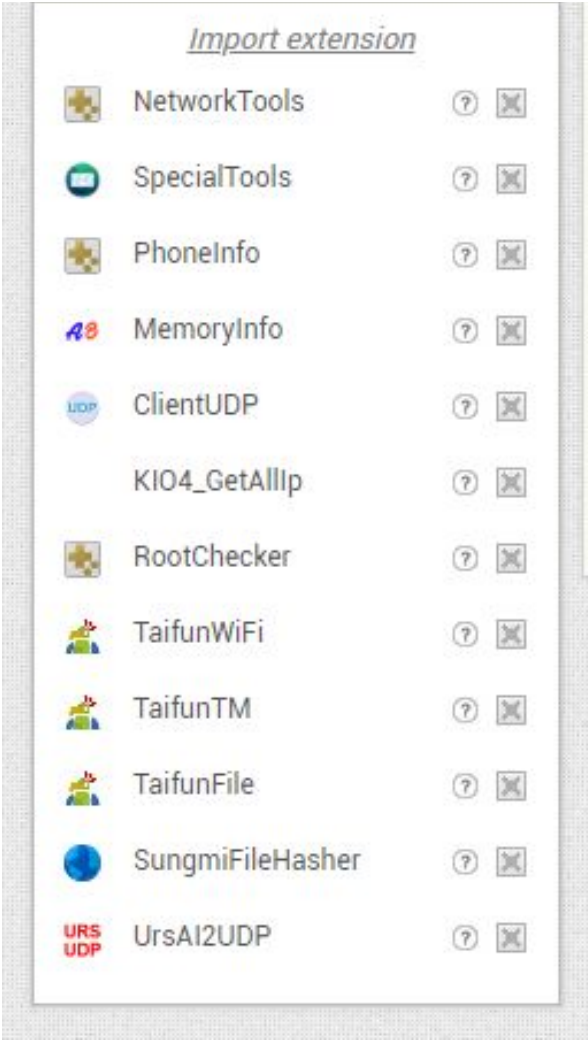
시스템 정보 조회

- **기기의 하드웨어 리비전 및 소프트웨어 버전 제공**

  하드웨어 버전, 안드로이드API, 부트로더, 루트유무, SIM 및 셀룰러 정보,

  소프트웨어 버전, RAM / ROM 사용량 등등

: 각기 다른 기기 사양 및 환경에 맞춘 포렌식 환경 구성 가능



Extension

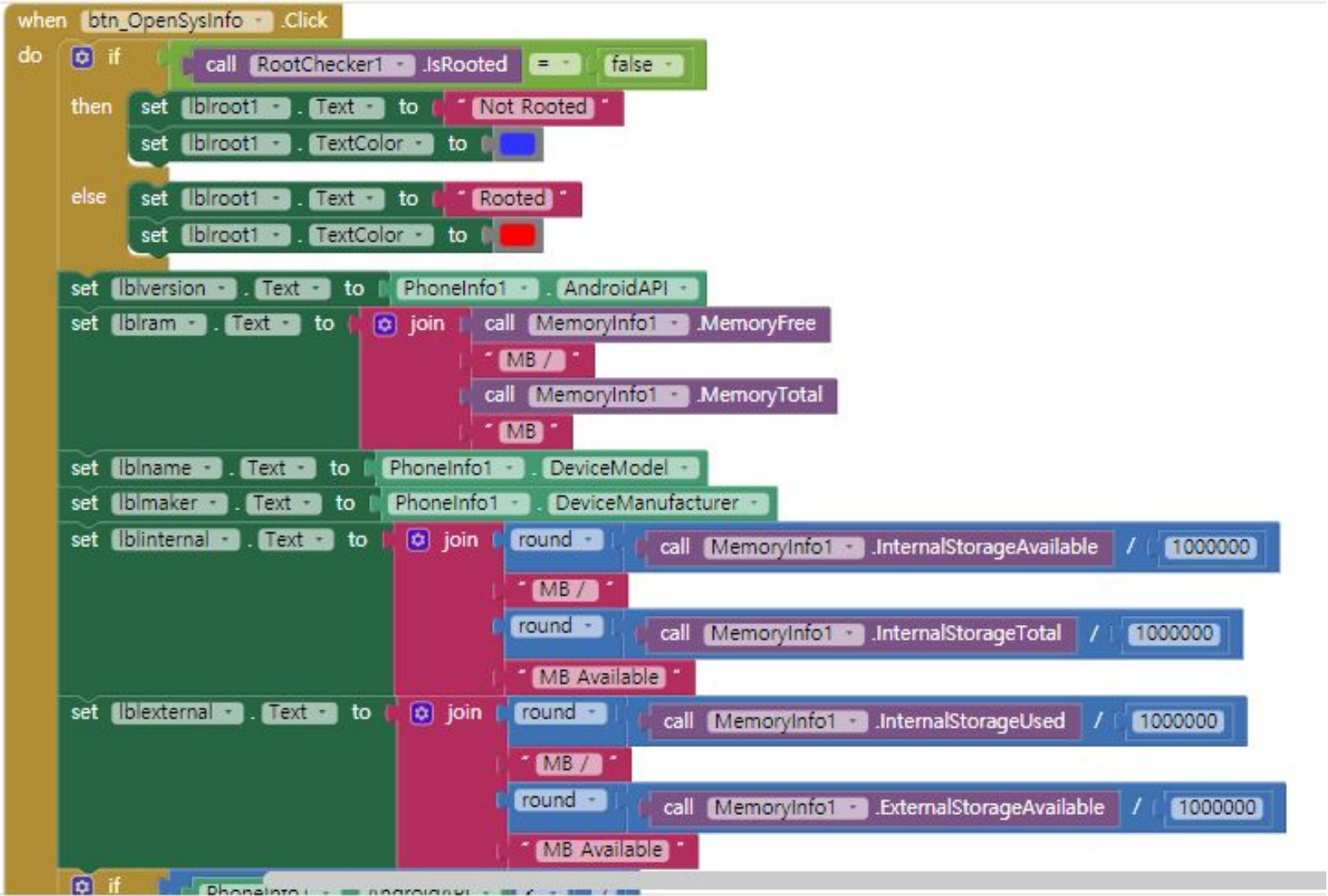
- **다양한 서드파티 확장 기능 존재**

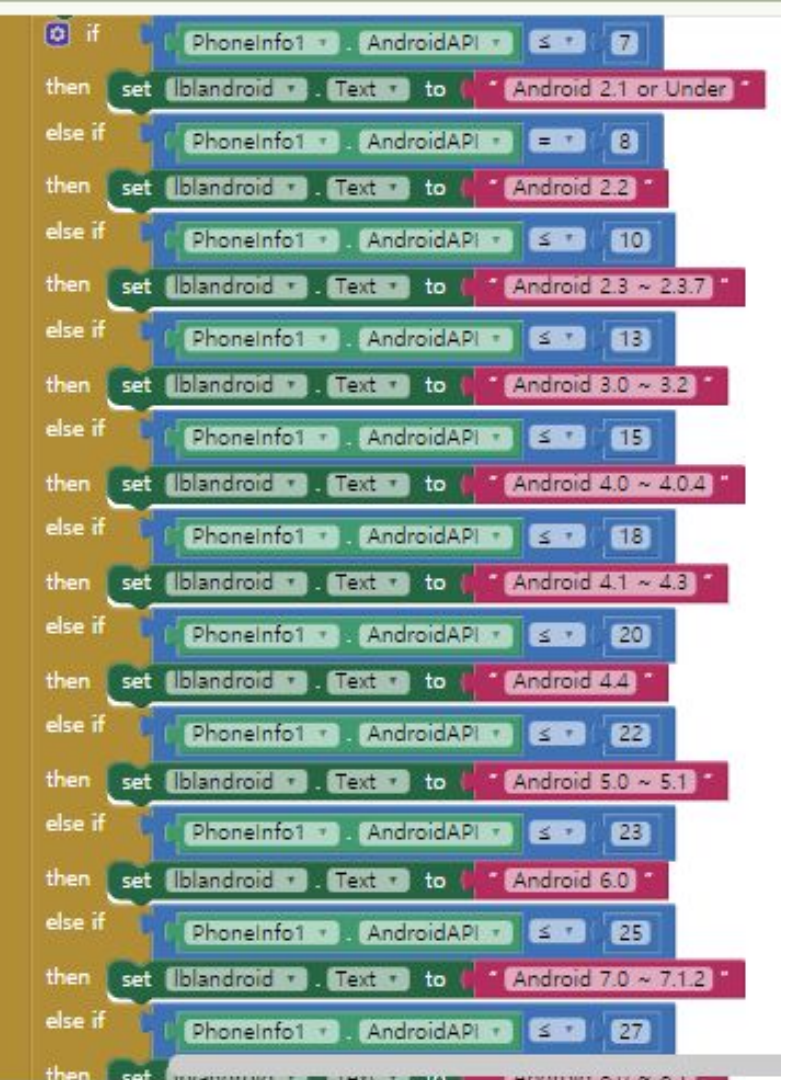
  자바 기반으로 작성된 *.aix 파일들.

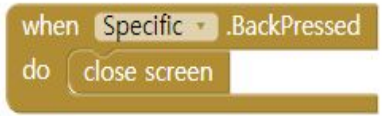
  개인 개발자 및 단체 개발자들이 다수 제작.

  유료화모델도 존재.

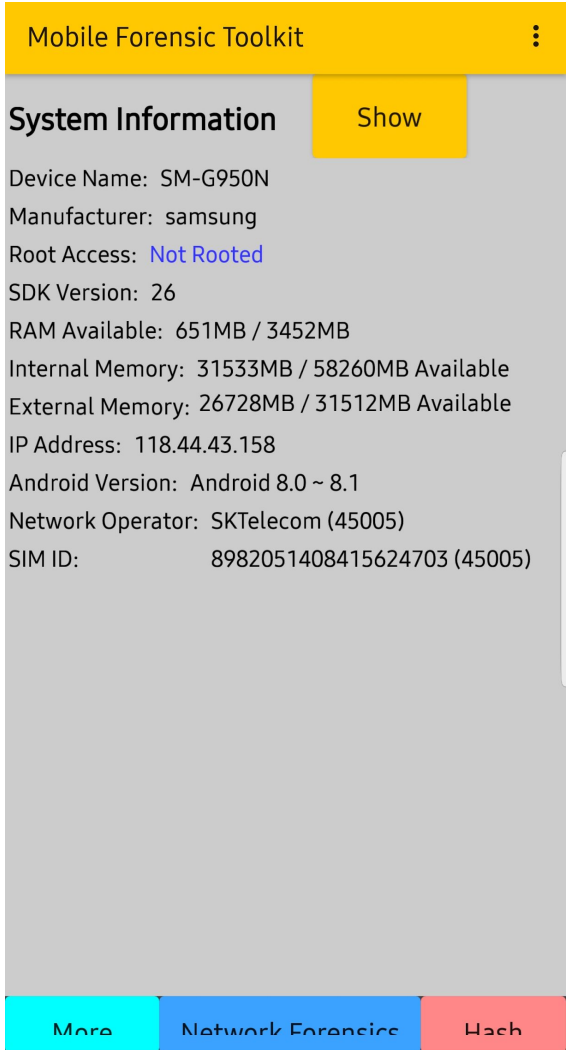
ex) UDP Server 및 System Log의 경우 추가 비용을 지불해야 함.
(실제 기능에서 배제)


when btn_OpenSysInfo .Click
do if call RootChecker1 .IsRooted = false
then set lblroot1 . Text to " Not Rooted "
set lblroot1 . TextColor to
else set lblroot1 . Text to " Rooted "
set lblroot1 . TextColor to
set lblversion . Text to PhoneInfo1 . AndroidAPI
set lblram . Text to join call MemoryInfo1 .MemoryFree
" MB / "
call MemoryInfo1 .MemoryTotal
" MB "
set lblname . Text to PhoneInfo1 . DeviceModel
set lblmaker . Text to PhoneInfo1 . DeviceManufacturer
set lblinternal . Text to join round call MemoryInfo1 .InternalStorageAvailable / 1000000
" MB / "
round call MemoryInfo1 .InternalStorageTotal / 1000000
" MB Available "
set lblexternal . Text to join round call MemoryInfo1 .InternalStorageUsed / 1000000
" MB / "
round call MemoryInfo1 .ExternalStorageAvailable / 1000000
" MB Available "
if


if PhoneInfo1 . AndroidAPI ≤ 7
then set lblandroid . Text to " Android 2.1 or Under "
else if PhoneInfo1 . AndroidAPI = 8
then set lblandroid . Text to " Android 2.2 "
else if PhoneInfo1 . AndroidAPI ≤ 10
then set lblandroid . Text to " Android 2.3 ~ 2.3.7 "
else if PhoneInfo1 . AndroidAPI ≤ 13
then set lblandroid . Text to " Android 3.0 ~ 3.2 "
else if PhoneInfo1 . AndroidAPI ≤ 15
then set lblandroid . Text to " Android 4.0 ~ 4.0.4 "
else if PhoneInfo1 . AndroidAPI ≤ 18
then set lblandroid . Text to " Android 4.1 ~ 4.3 "
else if PhoneInfo1 . AndroidAPI ≤ 20
then set lblandroid . Text to " Android 4.4 "
else if PhoneInfo1 . AndroidAPI ≤ 22
then set lblandroid . Text to " Android 5.0 ~ 5.1 "
else if PhoneInfo1 . AndroidAPI ≤ 23
then set lblandroid . Text to " Android 6.0 "
else if PhoneInfo1 . AndroidAPI ≤ 25
then set lblandroid . Text to " Android 7.0 ~ 7.1.2 "
else if PhoneInfo1 . AndroidAPI ≤ 27

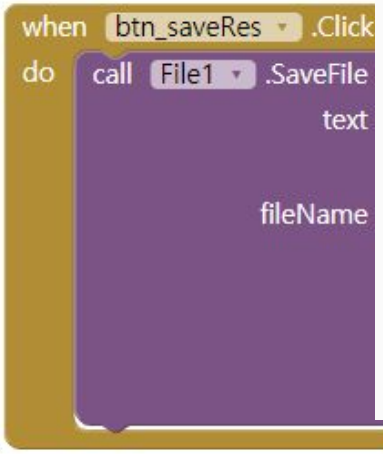

when Specific .BackPressed
do close screen

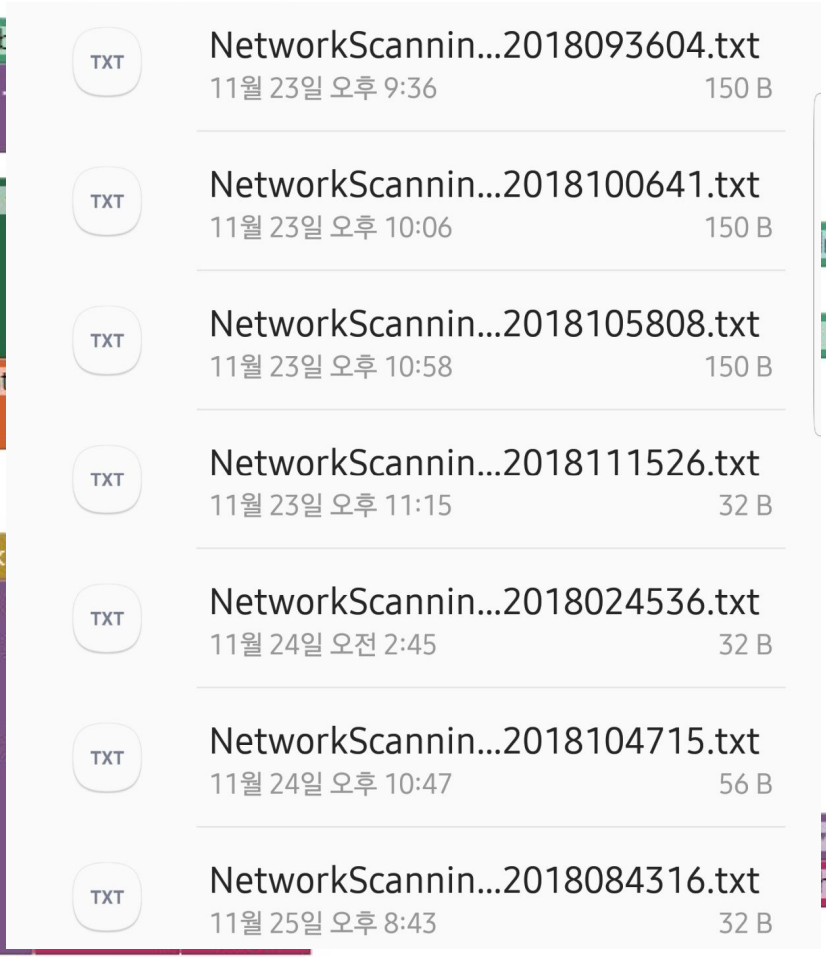
when Specific .Initialize
do set lbl_kernel . Text to SpecialTools1 . KernelVersion
set lbl_buildnumber . Text to SpecialTools1 . BuildNumber
set lbl_baseband . Text to SpecialTools1 . BasebandVersion
set lbl_bootloader . Text to SpecialTools1 . BootloaderVersion
set lbl_serial . Text to SpecialTools1 . SerialNumber
set lbl_country . Text to SpecialTools1 . CountryCode
set lbl_lang . Text to SpecialTools1 . LanguageCode

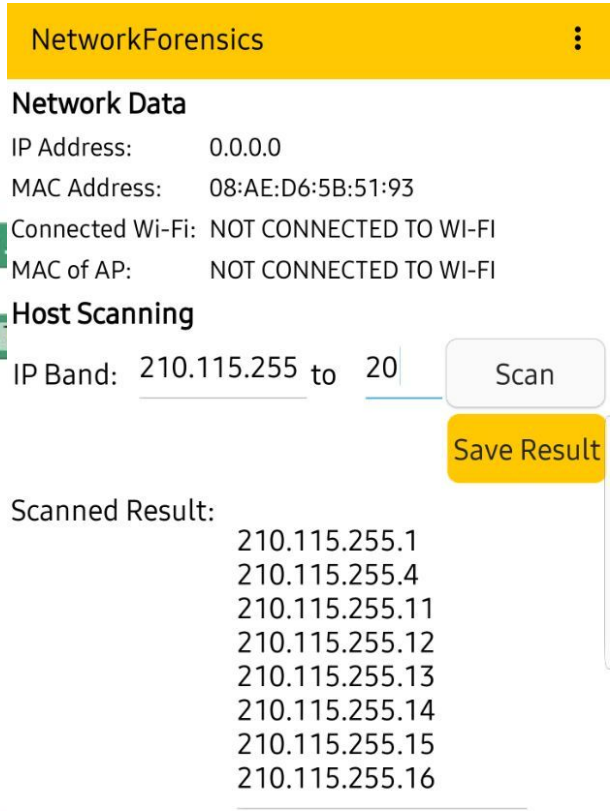


Kernel Version:	4.4.111-14502969-QB200
Build Number:	R16NW.G950NKSU3CRJ1
Baseband Version:	G950NKOU3CRJ1
Bootloader Version:	G950NKSU3CRJ1
Serial Number:	ce10171abab0001e04
Country Code:	KR
Language Code:	ko

when btnScan .Click
do if is empty
then call Notifier1
else set txtboxResult
set global net_Dat

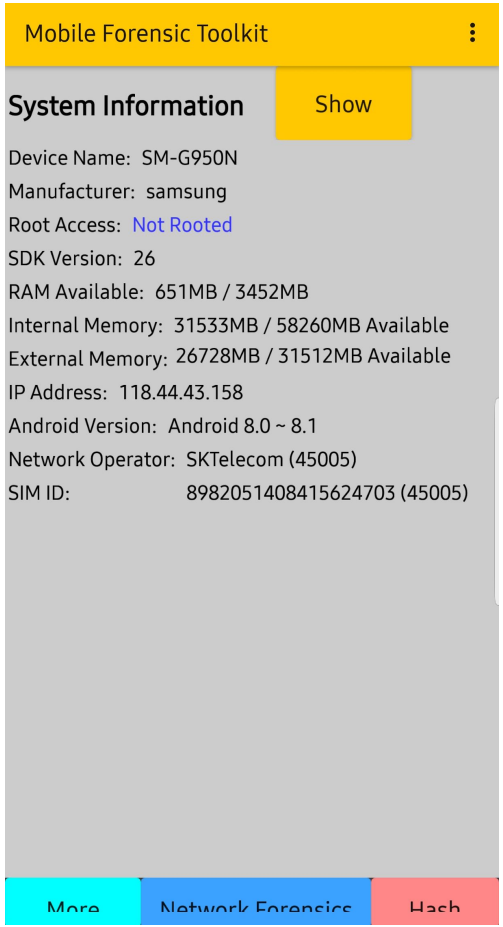

when btn_saveRes .Click
do call File1 .SaveFile
text
fileName

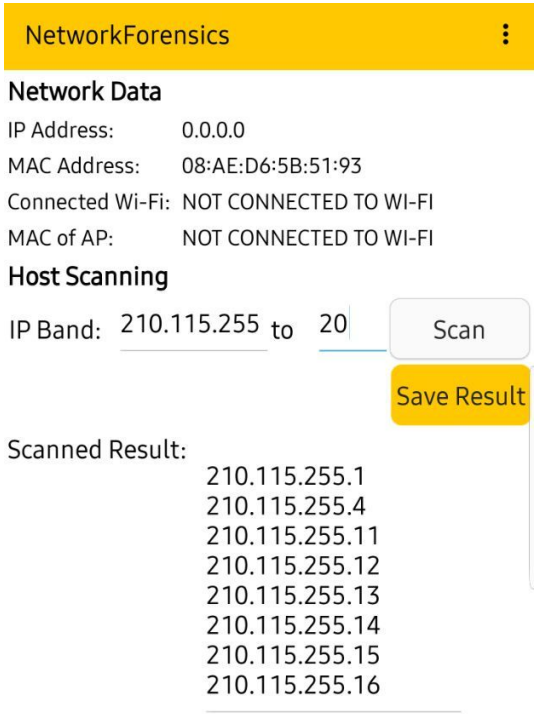

TXT
NetworkScannin...2018093604.txt
11월 23일 오후 9:36
150 B
TXT
NetworkScannin...2018100641.txt
11월 23일 오후 10:06
150 B
TXT
NetworkScannin...2018105808.txt
11월 23일 오후 10:58
150 B
TXT
NetworkScannin...2018111526.txt
11월 23일 오후 11:15
32 B
TXT
NetworkScannin...2018024536.txt
11월 24일 오전 2:45
32 B
TXT
NetworkScannin...2018104715.txt
11월 24일 오후 10:47
56 B
TXT
NetworkScannin...2018084316.txt
11월 25일 오후 8:43
32 B


NetworkForensics
Network Data
IP Address: 0.0.0.0
MAC Address: 08:AE:D6:5B:51:93
Connected Wi-Fi: NOT CONNECTED TO WI-FI
MAC of AP: NOT CONNECTED TO WI-FI
Host Scanning
IP Band: 210.115.255 to 20
Scan
Save Result
Scanned Result:
210.115.255.1
210.115.255.4
210.115.255.11
210.115.255.12
210.115.255.13
210.115.255.14
210.115.255.15
210.115.255.16

네트워크 포렌식 구동 영상

https://www.youtube.com/watch?v=JxvV8Mkxl2E&feature=youtu.be





THANK YOU!

lotsofstars1995@gmail.com

정보법과학연구집단
LEGAL INFORMATICS AND FORENSIC SCIENCE