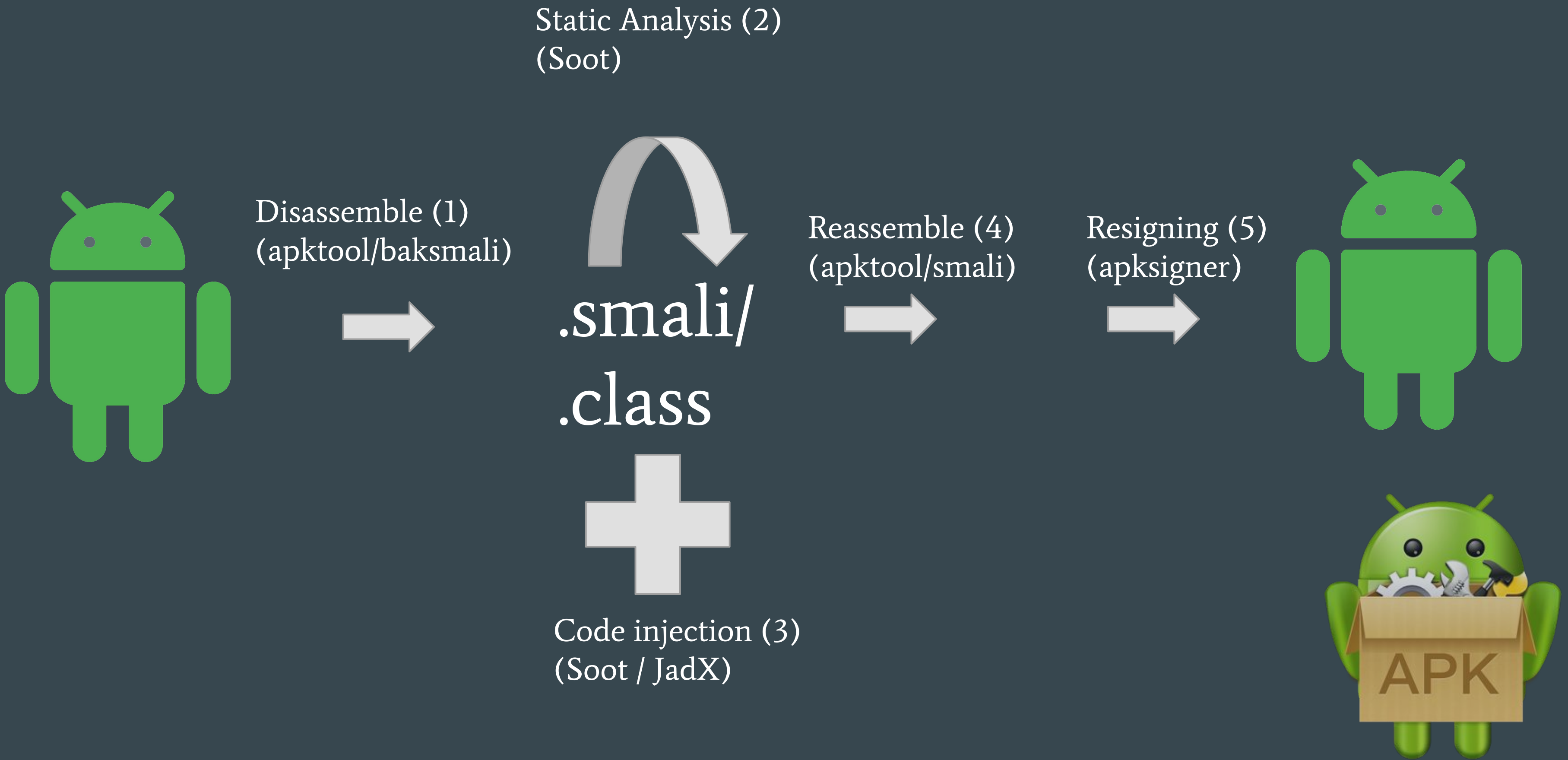
APK Reverse Engineering and Tampering Detection

- Semil Jain and Pranjal Patil

Part 1: APK Reverse Engineering

Part 2: Anti-Tampering Analysis

Part 1



Static Analysis (2)
(Soot)

Disassemble (1)
(apktool/baksmali)

.smali/
.class

Reassemble (4)
(apktool/smali)

Resigning (5)
(apksigner)

Code injection (3)
(Soot / JadX)

Lets Begin Hacking*...

*Only for Project purpose

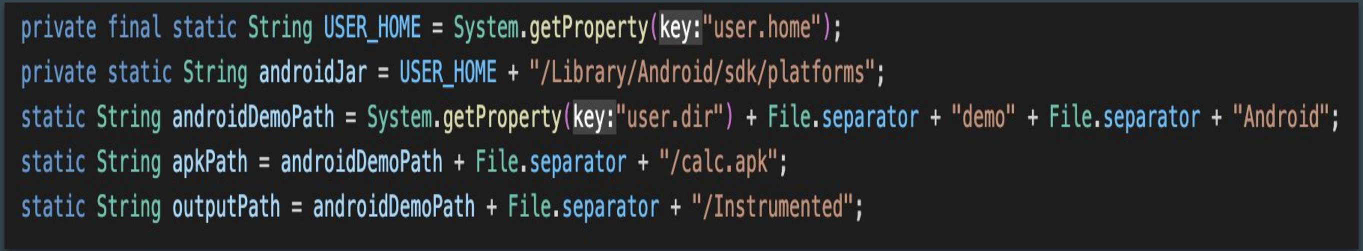
1. Working with Soot - A Java optimization framework

What did we hack?

- Instrumented an Android app using Soot
- Which application? - A simple calculator apk
- Printed the logs in the adb shell on every method call in the app

Implementation

- AndroidLogger.Java

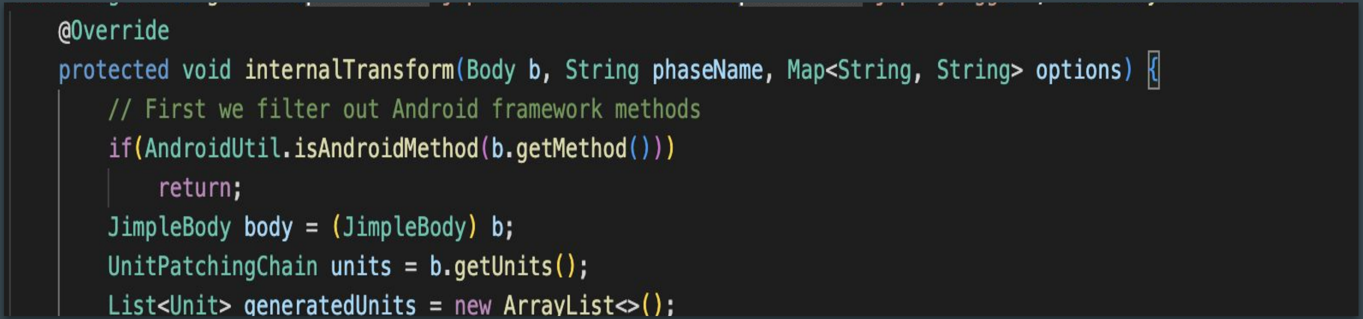


```
private final static String USER_HOME = System.getProperty(key:"user.home");
private static String androidJar = USER_HOME + "/Library/Android/sdk/platforms";
static String androidDemoPath = System.getProperty(key:"user.dir") + File.separator + "demo" + File.separator + "Android";
static String apkPath = androidDemoPath + File.separator + "/calc.apk";
static String outputPath = androidDemoPath + File.separator + "/Instrumented";
```

Setting properties

Implementation

- AndroidLogger.Java

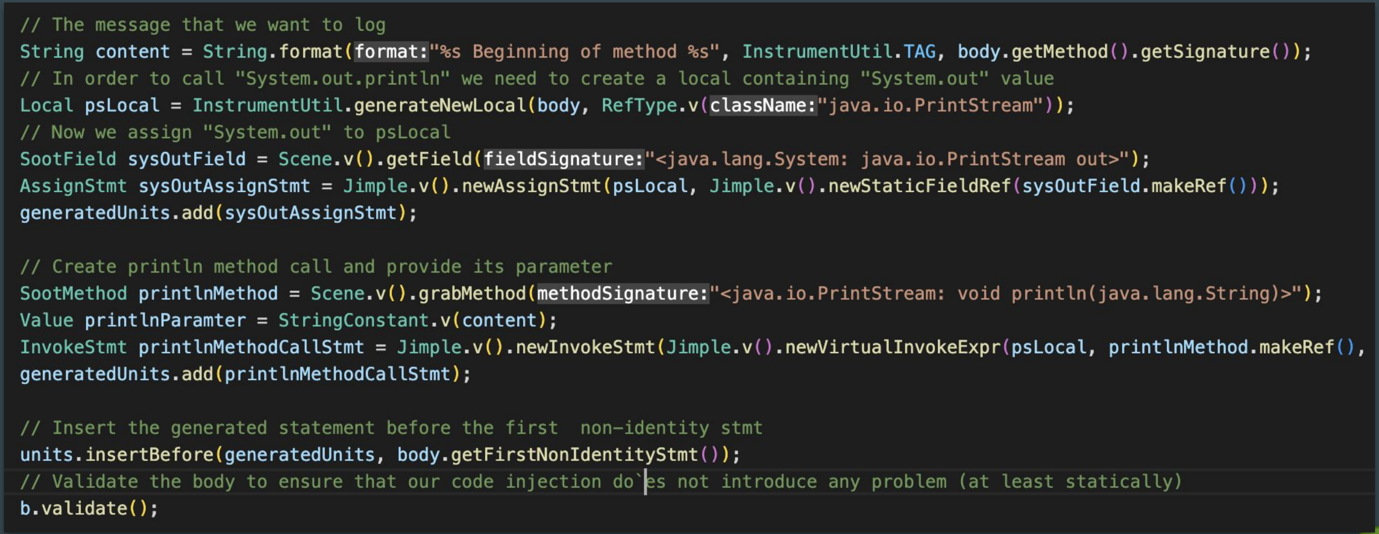


```java
@Override
protected void internalTransform(Body b, String phaseName, Map<String, String> options) {
    // First we filter out Android framework methods
    if(AndroidUtil.isAndroidMethod(b.getMethod()))
        return;
    JimpleBody body = (JimpleBody) b;
    UnitPatchingChain units = b.getUnits();
    List<Unit> generatedUnits = new ArrayList<>();
```

Getting methods and
creating Jimple body

Implementation

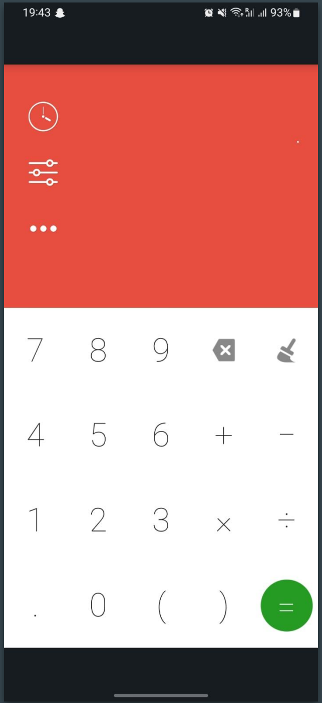
- AndroidLogger.Java

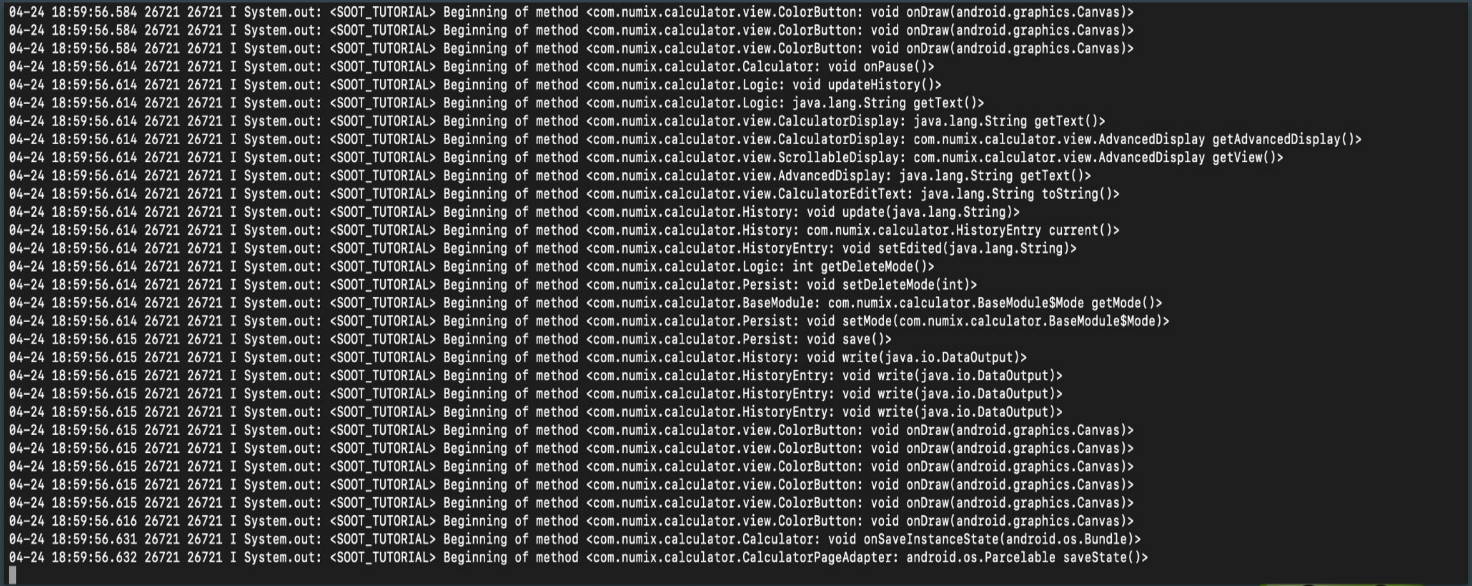


```
// The message that we want to log
String content = String.format(format:"%s Beginning of method %s", InstrumentUtil.TAG, body.getMethod().getSignature());
// In order to call "System.out.println" we need to create a local containing "System.out" value
Local psLocal = InstrumentUtil.generateNewLocal(body, RefType.v(className:"java.io.PrintStream"));
// Now we assign "System.out" to psLocal
SootField sysOutField = Scene.v().getField(fieldSignature:"<java.lang.System: java.io.PrintStream out>");
AssignStmt sysOutAssignStmt = Jimple.v().newAssignStmt(psLocal, Jimple.v().newStaticFieldRef(sysOutField.makeRef()));
generatedUnits.add(sysOutAssignStmt);

// Create println method call and provide its parameter
SootMethod printlnMethod = Scene.v().grabMethod(methodSignature:"<java.io.PrintStream: void println(java.lang.String)>");
Value printlnParamter = StringConstant.v(content);
InvokeStmt printlnMethodCallStmt = Jimple.v().newInvokeStmt(Jimple.v().newVirtualInvokeExpr(psLocal, printlnMethod.makeRef(),
generatedUnits.add(printlnMethodCallStmt);

// Insert the generated statement before the first  non-identity stmt
units.insertBefore(generatedUnits, body.getFirstNonIdentityStmt());
// Validate the body to ensure that our code injection do`es not introduce any problem (at least statically)
b.validate();
```

Creating println calls
and adding to methods

Results





```
04-24 18:59:56.584 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.ColorButton: void onDraw(android.graphics.Canvas)>
04-24 18:59:56.584 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.ColorButton: void onDraw(android.graphics.Canvas)>
04-24 18:59:56.584 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.ColorButton: void onDraw(android.graphics.Canvas)>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.Calculator: void onPause()>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.Logic: void updateHistory()>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.Logic: java.lang.String getText()>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.CalculatorDisplay: java.lang.String getText()>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.CalculatorDisplay: com.numix.calculator.view.AdvancedDisplay getAdvancedDisplay()>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.ScrollableDisplay: com.numix.calculator.view.AdvancedDisplay getView()>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.AdvancedDisplay: java.lang.String getText()>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.CalculatorEditText: java.lang.String toString()>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.History: void update(java.lang.String)>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.History: com.numix.calculator.HistoryEntry current()>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.HistoryEntry: void setEdited(java.lang.String)>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.Logic: int getDeleteMode()>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.Persist: void setDeleteMode(int)>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.BaseModule: com.numix.calculator.BaseModule$Mode getMode()>
04-24 18:59:56.614 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.Persist: void setMode(com.numix.calculator.BaseModule$Mode)>
04-24 18:59:56.615 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.Persist: void save()>
04-24 18:59:56.615 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.History: void write(java.io.DataOutput)>
04-24 18:59:56.615 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.HistoryEntry: void write(java.io.DataOutput)>
04-24 18:59:56.615 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.HistoryEntry: void write(java.io.DataOutput)>
04-24 18:59:56.615 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.HistoryEntry: void write(java.io.DataOutput)>
04-24 18:59:56.615 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.ColorButton: void onDraw(android.graphics.Canvas)>
04-24 18:59:56.615 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.ColorButton: void onDraw(android.graphics.Canvas)>
04-24 18:59:56.615 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.ColorButton: void onDraw(android.graphics.Canvas)>
04-24 18:59:56.615 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.ColorButton: void onDraw(android.graphics.Canvas)>
04-24 18:59:56.615 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.ColorButton: void onDraw(android.graphics.Canvas)>
04-24 18:59:56.616 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.view.ColorButton: void onDraw(android.graphics.Canvas)>
04-24 18:59:56.631 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.Calculator: void onSaveInstanceState(android.os.Bundle)>
04-24 18:59:56.632 26721 26721 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.calculator.CalculatorPageAdapter: android.os.Parcelable saveState()>
```

ADB Shell Logs

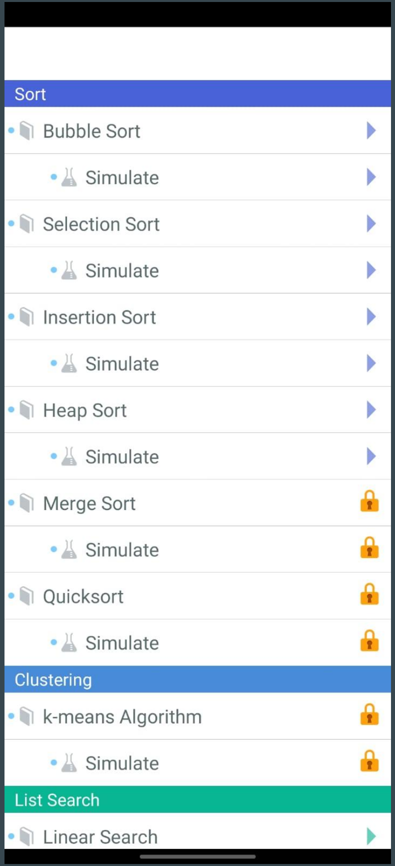
2. Working with Apktool, Smali files and JADX

What did we hack?

- Application features altering
- Which application? - Algorithms teaching application (On Playstore)
- Removed the Premium lock on videos and made it free

Implementation

Algorithms.apk



Sort

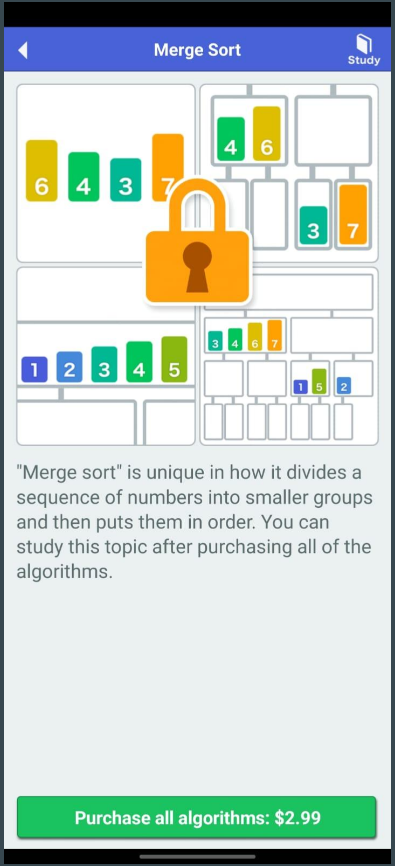
- Bubble Sort
  - Simulate
- Selection Sort
  - Simulate
- Insertion Sort
  - Simulate
- Heap Sort
  - Simulate
- Merge Sort
  - Simulate
- Quicksort
  - Simulate

Clustering

- k-means Algorithm
  - Simulate

List Search

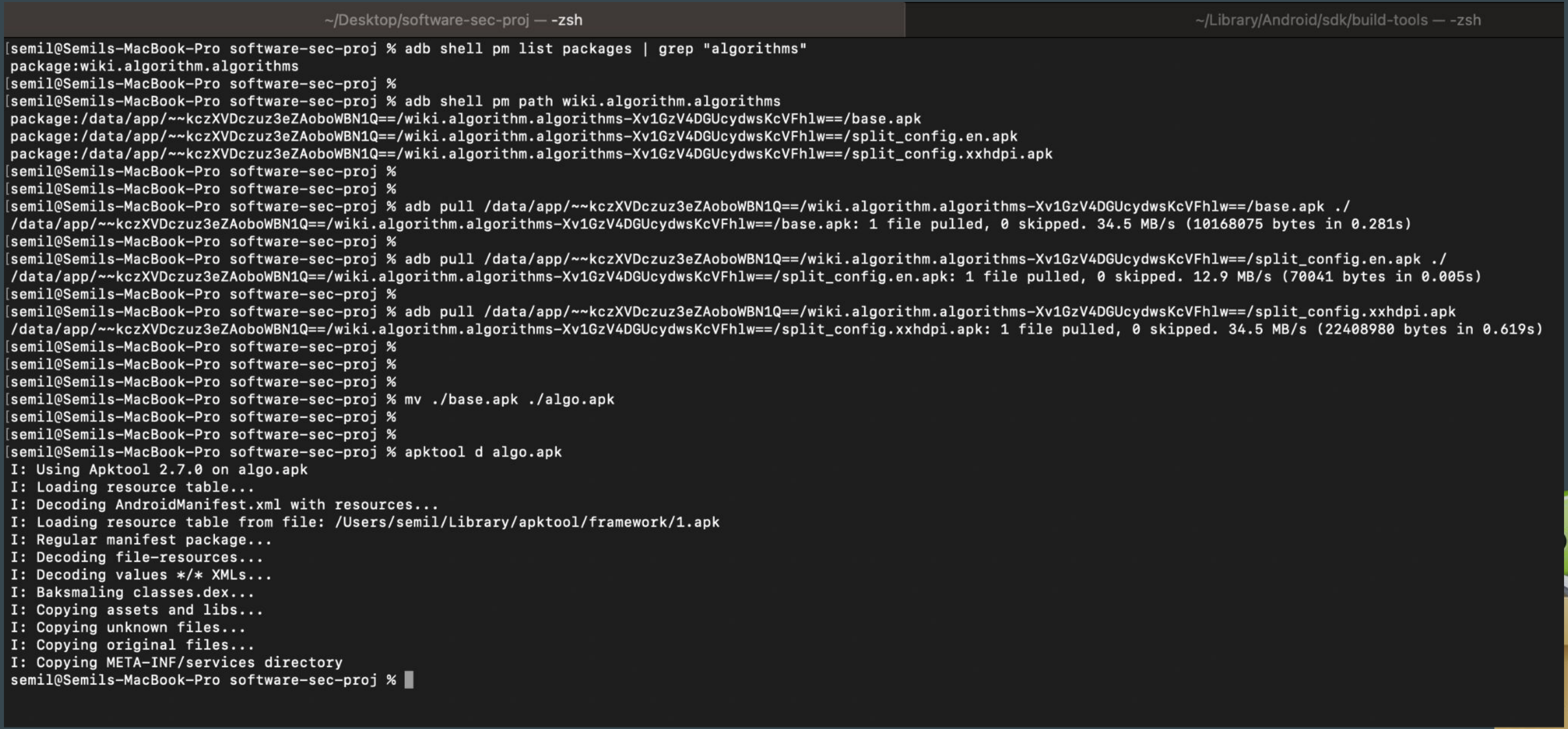
- Linear Search



"Merge sort" is unique in how it divides a sequence of numbers into smaller groups and then puts them in order. You can study this topic after purchasing all of the algorithms.

Implementation

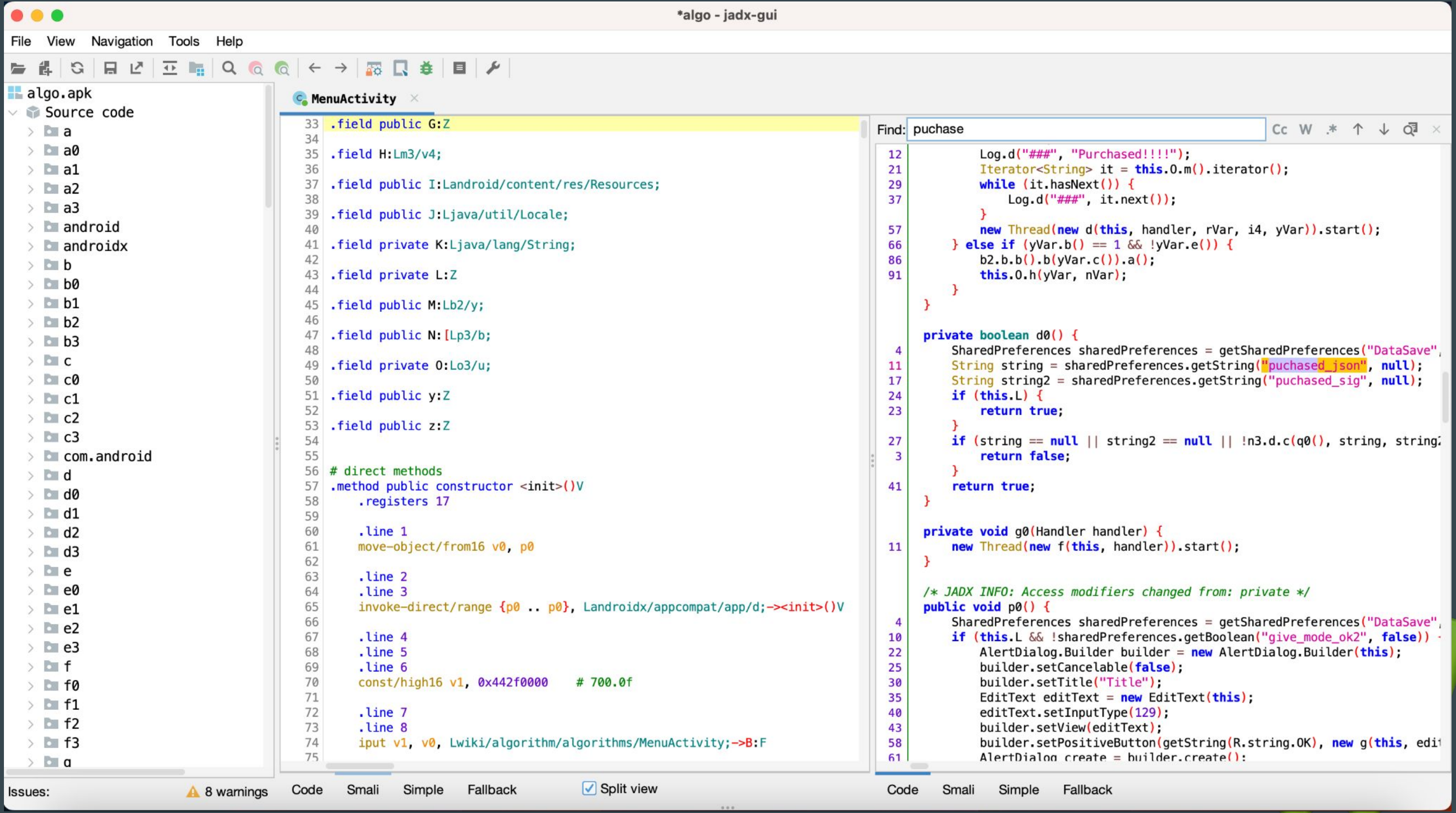
Decompile with Apktool


~/Desktop/software-sec-proj — -zsh
~/Library/Android/sdk/build-tools — -zsh

```
[semil@Semils-MacBook-Pro software-sec-proj % adb shell pm list packages | grep "algorithms"
 package:wiki.algorithm.algorithms
[semil@Semils-MacBook-Pro software-sec-proj %
[semil@Semils-MacBook-Pro software-sec-proj % adb shell pm path wiki.algorithm.algorithms
 package:/data/app/~~kczXVDczuz3eZAoboWBN1Q==/wiki.algorithm.algorithms-Xv1GzV4DGUcydwsKcVFhlw==/base.apk
 package:/data/app/~~kczXVDczuz3eZAoboWBN1Q==/wiki.algorithm.algorithms-Xv1GzV4DGUcydwsKcVFhlw==/split_config.en.apk
 package:/data/app/~~kczXVDczuz3eZAoboWBN1Q==/wiki.algorithm.algorithms-Xv1GzV4DGUcydwsKcVFhlw==/split_config.xxhdpi.apk
[semil@Semils-MacBook-Pro software-sec-proj %
[semil@Semils-MacBook-Pro software-sec-proj %
[semil@Semils-MacBook-Pro software-sec-proj % adb pull /data/app/~~kczXVDczuz3eZAoboWBN1Q==/wiki.algorithm.algorithms-Xv1GzV4DGUcydwsKcVFhlw==/base.apk ./
 /data/app/~~kczXVDczuz3eZAoboWBN1Q==/wiki.algorithm.algorithms-Xv1GzV4DGUcydwsKcVFhlw==/base.apk: 1 file pulled, 0 skipped. 34.5 MB/s (10168075 bytes in 0.281s)
[semil@Semils-MacBook-Pro software-sec-proj %
[semil@Semils-MacBook-Pro software-sec-proj % adb pull /data/app/~~kczXVDczuz3eZAoboWBN1Q==/wiki.algorithm.algorithms-Xv1GzV4DGUcydwsKcVFhlw==/split_config.en.apk ./
 /data/app/~~kczXVDczuz3eZAoboWBN1Q==/wiki.algorithm.algorithms-Xv1GzV4DGUcydwsKcVFhlw==/split_config.en.apk: 1 file pulled, 0 skipped. 12.9 MB/s (70041 bytes in 0.005s)
[semil@Semils-MacBook-Pro software-sec-proj %
[semil@Semils-MacBook-Pro software-sec-proj % adb pull /data/app/~~kczXVDczuz3eZAoboWBN1Q==/wiki.algorithm.algorithms-Xv1GzV4DGUcydwsKcVFhlw==/split_config.xxhdpi.apk
 /data/app/~~kczXVDczuz3eZAoboWBN1Q==/wiki.algorithm.algorithms-Xv1GzV4DGUcydwsKcVFhlw==/split_config.xxhdpi.apk: 1 file pulled, 0 skipped. 34.5 MB/s (22408980 bytes in 0.619s)
[semil@Semils-MacBook-Pro software-sec-proj %
[semil@Semils-MacBook-Pro software-sec-proj %
[semil@Semils-MacBook-Pro software-sec-proj %
[semil@Semils-MacBook-Pro software-sec-proj % mv ./base.apk ./algo.apk
[semil@Semils-MacBook-Pro software-sec-proj %
[semil@Semils-MacBook-Pro software-sec-proj %
[semil@Semils-MacBook-Pro software-sec-proj % apktool d algo.apk
 I: Using Apktool 2.7.0 on algo.apk
 I: Loading resource table...
 I: Decoding AndroidManifest.xml with resources...
 I: Loading resource table from file: /Users/semil/Library/apktool/framework/1.apk
 I: Regular manifest package...
 I: Decoding file-resources...
 I: Decoding values */* XMLs...
 I: Baksmaling classes.dex...
 I: Copying assets and libs...
 I: Copying unknown files...
 I: Copying original files...
 I: Copying META-INF/services directory
 semil@Semils-MacBook-Pro software-sec-proj % ▌
```

Implementation

View with Jadx-gui - `jadx-gui algo.apk`

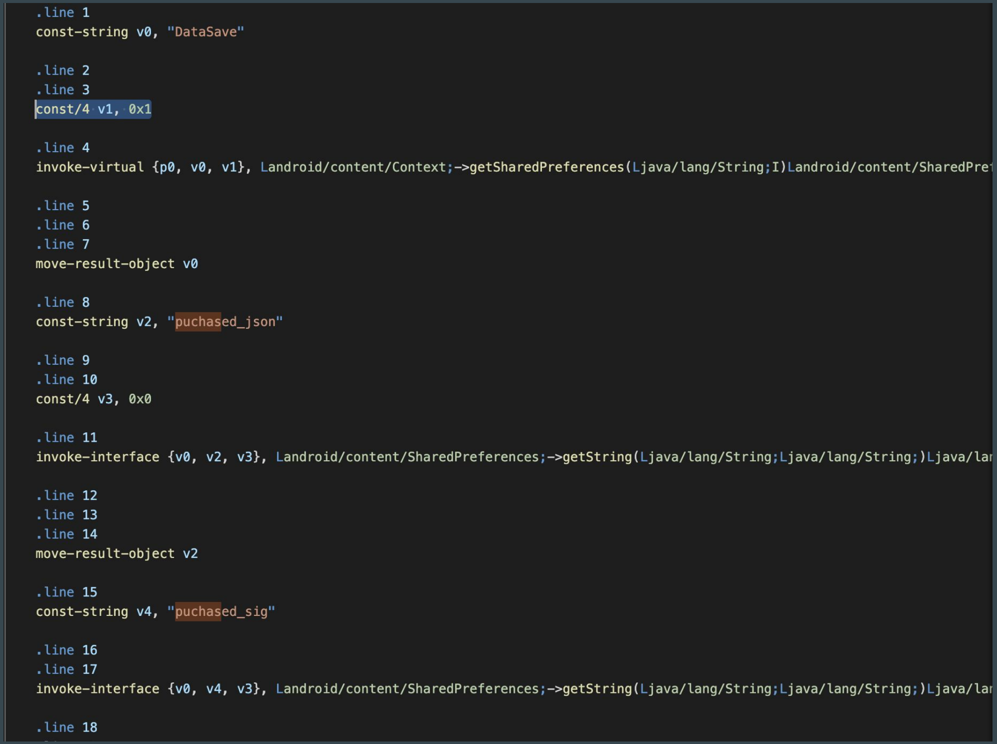


```
.field public G:Z

.field H:Lm3/v4;

.field public I:Landroid/content/res/Resources;

.field public J:Ljava/util/Locale;

.field private K:Ljava/lang/String;

.field private L:Z

.field public M:Lb2/y;

.field public N:[Lp3/b;

.field private O:Lo3/u;

.field public y:Z

.field public z:Z


# direct methods
.method public constructor <init>()V
    .registers 17

    .line 1
    move-object/from16 v0, p0

    .line 2
    .line 3
    invoke-direct/range {p0 .. p0}, Landroidx/appcompat/app/d;-><init>()V

    .line 4
    .line 5
    .line 6
    const/high16 v1, 0x442f0000    # 700.0f

    .line 7
    .line 8
    iput v1, v0, Lwiki/algorithm/algorithms/MenuActivity;->B:F
```

```
            Log.d("###", "Purchased!!!!");
            Iterator<String> it = this.O.m().iterator();
            while (it.hasNext()) {
                Log.d("###", it.next());
            }
            new Thread(new d(this, handler, rVar, i4, yVar)).start();
        } else if (yVar.b() == 1 && !yVar.e()) {
            b2.b.b().b(yVar.c()).a();
            this.O.h(yVar, nVar);
        }
    }

    private boolean d0() {
        SharedPreferences sharedPreferences = getSharedPreferences("DataSave",
        String string = sharedPreferences.getString("puchased_json", null);
        String string2 = sharedPreferences.getString("puchased_sig", null);
        if (this.L) {
            return true;
        }
        if (string == null || string2 == null || !n3.d.c(q0(), string, string2
            return false;
        }
        return true;
    }

    private void g0(Handler handler) {
        new Thread(new f(this, handler)).start();
    }

    /* JADX INFO: Access modifiers changed from: private */
    public void p0() {
        SharedPreferences sharedPreferences = getSharedPreferences("DataSave",
        if (this.L && !sharedPreferences.getBoolean("give_mode_ok2", false)) -
            AlertDialog.Builder builder = new AlertDialog.Builder(this);
            builder.setCancelable(false);
            builder.setTitle("Title");
            EditText editText = new EditText(this);
            editText.setInputType(129);
            builder.setView(editText);
            builder.setPositiveButton(getString(R.string.OK), new g(this, edit
            AlertDialog create = builder.create();
```

Implementation

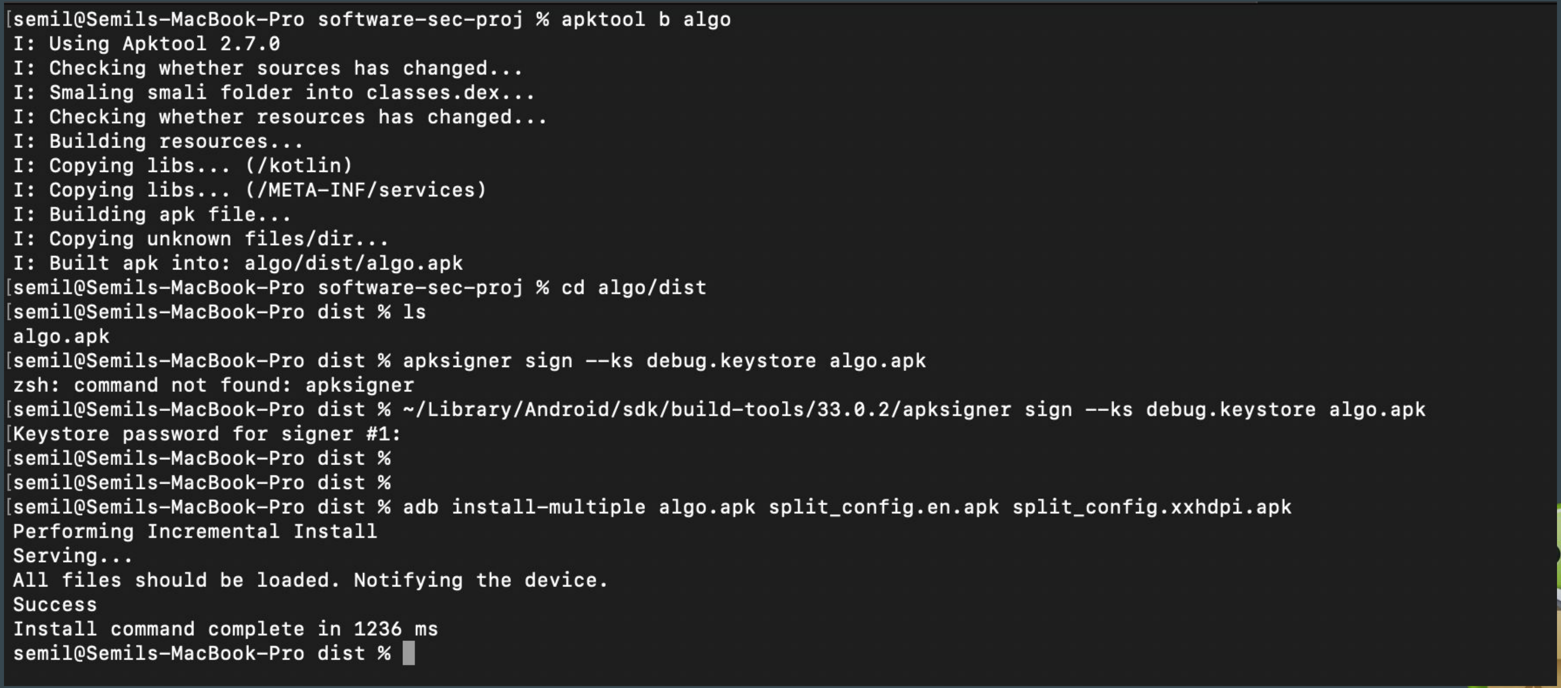
Make changes in the smali file and recompile the apk using Apktool



```
.line 1
const-string v0, "DataSave"

.line 2
.line 3
const/4 v1, 0x1

.line 4
invoke-virtual {p0, v0, v1}, Landroid/content/Context;->getSharedPreferences(Ljava/lang/String;I)Landroid/content/SharedPref

.line 5
.line 6
.line 7
move-result-object v0

.line 8
const-string v2, "puchased_json"

.line 9
.line 10
const/4 v3, 0x0

.line 11
invoke-interface {v0, v2, v3}, Landroid/content/SharedPreferences;->getString(Ljava/lang/String;Ljava/lang/String;)Ljava/lar

.line 12
.line 13
.line 14
move-result-object v2

.line 15
const-string v4, "puchased_sig"

.line 16
.line 17
invoke-interface {v0, v4, v3}, Landroid/content/SharedPreferences;->getString(Ljava/lang/String;Ljava/lang/String;)Ljava/lar

.line 18
```

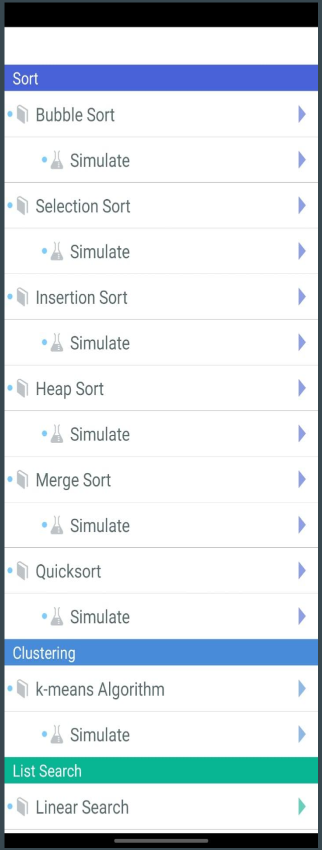
Implementation

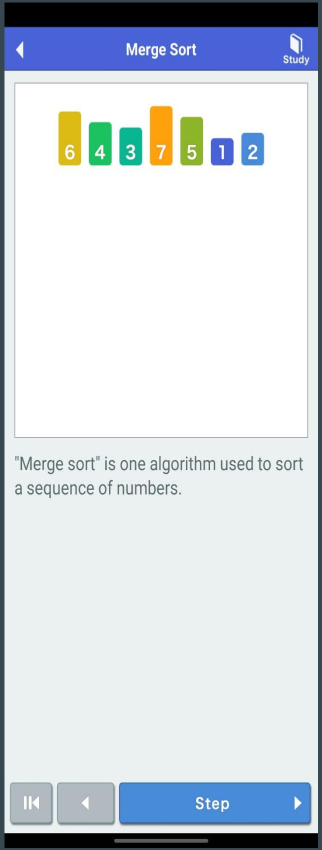
APK Signing



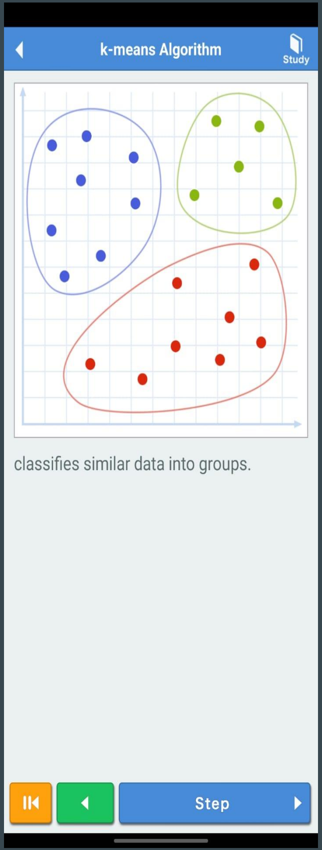
```
[semil@Semils-MacBook-Pro software-sec-proj % apktool b algo
 I: Using Apktool 2.7.0
 I: Checking whether sources has changed...
 I: Smaling smali folder into classes.dex...
 I: Checking whether resources has changed...
 I: Building resources...
 I: Copying libs... (/kotlin)
 I: Copying libs... (/META-INF/services)
 I: Building apk file...
 I: Copying unknown files/dir...
 I: Built apk into: algo/dist/algo.apk
[semil@Semils-MacBook-Pro software-sec-proj % cd algo/dist
[semil@Semils-MacBook-Pro dist % ls
 algo.apk
[semil@Semils-MacBook-Pro dist % apksigner sign --ks debug.keystore algo.apk
 zsh: command not found: apksigner
[semil@Semils-MacBook-Pro dist % ~/Library/Android/sdk/build-tools/33.0.2/apksigner sign --ks debug.keystore algo.apk
[Keystore password for signer #1:
[semil@Semils-MacBook-Pro dist %
[semil@Semils-MacBook-Pro dist %
[semil@Semils-MacBook-Pro dist % adb install-multiple algo.apk split_config.en.apk split_config.xxhdpi.apk
 Performing Incremental Install
 Serving...
 All files should be loaded. Notifying the device.
 Success
 Install command complete in 1236 ms
 semil@Semils-MacBook-Pro dist % 
```

Results





"Merge sort" is one algorithm used to sort a sequence of numbers.



classifies similar data into groups.

Lets Prevent Hacking*...

*No conditions

Part 2

Anti-Tampering Analysis

Some Techniques

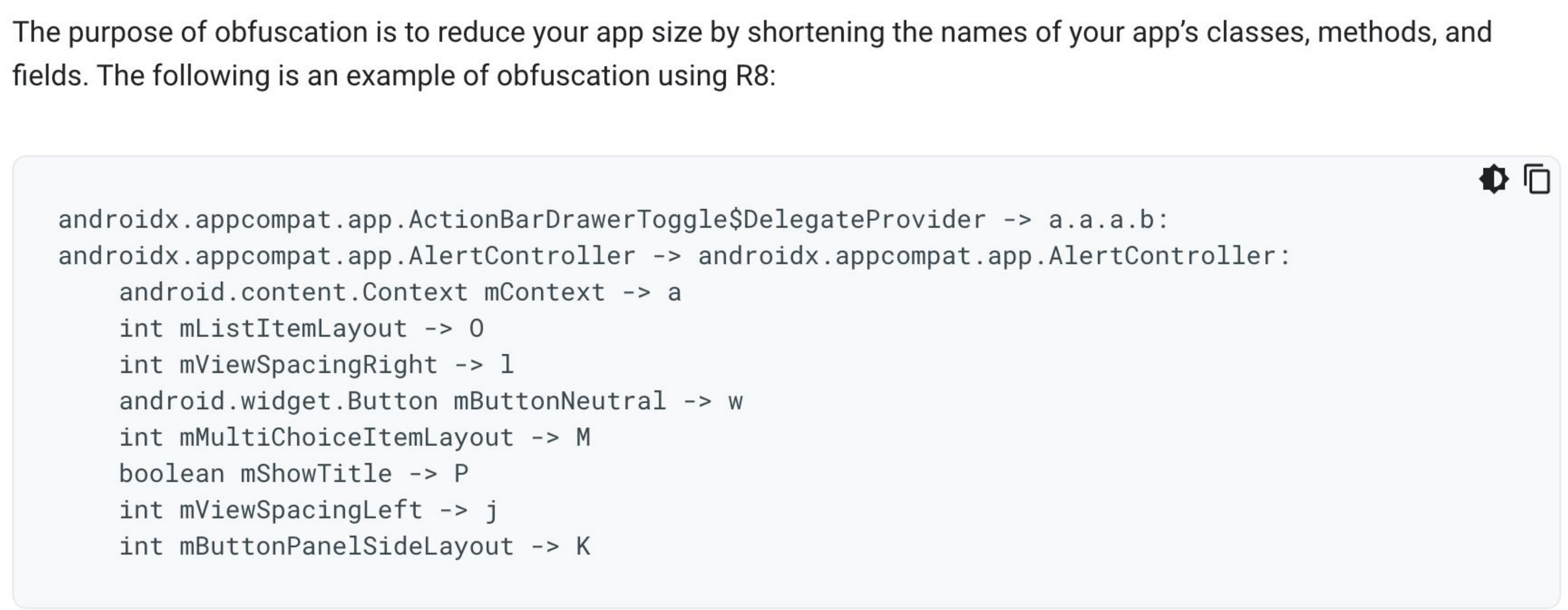
- Code Obfuscation

- APK Signature Comparison

- Protection Fingerprints

Code Obfuscation

Android Proguard

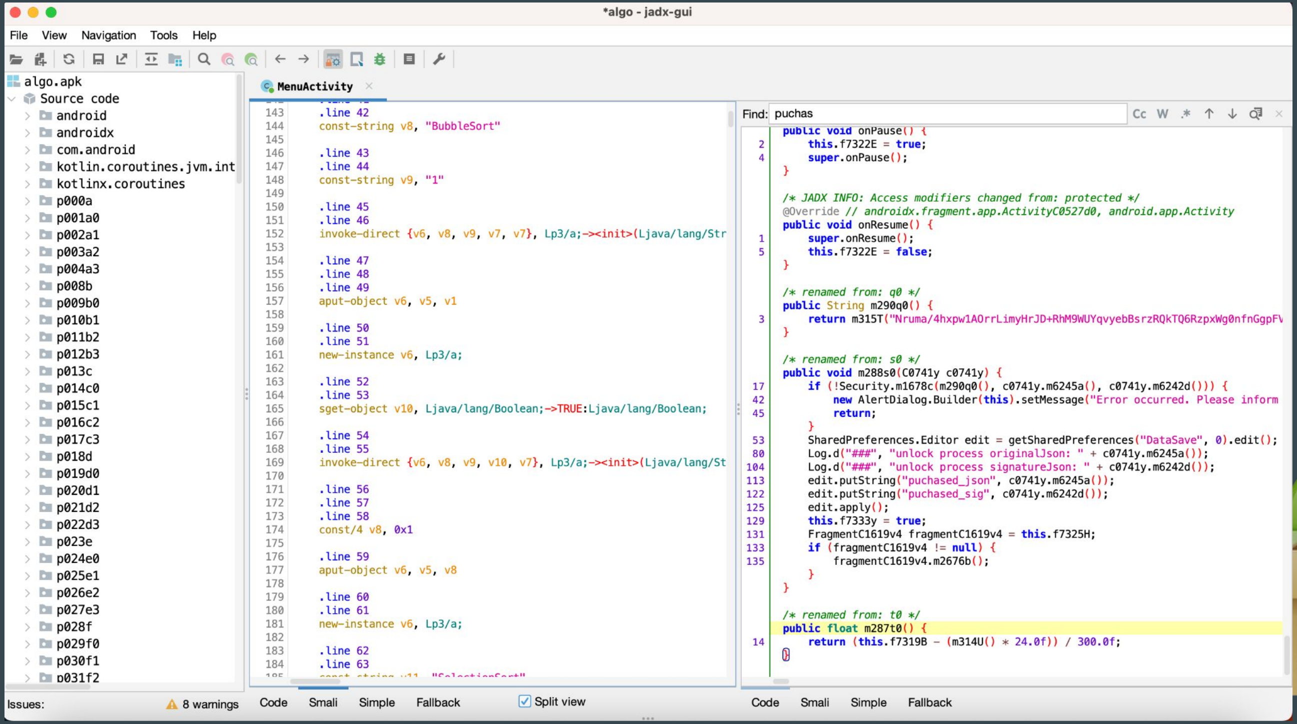


The purpose of obfuscation is to reduce your app size by shortening the names of your app’s classes, methods, and fields. The following is an example of obfuscation using R8:

```
androidx.appcompat.app.ActionBarDrawerToggle$DelegateProvider -> a.a.a.b:
androidx.appcompat.app.AlertController -> androidx.appcompat.app.AlertController:
    android.content.Context mContext -> a
    int mListItemLayout -> O
    int mViewSpacingRight -> l
    android.widget.Button mButtonNeutral -> w
    int mMultiChoiceItemLayout -> M
    boolean mShowTitle -> P
    int mViewSpacingLeft -> j
    int mButtonPanelSideLayout -> K
```

Code Obfuscation

In our Algorithms apk

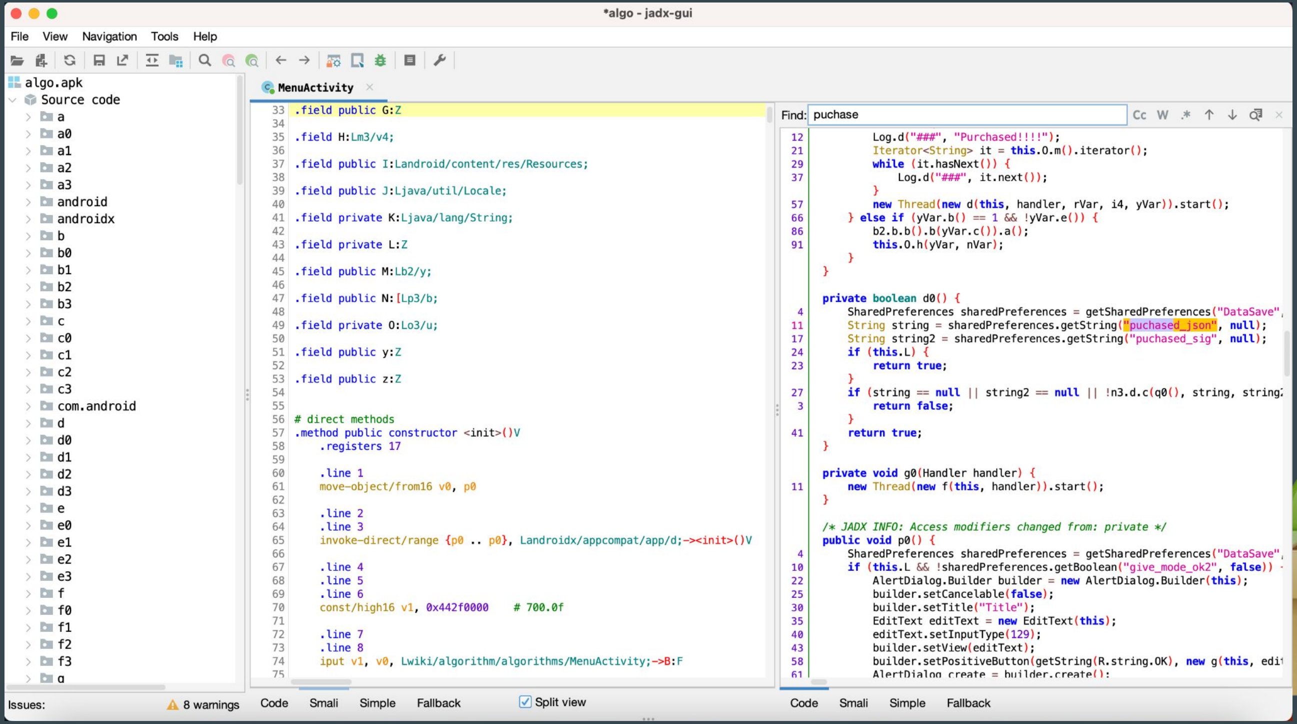


```
    .line 42
    const-string v8, "BubbleSort"

    .line 43
    .line 44
    const-string v9, "1"

    .line 45
    .line 46
    invoke-direct {v6, v8, v9, v7, v7}, Lp3/a;-><init>(Ljava/lang/Str

    .line 47
    .line 48
    .line 49
    aput-object v6, v5, v1

    .line 50
    .line 51
    new-instance v6, Lp3/a;

    .line 52
    .line 53
    sget-object v10, Ljava/lang/Boolean;->TRUE:Ljava/lang/Boolean;

    .line 54
    .line 55
    invoke-direct {v6, v8, v9, v10, v7}, Lp3/a;-><init>(Ljava/lang/St

    .line 56
    .line 57
    .line 58
    const/4 v8, 0x1

    .line 59
    aput-object v6, v5, v8

    .line 60
    .line 61
    new-instance v6, Lp3/a;

    .line 62
    .line 63
    const-string v11, "SelectionSort"
```

```
public void onPause() {
    this.f7322E = true;
    super.onPause();
}

/* JADX INFO: Access modifiers changed from: protected */
@Override // androidx.fragment.app.ActivityC0527d0, android.app.Activity
public void onResume() {
    super.onResume();
    this.f7322E = false;
}

/* renamed from: q0 */
public String m290q0() {
    return m315T("Nruma/4hxpw1AOrrLimyHrJD+RhM9WUYqvyebBsrzRQkTQ6RzpxWg0nfnGgpFV
}

/* renamed from: s0 */
public void m288s0(C0741y c0741y) {
    if (!Security.m1678c(m290q0(), c0741y.m6245a(), c0741y.m6242d())) {
        new AlertDialog.Builder(this).setMessage("Error occurred. Please inform
        return;
    }
    SharedPreferences.Editor edit = getSharedPreferences("DataSave", 0).edit();
    Log.d("###", "unlock process originalJson: " + c0741y.m6245a());
    Log.d("###", "unlock process signatureJson: " + c0741y.m6242d());
    edit.putString("puchased_json", c0741y.m6245a());
    edit.putString("puchased_sig", c0741y.m6242d());
    edit.apply();
    this.f7333y = true;
    FragmentC1619v4 fragmentC1619v4 = this.f7325H;
    if (fragmentC1619v4 != null) {
        fragmentC1619v4.m2676b();
    }
}

/* renamed from: t0 */
public float m287t0() {
    return (this.f7319B - (m314U() * 24.0f)) / 300.0f;
}
```

Code De-Obfuscation

Jadx-gui Integrated de-obfuscation



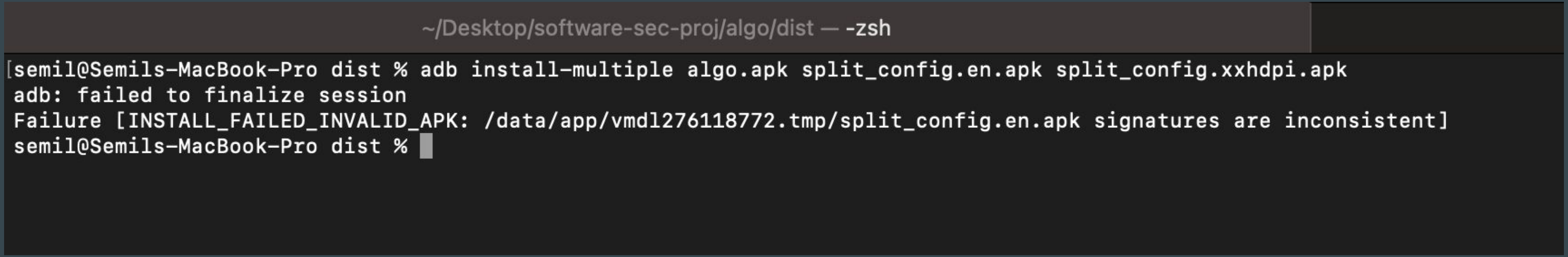
☑ Split view

Find: puchase

```
.field public G:Z

.field H:Lm3/v4;

.field public I:Landroid/content/res/Resources;

.field public J:Ljava/util/Locale;

.field private K:Ljava/lang/String;

.field private L:Z

.field public M:Lb2/y;

.field public N:[Lp3/b;

.field private O:Lo3/u;

.field public y:Z

.field public z:Z


# direct methods
.method public constructor <init>()V
    .registers 17

    .line 1
    move-object/from16 v0, p0

    .line 2
    .line 3
    invoke-direct/range {p0 .. p0}, Landroidx/appcompat/app/d;-><init>()V

    .line 4
    .line 5
    .line 6
    const/high16 v1, 0x442f0000    # 700.0f

    .line 7
    .line 8
    iput v1, v0, Lwiki/algorithm/algorithms/MenuActivity;->B:F
```

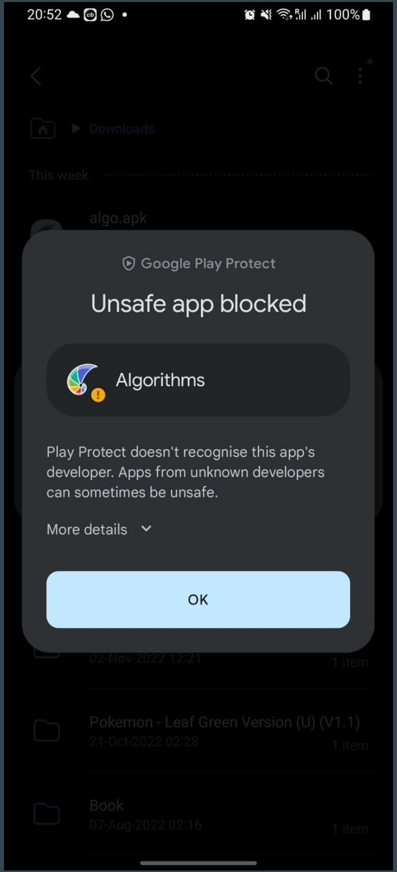
```
            Log.d("###", "Purchased!!!!");
            Iterator<String> it = this.O.m().iterator();
            while (it.hasNext()) {
                Log.d("###", it.next());
            }
            new Thread(new d(this, handler, rVar, i4, yVar)).start();
        } else if (yVar.b() == 1 && !yVar.e()) {
            b2.b.b().b(yVar.c()).a();
            this.O.h(yVar, nVar);
        }
    }

    private boolean d0() {
        SharedPreferences sharedPreferences = getSharedPreferences("DataSave",
        String string = sharedPreferences.getString("puchased_json", null);
        String string2 = sharedPreferences.getString("puchased_sig", null);
        if (this.L) {
            return true;
        }
        if (string == null || string2 == null || !n3.d.c(q0(), string, string2
            return false;
        }
        return true;
    }

    private void g0(Handler handler) {
        new Thread(new f(this, handler)).start();
    }

    /* JADX INFO: Access modifiers changed from: private */
    public void p0() {
        SharedPreferences sharedPreferences = getSharedPreferences("DataSave",
        if (this.L && !sharedPreferences.getBoolean("give_mode_ok2", false)) 
            AlertDialog.Builder builder = new AlertDialog.Builder(this);
            builder.setCancelable(false);
            builder.setTitle("Title");
            EditText editText = new EditText(this);
            editText.setInputType(129);
            builder.setView(editText);
            builder.setPositiveButton(getString(R.string.OK), new g(this, edi
            AlertDialog create = builder.create();
```

APK Signature verification



```
[semil@Semils-MacBook-Pro dist % adb install-multiple algo.apk split_config.en.apk split_config.xxhdpi.apk
 adb: failed to finalize session
 Failure [INSTALL_FAILED_INVALID_APK: /data/app/vmdl276118772.tmp/split_config.en.apk signatures are inconsistent]
 semil@Semils-MacBook-Pro dist % 
```

APK Signature verification



20:52 100%

Downloads

This week

algo.apk

Google Play Protect

Unsafe app blocked

Algorithms

Play Protect doesn't recognise this app's developer. Apps from unknown developers can sometimes be unsafe.

More details

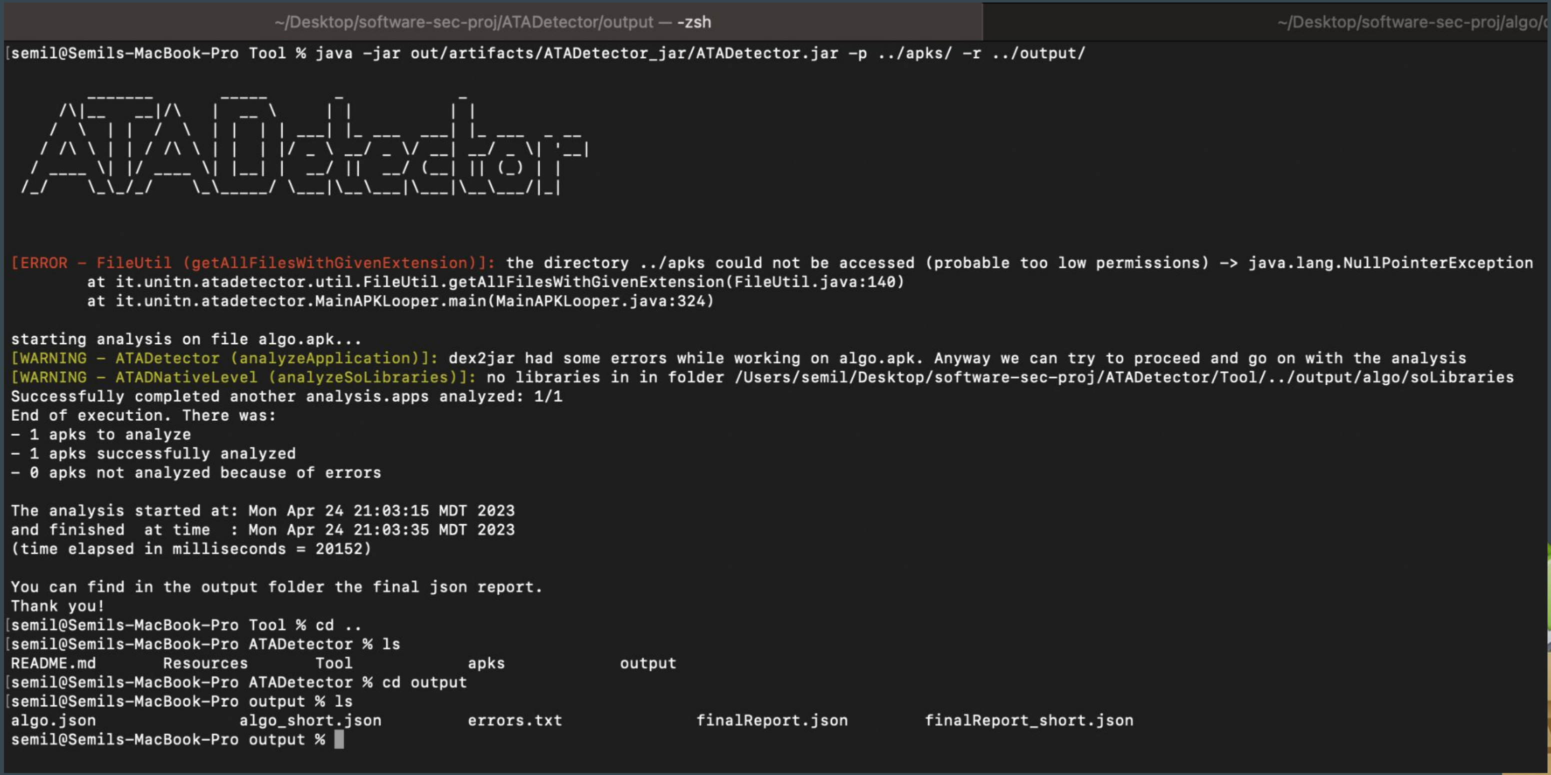
OK

02-Nov-2022 12:21 1 item

Pokemon - Leaf Green Version (U) (V1.1)
21-Oct-2022 02:28 1 item

Book
07-Aug-2022 02:16 1 item

Protection fingerprints

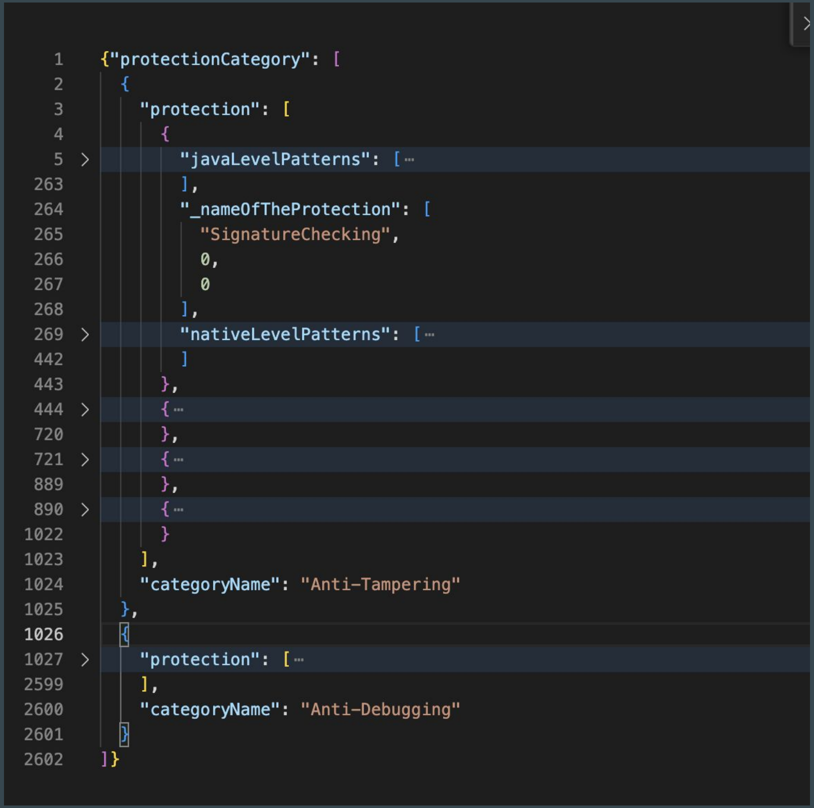


~/Desktop/software-sec-proj/ATADetector/output — -zsh

~/Desktop/software-sec-proj/algo/c

```
[semil@Semils-MacBook-Pro Tool % java -jar out/artifacts/ATADetector_jar/ATADetector.jar -p ../apks/ -r ../output/

          _______      _____       _            _
     /\|__   __|/\   |  __ \     | |          | |
    /  \  | |  /  \  | |  | | ___| |_ ___  ___| |_ ___  _ __
   / /\ \ | | / /\ \ | |  | |/ _ \ __/ _ \/ __| __/ _ \| '__|
  / ____ \| |/ ____ \| |__| |  __/ ||  __/ (__| || (_) | |
 /_/    \_\_/_/    \_\_____/ \___|\__\___|\___|\__\___/|_|



[ERROR - FileUtil (getAllFilesWithGivenExtension)]: the directory ../apks could not be accessed (probable too low permissions) -> java.lang.NullPointerException
        at it.unitn.atadetector.util.FileUtil.getAllFilesWithGivenExtension(FileUtil.java:140)
        at it.unitn.atadetector.MainAPKLooper.main(MainAPKLooper.java:324)

starting analysis on file algo.apk...
[WARNING - ATADetector (analyzeApplication)]: dex2jar had some errors while working on algo.apk. Anyway we can try to proceed and go on with the analysis
[WARNING - ATADNativeLevel (analyzeSoLibraries)]: no libraries in in folder /Users/semil/Desktop/software-sec-proj/ATADetector/Tool/../output/algo/soLibraries
Successfully completed another analysis.apps analyzed: 1/1
End of execution. There was:
- 1 apks to analyze
- 1 apks successfully analyzed
- 0 apks not analyzed because of errors

The analysis started at: Mon Apr 24 21:03:15 MDT 2023
and finished  at time  : Mon Apr 24 21:03:35 MDT 2023
(time elapsed in milliseconds = 20152)

You can find in the output folder the final json report.
Thank you!
[semil@Semils-MacBook-Pro Tool % cd ..
[semil@Semils-MacBook-Pro ATADetector % ls
README.md       Resources       Tool            apks            output
[semil@Semils-MacBook-Pro ATADetector % cd output
[semil@Semils-MacBook-Pro output % ls
algo.json               algo_short.json         errors.txt              finalReport.json        finalReport_short.json
semil@Semils-MacBook-Pro output % █
```

Protection fingerprints



```
{"protectionCategory": [
  {
    "protection": [
      {
        "javaLevelPatterns": […
        ],
        "_nameOfTheProtection": [
          "SignatureChecking",
          0,
          0
        ],
        "nativeLevelPatterns": […
        ]
      },
      {…
      },
      {…
      },
      {…
      }
    ],
    "categoryName": "Anti-Tampering"
  },
  {
    "protection": […
    ],
    "categoryName": "Anti-Debugging"
  }
]}
```

Thank you!!

Any Questions…?