<https://www.honeynet.org/gsoc/ideas>

The Honeynet Project is a leading international 501c3 non-profit security research organization, dedicated to investigating the latest attacks and developing open source security tools to improve Internet security. The Honeynet Project engages broader security community via Google Summer of Code (GSoC) and other efforts to expand security tool development. For organizations interested in continuing their own research about cyber threats, we provide the tools and techniques we have developed. Recent tools examples include Cuckoo, Capture-HPC, Glastopf, HoneyC, Honeyd, Honeywall.

Ref : <https://source.android.com/devices/tech/dalvik/>

Android runtime (ART) is the managed runtime used by applications and some system services on Android. ART and its predecessor Dalvik were originally created specifically for the Android project. ART as the runtime executes the Dalvik Executable format and Dex bytecode specification.

ART and Dalvik are compatible runtimes running Dex bytecode, so apps developed for Dalvik should work when running with ART. However, some techniques that work on Dalvik do not work on ART. For information about the most important issues, see [Verifying App Behavior on the Android Runtime (ART)](http://developer.android.com/guide/practices/verifying-apps-art.html).

check ART Compatibility :

ref: <http://developer.android.com/guide/practices/verifying-apps-art.html>

With Android 4.4, we are beginning to roll out a new Android runtime, **ART**. This runtime offers a number of new features that improve performance and smoothness of the Android platform and apps. (You can find more information about ART's new features in [Introducing ART](http://source.android.com/devices/tech/dalvik/art.html).)

Currently, ART is available on a number of Android 4.4 devices, such as the Nexus 4, Nexus 5, Nexus 7, and Google Play edition devices. At this time, all devices still use Dalvik as the default runtime. We encourage you to test your apps for ART compatibility and to take advantage of ART's new features. However, for the time being, you should also take care to maintain compatibility with Dalvik.

This document lets you know about things to watch for when migrating an existing app to be compatible with ART. Most apps should just work when running with ART. However, some techniques that work on Dalvik do not work on ART. This document discusses some of these issues.

[**DroidBox**](http://code.google.com/p/droidbox/), authored by Patrick Lantz, is a sandbox for the Android platform. "It focuses on detecting information leaks that were derived from performing taint analysis for information-flow tracking on Android trojan applications. DroidBox is capable to identify information leaks of contacts, SMS data, IMEI, GPS coordinates, installed apps, phone numbers, network traffic and file operations."

*DroidBox* is very easy to use and consists of an own system image and kernel meant to log one applications activities. Using adb logcat *DroidBox* will look for certain debug messages and collect anything related to the monitored app. However I must say that logged data isn't always complete. Sometimes you'll get only a *striped* version of the data which caused the activity. In that case it's almost impossible e.g. to have a deep look at the network traffic (especially HTTP). You won't be able to construct a full request-response-sequence due to missing data. Nevertheless you can use DroidBox to get an overview of malicious activities triggered by the app. For a more technical analysis of the data you'll need additional tools (more to come in future posts).

Ref : <http://blog.dornea.nu/2014/08/05/android-dynamic-code-analysis-mastering-droidbox/>

### **Requirements for DroidBox**

First you'll have to install some requirements DroidBox needs. First make sure you have the system relevant packages installed:

root@kali:~*# apt-get install python-virtualenv libatlas-dev liblapack-dev libblas-dev*

You'll need those in order to use scipy, matplotlib and numpy along with Droidbox. Now create a virtual environment and install *python* dependencies:

root@kali:~/work/apk*# mkdir env*  
root@kali:~/work/apk*# virtualenv env*  
...  
root@kali:~/work/apk*# source env/bin/activate*  
(env)root@kali:~/work/apk*# pip install numpy scipy matplotlib*

### **Install Droidbox**

Download the package:

(env)root@kali:~/work/apk*# wget https://droidbox.googlecode.com/files/DroidBox411RC.tar.gz*

Literature analysis:

<http://cs.ucsb.edu/~iland/AndroidMalwareDetection.pdf>

### Android Versions and API

The code names match the following version numbers, along with API levels and NDK releases provided for convenience:

| Code name | Version | API level |
| --- | --- | --- |
| Marshmallow | 6.0 | API level 23 |
| Lollipop | 5.1 | API level 22 |
| Lollipop | 5.0 | API level 21 |
| KitKat | 4.4 - 4.4.4 | API level 19 |
| Jelly Bean | 4.3.x | API level 18 |
| Jelly Bean | 4.2.x | API level 17 |
| Jelly Bean | 4.1.x | API level 16 |
| Ice Cream Sandwich | 4.0.3 - 4.0.4 | API level 15, NDK 8 |
| Ice Cream Sandwich | 4.0.1 - 4.0.2 | API level 14, NDK 7 |
| Honeycomb | 3.2.x | API level 13 |
| Honeycomb | 3.1 | API level 12, NDK 6 |
| Honeycomb | 3.0 | API level 11 |
| Gingerbread | 2.3.3 - 2.3.7 | API level 10 |
| Gingerbread | 2.3 - 2.3.2 | API level 9, NDK 5 |
| Froyo | 2.2.x | API level 8, NDK 4 |
| Eclair | 2.1 | API level 7, NDK 3 |
| Eclair | 2.0.1 | API level 6 |
| Eclair | 2.0 | API level 5 |
| Donut | 1.6 | API level 4, NDK 2 |
| Cupcake | 1.5 | API level 3, NDK 1 |
| (no code name) | 1.1 | API level 2 |
| (no code name) | 1.0 | API level 1 |

## **Source Code Tags and Builds**

Starting with Donut, the exact list of tags and builds is in the following table. Factory images and binaries for Nexus devices can be downloaded from:

<https://developers.google.com/android/nexus/images>

<https://developers.google.com/android/nexus/drivers>

| Build | Branch | Version | Supported devices |
| --- | --- | --- | --- |
| M5C14J | android-6.0.1\_r31 | Marshmallow | Pixel C |
| MOB30D | android-6.0.1\_r30 | Marshmallow | Nexus 5, Nexus 6, Nexus 7 (flo/deb), Nexus 9 (volantis/volantisg), Nexus Player, and Android One |
| MHC19Q | android-6.0.1\_r24 | Marshmallow | Nexus 5X, Nexus 6P |
| MHC19J | android-6.0.1\_r22 | Marshmallow | Nexus 5X |
| MHC19I | android-6.0.1\_r21 | Marshmallow | Nexus 6P |
| MMB29X | android-6.0.1\_r20 | Marshmallow | Nexus 5, Nexus 6, Nexus 7 (deb), Nexus 9 (volantisg) |
| MXC14G | android-6.0.1\_r18 | Marshmallow | Pixel C |
| MMB29V | android-6.0.1\_r17 | Marshmallow | Nexus 5, Nexus 5X, Nexus 6, Nexus 6P, Nexus 7 (flo/deb), Nexus 9 (volantis/volantisg) |
| MXB48T | android-6.0.1\_r16 | Marshmallow | Pixel C |
| MMB29U | android-6.0.1\_r13 | Marshmallow | Nexus Player |
| MMB29R | android-6.0.1\_r12 | Marshmallow | Nexus 9 (volantis/volantisg) |
| MMB29Q | android-6.0.1\_r11 | Marshmallow | Nexus 5, Nexus 5X, Nexus 6, Nexus 6P, Nexus 7 (flo/deb) |
| MMB29T | android-6.0.1\_r10 | Marshmallow | Nexus Player |
| MMB29S | android-6.0.1\_r9 | Marshmallow | Nexus 5, Nexus 6, Nexus 9 (volantis/volantisg) |
| MMB29P | android-6.0.1\_r8 | Marshmallow | Nexus 5X, Nexus 6P |
| MMB29O | android-6.0.1\_r7 | Marshmallow | Nexus 7 (flo/deb) |
| MXB48K | android-6.0.1\_r5 | Marshmallow | Pixel C |
| MXB48J | android-6.0.1\_r4 | Marshmallow | Pixel C |
| MMB29M | android-6.0.1\_r3 | Marshmallow | Nexus 6P, Nexus Player |
| MMB29K | android-6.0.1\_r1 | Marshmallow | Nexus 5, Nexus 5X, Nexus 6, Nexus 7 (flo/deb), Nexus 9 (volantis/volantisg) |
| MMB29N | android-6.0.0\_r41 | Marshmallow | Nexus 6P |
| MDB08M | android-6.0.0\_r26 | Marshmallow | Nexus 5X, Nexus 6P |
| MDB08L | android-6.0.0\_r25 | Marshmallow | Nexus 5X, Nexus 6P |
| MDB08K | android-6.0.0\_r24 | Marshmallow | Nexus 6P |
| MDB08I | android-6.0.0\_r23 | Marshmallow | Nexus 5X |
| MDA89E | android-6.0.0\_r12 | Marshmallow | Nexus 5X |
| MDA89D | android-6.0.0\_r11 | Marshmallow | Nexus 6P |
| MRA59B | android-6.0.0\_r7 | Marshmallow | Nexus 7 (deb) |
| MRA58X | android-6.0.0\_r6 | Marshmallow | Nexus 6 |
| MRA58V | android-6.0.0\_r5 | Marshmallow | Nexus 7 (flo/deb) |
| MRA58U | android-6.0.0\_r4 | Marshmallow | Nexus 7 (flo) |
| MRA58N | android-6.0.0\_r2 | Marshmallow | Nexus 5, Nexus 6, Nexus 7 (flo/deb), Nexus 9 (volantis/volantisg), Nexus Player |
| MRA58K | android-6.0.0\_r1 | Marshmallow | Nexus 5, Nexus 6, Nexus 7 (flo/deb), Nexus 9 (volantis/volantisg), Nexus Player |
| LMY49J | android-5.1.1\_r37 | Lollipop | Nexus 10 |
| LMY49I | android-5.1.1\_r36 | Lollipop | Nexus 10 |
| LMY49H | android-5.1.1\_r35 | Lollipop | Nexus 10 |
| LMY49G | android-5.1.1\_r34 | Lollipop | Nexus 10 |
| LMY49F | android-5.1.1\_r33 | Lollipop | Nexus 9 (volantisg), Nexus 10 |
| LMY48Z | android-5.1.1\_r30 | Lollipop | Nexus 6, Nexus 7 (deb), Nexus 9 (volantisg), Nexus 10 |
| LYZ28N | android-5.1.1\_r28 | Lollipop | Nexus 6 (For T-Mobile ONLY) |
| LMY48Y | android-5.1.1\_r26 | Lollipop | Nexus 6 |
| LMY48X | android-5.1.1\_r25 | Lollipop | Nexus 6, Nexus 7 (deb), Nexus 9 (volantisg), Nexus 10 |
| LMY48W | android-5.1.1\_r24 | Lollipop | Nexus 6 |
| LVY48H | android-5.1.1\_r23 | Lollipop | Nexus 6 (For Project Fi ONLY) |
| LYZ28M | android-5.1.1\_r22 | Lollipop | Nexus 6 (For T-Mobile ONLY) |
| LMY48U | android-5.1.1\_r20 | Lollipop | Nexus 7 (deb) |
| LMY48T | android-5.1.1\_r19 | Lollipop | Nexus 4, Nexus 6, Nexus 9 (volantis/volantisg), Nexus 10 |
| LVY48F | android-5.1.1\_r18 | Lollipop | Nexus 6 (For Project Fi ONLY) |
| LYZ28K | android-5.1.1\_r17 | Lollipop | Nexus 6 (For T-Mobile ONLY) |
| LMY48P | android-5.1.1\_r16 | Lollipop | Nexus 7 (deb) |
| LMY48N | android-5.1.1\_r15 | Lollipop | Nexus Player |
| LMY48M | android-5.1.1\_r14 | Lollipop | Nexus 4, Nexus 5, Nexus 6, Nexus 7 (flo), Nexus 9 (volantis/volantisg), Nexus 10 |
| LVY48E | android-5.1.1\_r13 | Lollipop | Nexus 6 (For Project Fi ONLY) |
| LYZ28J | android-5.1.1\_r12 | Lollipop | Nexus 6 (For T-Mobile ONLY) |
| LMY48J | android-5.1.1\_r10 | Lollipop | Nexus Player |
| LMY48I | android-5.1.1\_r9 | Lollipop | Nexus 4, Nexus 5, Nexus 6, Nexus 7 (flo), Nexus 9 (volantis/volantisg), Nexus 10 |
| LVY48C | android-5.1.1\_r8 | Lollipop | Nexus 6 (For Project Fi ONLY) |
| LMY48G | android-5.1.1\_r6 | Lollipop | Nexus 7 (flo) |
| LYZ28E | android-5.1.1\_r5 | Lollipop | Nexus 6 (For T-Mobile ONLY) |
| LMY47Z | android-5.1.1\_r4 | Lollipop | Nexus 6 (All carriers except T-Mobile US) |
| LMY48B | android-5.1.1\_r3 | Lollipop | Nexus 5 |
| LMY47X | android-5.1.1\_r2 | Lollipop | Nexus 9 (volantis) |
| LMY47V | android-5.1.1\_r1 | Lollipop | Nexus 7 (flo/grouper), Nexus 10, Nexus Player |
| LMY47O | android-5.1.0\_r5 | Lollipop | Nexus 4, Nexus 7 (flo/deb) |
| LMY47M | android-5.1.0\_r4 | Lollipop | Nexus 6 (For T-Mobile ONLY) |
| LMY47I | android-5.1.0\_r3 | Lollipop | Nexus 5, Nexus 6 |
| LMY47E | android-5.1.0\_r2 | Lollipop | Nexus 6 |
| LMY47D | android-5.1.0\_r1 | Lollipop | Nexus 5, Nexus 6, Nexus 7 (grouper/tilapia), Nexus 10, Nexus Player |
| LRX22L | android-5.0.2\_r3 | Lollipop | Nexus 9 (volantis/volantisg) |
| LRX22G | android-5.0.2\_r1 | Lollipop | Nexus 7 (flo/deb/grouper/tilapia), Nexus 10 |
| LRX22C | android-5.0.1\_r1 | Lollipop | Nexus 4, Nexus 5, Nexus 6 (shamu), Nexus 7 (flo), Nexus 9 (volantis/volantisg), Nexus 10 |
| LRX21V | android-5.0.0\_r7.0.1 | Lollipop | Nexus Player (fugu) |
| LRX21T | android-5.0.0\_r6.0.1 | Lollipop | Nexus 4 |
| LRX21R | android-5.0.0\_r5.1.0.1 | Lollipop | Nexus 9 (volantis) |
| LRX21Q | android-5.0.0\_r5.0.1 | Lollipop | Nexus 9 (volantis) |
| LRX21P | android-5.0.0\_r4.0.1 | Lollipop | Nexus 7 (flo/grouper), Nexus 10 |
| LRX21O | android-5.0.0\_r3.0.1 | Lollipop | Nexus 5 (hammerhead), Nexus 6 (shamu) |
| LRX21M | android-5.0.0\_r2.0.1 | Lollipop | Nexus Player (fugu) |
| LRX21L | android-5.0.0\_r1.0.1 | Lollipop | Nexus 9 (volantis) |
| KTU84Q | android-4.4.4\_r2 | KitKat | Nexus 5 (hammerhead) (For 2Degrees/NZ, Telstra/AUS and India ONLY) |
| KTU84P | android-4.4.4\_r1 | KitKat | Nexus 5, Nexus 7 (flo/deb/grouper/tilapia), Nexus 4, Nexus 10 |
| KTU84M | android-4.4.3\_r1.1 | KitKat | Nexus 5 (hammerhead) |
| KTU84L | android-4.4.3\_r1 | KitKat | Nexus 7 (flo/deb/grouper/tilapia), Nexus 4, Nexus 10 |
| KVT49L | android-4.4.2\_r2 | KitKat | Nexus 7 (deb Verizon) |
| KOT49H | android-4.4.2\_r1 | KitKat | Nexus 5, Nexus 7 (flo/deb/grouper/tilapia), Nexus 4, Nexus 10 |
| KOT49E | android-4.4.1\_r1 | KitKat | Nexus 5, Nexus 7 (flo/deb/grouper/tilapia), Nexus 4, Nexus 10 |
| KRT16S | android-4.4\_r1.2 | KitKat | Nexus 7 (flo/deb/grouper/tilapia), Nexus 4, Nexus 10 |
| KRT16M | android-4.4\_r1 | KitKat | Nexus 5 (hammerhead) |
| JLS36I | android-4.3.1\_r1 | Jelly Bean | Nexus 7 (deb) |
| JLS36C | android-4.3\_r3 | Jelly Bean | Nexus 7 (deb) |
| JSS15R | android-4.3\_r2.3 | Jelly Bean | Nexus 7 (flo) |
| JSS15Q | android-4.3\_r2.2 | Jelly Bean | Nexus 7 (flo) |
| JSS15J | android-4.3\_r2.1 | Jelly Bean | Nexus 7 (flo/deb) |
| JSR78D | android-4.3\_r2 | Jelly Bean | Nexus 7 (deb) |
| JWR66Y | android-4.3\_r1.1 | Jelly Bean | Galaxy Nexus, Nexus 7 (grouper/tilapia), Nexus 4, Nexus 10 |
| JWR66V | android-4.3\_r1 | Jelly Bean | Galaxy Nexus, Nexus 7 (grouper/tilapia), Nexus 4, Nexus 10 |
| JWR66N | android-4.3\_r0.9.1 | Jelly Bean | Galaxy Nexus, Nexus 7 (grouper/tilapia/flo), Nexus 4, Nexus 10 |
| JWR66L | android-4.3\_r0.9 | Jelly Bean | Nexus 7 |
| JDQ39E | android-4.2.2\_r1.2 | Jelly Bean | Nexus 4 |
| JDQ39B | android-4.2.2\_r1.1 | Jelly Bean | Nexus 7 |
| JDQ39 | android-4.2.2\_r1 | Jelly Bean | Galaxy Nexus, Nexus 7, Nexus 4, Nexus 10 |
| JOP40G | android-4.2.1\_r1.2 | Jelly Bean | Nexus 4 |
| JOP40F | android-4.2.1\_r1.1 | Jelly Bean | Nexus 10 |
| JOP40D | android-4.2.1\_r1 | Jelly Bean | Galaxy Nexus, Nexus 7, Nexus 4, Nexus 10 |
| JOP40C | android-4.2\_r1 | Jelly Bean | Galaxy Nexus, Nexus 7, Nexus 4, Nexus 10 |
| JZO54M | android-4.1.2\_r2.1 | Jelly Bean |  |
| JZO54L | android-4.1.2\_r2 | Jelly Bean |  |
| JZO54K | android-4.1.2\_r1 | Jelly Bean | Nexus S, Galaxy Nexus, Nexus 7 |
| JRO03S | android-4.1.1\_r6.1 | Jelly Bean | Nexus 7 |
| JRO03R | android-4.1.1\_r6 | Jelly Bean | Nexus S 4G |
| JRO03O | android-4.1.1\_r5 | Jelly Bean | Galaxy Nexus |
| JRO03L | android-4.1.1\_r4 | Jelly Bean | Nexus S |
| JRO03H | android-4.1.1\_r3 | Jelly Bean |  |
| JRO03E | android-4.1.1\_r2 | Jelly Bean | Nexus S |
| JRO03D | android-4.1.1\_r1.1 | Jelly Bean | Nexus 7 |
| JRO03C | android-4.1.1\_r1 | Jelly Bean | Galaxy Nexus |
| IMM76L | android-4.0.4\_r2.1 | Ice Cream Sandwich |  |
| IMM76K | android-4.0.4\_r2 | Ice Cream Sandwich | Galaxy Nexus |
| IMM76I | android-4.0.4\_r1.2 | Ice Cream Sandwich | Galaxy Nexus |
| IMM76D | android-4.0.4\_r1.1 | Ice Cream Sandwich | Nexus S, Nexus S 4G, Galaxy Nexus |
| IMM76 | android-4.0.4\_r1 | Ice Cream Sandwich |  |
| IML77 | android-4.0.3\_r1.1 | Ice Cream Sandwich |  |
| IML74K | android-4.0.3\_r1 | Ice Cream Sandwich | Nexus S |
| ICL53F | android-4.0.2\_r1 | Ice Cream Sandwich | Galaxy Nexus |
| ITL41F | android-4.0.1\_r1.2 | Ice Cream Sandwich | Galaxy Nexus |
| ITL41D | android-4.0.1\_r1.1 | Ice Cream Sandwich | Galaxy Nexus |
| ITL41D | android-4.0.1\_r1 | Ice Cream Sandwich | Galaxy Nexus |
| GWK74 | android-2.3.7\_r1 | Gingerbread | Nexus S 4G |
| GRK39F | android-2.3.6\_r1 | Gingerbread | Nexus One, Nexus S |
| GRK39C | android-2.3.6\_r0.9 | Gingerbread | Nexus S |
| GRJ90 | android-2.3.5\_r1 | Gingerbread | Nexus S 4G |
| GRJ22 | android-2.3.4\_r1 | Gingerbread | Nexus One, Nexus S, Nexus S 4G |
| GRJ06D | android-2.3.4\_r0.9 | Gingerbread | Nexus S 4G |
| GRI54 | android-2.3.3\_r1.1 | Gingerbread | Nexus S |
| GRI40 | android-2.3.3\_r1 | Gingerbread | Nexus One, Nexus S |
| GRH78C | android-2.3.2\_r1 | Gingerbread | Nexus S |
| GRH78 | android-2.3.1\_r1 | Gingerbread | Nexus S |
| GRH55 | android-2.3\_r1 | Gingerbread | earliest Gingerbread version, Nexus S |
| FRK76C | android-2.2.3\_r2 | Froyo |  |
| FRK76 | android-2.2.3\_r1 | Froyo |  |
| FRG83G | android-2.2.2\_r1 | Froyo | Nexus One |
| FRG83D | android-2.2.1\_r2 | Froyo | Nexus One |
| FRG83 | android-2.2.1\_r1 | Froyo | Nexus One |
| FRG22D | android-2.2\_r1.3 | Froyo |  |
| FRG01B | android-2.2\_r1.2 | Froyo |  |
| FRF91 | android-2.2\_r1.1 | Froyo | Nexus One |
| FRF85B | android-2.2\_r1 | Froyo | Nexus One |
| EPF21B | android-2.1\_r2.1p2 | Eclair |  |
| ESE81 | android-2.1\_r2.1s | Eclair |  |
| EPE54B | android-2.1\_r2.1p | Eclair | Nexus One |
| ERE27 | android-2.1\_r2 | Eclair | Nexus One |
| ERD79 | android-2.1\_r1 | Eclair | Nexus One |
| ESD56 | android-2.0.1\_r1 | Eclair |  |
| ESD20 | android-2.0\_r1 | Eclair |  |
| DMD64 | android-1.6\_r1.5 | Donut |  |
| DRD20 | android-1.6\_r1.4 |  |  |
| DRD08 | android-1.6\_r1.3 |  |  |
| DRC92 | android-1.6\_r1.2 |  |  |