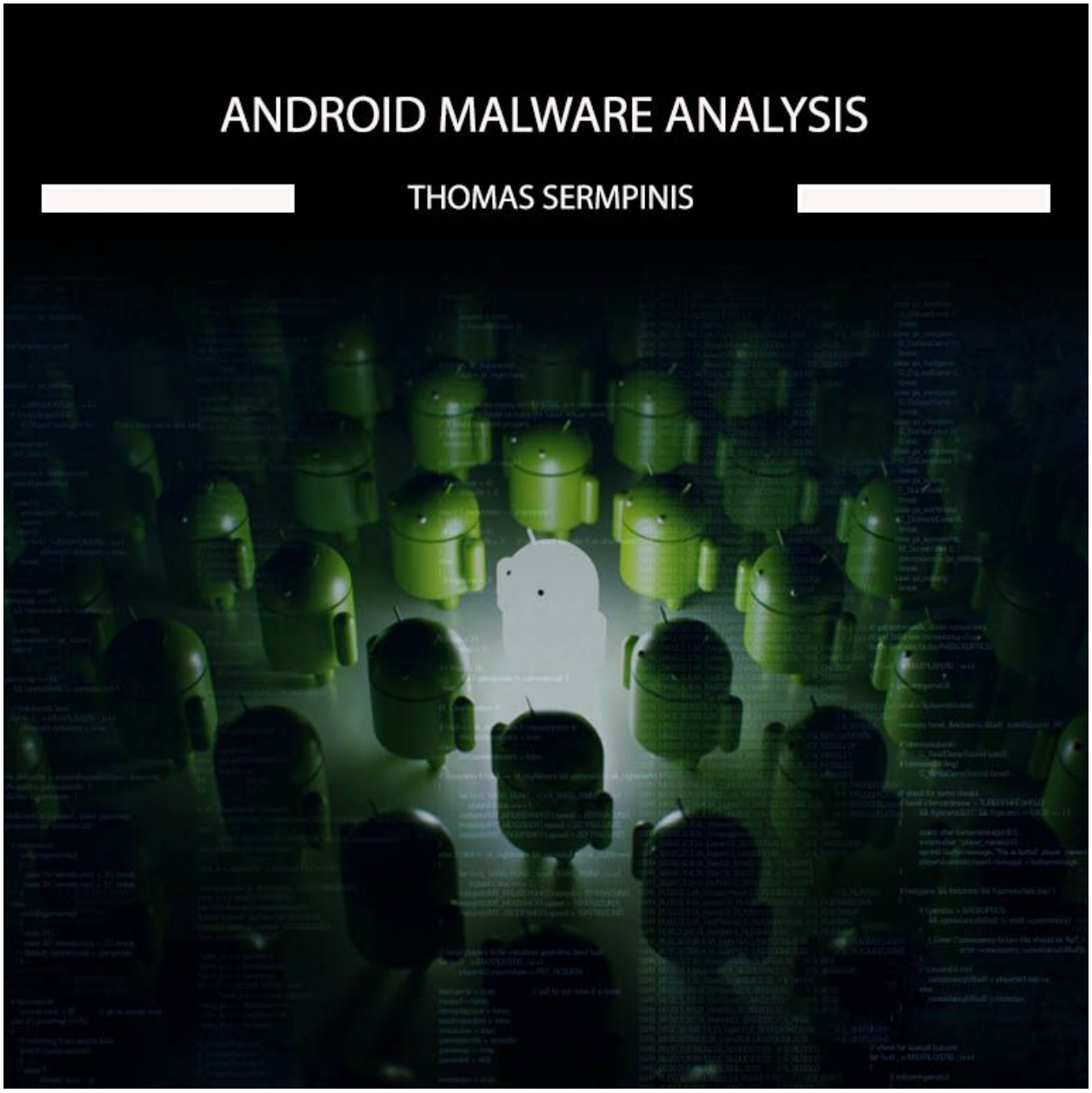


Online course setup material

eForensics Magazine

In this section, we are going to see some basic steps that will prepare your lab environment for the course "Android Malware Analysis". We will basically see where we can find the tools that we will need and how we can install them in our system.

Java Installation

Android applications are based in Java, so if we use the SDK on a terminal, we will need Java installed in our system, and especially the Java Development Kit. We can find it and download it from here:

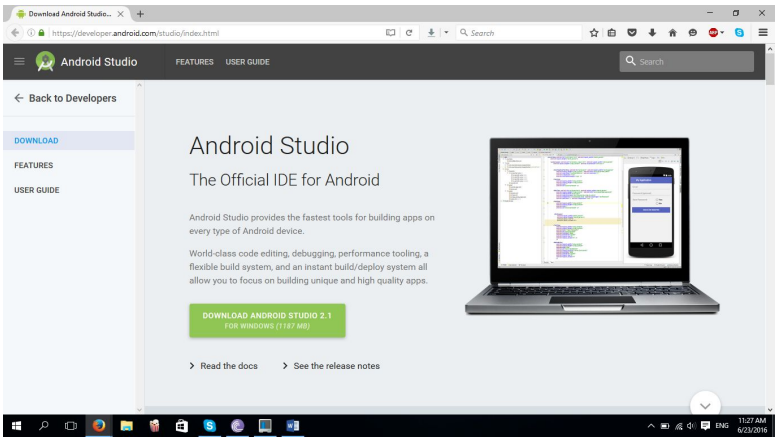
ttp://www.oracle.com/technetwork/java/javase/downloads/index.html

Currently, the JDK is in the 8th version, and the installation is as easy as it gets with no weird things. Just hit next and you will be ready. The installation is the same for Windows and MacOS.

Android Studio

The next tool that we will need is Android Studio, which is in version 2.1 and we can easily download the executable installation file from Google's website here:

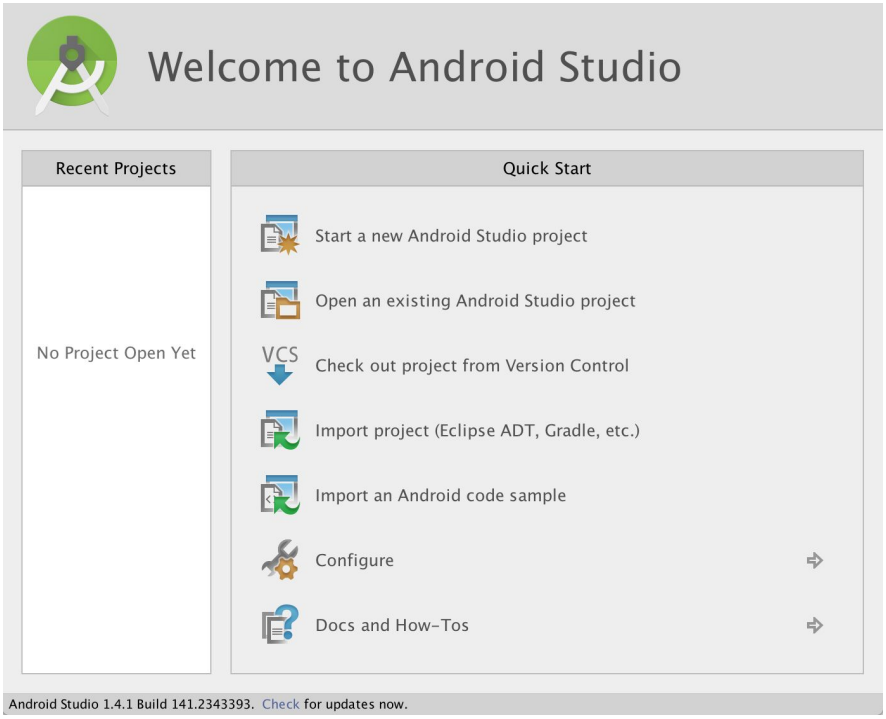
https://developer.android.com/studio/index.html



Google constantly updates this page, so the version you see may very well be newer than the screenshot above. Once you click the button, you'll see a request to agree to the terms and conditions. Accept and click the blue button underneath titled Download Android Studio. Once the download is complete, we can install Android Studio similarly to how we installed Java or any other program. The download page will redirect to a page that contains installation instructions for OS X, Windows and Linux Operating Systems.

Once installation wraps itself up, we go ahead and launch Android Studio. The setup wizard will greet us, as it is the first time it loads, where we click Next to move to the Install Type screen. We now select the standard option and click next. This whole process will probably take several minutes. On the Verify Settings window, you will have an opportunity to confirm your setup. Click Finish to start downloading the SDK components. Once everything downloads, click Finish.

After a few minutes, we will see the welcome screen, which serves as our gateway to building all things Android.



Even though we just downloaded, it is possible that a new version is available so make a quick check for updates by clicking check for updates at the bottom of the welcome screen. If an update is available, a window will appear where we select Update Now and let it do its thing.

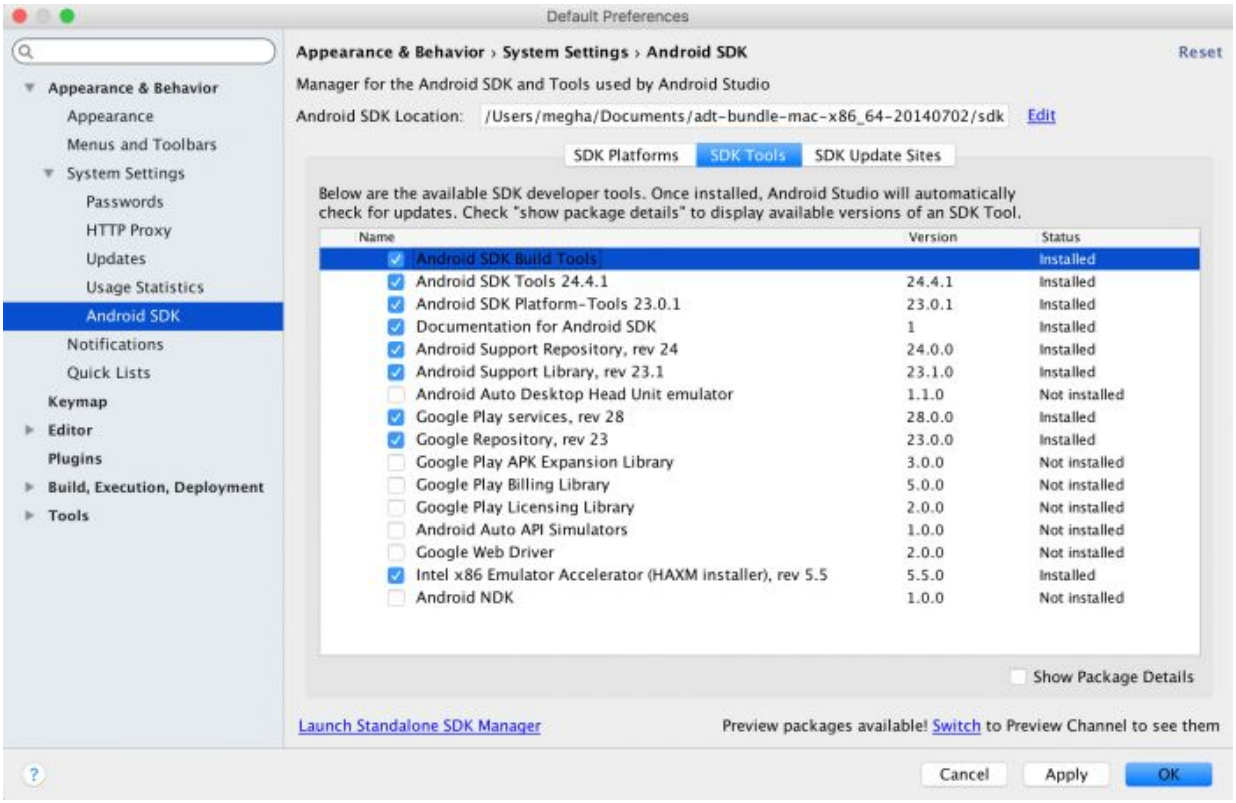
Now, our installation of Android Studio is complete, so let's continue.

Android SDK

Each version of Android has its own SDK (Software Development Kit) that enables us to create applications for the Android platform. With the Android Studio installation, we have already installed the Android SDK. However, it's useful to know how to install additional versions of the SDK so that we can develop for all supported versions of Android. To make additional installations in the SDK, from the Android Studio welcome screen, we click Configure. From the new menu we select the SDK Manager option.

The first tab of this window, SDK Platforms, lists the Android SDK platform(s) available for download. We enable the Show Package Details option to see individual SDK components, such as the platform itself and the sources pertaining to the API level, like system image. Take note of the checkbox next to the SDK platform; it will be pre-selected if an update is available.

By default, the SDK Manager installs the latest packages and tools. If we wish to install other SDKs, we just select them for installation.



VirtualBox

Many tools for Android Application Analysis are written for the Linux platform, and to make the use of a Linux OS pain-free, we suggest you install it as a virtual machine in VirtualBox, which is free, or VMware. Of course, you can install Linux on your system or boot from a bootable CD or USB, but we think that the best way is to install it in a virtual machine.

The installation is, once again, pretty straight forward. We download the executable installation file from here https://www.virtualbox.org/wiki/Downloads, and we continue with the installation, as with every program.

Now that we have the virtualization program installed, we select the Linux distribution we want to use. If you do not know any, download Ubuntu from here http://www.ubuntu.com/download/desktop which is one of the most famous distributions.

Now we open VirtualBox and select new from the top left corner. A new menu opens where we start to build our virtual machine. In the next window we enter the name of the VM. If the name entered matches the OS, like we did above, the "OS Type" should automatically select the right parameters. If the "OS Type" is not correct, we fix it and click continue.

We now select the amount of RAM for the VM. We can change this setting later. Keep in mind that while the VM is running, it will consume all of the RAM you specify here, and it will not be available to the host OS. We continue and select "Create a new hard disk". Now we choose "VDI" for the type of disk image we want to create and continue again.

We continue by selecting the maximum size of the virtual disk (>4gb). We cannot easily modify this setting later, so adjust accordingly. We should now be at the "Summary" screen for the virtual disk image now. We click "Create".

Now that we have a suitable disk image, another "Summary" screen will appear for the virtual machine. We click "Create" again and our virtual machine is ready for use. To boot it we click on our virtual machine in the left column of the VirtualBox Manager, and select "Start." We should be greeted with the "First Run Wizard" where we click continue.

Linux Tools Installation

In this course, we will use many Linux tools, as we said. The installation idea is the same for most of the tools, so if during the course you see a new tool, I will give you the command line(s) that you have to execute in the terminal to install the tool, and you will be OK.