

Tutorial: Practical Program Analysis for Discovering Android Malware

Module 0: Laboratory Setup

Suresh Kothari – kothari@iastate.edu

Benjamin Holland – bholland@iastate.edu

Acknowledgment: co-workers and students

DARPA contracts FA8750-12-2-0126 & FA8750-15-2-0080



IOWA STATE
UNIVERSITY

Notice

Learning this material is like learning to swim. The best way to learn is to jump in and try it yourself. There will be breakout sessions for you to practice material with your peers.

We highly encourage to you complete the Module 0 Prelab Setup in the following slides before coming to the tutorial!

That being said the solutions to hands on material will be demonstrated at the end of each break out session so if your goal is to learn the theory and you just want to watch, that is fine too.

Material Updates/Errata Notice

- Updated versions of these slides, code, and other materials are available at: <https://github.com/benjholla/MILCOM2015>

Prelab

- To setup your machine for lab exercises, please complete the Module 0 prelab steps before arriving at the tutorial
- Optionally, a preconfigured virtual machine will be provided at the beginning of the tutorial session
- Please contact bholland@iastate.edu with setup questions
- Stop at Module 1
- Requirement:
 - Access to a machine with ≥ 4 GB of RAM, 8 recommended!

Download Eclipse

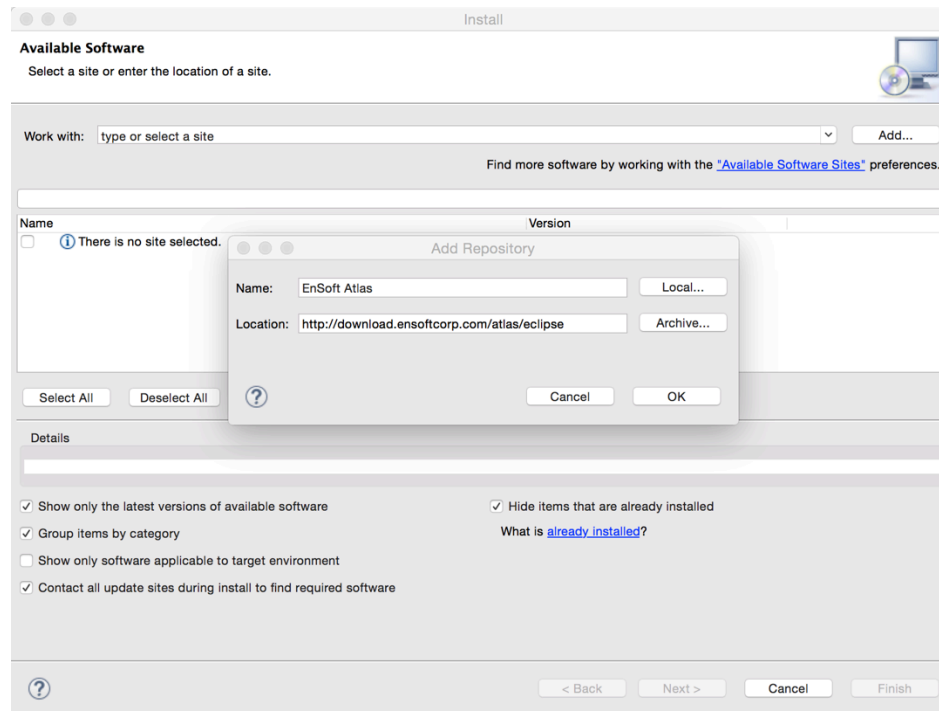
- Download Eclipse Luna for Mac, Windows, or Linux
 - Download the “Eclipse IDE for Java Developers” package
 - <https://www.eclipse.org/downloads/packages/release/Luna/SR2>
- Create a directory called “MILCOM2015”
- Extract the “eclipse” folder of the Eclipse download to “MILCOM2015”
- Inside “MILCOM2015” create a folder called “workspace” and a folder called “git”.

Launch Eclipse

- Inside the “MILCOM2015/eclipse” folder double click the Eclipse binary to launch Eclipse.
- When Eclipse launches, press the “Browse...” button and navigate to the “MILCOM2015/workspace” folder. Press “OK” to launch Eclipse with the selected workspace.

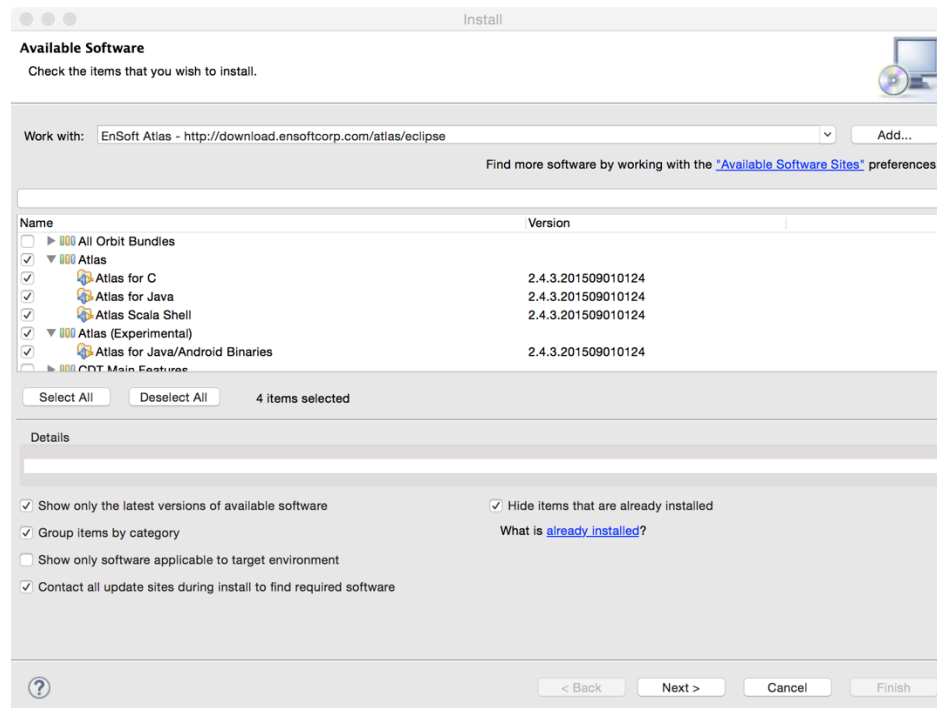
Install Atlas Professional

- Within Eclipse, navigate to Help → Install New Software...
- Press “Add...” and enter “EnSoft Atlas” in the “Name” field and <http://download.ensoftcorp.com/atlas/eclipse> in the “Location” field.



Install Atlas Professional

- Select the “Atlas” **AND** “Atlas (Experimental)” features.
- Press “Next”, accept the license agreement, and press “OK” to install unsigned content. Restart Eclipse.

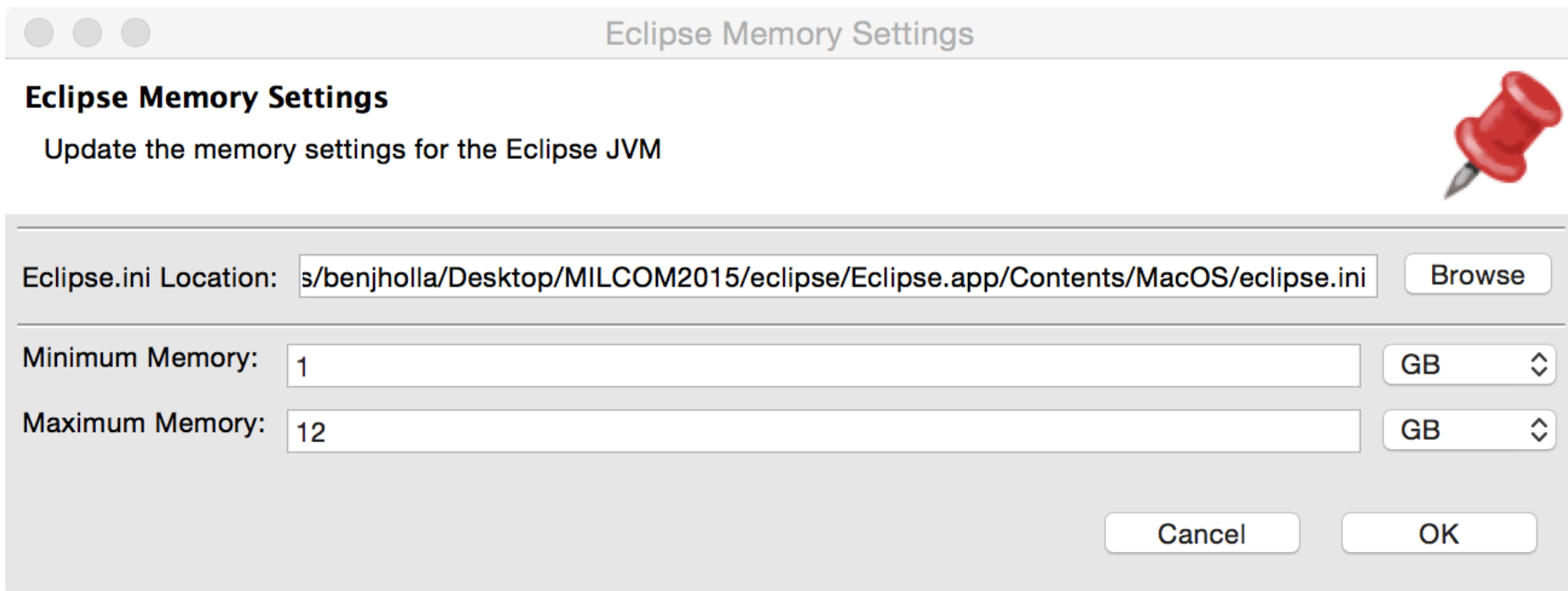


Enter Atlas License Key

- In Eclipse, navigate to Eclipse/Window → Preferences → Atlas → License and enter your License key and License email, which can be obtained through one of the following methods:
 - An Atlas License for the MILCOM2015 Practical Program Analysis for Discovering Android Malware Tutorial will be provided during the tutorial.
 - For Academics, a complimentary 1 year license is available at: <http://www.ensoftcorp.com/atlas/academic-license/>
 - A 1 month trial license at: <http://www.ensoftcorp.com/atlas/trial/>

Configure Memory Settings

- Inside Eclipse, navigate to Atlas → Eclipse Memory Settings
- Enter a minimum of 1GB and a maximum of ≥ 6 GB
- Press OK and then restart Eclipse



Eclipse Memory Settings
Update the memory settings for the Eclipse JVM

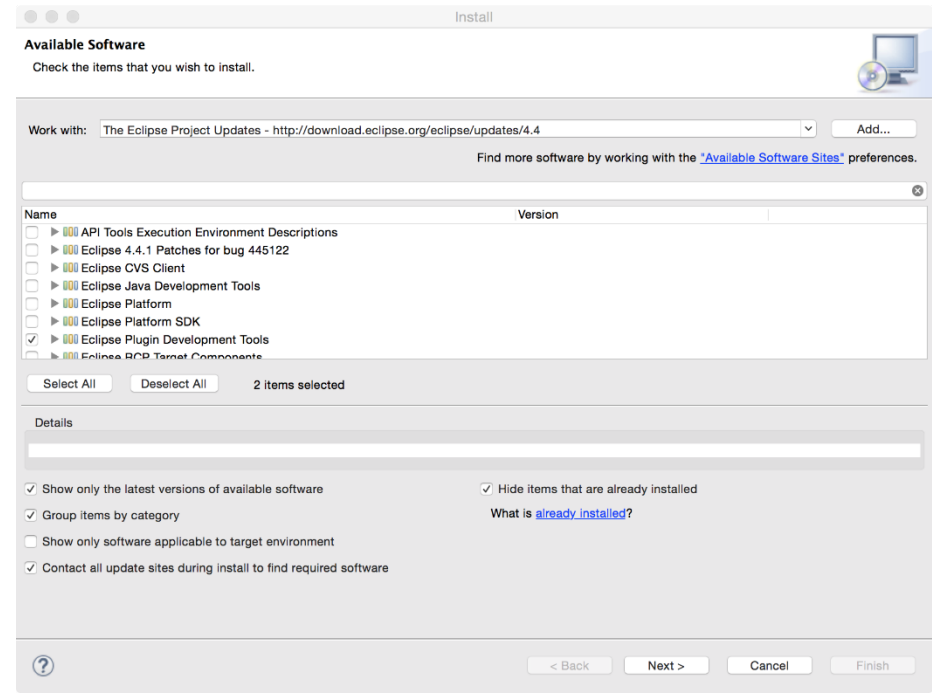
Eclipse.ini Location:

Minimum Memory:

Maximum Memory:

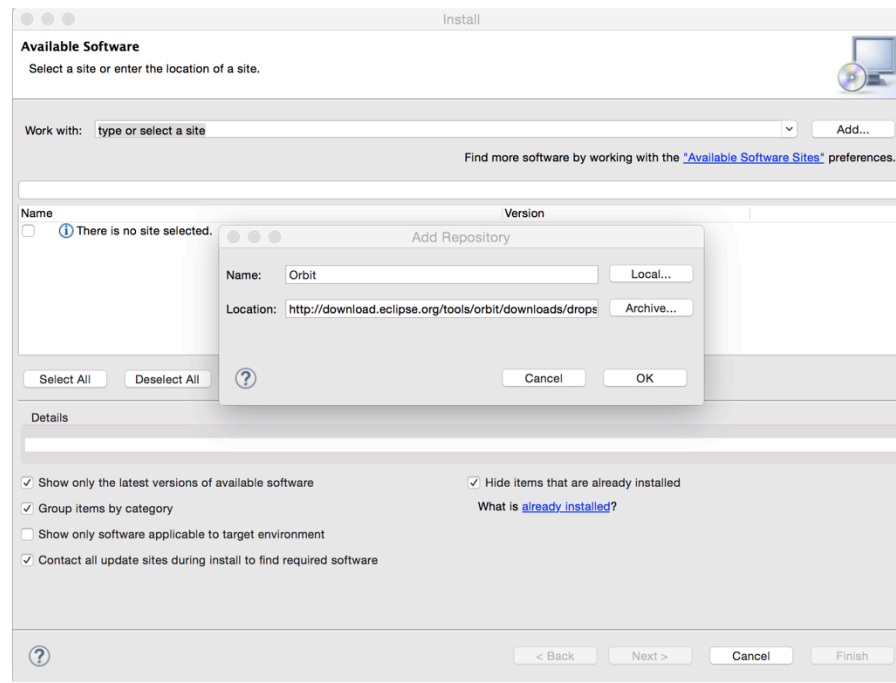
Install Eclipse Plugin Development Tools

- Within Eclipse, navigate to Help → Install New Software...
- In the “Works With:” field, search for “Updates”. Select the “The Eclipse Project Updates” update site.
- Select the “Eclipse Plugin Development Tools” feature for installation. Restart Eclipse.



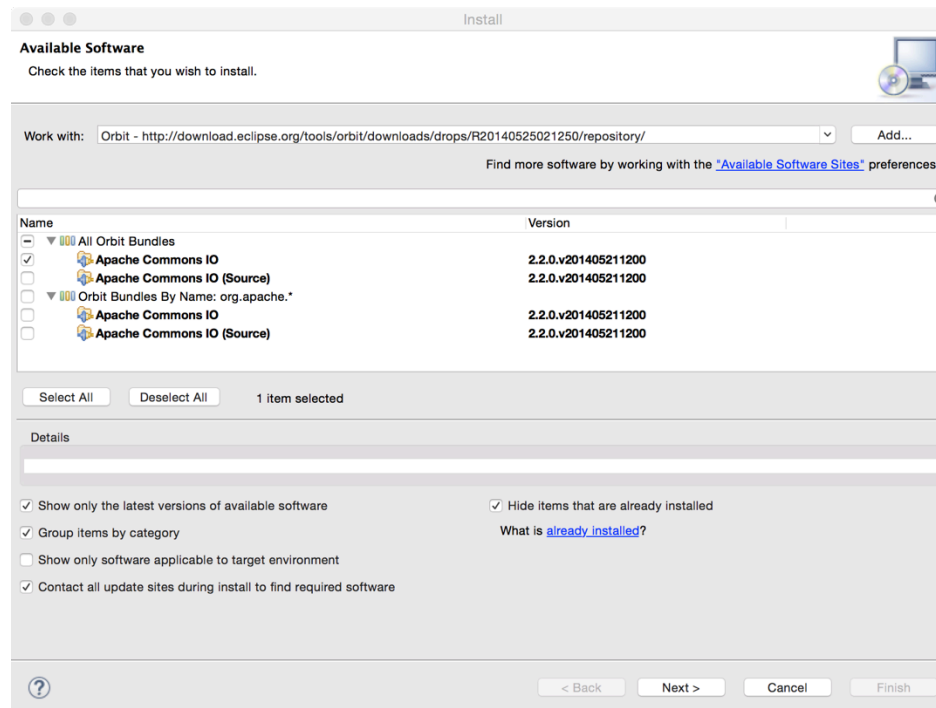
Install Apache Commons

- Within Eclipse, navigate to Help → Install New Software...
- Press “Add...” and enter “Orbit” in the “Name” field and <http://download.eclipse.org/tools/orbit/downloads/drops/R20140525021250/repository/> in the “Location” field.



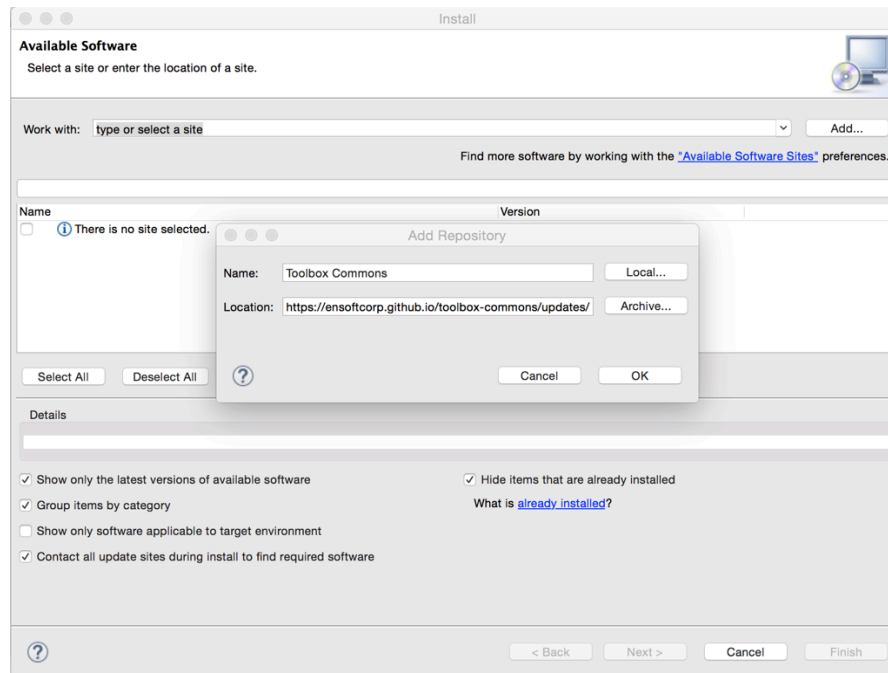
Install Apache Commons

- Search for “Commons IO”
- Select the Apache Commons IO feature, press “Next”, accept the license agreement. Restart Eclipse.



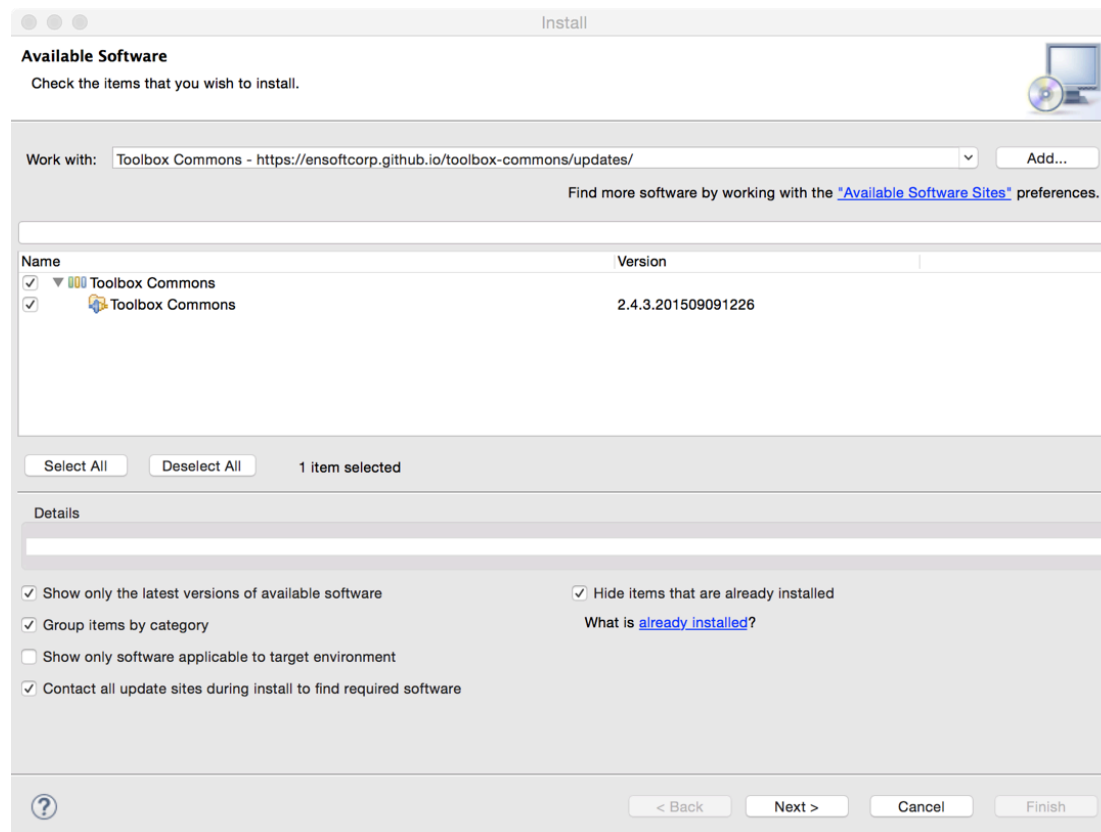
Install Toolbox Commons

- Within Eclipse, navigate to Help → Install New Software...
- Press “Add...” and enter “Toolbox Commons” in the “Name” field and <https://ensoftcorp.github.io/toolbox-commons/updates/> in the “Location” field.
- Details: <https://ensoftcorp.github.io/toolbox-commons/>



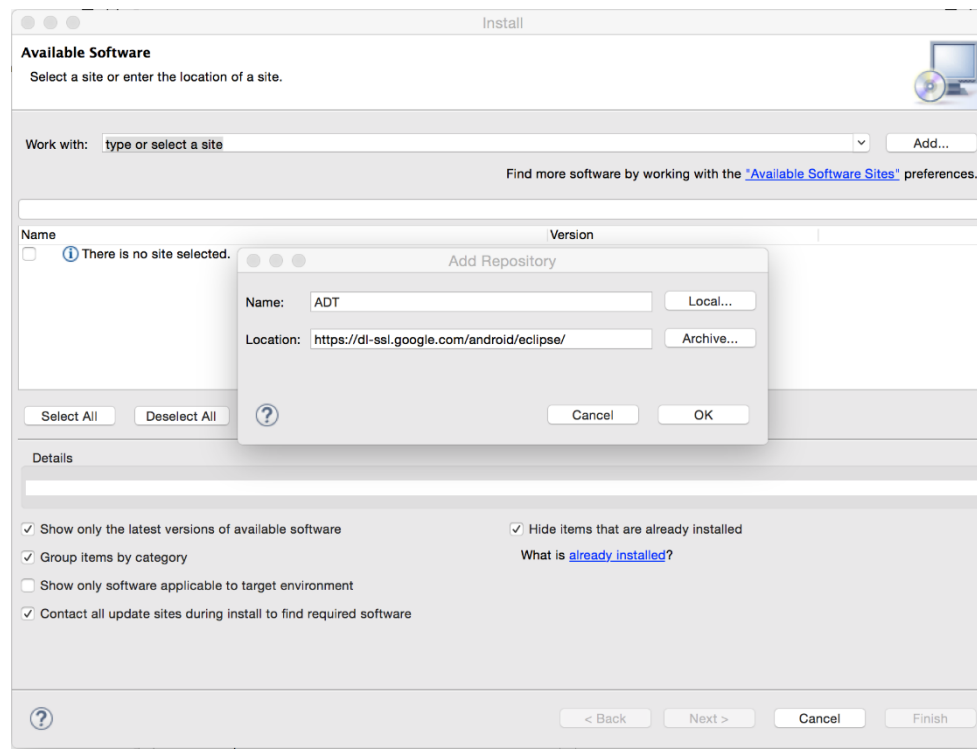
Install Toolbox Commons

- Select the Toolbox Commons feature, press “Next”, accept the license agreement. Restart Eclipse.



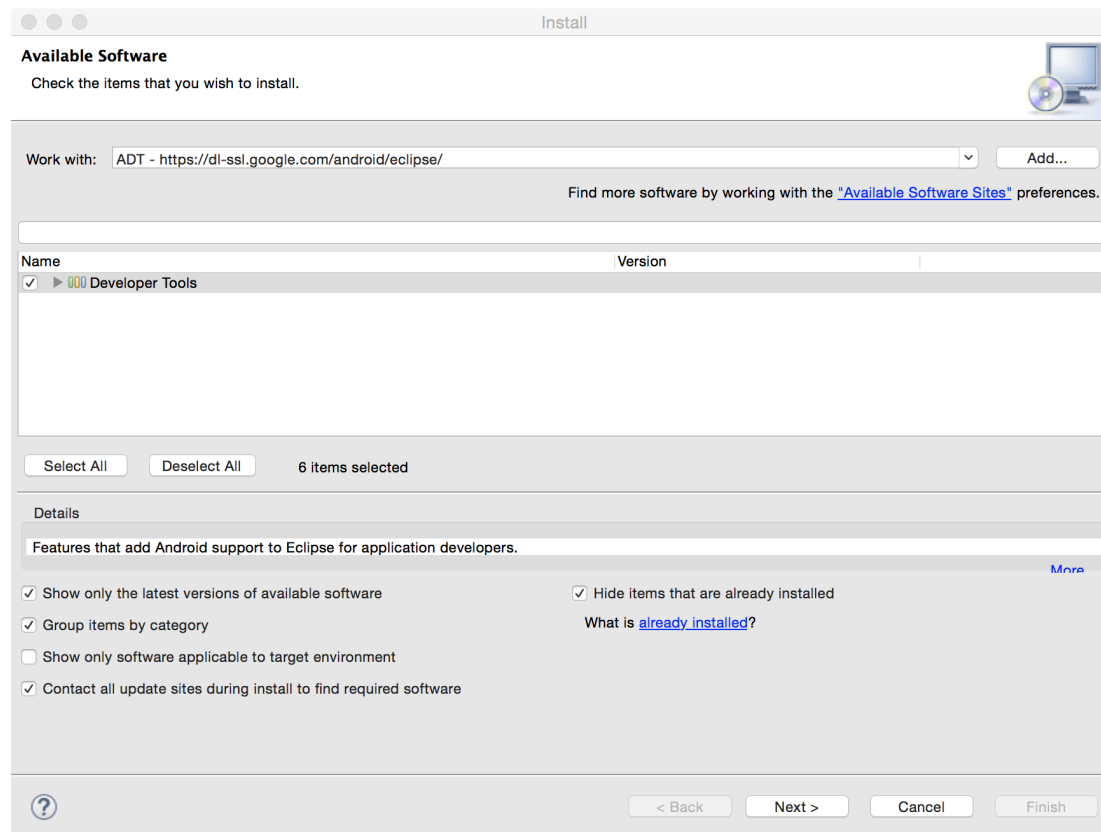
Install Android Development Toolkit

- Within Eclipse, navigate to Help → Install New Software...
- Press “Add...” and enter “ADT” in the “Name” field and <https://dl-ssl.google.com/android/eclipse/> in the “Location” field.



Install Android Development Toolkit

- Select the Developer Tools feature, press “Next”, accept the license agreement. Restart Eclipse.

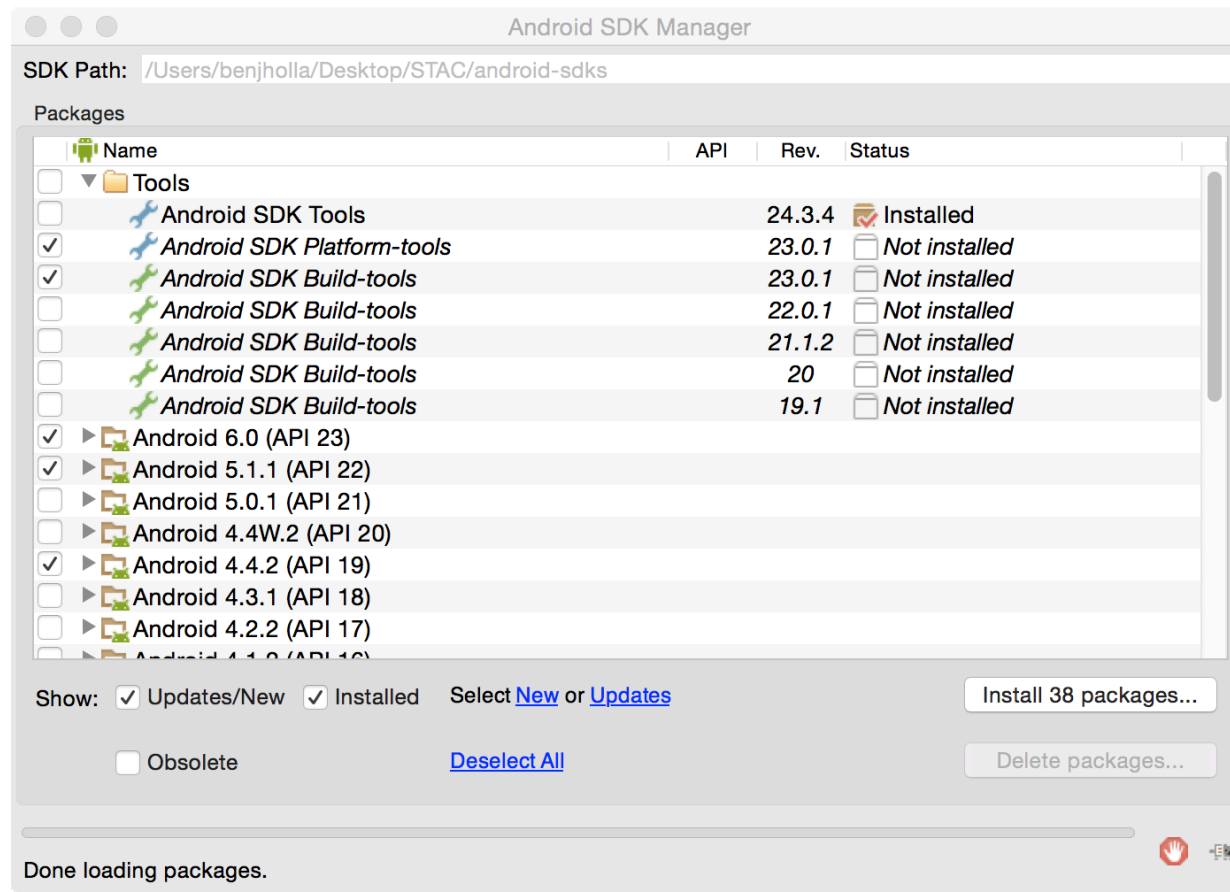


Install Android Development Toolkit

- Download the Standalone SDK Tools for your OS
 - <https://developer.android.com/sdk/installing/index.html?pkg=tools>
- Extract the contents of the Standalone SDK Tools download to the “MILCOM2015/android-sdks” folder.
- Within Eclipse, navigate to Eclipse or Window → Preferences → Android. Press the “Browse...” button and navigate to the “MILCOM2015/android-sdks” folder. Press Apply.
- If the SDK Manager does not appear automatically, navigate to Window → Android SDK Manager.

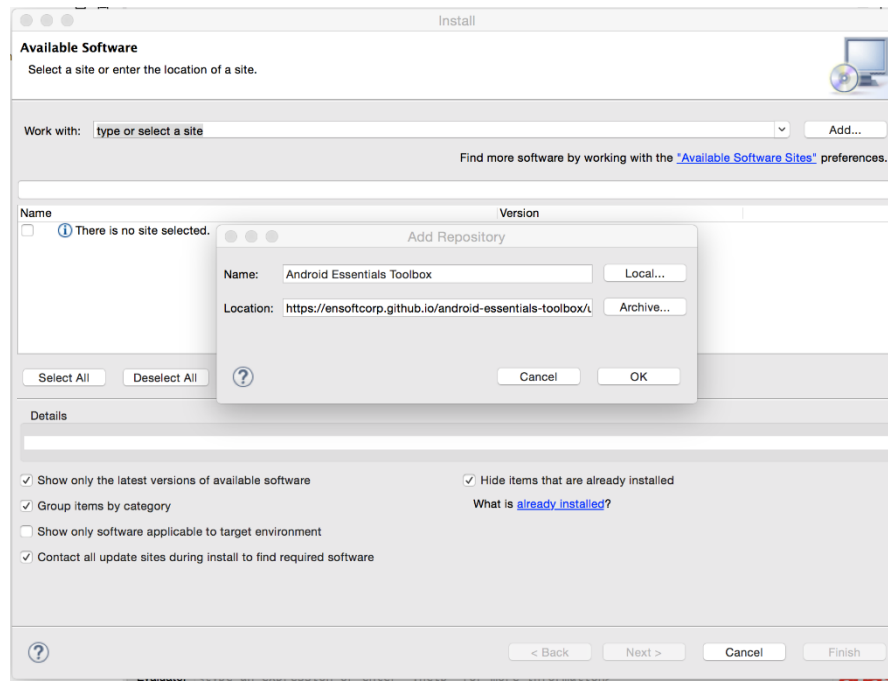
Install Android Development Toolkit

- Download the latest SDK Platforms for Android as well as API 19.



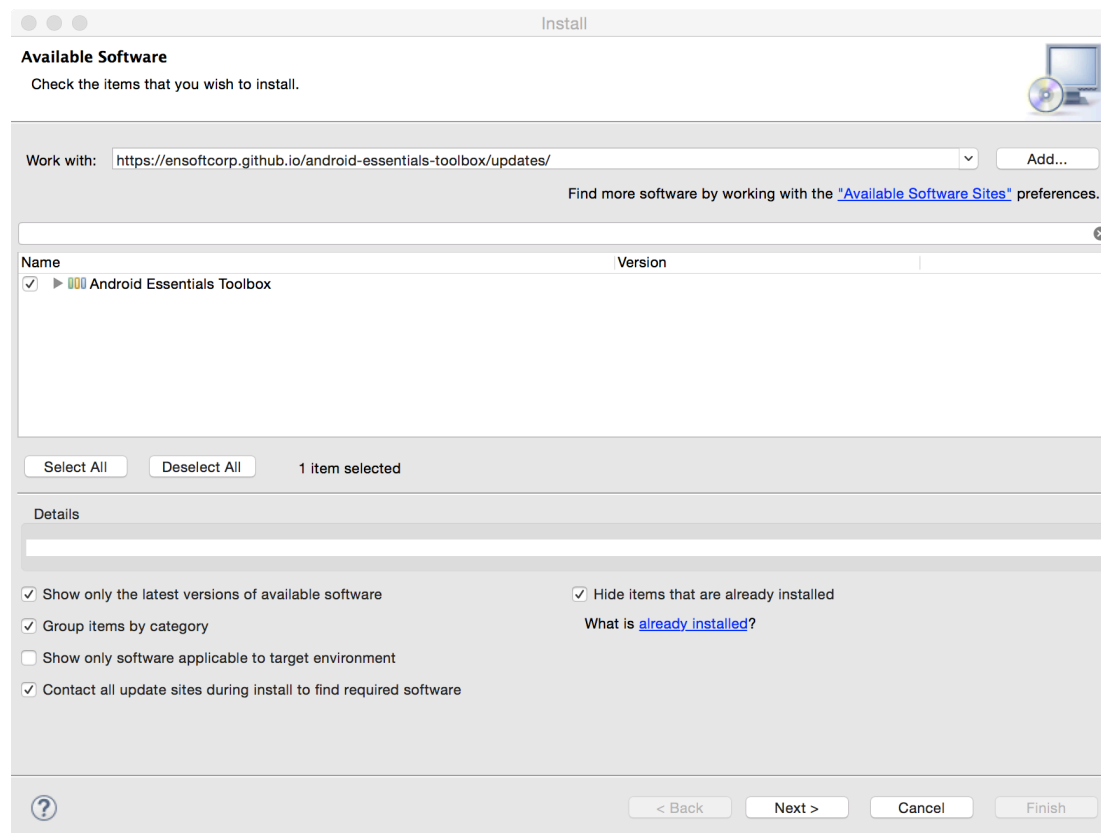
Install Android Essentials Toolbox

- Within Eclipse, navigate to Help → Install New Software...
- Press “Add...” and enter “Android Essentials Toolbox” in the “Name” field and <https://ensoftcorp.github.io/android-essentials-toolbox/updates/> in the “Location” field.
- Details: <https://ensoftcorp.github.io/android-essentials-toolbox/>



Install Android Essentials Toolbox

- Select the Android Essentials Toolbox feature, press “Next”, accept the license agreement. Restart Eclipse.



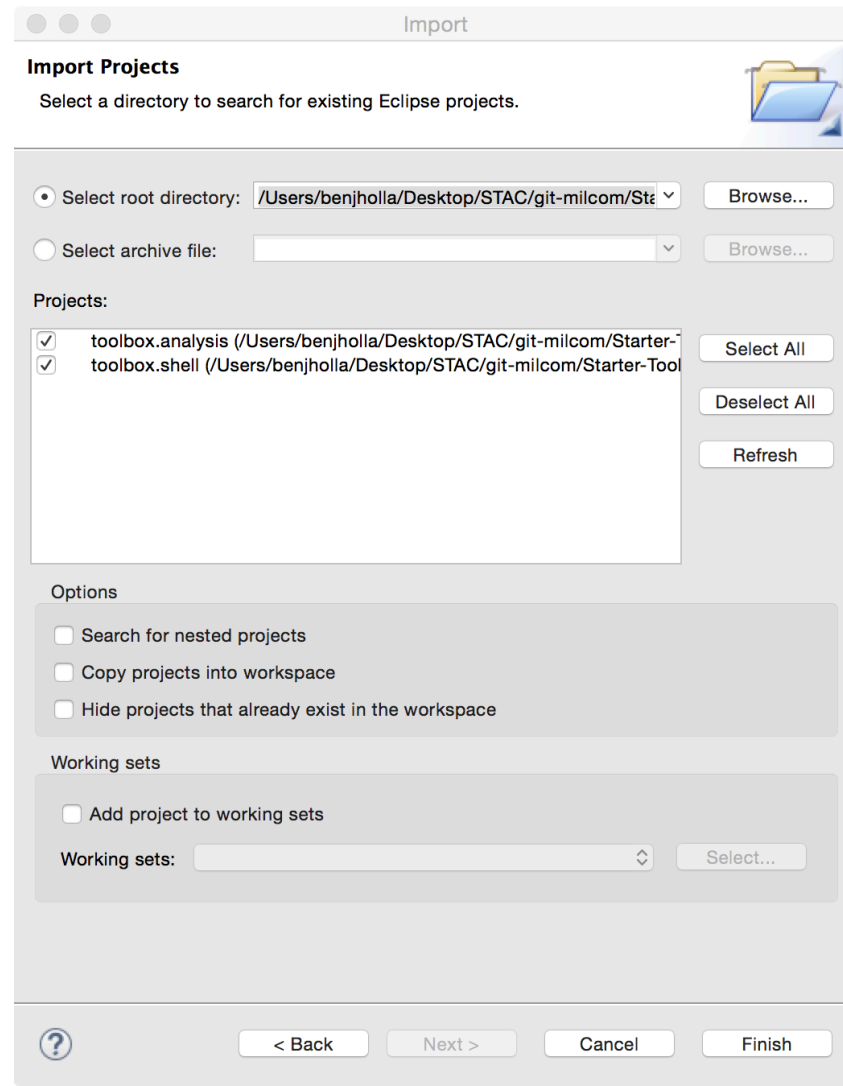
Import the LearningAtlas projects

- On the command line navigate to the “MILCOM2015/git” folder
- Clone the [LearningAtlas](https://github.com/EnSoftCorp/LearningAtlas.git) repository into the “MILCOM2015/git” folder with the following command:
 - *git clone* <https://github.com/EnSoftCorp/LearningAtlas.git>
- Navigate to File → Import... → General → Existing Projects into Workspace
- In the “Select Root Directory” field, press “Browse...” and navigate to the “MILCOM2015/git/LearningAtlas” folder
- Select the “HelloWorld” project and press the “Finish” button to import the project

Import the Starter Toolbox

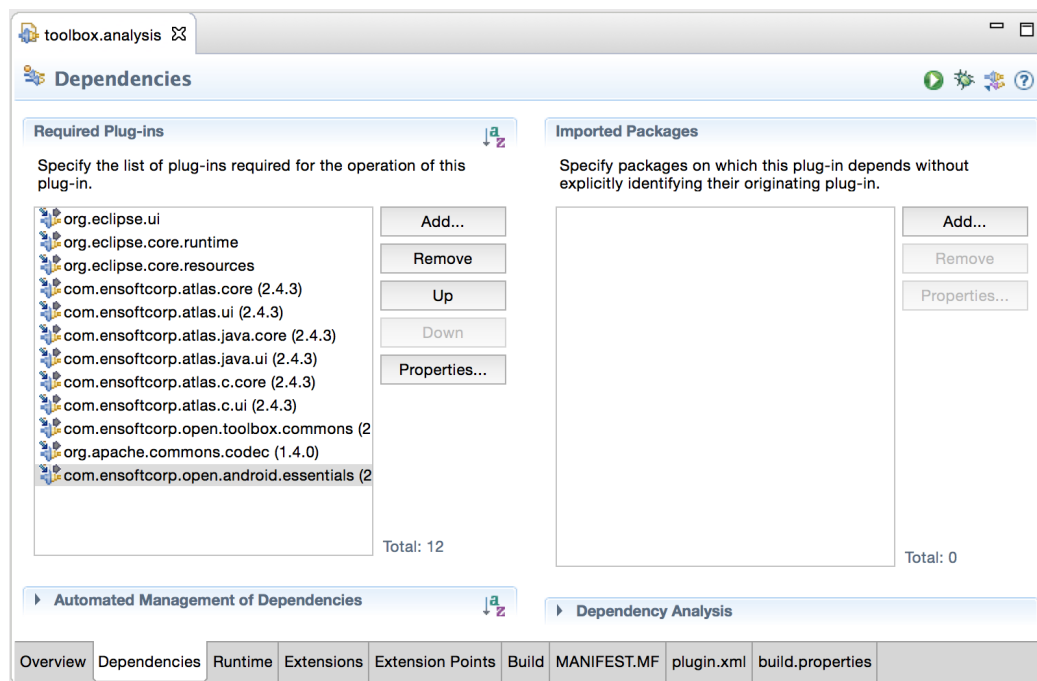
- On the command line navigate to the “MILCOM2015/git” folder
- Clone the [Starter-Toolbox](#) into the “MILCOM2015/git” folder with the following command:
 - *git clone* <https://github.com/EnSoftCorp/Starter-Toolbox.git>
 - Alternatively fork the repository and clone the forked project
- Navigate to File → Import... → General → Existing Projects into Workspace
- In the “Select Root Directory” field, press “Browse...” and navigate to the “MILCOM2015/git/Starter-Toolbox” folder
- Select both the “toolbox.analysis” and “toolbox.shell” projects and press the “Finish” button to import the projects

Import the Starter Toolbox



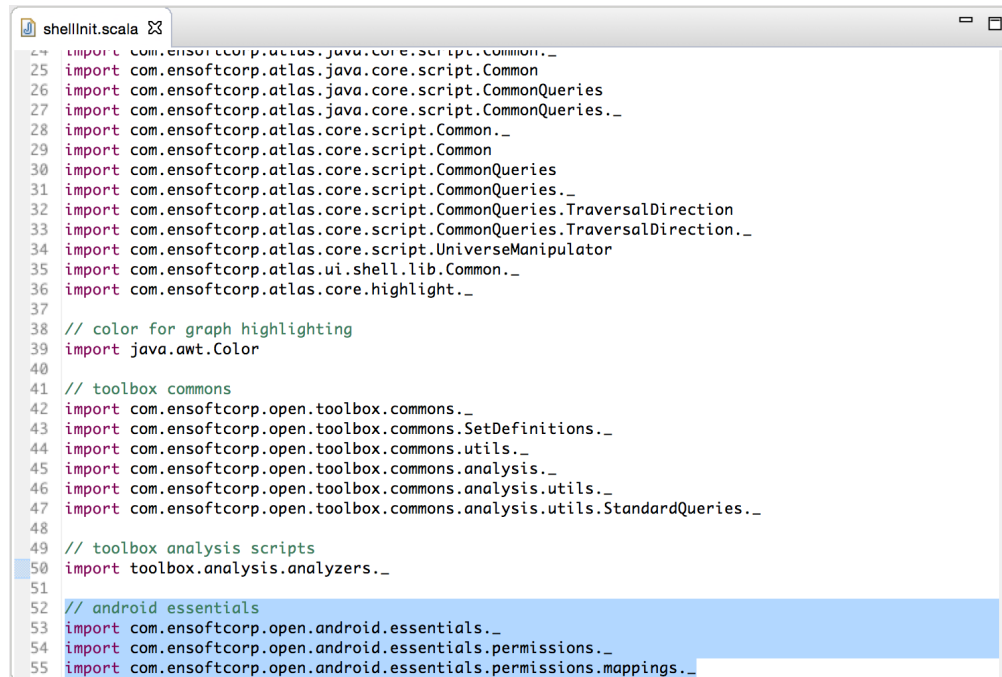
Import the Starter Toolbox

- Within the “toolbox.analysis” project open the “META-INF/MANIFEST.MF” file. Under the dependencies tab and add a dependency on the “com.ensoftcorp.open.android.essentials” plugin.
 - Note: Make sure to check the “Reexport this dependency” checkbox when adding the dependency



Import the Starter Toolbox

- Within the “toolbox.shell” project open the “shellInit.scala” file. Add the following import statements.
 - import com.ensoftcorp.open.android.essentials._
 - import com.ensoftcorp.open.android.essentials.permissions._
 - import com.ensoftcorp.open.android.essentials.permissions.mappings._



```
24 import com.ensoftcorp.atlas.java.core.script.Common._
25 import com.ensoftcorp.atlas.java.core.script.Common
26 import com.ensoftcorp.atlas.java.core.script.CommonQueries
27 import com.ensoftcorp.atlas.java.core.script.CommonQueries._
28 import com.ensoftcorp.atlas.core.script.Common._
29 import com.ensoftcorp.atlas.core.script.Common
30 import com.ensoftcorp.atlas.core.script.CommonQueries
31 import com.ensoftcorp.atlas.core.script.CommonQueries._
32 import com.ensoftcorp.atlas.core.script.CommonQueries.TraversalDirection
33 import com.ensoftcorp.atlas.core.script.CommonQueries.TraversalDirection._
34 import com.ensoftcorp.atlas.core.script.UniverseManipulator
35 import com.ensoftcorp.atlas.ui.shell.lib.Common._
36 import com.ensoftcorp.atlas.core.highlight._
37
38 // color for graph highlighting
39 import java.awt.Color
40
41 // toolbox commons
42 import com.ensoftcorp.open.toolbox.commons._
43 import com.ensoftcorp.open.toolbox.commons.SetDefinitions._
44 import com.ensoftcorp.open.toolbox.commons.utils._
45 import com.ensoftcorp.open.toolbox.commons.analysis._
46 import com.ensoftcorp.open.toolbox.commons.analysis.utils._
47 import com.ensoftcorp.open.toolbox.commons.analysis.utils.StandardQueries._
48
49 // toolbox analysis scripts
50 import toolbox.analysis.analyzers._
51
52 // android essentials
53 import com.ensoftcorp.open.android.essentials._
54 import com.ensoftcorp.open.android.essentials.permissions._
55 import com.ensoftcorp.open.android.essentials.permissions.mappings._
```

Open the Atlas Shell

- Within Eclipse, navigate to Atlas → Manage Project Settings. Select the “HelloWorld” project (or the project(s) you want to analyze) and make sure that it is the only project listed in the “Map” category. Press OK to save changes.
- Next, navigate to Window → Show View → Other... → Atlas → Atlas Shell and press OK. Select the “toolbox.shell” project and press OK.

Your Eclipse Should Now Look Something Like This...

