MILCOM2015
LEVERAGING TECHNOLOGY—THE JOINT IMPERATIVE
OCTOBER 26–28, 2015•TAMPA, FL

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

ensoft
conquer complexity

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

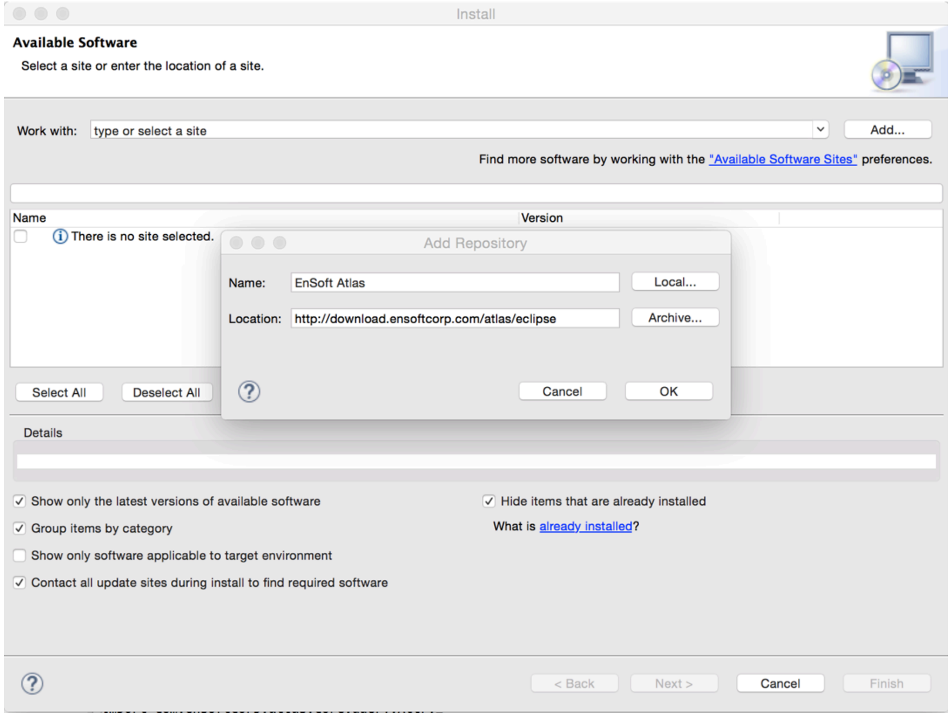
- Download Eclipse Luna for Mac, Windows, or Linux
  - Download the “Eclipse IDE for Java Developers” package
  - https://www.eclipse.org/downloads/packages/release/Luna/SR2
- Create a directory called “MILCOM2015”
- Extract the “eclipse” folder of the Eclipse download to “MILCOM2015”
- Inside “MILCOM2015”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

Available Software

Select a site or enter the location of a site.

Work with: type or select a site

Find more software by working with the "Available Software Sites" preferences.

Name	Version
□ There is no site selected.	

Add Repository

Name: EnSoft Atlas

Location: http://download.ensoftcorp.com/atlas/eclipse

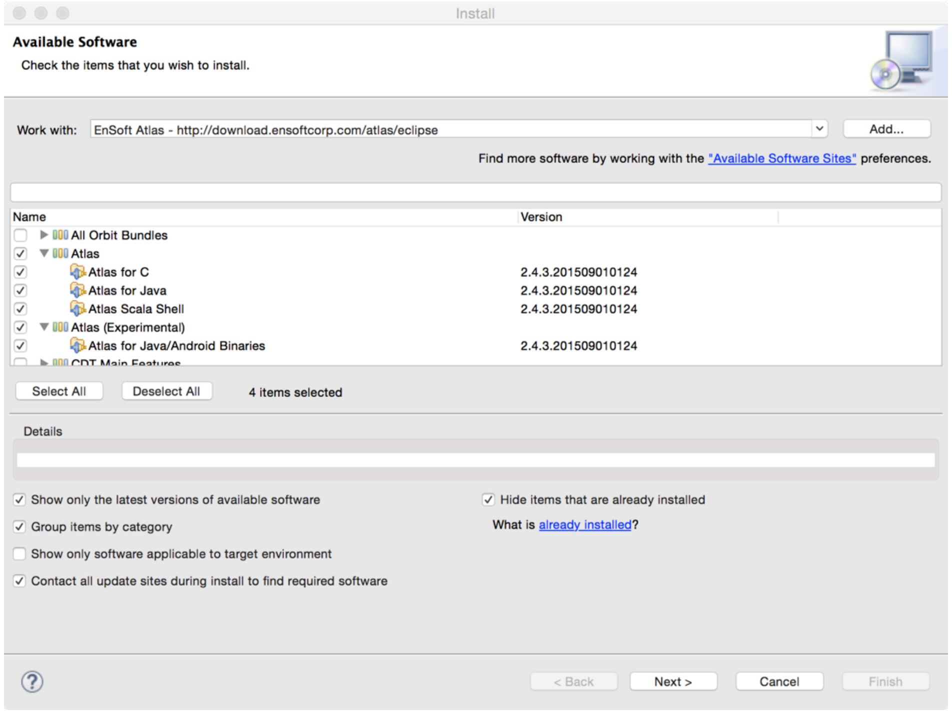
Details

☑ Show only the latest versions of available software
☑ Group items by category
□ Show only software applicable to target environment
☑ Contact all update sites during install to find required software

☑ Hide items that are already installed
What is already installed?

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.



Available Software

Check the items that you wish to install.

Work with: EnSoft Atlas - http://download.ensoftcorp.com/atlas/eclipse

Find more software by working with the "Available Software Sites" preferences.

Name	Version
□ ▶ All Orbit Bundles	
☑ ▼ Atlas	
☑ Atlas for C	2.4.3.201509010124
☑ Atlas for Java	2.4.3.201509010124
☑ Atlas Scala Shell	2.4.3.201509010124
☑ ▼ Atlas (Experimental)	
☑ Atlas for Java/Android Binaries	2.4.3.201509010124
□ ▶ CDT Main Features	

4 items selected

Details

☑ Show only the latest versions of available software
☑ Group items by category
□ Show only software applicable to target environment
☑ Contact all update sites during install to find required software

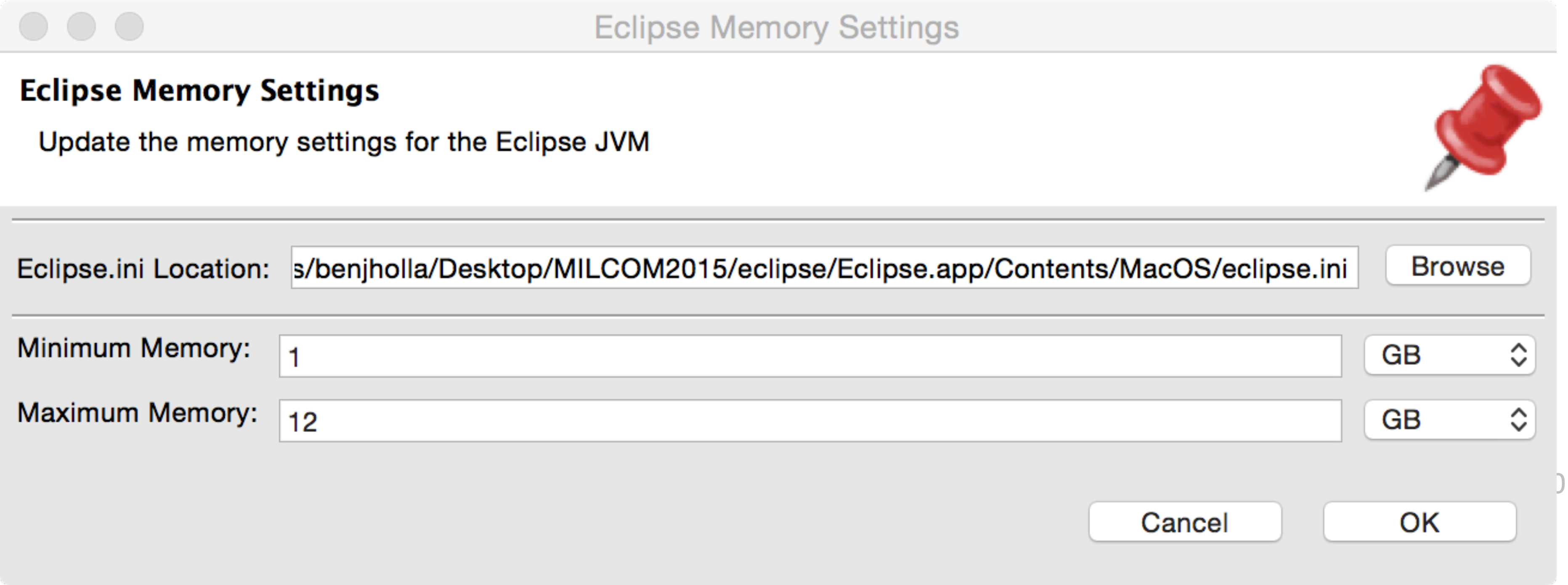
☑ Hide items that are already installed
What is already installed?

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

Eclipse Memory Settings

Update the memory settings for the Eclipse JVM

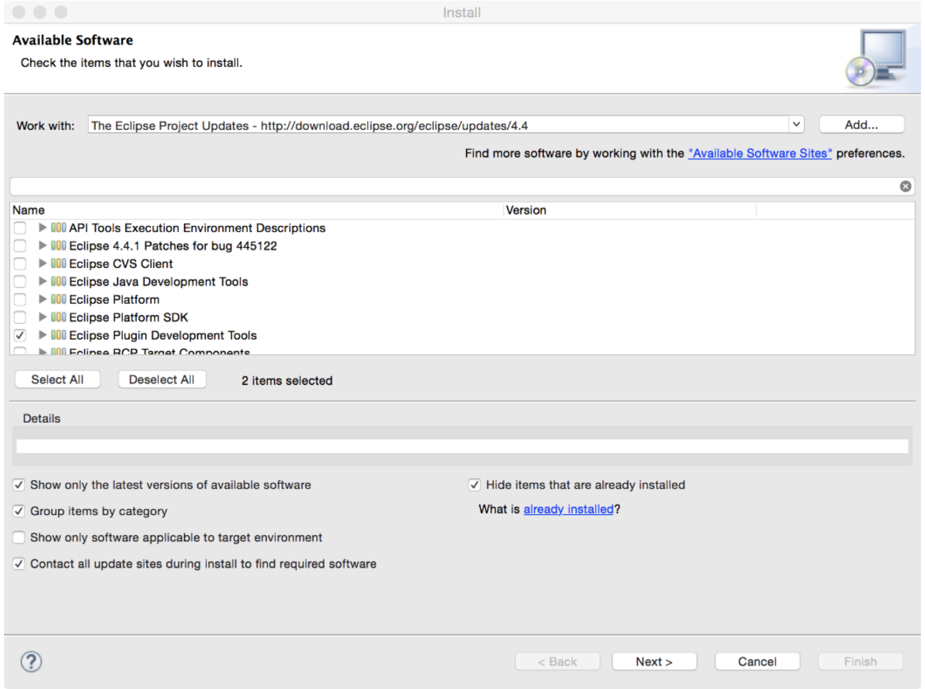
Eclipse.ini Location: s/benjholla/Desktop/MILCOM2015/eclipse/Eclipse.app/Contents/MacOS/eclipse.ini

Minimum Memory: 1 GB

Maximum Memory: 12 GB

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.



Available Software

Check the items that you wish to install.

Work with: The Eclipse Project Updates - http://download.eclipse.org/eclipse/updates/4.4

Find more software by working with the "Available Software Sites" preferences.

Name	Version
□ ▶ API Tools Execution Environment Descriptions	
□ ▶ Eclipse 4.4.1 Patches for bug 445122	
□ ▶ Eclipse CVS Client	
□ ▶ Eclipse Java Development Tools	
□ ▶ Eclipse Platform	
□ ▶ Eclipse Platform SDK	
☑ ▶ Eclipse Plugin Development Tools	
□ ▶ Eclipse RCP Target Components	

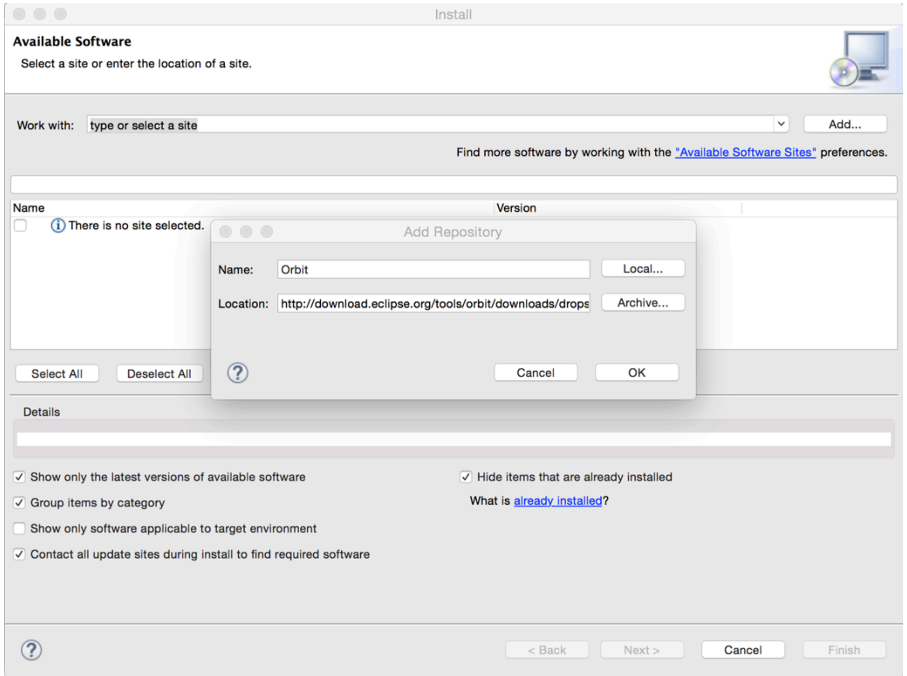
2 items selected

Details

☑ Show only the latest versions of available software
☑ Group items by category
□ Show only software applicable to target environment
☑ Contact all update sites during install to find required software
☑ Hide items that are already installed
What is already installed?

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

Available Software

Select a site or enter the location of a site.

Work with: type or select a site

Find more software by working with the "Available Software Sites" preferences.

Name | Version

There is no site selected.

Add Repository

Name: Orbit

Location: http://download.eclipse.org/tools/orbit/downloads/drops

Details

☑ Show only the latest versions of available software

☑ Group items by category

□ Show only software applicable to target environment

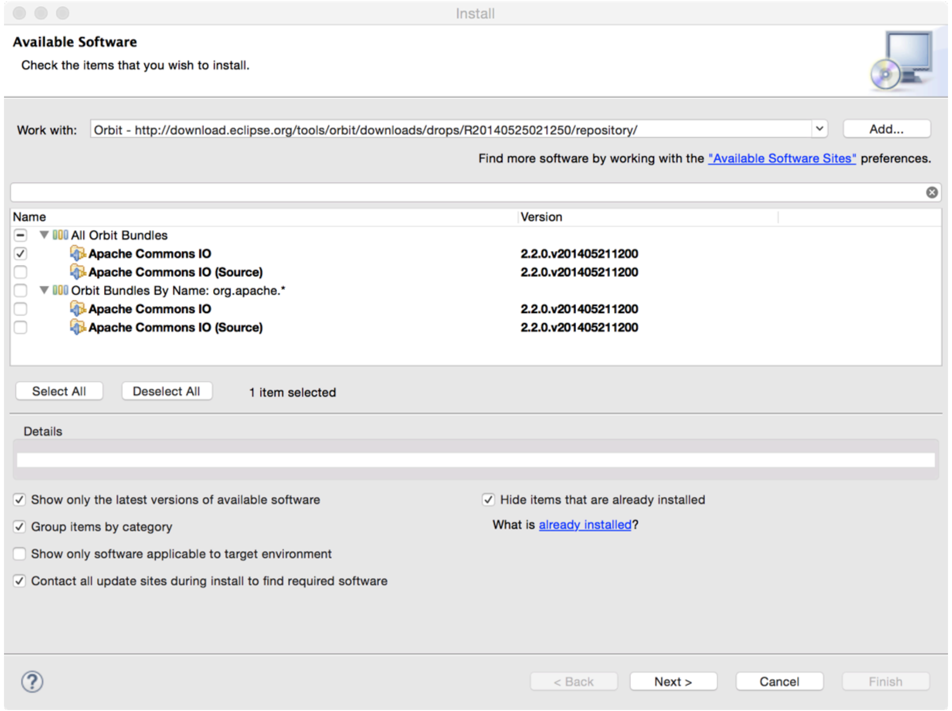
☑ Contact all update sites during install to find required software

☑ Hide items that are already installed

What is already installed?

Install Apache Commons

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



Install

Available Software

Check the items that you wish to install.

Work with: Orbit - http://download.eclipse.org/tools/orbit/downloads/drops/R20140525021250/repository/

Find more software by working with the "Available Software Sites" preferences.

Name	Version
⊟ ▼ All Orbit Bundles	
☑ Apache Commons IO	2.2.0.v201405211200
□ Apache Commons IO (Source)	2.2.0.v201405211200
□ ▼ Orbit Bundles By Name: org.apache.*	
□ Apache Commons IO	2.2.0.v201405211200
□ Apache Commons IO (Source)	2.2.0.v201405211200

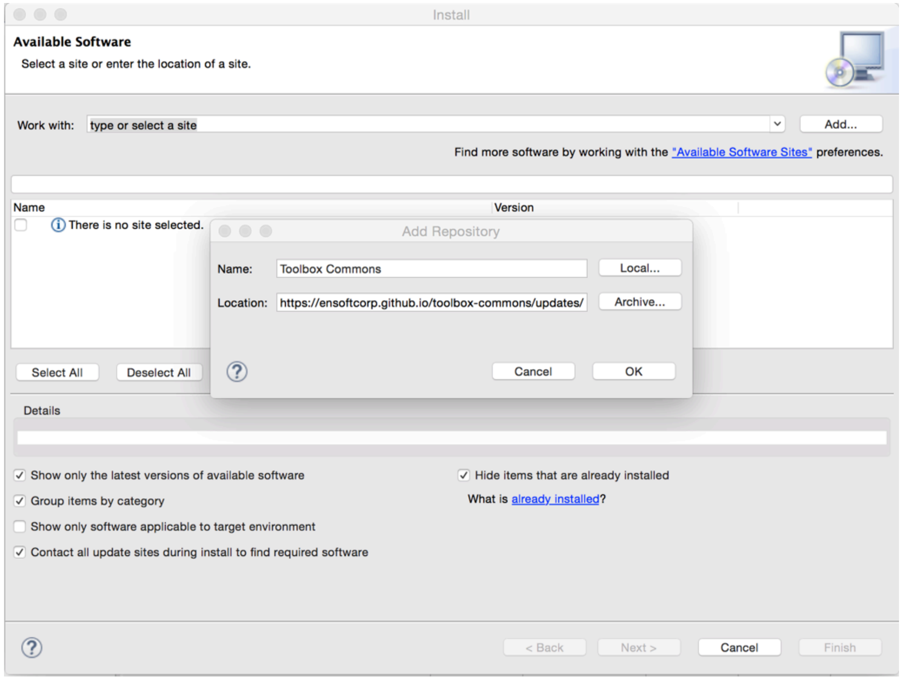
1 item selected

Details

☑ Show only the latest versions of available software
☑ Group items by category
□ Show only software applicable to target environment
☑ Contact all update sites during install to find required software
☑ Hide items that are already installed
What is already installed?

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

Available Software

Select a site or enter the location of a site.

Work with: type or select a site

Find more software by working with the "Available Software Sites" preferences.

Name | Version

□ There is no site selected.

Add Repository

Name: Toolbox Commons

Location: https://ensoftcorp.github.io/toolbox-commons/updates/

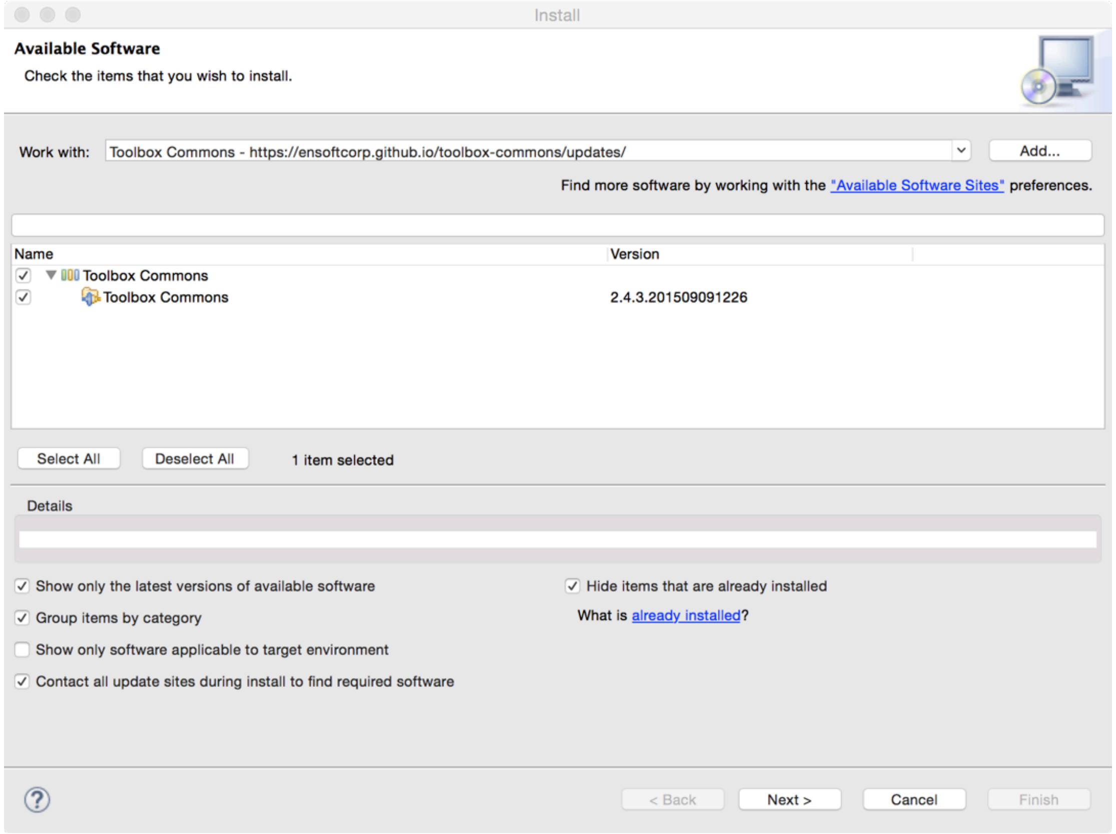
Details

☑ Show only the latest versions of available software
☑ Group items by category
□ Show only software applicable to target environment
☑ Contact all update sites during install to find required software
☑ Hide items that are already installed

What is already installed?

Install Toolbox Commons

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



Available Software

Check the items that you wish to install.

Work with: Toolbox Commons - https://ensoftcorp.github.io/toolbox-commons/updates/

Find more software by working with the "Available Software Sites" preferences.

Name	Version
☑ ▼ Toolbox Commons	
☑ Toolbox Commons	2.4.3.201509091226

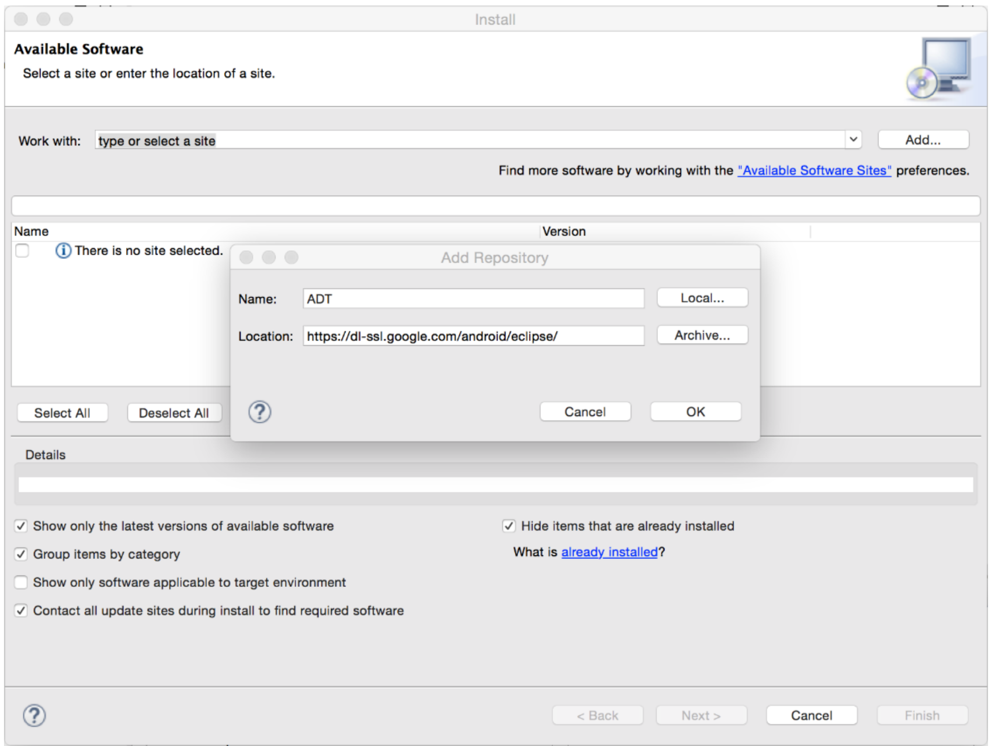
1 item selected

Details

☑ Show only the latest versions of available software
☑ Group items by category
□ Show only software applicable to target environment
☑ Contact all update sites during install to find required software
☑ Hide items that are already installed
What is already installed?

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

Available Software

Select a site or enter the location of a site.

Work with: type or select a site

Find more software by working with the "Available Software Sites" preferences.

Name	Version
□ ⓘ There is no site selected.	

Add Repository

Name: ADT

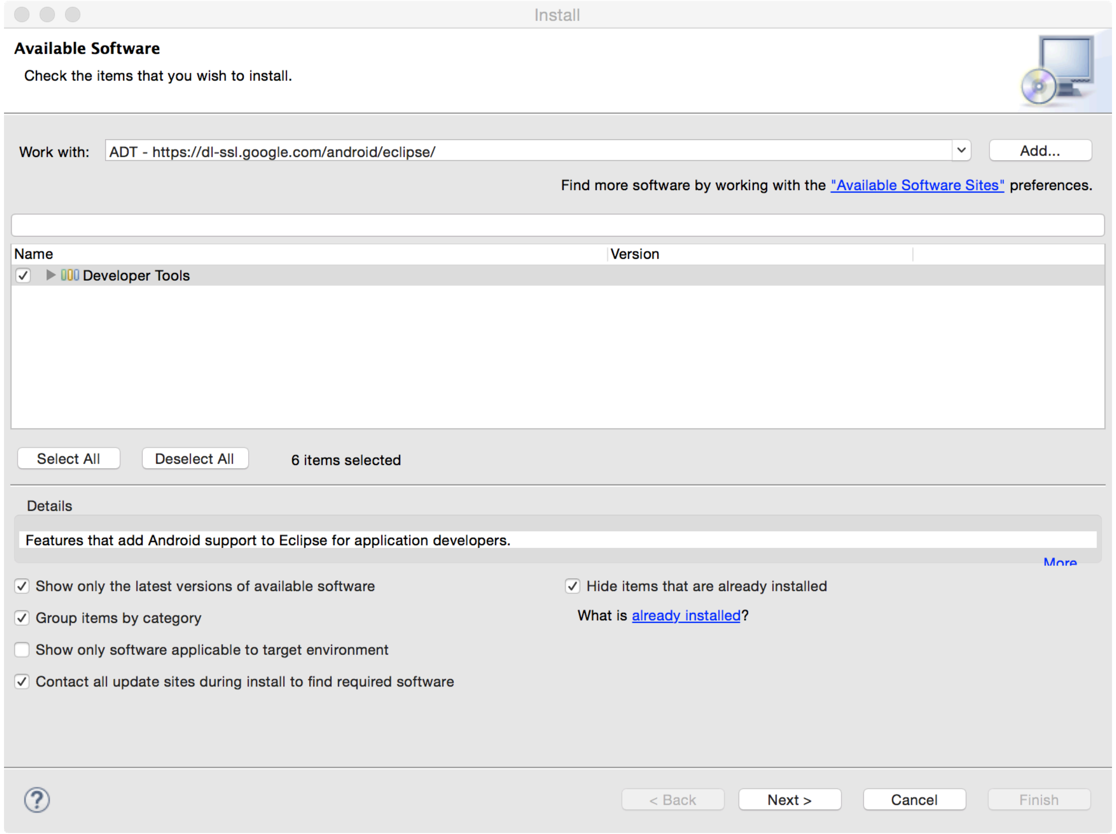
Location: https://dl-ssl.google.com/android/eclipse/

Details

☑ Show only the latest versions of available software
☑ Group items by category
□ Show only software applicable to target environment
☑ Contact all update sites during install to find required software
☑ Hide items that are already installed
What is already installed?

Install Android Development Toolkit

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



Install

Available Software

Check the items that you wish to install.

Work with: ADT - https://dl-ssl.google.com/android/eclipse/ [Add...]

Find more software by working with the "Available Software Sites" preferences.

Name	Version
☑ ▶ Developer Tools	

[Select All] [Deselect All] 6 items selected

Details

Features that add Android support to Eclipse for application developers.

More

☑ Show only the latest versions of available software
☑ Group items by category
□ Show only software applicable to target environment
☑ Contact all update sites during install to find required software

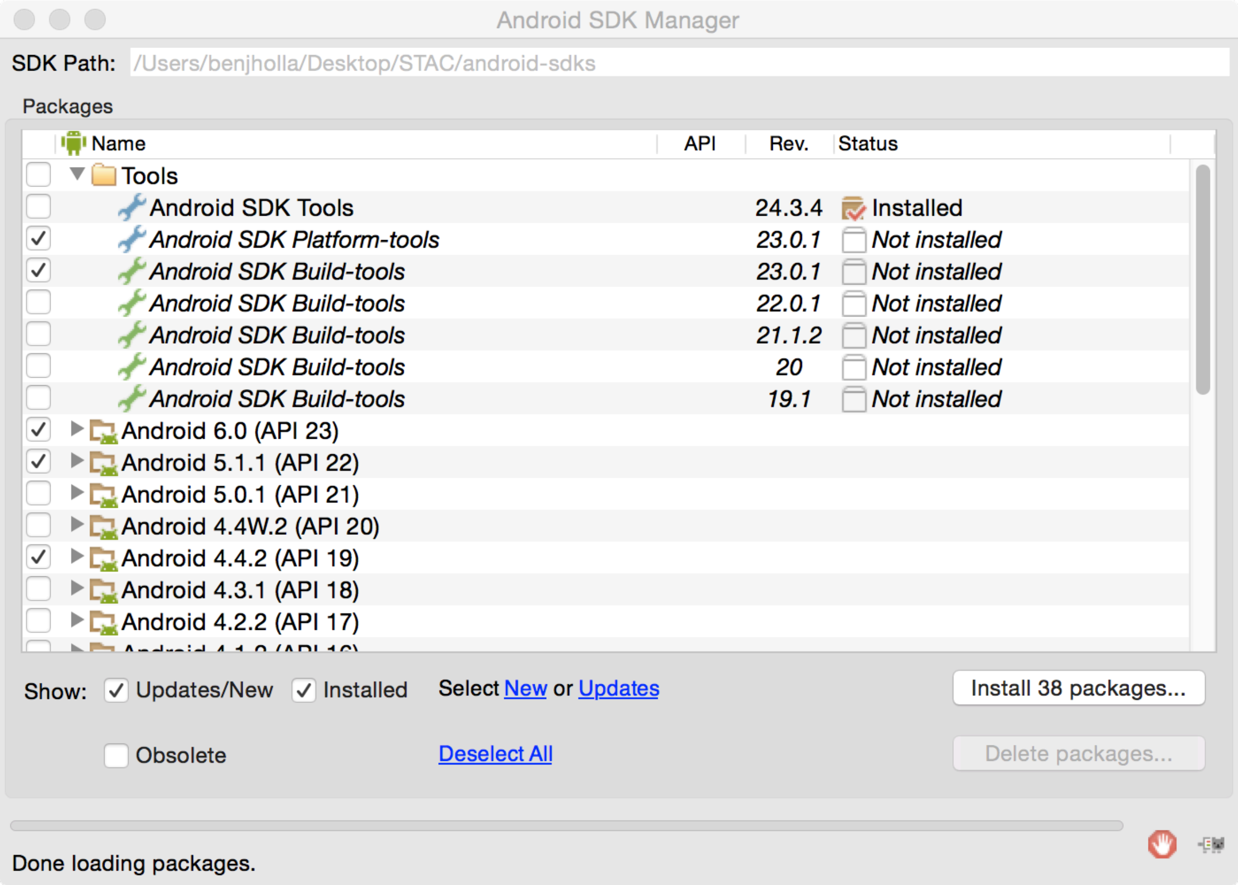
☑ Hide items that are already installed
What is already installed?

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.



Android SDK Manager

SDK Path: /Users/benjholla/Desktop/STAC/android-sdks

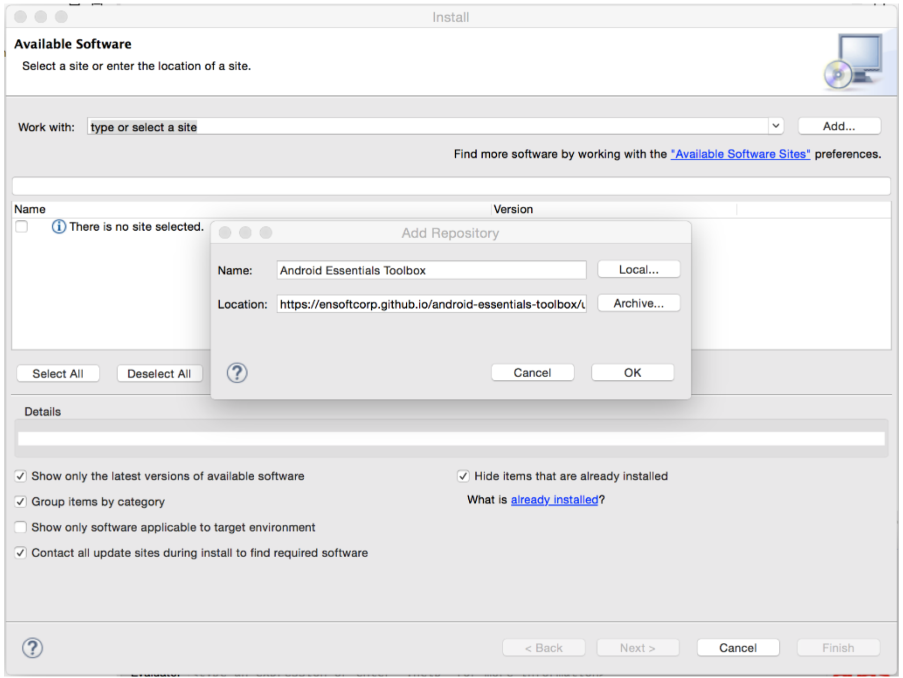
Packages

	Name	API	Rev.	Status
□	▼ Tools			
□	Android SDK Tools		24.3.4	Installed
☑	*Android SDK Platform-tools*		*23.0.1*	*Not installed*
☑	*Android SDK Build-tools*		*23.0.1*	*Not installed*
□	*Android SDK Build-tools*		*22.0.1*	*Not installed*
□	*Android SDK Build-tools*		*21.1.2*	*Not installed*
□	*Android SDK Build-tools*		*20*	*Not installed*
□	*Android SDK Build-tools*		*19.1*	*Not installed*
☑	▶ Android 6.0 (API 23)			
☑	▶ Android 5.1.1 (API 22)			
□	▶ Android 5.0.1 (API 21)			
□	▶ Android 4.4W.2 (API 20)			
☑	▶ Android 4.4.2 (API 19)			
□	▶ Android 4.3.1 (API 18)			
□	▶ Android 4.2.2 (API 17)			
□	▶ Android 4.1.2 (API 16)			

Done loading packages.

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/



Available Software

Select a site or enter the location of a site.

Work with: type or select a site

Find more software by working with the "Available Software Sites" preferences.

Name	Version
□ ⓘ There is no site selected.	

Name: Android Essentials Toolbox

Location: https://ensoftcorp.github.io/android-essentials-toolbox/u

Details

☑ Show only the latest versions of available software

☑ Group items by category

□ Show only software applicable to target environment

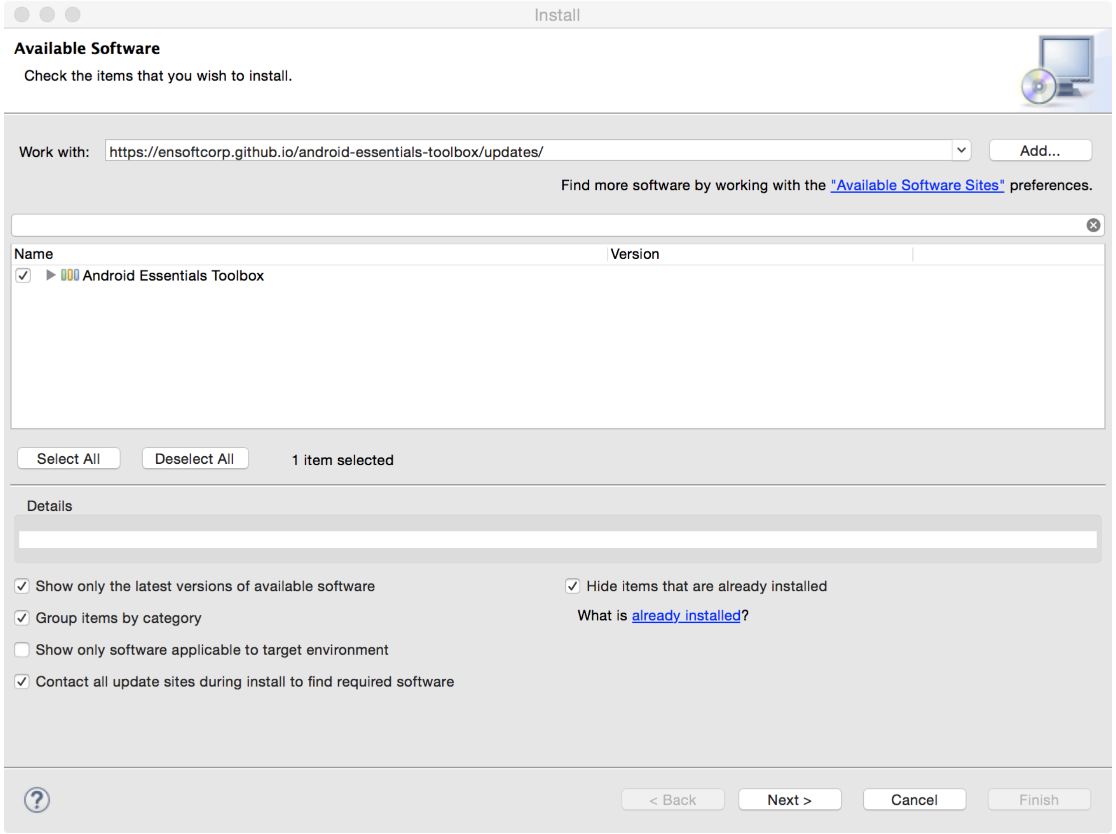
☑ Contact all update sites during install to find required software

☑ Hide items that are already installed

What is already installed?

Install Android Essentials Toolbox

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



Install

Available Software

Check the items that you wish to install.

Work with: https://ensoftcorp.github.io/android-essentials-toolbox/updates/

Find more software by working with the "Available Software Sites" preferences.

Name	Version
☑ ▶ Android Essentials Toolbox	

1 item selected

Details

☑ Show only the latest versions of available software

☑ Group items by category

☐ Show only software applicable to target environment

☑ Contact all update sites during install to find required software

☑ Hide items that are already installed

What is already installed?

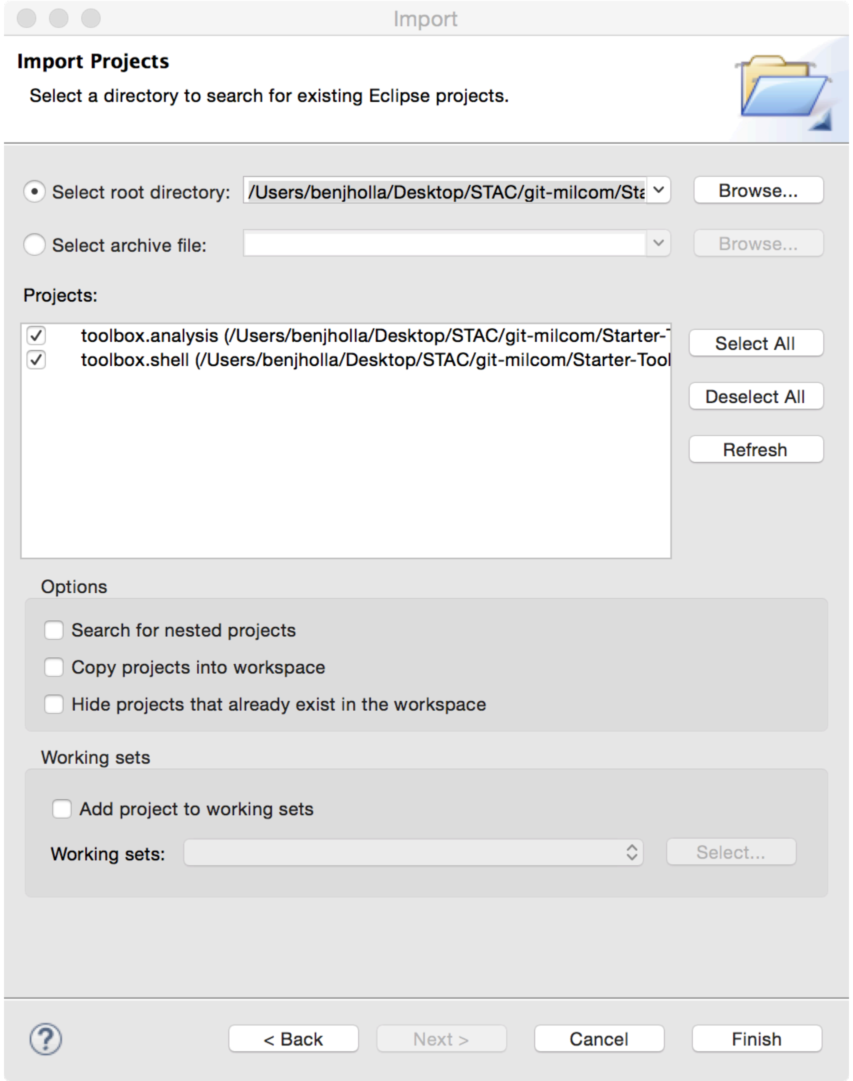
Import the LearningAtlas projects

- On the command line navigate to the “MILCOM2015/git” folder
- Clone the LearningAtlas 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

Import Projects

Select a directory to search for existing Eclipse projects.

● Select root directory: /Users/benjholla/Desktop/STAC/git-milcom/Sta

○ Select archive file:

Projects:

- ☑ toolbox.analysis (/Users/benjholla/Desktop/STAC/git-milcom/Starter-
- ☑ toolbox.shell (/Users/benjholla/Desktop/STAC/git-milcom/Starter-Tool

Options

- □ Search for nested projects
- □ Copy projects into workspace
- □ Hide projects that already exist in the workspace

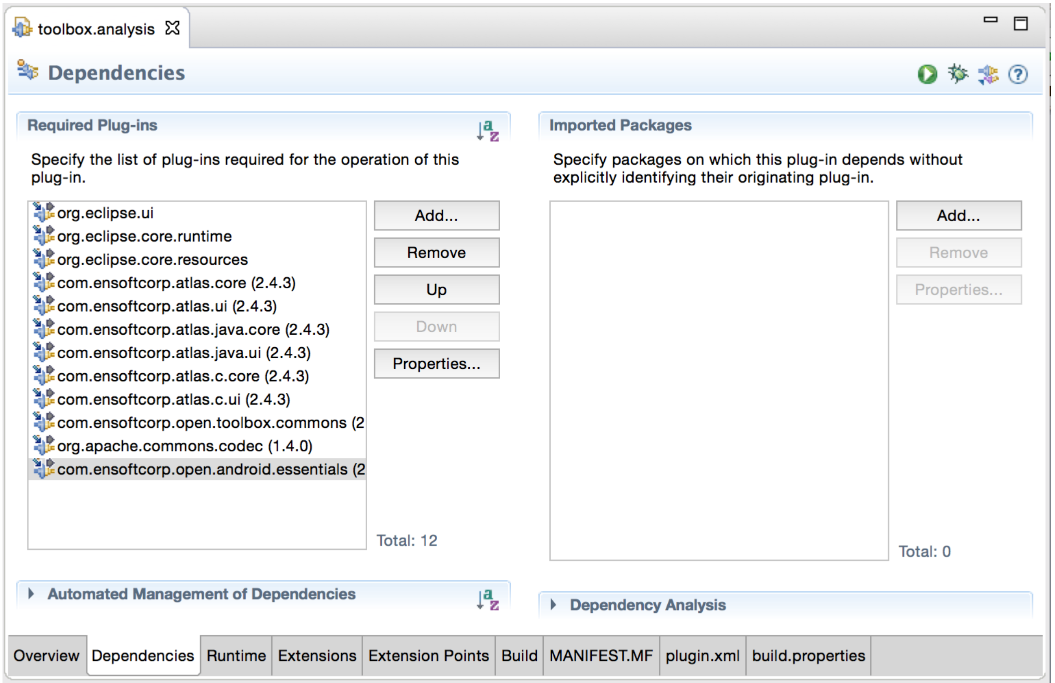
Working sets

- □ Add project to working sets

Working sets:

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



Required Plug-ins

Specify the list of plug-ins required for the operation of this plug-in.

org.eclipse.ui
org.eclipse.core.runtime
org.eclipse.core.resources
com.ensoftcorp.atlas.core (2.4.3)
com.ensoftcorp.atlas.ui (2.4.3)
com.ensoftcorp.atlas.java.core (2.4.3)
com.ensoftcorp.atlas.java.ui (2.4.3)
com.ensoftcorp.atlas.c.core (2.4.3)
com.ensoftcorp.atlas.c.ui (2.4.3)
com.ensoftcorp.open.toolbox.commons (2
org.apache.commons.codec (1.4.0)
com.ensoftcorp.open.android.essentials (2

Total: 12

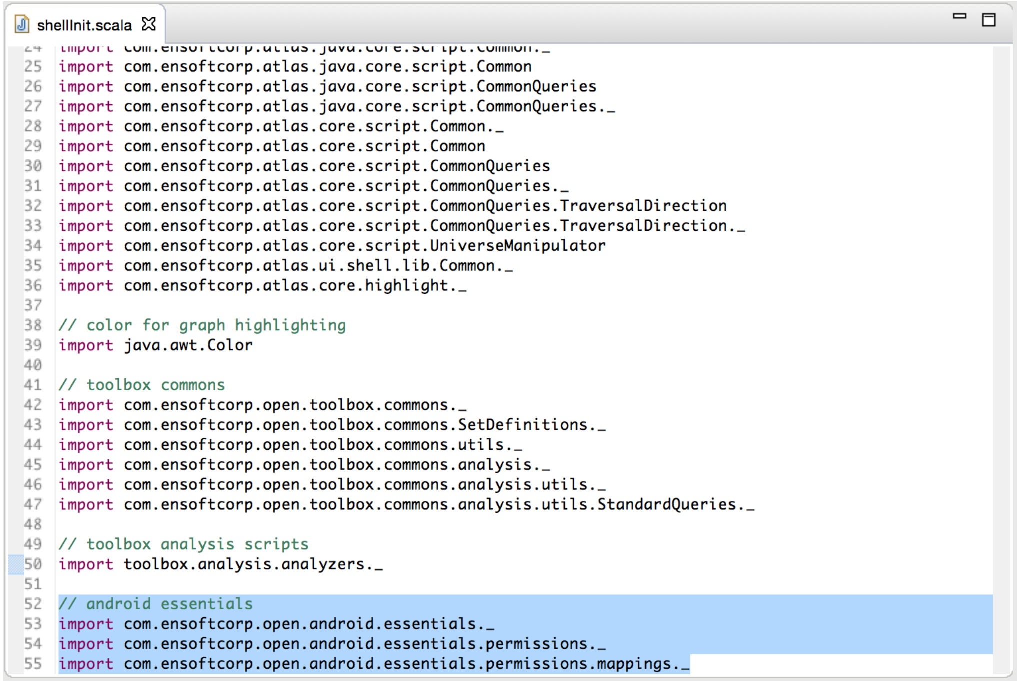
Imported Packages

Specify packages on which this plug-in depends without explicitly identifying their originating plug-in.

Total: 0

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._

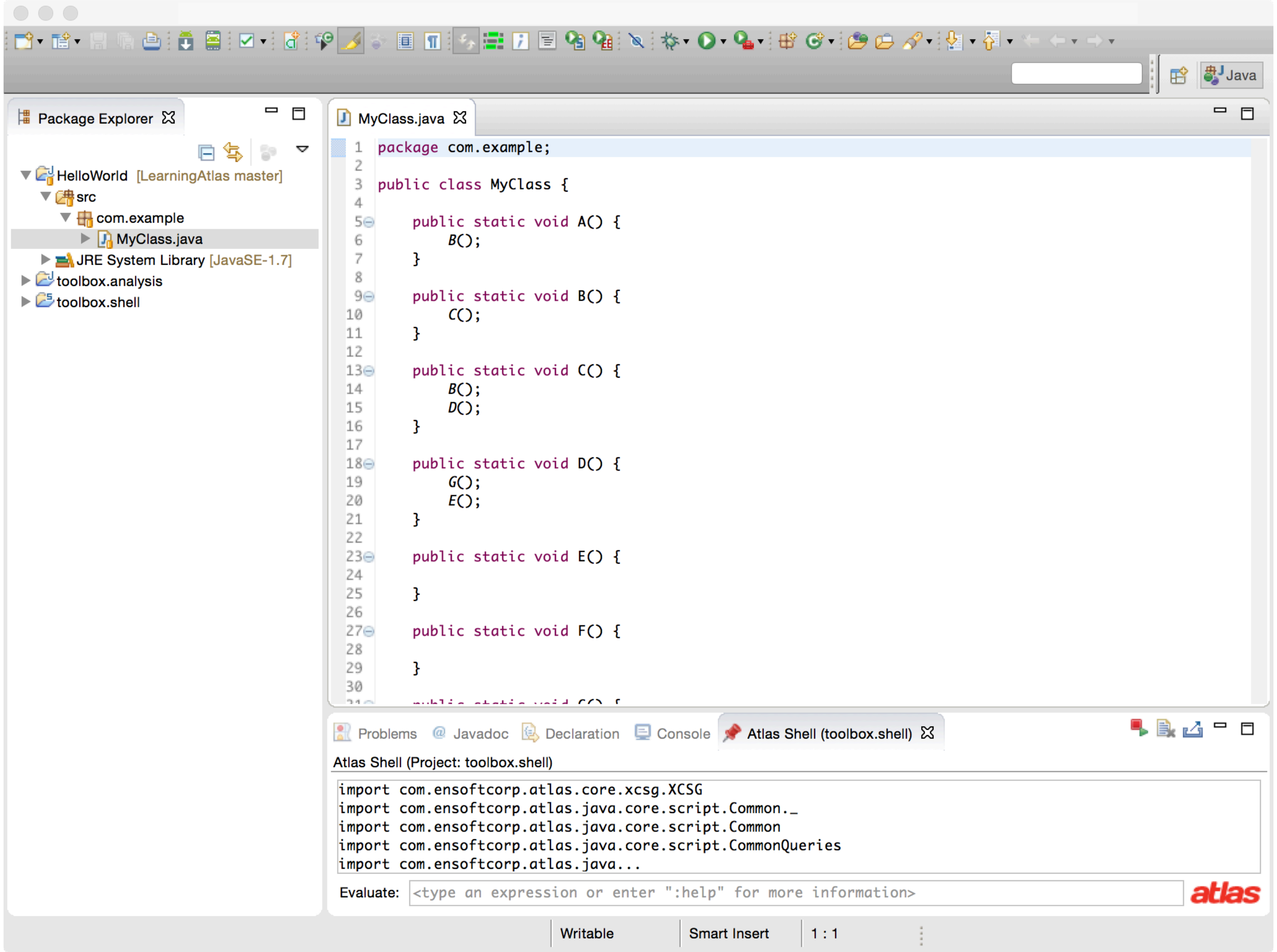


```
import com.ensoftcorp.atlas.java.core.script.Common._
import com.ensoftcorp.atlas.java.core.script.Common
import com.ensoftcorp.atlas.java.core.script.CommonQueries
import com.ensoftcorp.atlas.java.core.script.CommonQueries._
import com.ensoftcorp.atlas.core.script.Common._
import com.ensoftcorp.atlas.core.script.Common
import com.ensoftcorp.atlas.core.script.CommonQueries
import com.ensoftcorp.atlas.core.script.CommonQueries._
import com.ensoftcorp.atlas.core.script.CommonQueries.TraversalDirection
import com.ensoftcorp.atlas.core.script.CommonQueries.TraversalDirection._
import com.ensoftcorp.atlas.core.script.UniverseManipulator
import com.ensoftcorp.atlas.ui.shell.lib.Common._
import com.ensoftcorp.atlas.core.highlight._

// color for graph highlighting
import java.awt.Color

// toolbox commons
import com.ensoftcorp.open.toolbox.commons._
import com.ensoftcorp.open.toolbox.commons.SetDefinitions._
import com.ensoftcorp.open.toolbox.commons.utils._
import com.ensoftcorp.open.toolbox.commons.analysis._
import com.ensoftcorp.open.toolbox.commons.analysis.utils._
import com.ensoftcorp.open.toolbox.commons.analysis.utils.StandardQueries._

// toolbox analysis scripts
import toolbox.analysis.analyzers._

// android essentials
import com.ensoftcorp.open.android.essentials._
import com.ensoftcorp.open.android.essentials.permissions._
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…


Java
Package Explorer
HelloWorld [LearningAtlas master]
src
com.example
MyClass.java
JRE System Library [JavaSE-1.7]
toolbox.analysis
toolbox.shell
MyClass.java
Problems
Javadoc
Declaration
Console
Atlas Shell (toolbox.shell)
Atlas Shell (Project: toolbox.shell)
Evaluate:
<type an expression or enter ":help" for more information>
atlas
Writable
Smart Insert
1 : 1

```java
package com.example;

public class MyClass {

    public static void A() {
        B();
    }

    public static void B() {
        C();
    }

    public static void C() {
        B();
        D();
    }

    public static void D() {
        G();
        E();
    }

    public static void E() {

    }

    public static void F() {

    }

    public static void G() {
```

```
import com.ensoftcorp.atlas.core.xcsg.XCSG
import com.ensoftcorp.atlas.java.core.script.Common._
import com.ensoftcorp.atlas.java.core.script.Common
import com.ensoftcorp.atlas.java.core.script.CommonQueries
import com.ensoftcorp.atlas.java...
```