**Name: Surya Devathi**

**WSU ID: n659a624**

**Question 1**

Please describe the general approach of IccTA according to Figure 2.

Ans: The steps in the general approach of IccTA are:

First Step: IccTA makes use of Dexpler which transforms the Dalcvick bytecode into Jimple which is a Soot’s internal representation.

Second Step: IccTA extracts the ICC links.

Third Step: It stores all the ICC links and all the other data in the database.

Fourth Step: In this step,

* IccTA modify the Jimple to come directly connect the components to enable data flow analysis.
* In this step the modified version which is of Flow Droid it builds a complete control-flow graph of the Android Application.

Fifth Step: This the last step in which IccTA stores the reported tainted path(leaks) into the database.

**Question 2**

How to perform taint flow analysis for ICC method startActivity().

Ans:

The above codes show how taint analysis is performed in the ICC method. In this Activity1 and Activity2 are linked. It creates helper class named IpcSc which acts a link connecting the source and destination. Then the startActivity is then removed and replaced by a statement calling the generated helper method. In this IccTA generates a constructor which takes a parameter, a dummy main method is called to fill al the related methods and then it overrides getIntent method. This intent is callee component. This behavior in which all the intent is explicitly transferring the to the destination component and uses customized constructor method. Activity2 takes the Intent as its parameter and stores it to newly generated field. The original method models the Android system by returning the object as its given parameter. The helper method redirect0 constructs an object of type Activity2 (the target component) and initializes the new object with the Intent given as parameter to the helper method. Then, it calls the dummyMain method of Activity2.