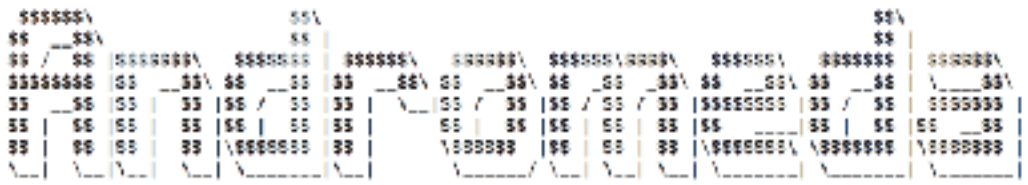


Created by : Shivang Desai
Powered by : Frida

Andromeda is a GUI based automated Android application analysis toolkit powered by Frida and Python.

What is Andromeda ?

In order to ease the use of Frida during app analysis/assessment and to keep things organized, Andromeda was built. Andromeda is a GUI (Graphical User Interface) based on Frida and powered by Python under the hood.
Andromeda helps researcher/pentester during dynamic app analysis with features like classes and methods enumeration, hooking and intercepting particular methods with ease of clicks.
It also creates javascript snippets, on the run, which further helps in hooking and interception.
For those who prefer typical CLI based approach, one of the Andromeda's feature allows to fulfill this need. It takes care of Javascript snippets and allows researcher to interact with CLI at the same time. (See next section for more details)

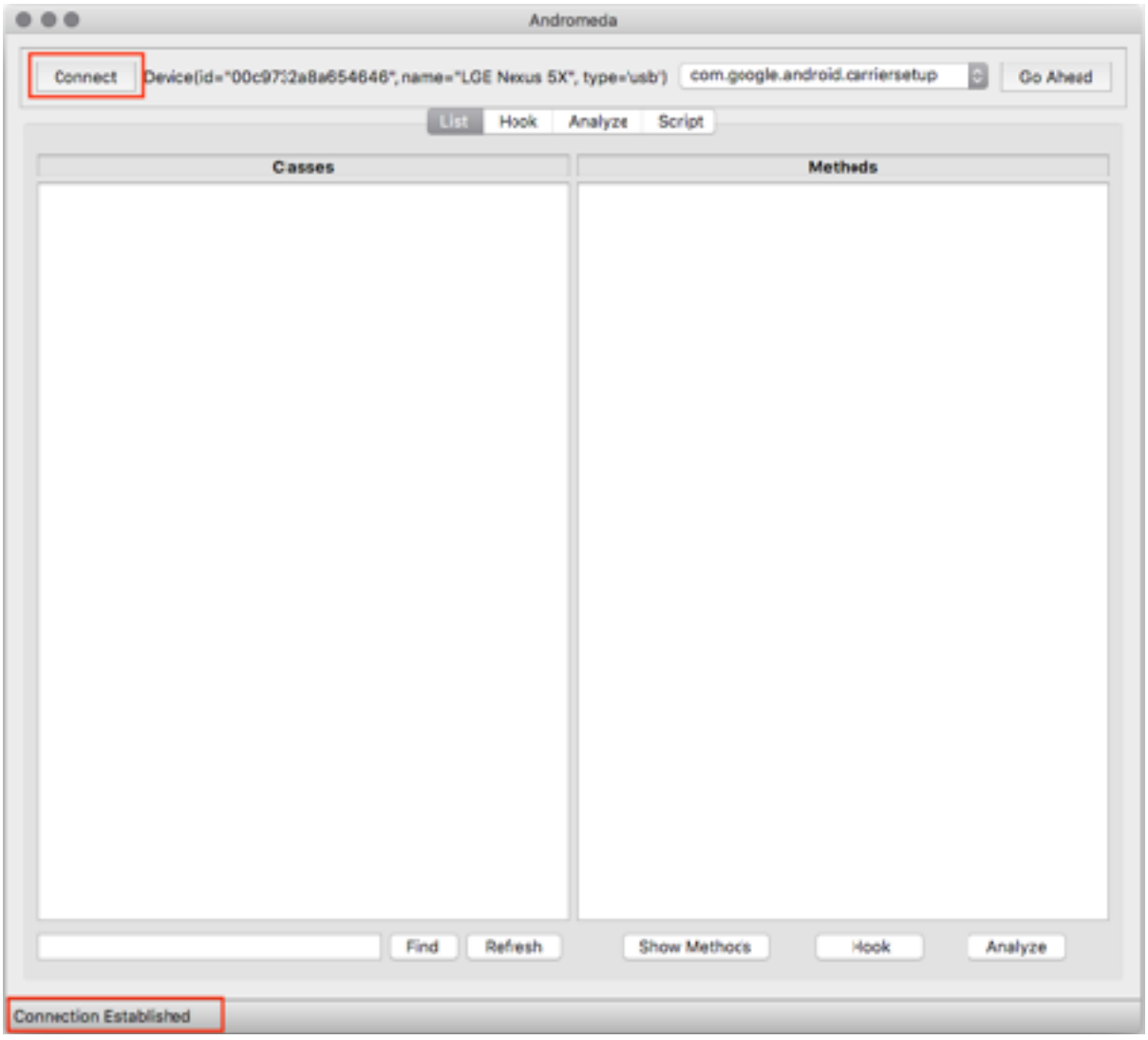
Features :

1. Ease Of Use
2. Classes Enumeration
3. Methods Enumeration
4. Hooking
5. Memory Analysis
6. Menus for saving and editing project. (TBD)
7. Add-on : Andromeda Demo App.

Detailed Description

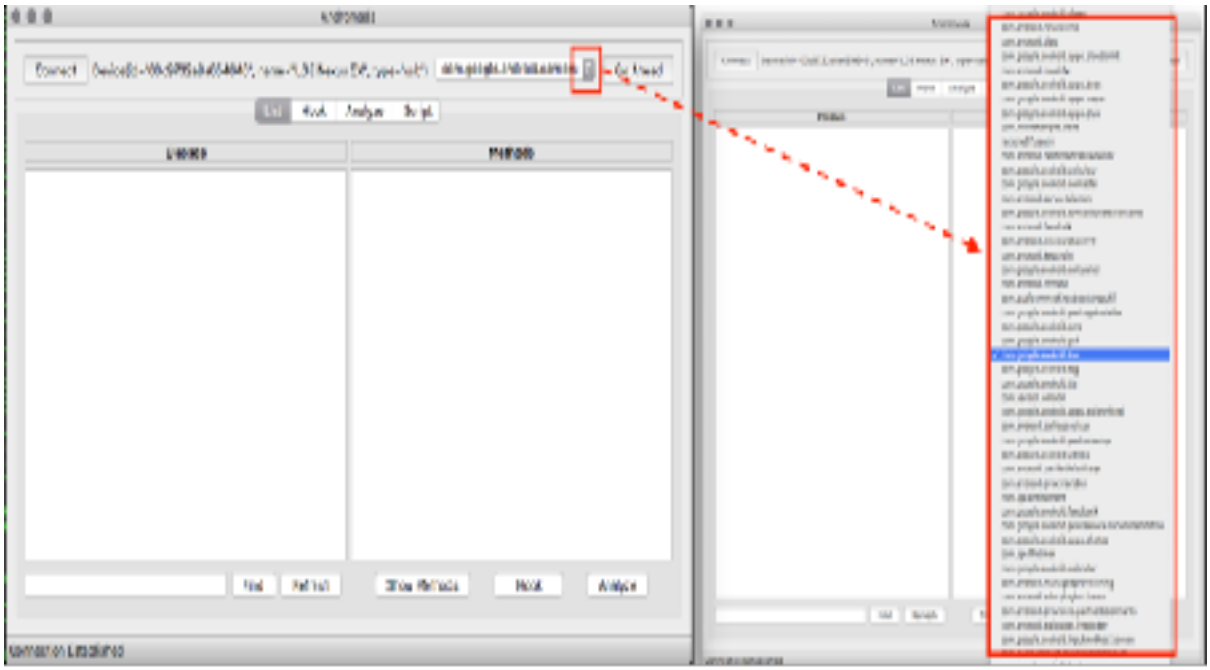
1. **Ease Of Use**

    - Andromeda provides a Graphical User Interface(henceforth “GUI”) to achieve every functionality like enumeration, hooking as well as intercepting methods.
    - It auto connects with Android device/emulator with single click using “Connect” button seen in screenshot below.



Andromeda GUI : Starting Layout

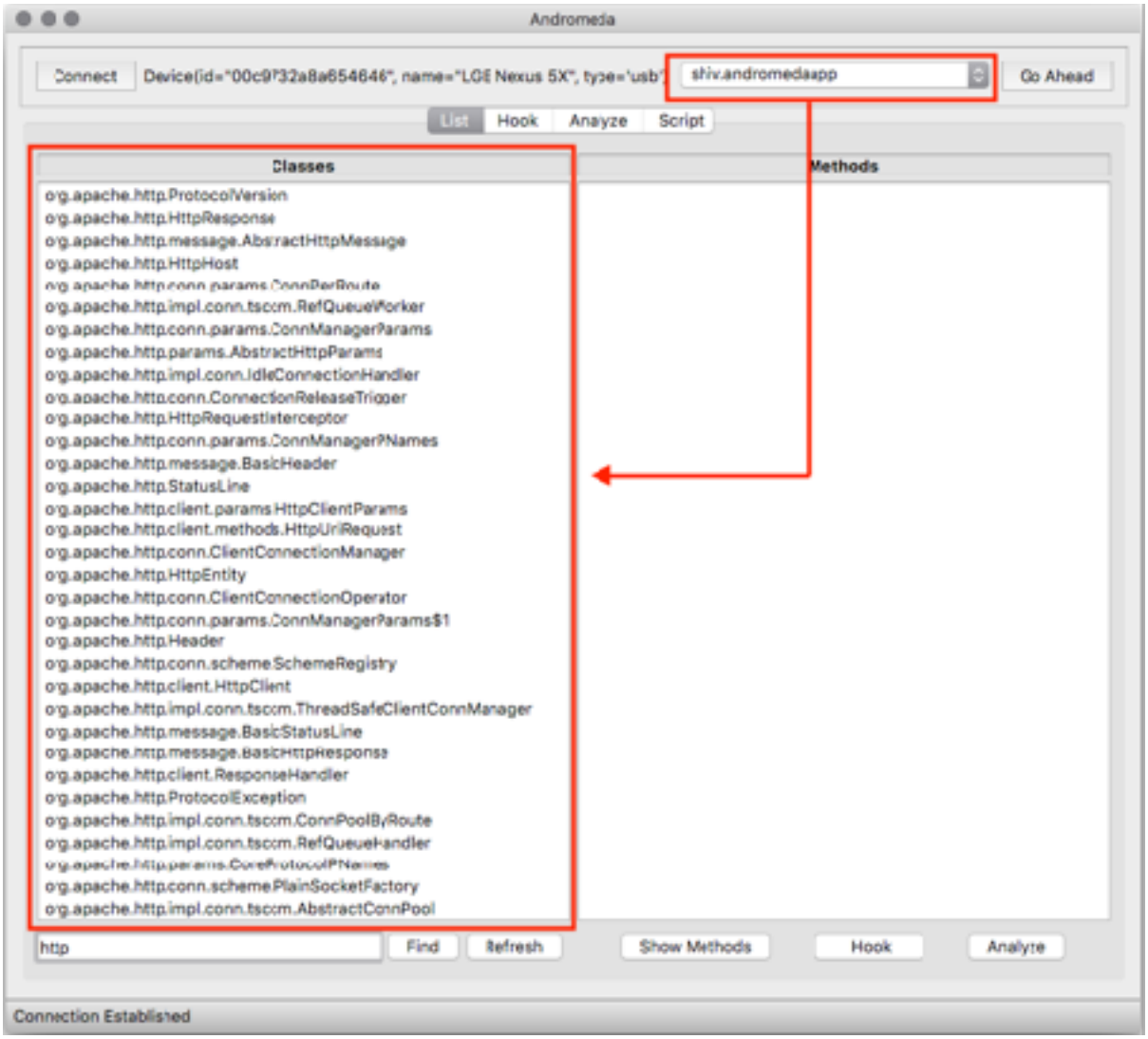
- Upon successful connection, it displays all the package names available on android device/emulator. This makes it easy for researcher/pentester to select app dynamically and proceed with his/her analysis.



Andromeda GUI : Loading Package Names from Device

2. Classes Enumeration

Once the package name is finalized from list provided by Andromeda, one can enumerate all the loaded classes under the package name. Many a times, loaded classes are huge in number and hence Andromeda provides a search feature.

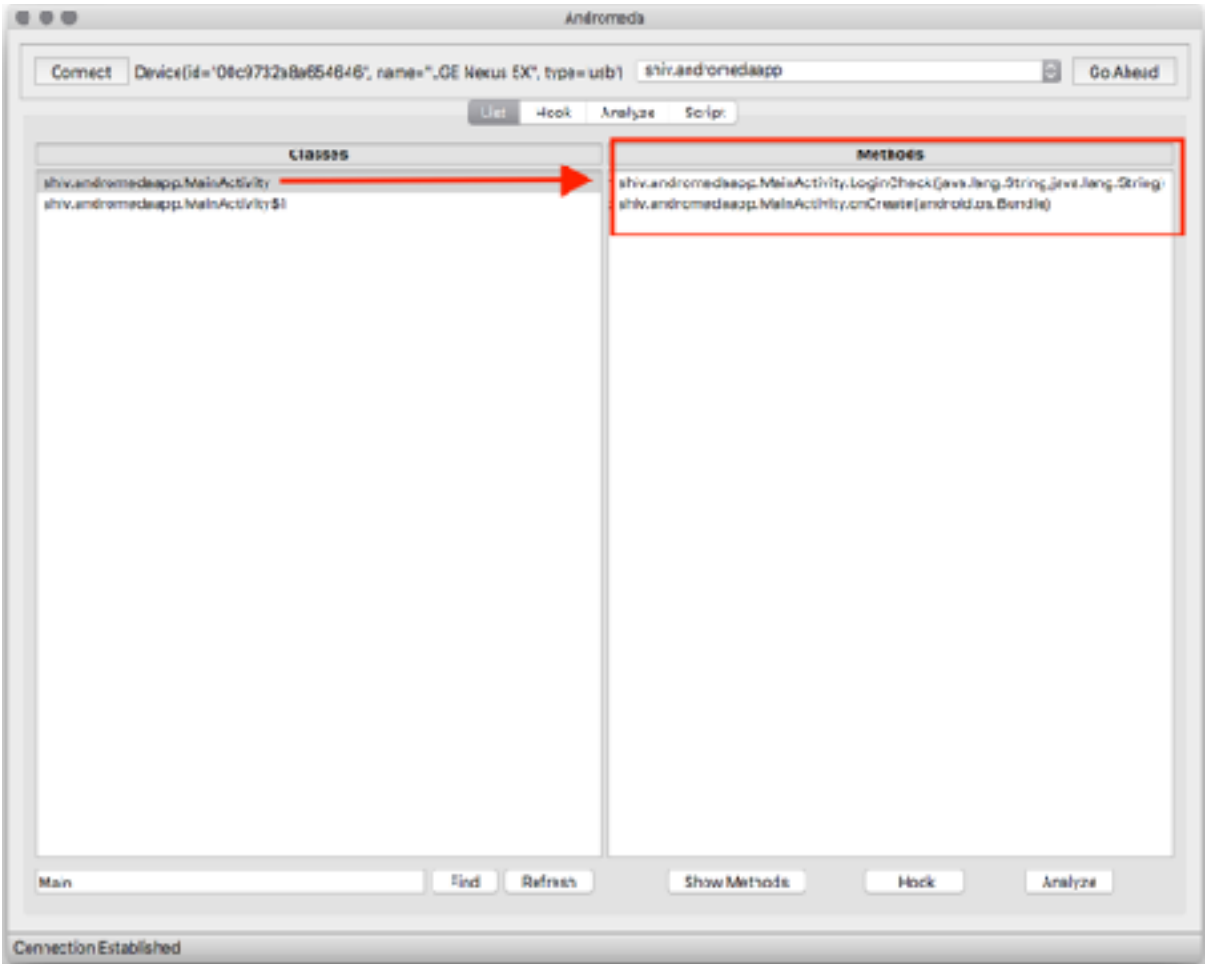


Andromeda GUI : Class Enumeration (Loaded Classes)

With an ease of click, user can easily find the desired class from long list of loaded classes.

3. Method Enumeration

Andromeda provides a simple functionality to enumerate methods under any specific loaded class. Screenshot below shows the list of methods found in selected class.

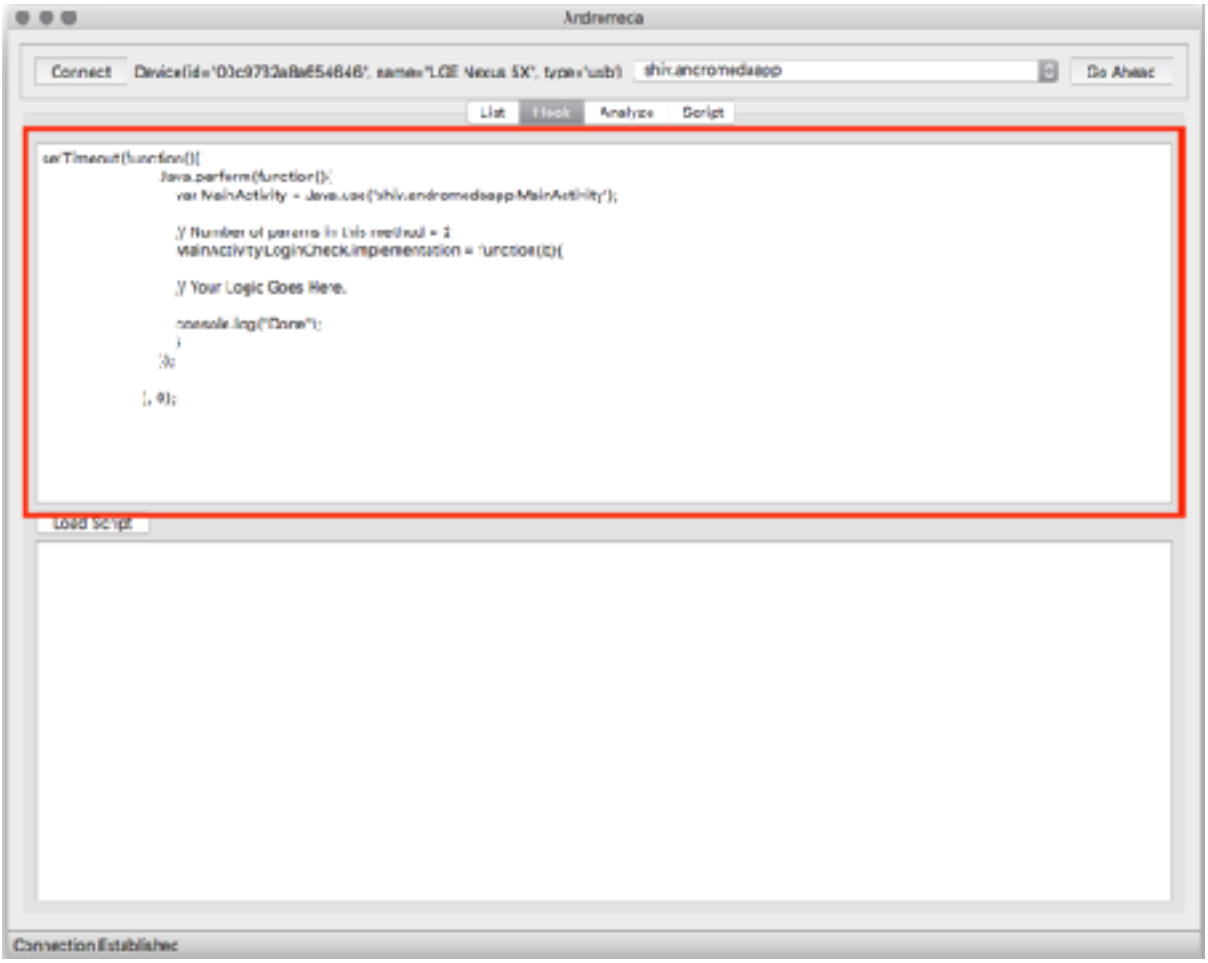


Andromeda GUI : Method Enumeration (Loaded Methods)

As seen above, *MainActivity* loads two methods named *onCreate* and *LogicCheck.* User can select the desired method and hooking is just a click away. He/She have to select the method for hooking and go ahead with *Hook* button provided in GUI. Andromeda will generate Javascript based on selected methods and required parameters.

4. Hooking

Next tab in Andromeda, allows user to work with dynamically generated custom javascript snippet. The snippet is designed according to selected method and required parameters.



Andromeda GUI : Auto-generated Javascript snippet

As seen in screenshot above, user selects *LoginCheck* method to be hooked and Andromeda prepares javascript template with desired syntax.

Depending on the logic implemented in method, user can play around with logic as well as intercept parameters dynamically.

5. **Memory Analysis (Under-Development)**

    - Memory Tab will be used for memory analysis during runtime using Frida.
    - Currently Andromeda allows user to search for strings in memory during runtime and also allows user to overwrite the string.
    - Andromeda will give functionalities to play around with memory addresses, find strings in memory dump, find patterns in dumps, etc.
    - (Other features will be added during development)

Refer Video for functionality in action
https://www.youtube.com/watch?v=wS4B5H97rz4

Tool is still in development phase and lots of new feature will be added

Thank You