

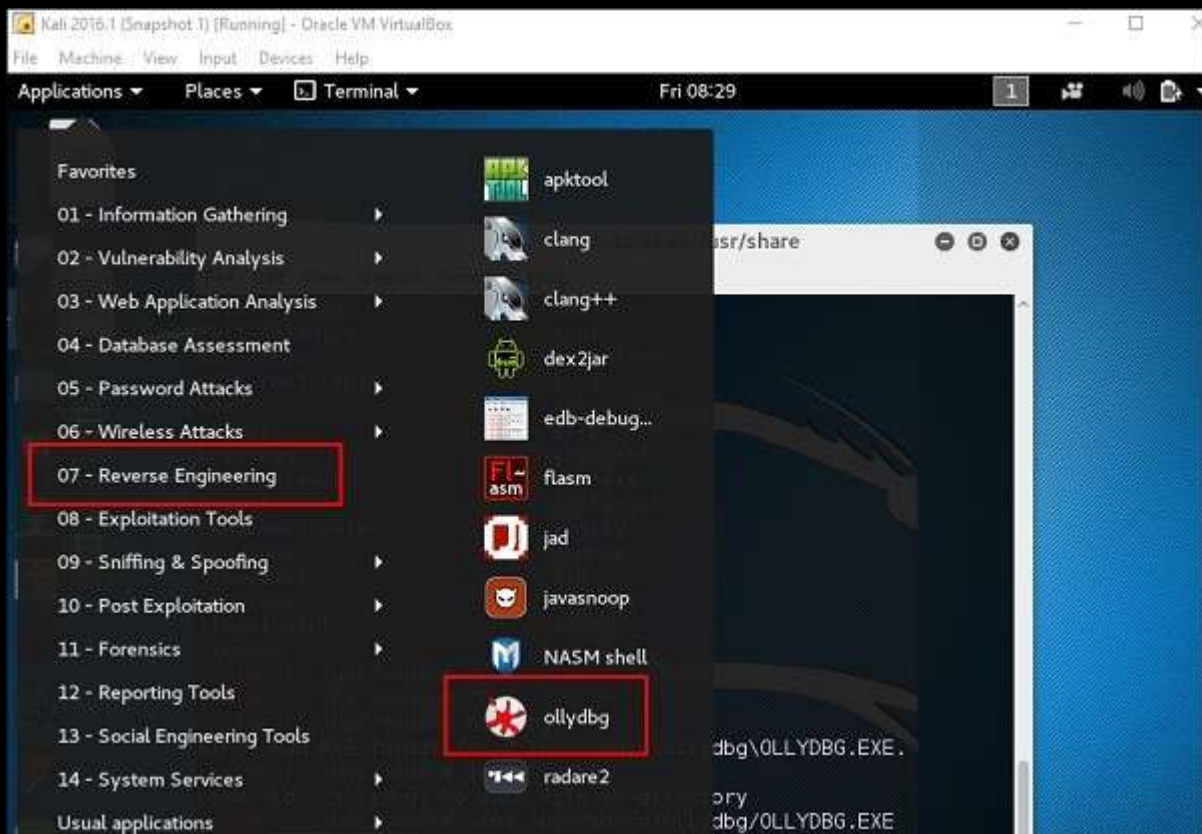
# Reverse Engineering

In this topic, we will learn about the reverse engineering tools of Kali Linux.

## OllyDbg

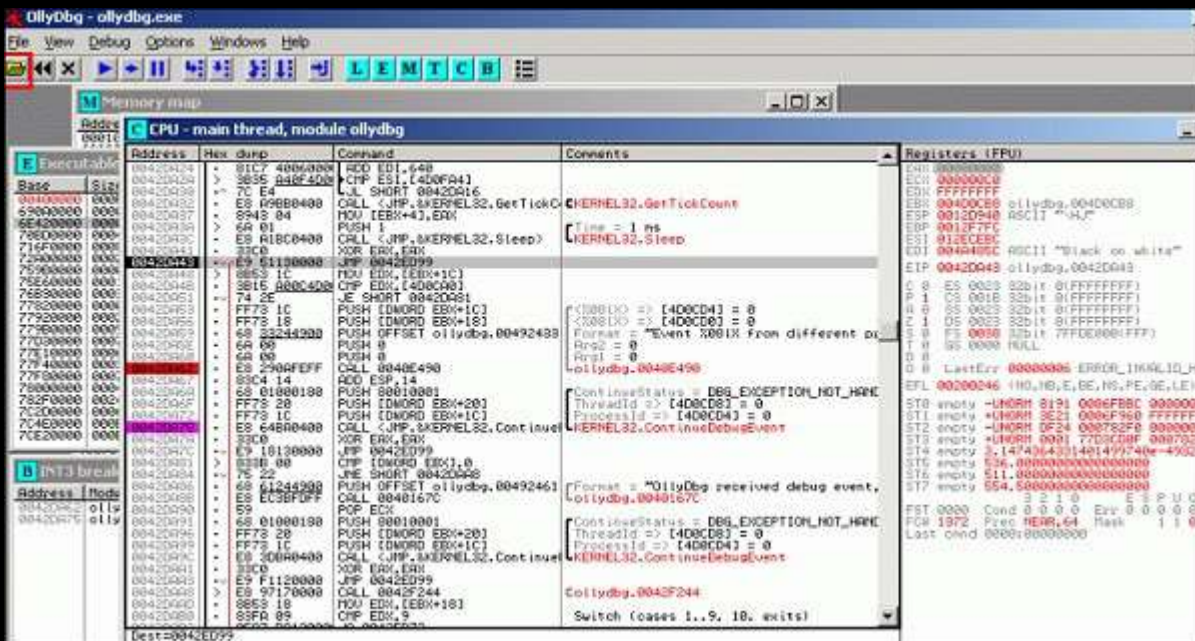
OllyDbg is a 32-bit assembler level analyzing debugger for Microsoft Windows applications. Emphasis on binary code analysis makes it particularly useful in cases where the source is unavailable. Generally, it is used to crack the commercial softwares.

To open it, go to Applications → Reverse Engineering → ollydbg



To load a EXE file, go the “Opening folder” in yellow color, which is shown in a red square in the above screenshot.

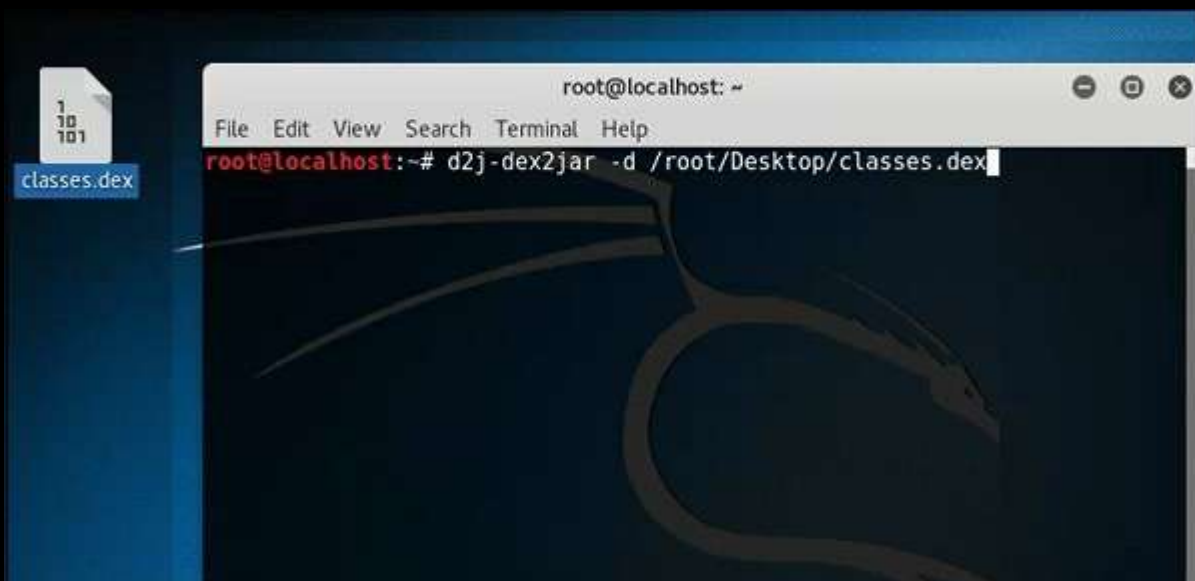
After loading, you will have the following view where you can change the binaries.



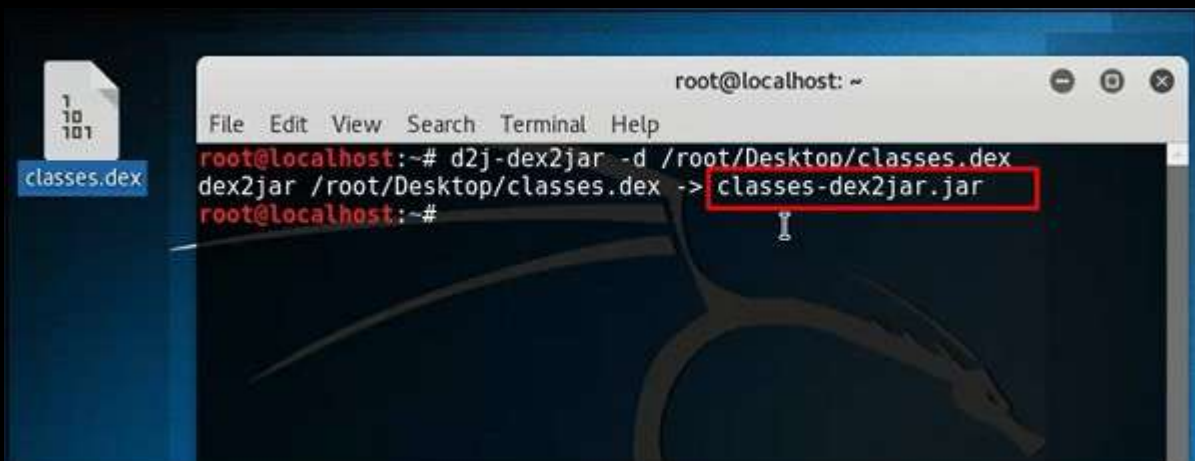
## dex2jar

This is an application that helps convert APK file (android) to JAR file in order to view the source code. To use it, open the terminal and write "d2j-dex2jar -d /file location".

In this case, the file is "classes.dex" on the desktop.




The following line shows that a JAR file has been created.



## jd-gui

JD-GUI is a standalone graphical utility that displays Java source codes of “.class” files. You can browse the reconstructed source code. In this case, we can reconstruct the file that we extracted from the dex2jar tool.

To launch it, open the terminal and write “**jd-gui**” and the following view will open.

To import the file, click the open folder  icon on the left upper corner and then import the file.



## apktool

Apktool is one of the best tools to reverse the whole android application. It can decode resources to nearly an original form and rebuild them after making modifications.

To open it, go to the terminal and write “**apktool**”.

To decompile a apk file, write “apktool d **apk file**”.

```
:/usr/share/apktool# apktool d [REDACTED].apk
```

Decompilation will start as shown in the following screenshot.

```
I: Using Apktool 2.0.0-RC4 on [REDACTED].apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
█
```