

iAppliScan – User Manual

Pre-requisites:

- Java run time - <http://www.oracle.com/technetwork/java/javase/downloads/index.html>
- iAppliScan - <http://blueinfy.com/#iAppliScan>

There are two versions of iAppliScan. Check the java version of your machine before downloading iAppliScan. Java version can be checked by “java version” command.

Get the 32 bit version if version shows 32 bit

```
C:\>java -version  
  
java version "1.6.0_35"  
  
Java(TM) SE Runtime Environment (build 1.6.0_35-b10)  
  
Java HotSpot(TM) Client VM (build 20.10-b01, mixed mode, sharing)
```

Get the 64 bit version if version shows 64 bit

```
C:\>java -version  
  
java version "1.6.0_24"  
  
Java(TM) SE Runtime Environment (build 1.6.0_24-b07)  
  
Java HotSpot(TM) 64-Bit Server VM (build 19.1-b02, mixed mode)
```

Overview of iAppliScan

Amongst the mobile attack vectors and security weakness, Local storage and its misuse is being considered as the key security concern from security and privacy standpoint. Unlike android, iOS does not provide any API to monitor file system directly. One needs to dig in to files/directories to find information stored in local storage across applications. Looking at the each file in the directory is a tedious and painful job while doing penetration testing of the target application. We need to have a simple utility to penetrate and analyze local storage in iOS platform. iAppliScan allows you to automate iOS application review. Current version of iAppliScan needs a jailbroken device with SSH access to interface. Device and iAppliScan needs to be in same network with access. Some of the interesting features of iAppliScan which one can leverage during the testing of the application-

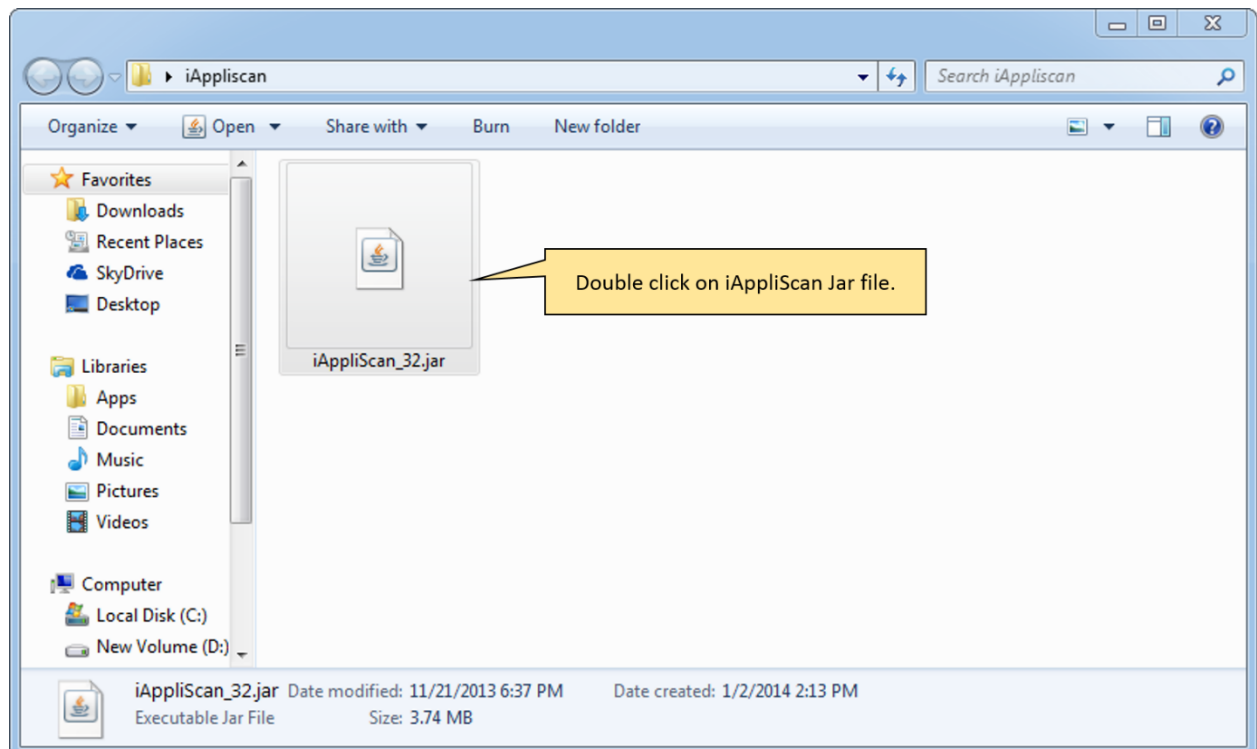
- Look for sensitive information in files/directories
- Find whether particular file exist or not
- Download file for further analysis
- Run external command

iAppliScan lets you automate the review of the iOS application with passing few parameters. It gives pointers to possible vulnerabilities or weakness of the application.

iAppliScan have wizard driven configuration which allows user to provide all possible options to run the tool. The current version of iAppliScan requires jailbroken device. This document will guide you on step by step on how to run and analyze results using iAppliScan.

Running iAppliScan

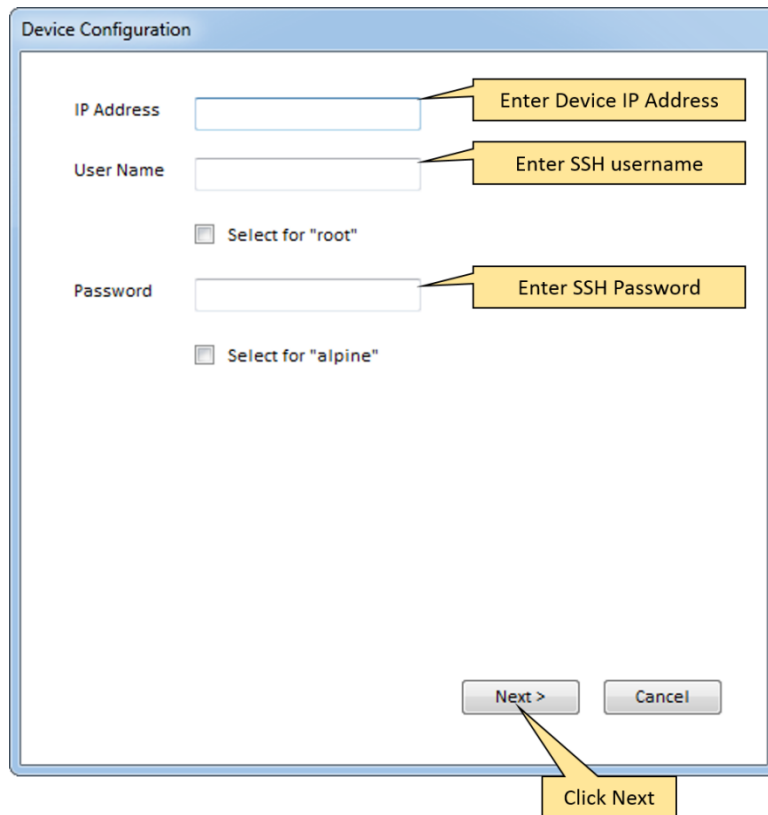
- Extract the zip file
- Double click on the JAR file



Note: Make sure the machine running iAppliScan and iDevice are in the same network.

Device Configuration

The first screen you will see on launching iAppliScan. This screen takes IP address, username and password to connect to iDevice.



The image shows a 'Device Configuration' dialog box with the following fields and options:

- IP Address:** A text input field with a callout bubble saying 'Enter Device IP Address'.
- User Name:** A text input field with a callout bubble saying 'Enter SSH username'.
- Select for "root":** A checkbox.
- Password:** A text input field with a callout bubble saying 'Enter SSH Password'.
- Select for "alpine":** A checkbox.
- Next >** and **Cancel** buttons at the bottom right.
- A callout bubble pointing to the 'Next >' button says 'Click Next'.

Note: Check the boxes to use "root" as username and "alpine" as password.

iAppliScan will connect to the device and get the list of installed application on clicking "Next"

Application Configuration

The screen allows you to select the application to be reviewed and prompts to select location where files can be downloaded.

The screenshot shows a dialog box titled "Application Configuration". It contains two main sections: "Select Application" and "Select Download Path".

- The "Select Application" section has a dropdown menu currently showing "DealSearch". A callout box points to this dropdown with the text: "Select application from list for analysis".
- The "Select Download Path" section has a text box containing the path "C:\Users\Laptop-7\Desktop\temp". To the right of the text box is a button with three dots "...". A callout box points to this button with the text: "Select path for the download directory where the files will be downloaded".
- At the bottom of the dialog box are three buttons: "< Back", "Next >", and "Cancel". A callout box points to the "Next >" button with the text: "Click Next".

Clicking next will take to the "Search within Files" configuration.

Search Within Files

Most application stores information in the local storage. To look for what information is stored in the local storage, one needs to provide list of the keywords which will be used while exploring different functionality of the application. This screen will give options to search keywords in selected application. There are three ways to supply keywords to iAppliScan

- Manual – User can add keywords (each keyword in new line)
- Load from File – User can load a file which contains list of keywords (each keyword in new line)
- Default – User can search for the default list of keywords

All three options can be used together. The following screen shows the options.

The screenshot shows a dialog box titled "Search Within Files". It contains three sections, each with a checkbox and a text area:

- ☒ **Enter Manual**: The text area contains "Virat", "Rohit", and "Test". A callout points to this area: "Enter keyword which needs to be searched with in application data".
- ☐ **Load from file**: The text area is empty. A callout points to this area: "Select file with new line separated keywords which needs to be searched with in application data".
- ☒ **Default**: The text area contains "username" and "password". A callout points to this area: "Check 'Default' checkbox to search default keywords with in application data".

At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel". A callout points to the "Next >" button: "Click Next".

Click on next for "Look for Files" screen

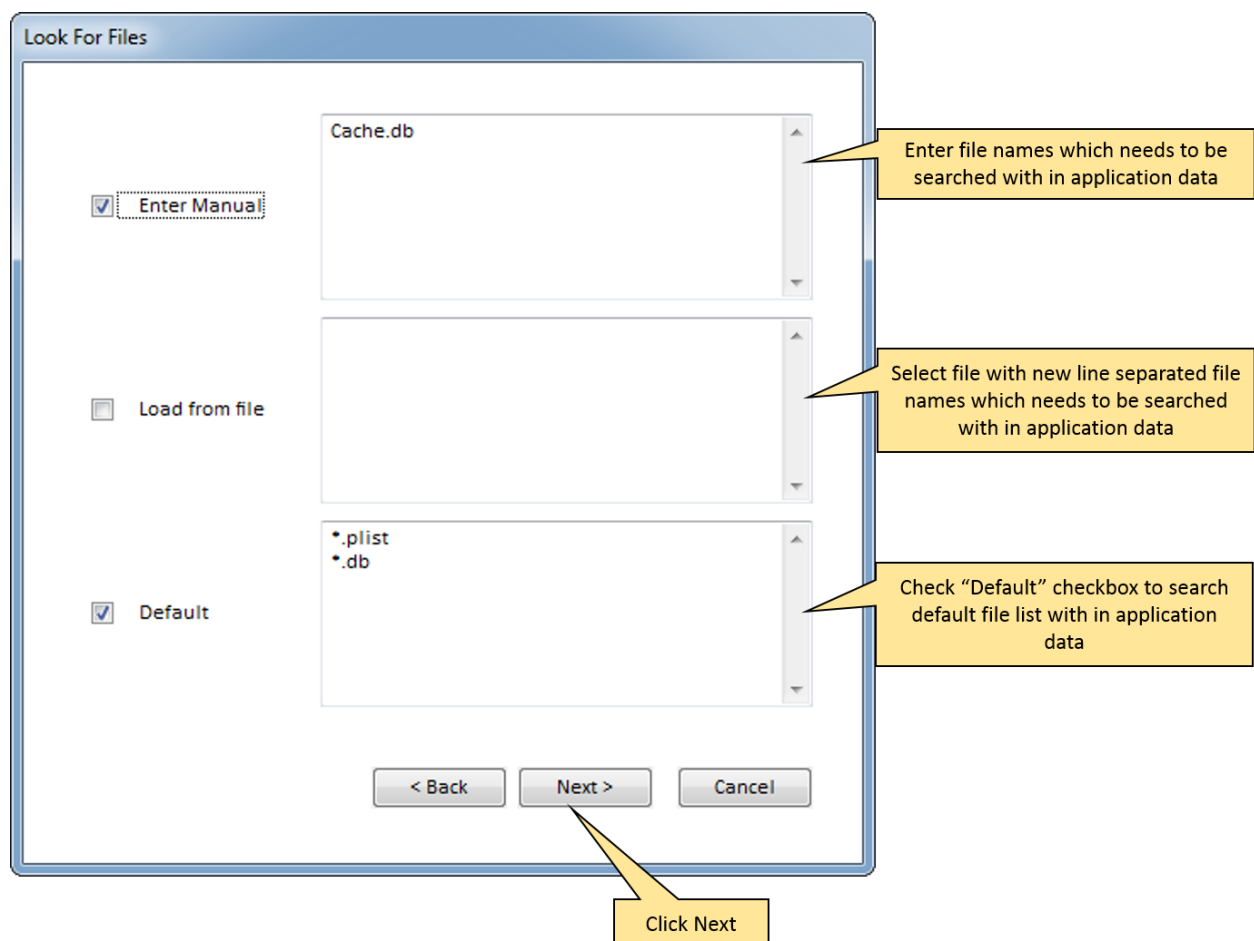
Search Files within Selected Application

Another set of attack on mobile is the information in different files i.e. cache.db or information in plist file. The same functionality can be utilized to find out whether particular type of file exist in the application i.e. *.txt, *.png. The “Look for files” allows regular expression based search in application directory and finds the path of the application where particular file has been located.

There are three ways to supply keywords to iAppliScan

- Manual – User can add keywords (each keyword in new line)
- Load from File – User can load a file which contains list of keywords (each keyword in new line)
- Default – User can search for the default list of keywords

All three options can be used together. The following screen shows the options.



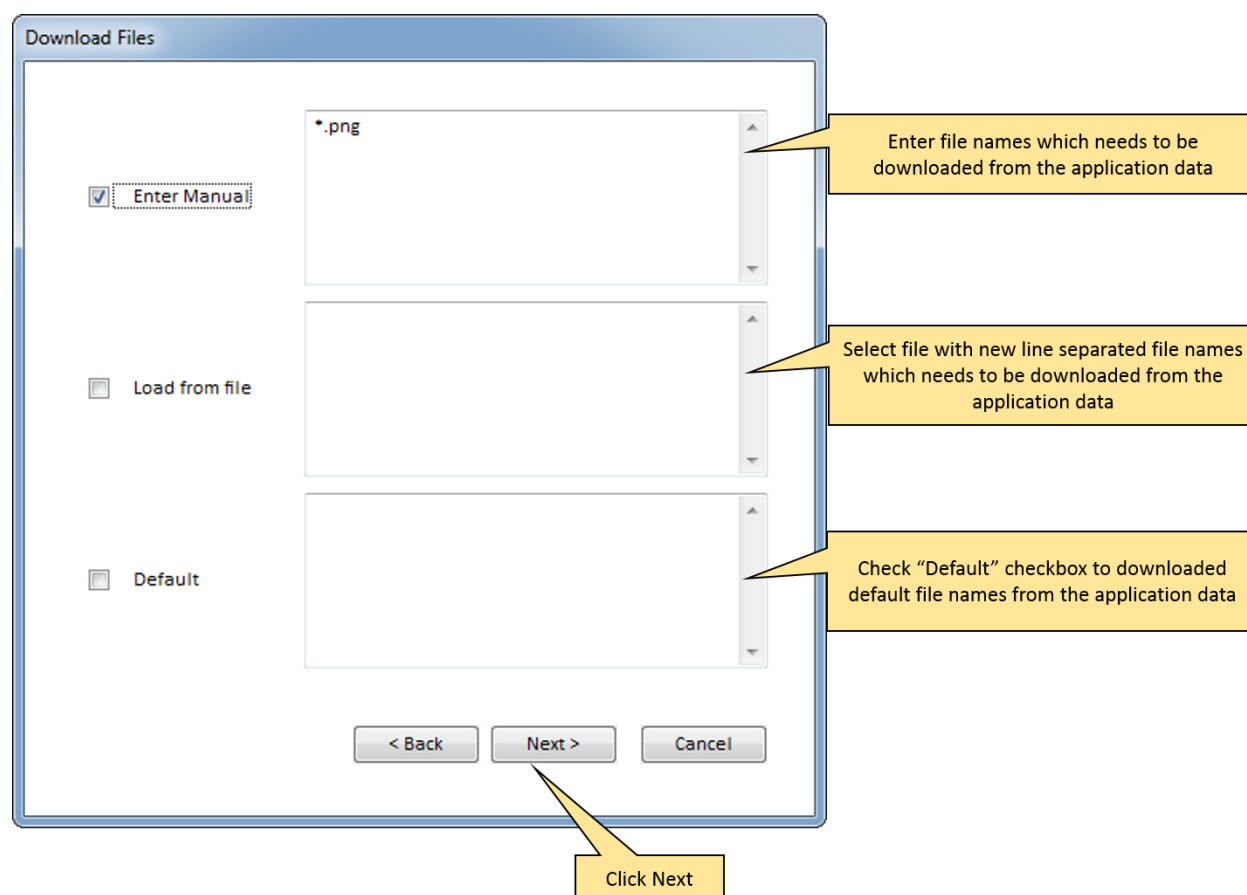
Download Files from the Selected Application

During the penetration testing, only information exist is not enough or the file exist is not enough to report. One need to verify the file i.e. the application can be storing the screenshot.png in the local storage but this screenshot can be blank screenshot. The download file feature allows you to download the files from the iDevice for further analysis.

There are three ways to supply keywords to iAppliScan

- Manual – User can add keywords (each keyword in new line)
- Load from File – User can load a file which contains list of keywords (each keyword in new line)
- Default – User can search for the default list of keywords

All three options can be used together. The following screen shows the options.



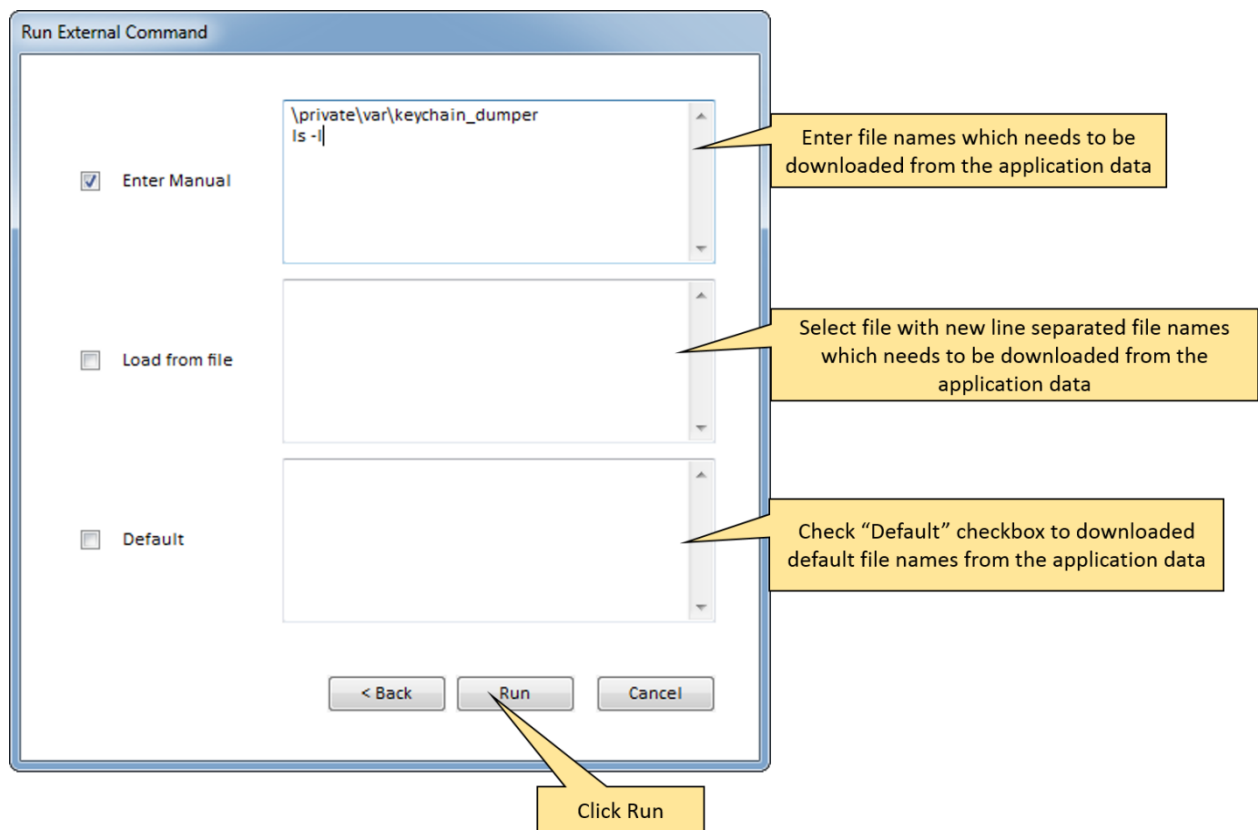
Run External Commands in Connected device

There is always a possibility that one wants to run his custom script or other available scripts i.e. keychain_dumper. The Run External command feature allows you to run any third party binary. It assumes that binary exist in the iDevice. User needs to specify complete path along with the command options to run the binary. The binary output will be displayed in the results pane.

There are three ways to supply keywords to iAppliScan

- Manual – User can add keywords (each keyword in new line)
- Load from File – User can load a file which contains list of keywords (each keyword in new line)
- Default – User can search for the default list of keywords

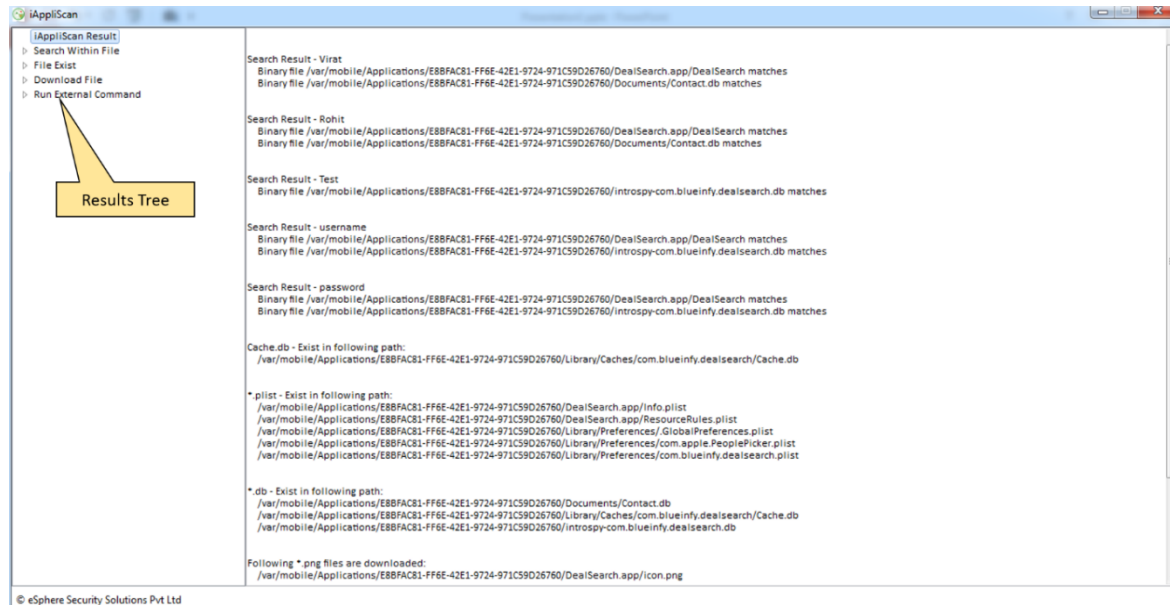
All three options can be used together. The following screen shows the options.



Clicking on "Run" will initiate the testing and display the output in the results pane as shown below.

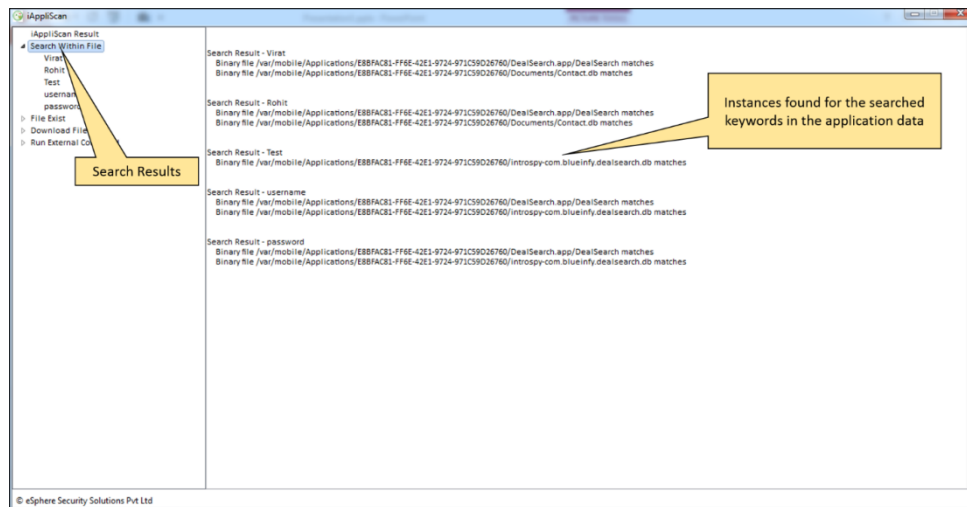
Result Pane

Result pane is divided in to two part. Left part is result tree which shows the list of the findings, right pane shows the detail about the findings. Clicking on Category will display finding results of the particular category.



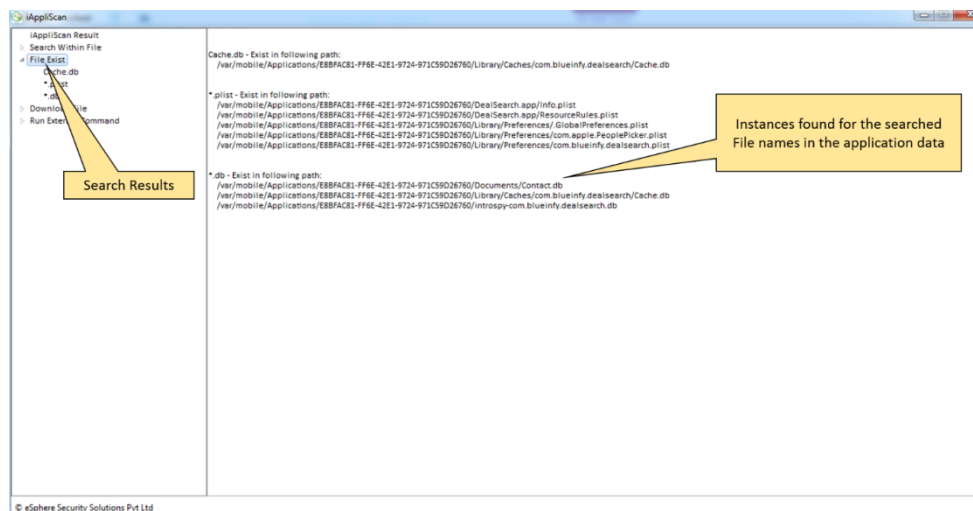
Application Scanning Results – Search within Files

Clicking on “Search Within Files” displays the result -



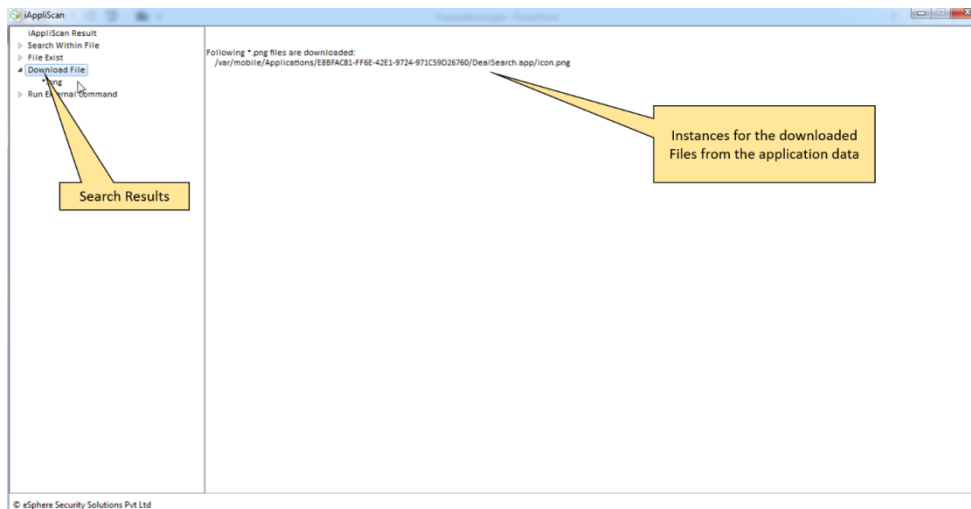
Application Scanning Results – File Exist

Clicking on “File Exist” displays the result -



Application Scanning Results - Download Files

Clicking on "Download Files" displays the result -



Application Scanning Results - Run External Command

Clicking on "Run External Command" displays the result -

