



Cyber Security and Forensics - I

05201296

Prof. Dipak L. Agrawal, Assistant Professor
Faculty of IT & Computer Science





CHAPTER-9

Introduction to kali linux / Santoku



Topics

- Digital Forensics Tools : Autopsy,
- Mobile forensics: (ADB) DIVA.apk





Digital Forensics Tools : Autopsy,

- Autopsy is one of the digital forensics tools use to investigate what happened on a computer. It offers a GUI access to variety of investigative command-line tools from The Sleuth Kit including image file hashing, deleted file recovery, file analysis and case management. Autopsy produces results in real time, making it more compatible over other forensics tools.



Autopsy

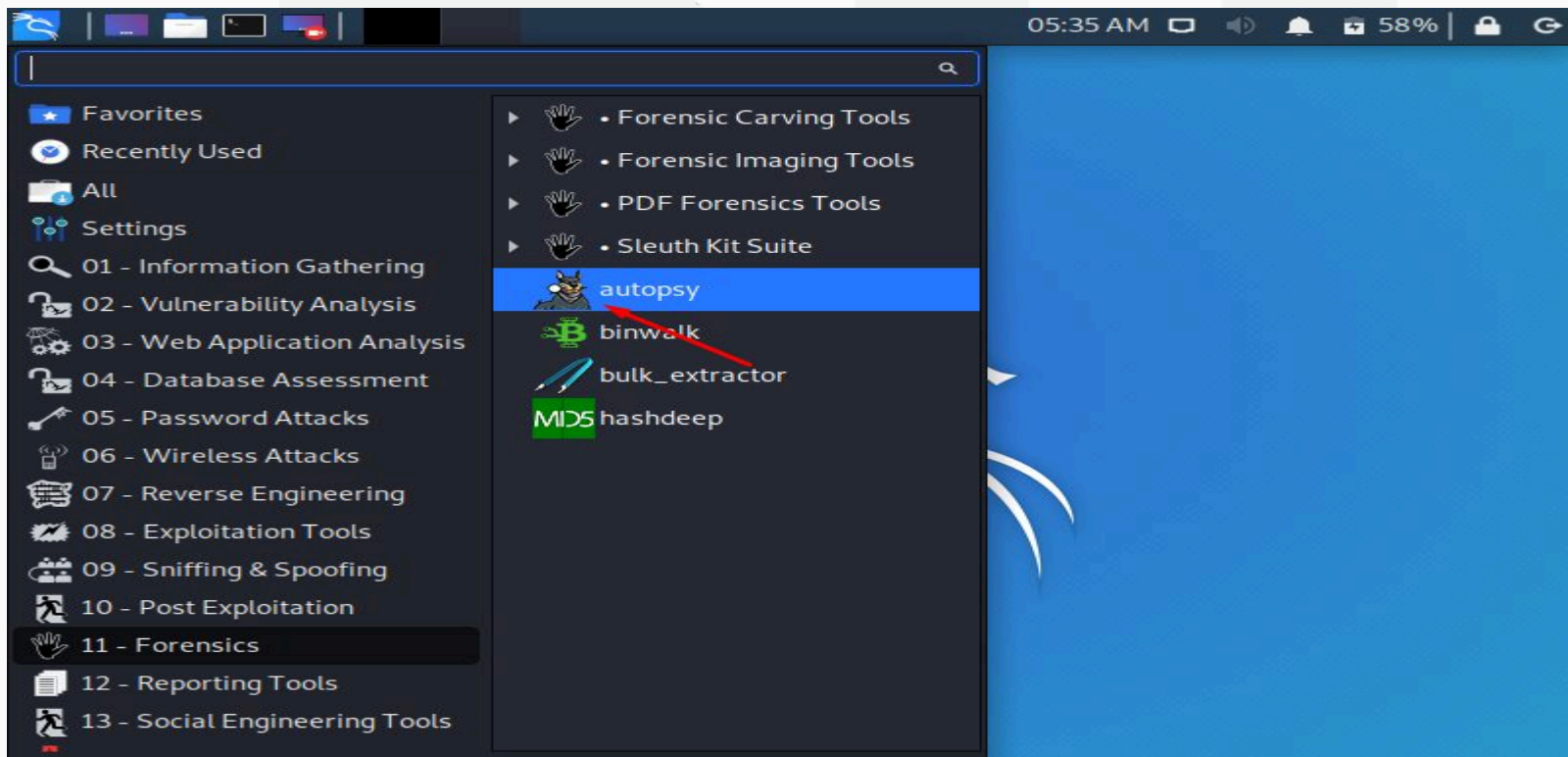
- It comes preinstalled in kali linux so Lets start the Kali Virtual Machine. You will find the option 'forensics' in the application tab. Select 'autopsy' from the list of forensics tools..





Autopsy

- Open Autopysy





Autopsy

- When you select autopsy, it will open a prompt where you see a program information, the version number listed as 2.24 with the path to the Evidence Locker folder as /var/lib/autopsy and an address `http://localhost:9999/autopsy` to open it on a web browser.

A screenshot of a terminal window titled "Shell No.1". The window displays the Autopsy Forensic Browser interface. It shows the version number 2.24 and the path to the Evidence Locker folder as /var/lib/autopsy. It also displays the start time, remote host, and local port. A URL is highlighted in a red box, and a prompt is shown at the bottom.

```
Shell No.1
File Actions Edit View Help
Shell No.1
-----
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
-----
Evidence Locker: /var/lib/autopsy
Start Time: Mon Feb 10 05:38:14 2020
Remote Host: localhost
Local Port: 9999
Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy
Keep this process running and use <ctrl-c> to exit
```

Autopsy

- Click on that link and open it in your Kali web browser, you will be redirected to the home page of autopsy. This tool is running on our local web server accessing the port 9999.





Autopsy

- Create a New Case
- There will be three options on the home page: 'OPEN CASE', 'NEW CASE', 'HELP'
- For forensic investigation, we need to create a new case and arrange all the information and evidences. Select 'NEW CASE'



Autopsy

- It will direct you to a page where you have been asked to add case name, description and investigator names. Note that you can add more than one investigator name because in these scenarios usually a team of forensic investigators work on a single case.

1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.

2. Description: An optional, one line description of this case.
3. Investigator Names: The optional names (with no spaces) of the investigators for this case.

a.	<input type="text" value="ehacking"/>	b.	<input type="text"/>
c.	<input type="text"/>	d.	<input type="text"/>
e.	<input type="text"/>	f.	<input type="text"/>
g.	<input type="text"/>	h.	<input type="text"/>
i.	<input type="text"/>	j.	<input type="text"/>

Autopsy

- After adding all the required information, select 'NEW CASE'

3. Investigator Names: The optional names (with no spaces) of the investigators for this case.

a. <input type="text" value="ehacking"/>	b. <input type="text"/>
c. <input type="text"/>	d. <input type="text"/>
e. <input type="text"/>	f. <input type="text"/>
g. <input type="text"/>	h. <input type="text"/>
i. <input type="text"/>	j. <input type="text"/>

NEW CASE **CANCEL** **HELP**

Autopsy

- This simply showing us the name of the case, the destination where it will be stored i.e. `/var/lib/autopsy/case01/`, and the destination where its configuration file will be stored i.e. `/var/lib/autopsy/case01/case.aut`
- Select 'ADD HOST' option below.

Creating Case: case01

Case directory (`/var/lib/autopsy/case01/`) created
Configuration file (`/var/lib/autopsy/case01/case.aut`) created

We must now create a host for this case.

Please select your name from the list:

ADD HOST



Autopsy

- Now you will be asked to enter the name of the computer you are investigating and the description of the investigation. After that it will ask you the time zone (leaving it blank will select the default setting), timeskew adjustments means a value in seconds to compensate for differences in time, path of alert hash means a path to the created database of bad hashes and a path of ignore hash database means specifying a path to the database of good hashes. Select 'ADD HOST' to continue.



Autopsy

Case: case01

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the



Autopsy

times.

GMT

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

ADD HOST CANCEL HELP



Autopsy

- Select 'ADD IMAGE' here.

Adding host: host1 to case case01

Host Directory (/var/lib/autopsy/case01/host1/) created

Configuration file (/var/lib/autopsy/case01/host1/host.aut) created

We must now import an image file for this host

ADD IMAGE



Autopsy

- Creating a Image File
- We need to import an image file of the system we want to investigate. Creating this image file is the first step of forensic investigation. The reason for doing this is analysis cannot be conducting on an original storage device. A disk Image can be defined as a file that stores the contents and structure of a data storage device such as a hard drive, CD drive, phone, tablet, RAM, or USB. This image file can be taken locally or remotely.
- There are several ways to get the image file. You can get this by different tools such as FTK imager or guymager. Or you can use CLI to acquire your image by using dd (disk-to-disk) command:
- # dd if=/dev/sda of=ehacking.img
- Where /dev/sda is the source and ehacking.img is the destination file.

Autopsy

- Once you get an image file, select 'ADD IMAGE' option here.

Case: case01
Host: host1

No images have been added to this host yet

Select the Add Image File button below to add one

ADD IMAGE FILE

CLOSE HOST

HELP

FILE ACTIVITY TIME LINES

IMAGE INTEGRITY

HASH DATABASES

VIEW NOTES

EVENT SEQUENCER

Autopsy

- Import the image to autopsy by specifying the location of the file and selecting the type whether it is Disk or Partition.
- Select the import method 'Copy' to copy it into the evidence locker and click on 'NEXT'.

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

2. Type
Please select if this image file is for a disk or a single partition.

☐ Disk ☒ Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

☐ Symlink ☒ Copy ☐ Move

NEXT



Autopsy

- To maintain the integrity of the image file we must calculate its Hash value. It is important to calculate the Hash so that we may be able to prove that the file has not been tampered.

Local Name: images/ehacking.img

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

- ☐ Ignore the hash value for this image.
- ☒ Calculate the hash value for this image.
- ☐ Add the following MD5 hash value for this image:

☐ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: fat12)

Mount Point:

File System Type:



Autopsy

- This showing the hash value of the image file and links the image into the evidence locker. Select ok to continue.

Calculating MD5 (this could take a while)

Current MD5: **BC1230A794439D0F5A24AF2FCF2CF48C**

Testing partitions

Copying image(s) into evidence locker (this could take a little while)

Image file added with ID `img2`

Volume image (0 to 0 - fat12 - C:) added with ID `vol2`

OK

ADD IMAGE


Autopsy

The Case Management Prompt

Now we have successfully imported the file for investigation. Let's check the integrity by selecting an option 'IMAGE INTEGRITY'.

Case: case01
Host: host1

Select a volume to analyze or add a new image file.

The interface shows a table with columns 'mount', 'name', and 'fs type'. The first row contains 'C:/' under 'mount', 'ehacking.img-0-0' under 'name', and 'fat12' under 'fs type'. There is a 'details' link to the right of the 'fs type' column. Below the table are buttons for 'ANALYZE', 'ADD IMAGE FILE', 'CLOSE HOST', and 'HELP'. At the bottom, there are buttons for 'FILE ACTIVITY TIME LINES', 'IMAGE INTEGRITY', 'HASH DATABASES', 'VIEW NOTES', and 'EVENT SEQUENCER'.

mount	name	fs type
<input checked="" type="radio"/> C:/	ehacking.img-0-0	fat12

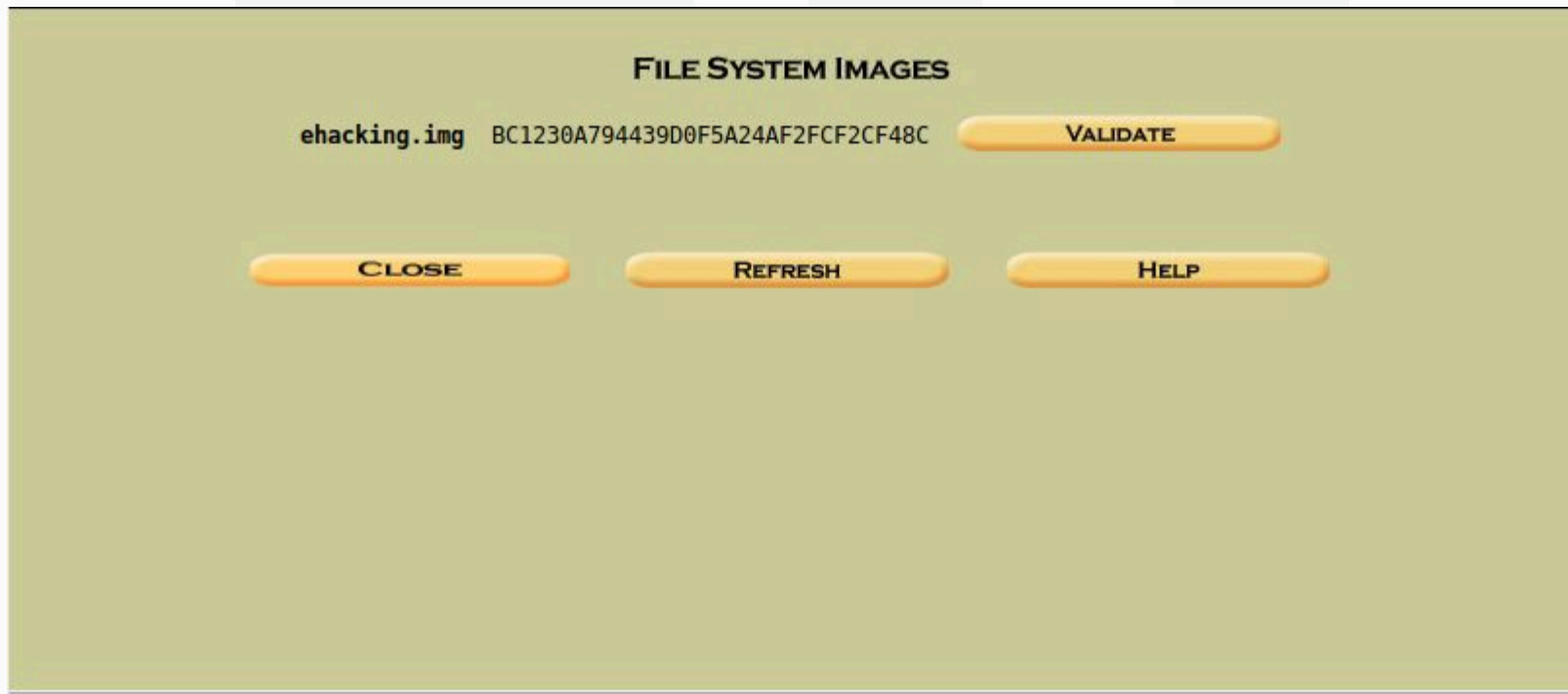
[details](#)

ANALYZE **ADD IMAGE FILE** **CLOSE HOST**
HELP

FILE ACTIVITY TIME LINES **IMAGE INTEGRITY** **HASH DATABASES**
VIEW NOTES **EVENT SEQUENCER**

Autopsy

This showing the name and the hash value of the file. Select 'VALIDATE'.



Autopsy

The validation is successful, displaying the same MD5 hashes in the bottom.

Original MD5: BC1230A794439D0F5A24AF2FCF2CF48C

Current MD5: BC1230A794439D0F5A24AF2FCF2CF48C

Pass



DIVA

- # DIVA Android App — Walkthrough

Diva



Welcome to DIVA!

DIVA (Damn insecure and vulnerable App) is an App intentionally designed to be insecure. The aim of the App is to teach developers/QA/security professionals, flaws that are generally present in the Apps due poor or insecure coding practices. If you are reading this you want to either learn App pentesting or secure coding and I sincerely hope that DIVA solves your purpose. So, sit back and enjoy the ride.

1. INSECURE LOGGING

2. HARDCODING ISSUES - PART 1

3. INSECURE DATA STORAGE - PART 1

4. INSECURE DATA STORAGE - PART 2

5. INSECURE DATA STORAGE - PART 3

6. INSECURE DATA STORAGE - PART 4

7. INPUT VALIDATION ISSUES - PART 1

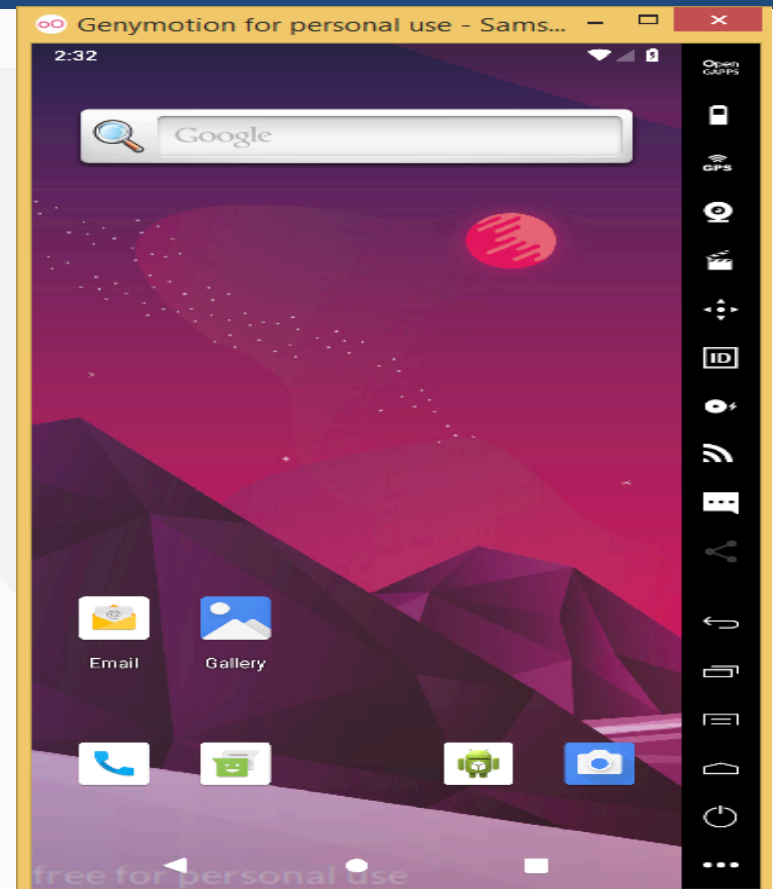
8. INPUT VALIDATION ISSUES - PART 2

9. ACCESS CONTROL ISSUES - PART 1

10. ACCESS CONTROL ISSUES - PART 2

VMWare Windows, Linux

- I have setup Platform Tools in environment variables. If you do not setup you have to place platform tools and apk file in same location or provide full path of their location.
- In order to install the Diva application run the Android Virtual machine.





DIVA

- Either you can Drag and Drop the APK file of DIVA on Android VM or you can install it with Android Debug Bridge (adb). Installation with ADB will be discussed here.
- Open Command Prompt and Navigate to the location of DIVA APK file..

A screenshot of a Windows Command Prompt window. The title bar reads 'C:\Windows\system32\cmd.exe'. The command prompt shows the current directory as 'C:\Users\Solomon\Desktop\Android Labs'. The user has entered the 'dir' command, and the output shows a directory listing. The file 'diva-beta.apk' is highlighted in yellow. The listing shows the file size as 1,502,294 bytes and the directory size as 48,904,261,632 bytes free.

```
C:\Windows\system32\cmd.exe

C:\Users\Solomon\Desktop\Android Labs>dir
Volume in drive C has no label.
Volume Serial Number is 3E95-E173

Directory of C:\Users\Solomon\Desktop\Android Labs

08/23/2020  02:16 PM  <DIR>          .
08/23/2020  02:16 PM  <DIR>          ..
01/02/2016  02:46 PM             1,502,294  diva-beta.apk
               1 File(s)            1,502,294 bytes
               2 Dir(s)  48,904,261,632 bytes free

C:\Users\Solomon\Desktop\Android Labs>
```



DIVA

- adb devices
- This command will show us status of any android device running on our system or not as shown in figure

A screenshot of a Windows command prompt window. The title bar reads 'C:\Windows\system32\cmd.exe'. The command prompt shows the following text:

```
C:\Users\Solomon\Desktop\Android Labs>adb devices
List of devices attached
192.168.219.102:5555    device

C:\Users\Solomon\Desktop\Android Labs>
```



DIVA

- As VM which we started earlier is running, now it's time to install DIVA application.
- You will get success status printed on command line as shown in figure

```
C:\Windows\system32\cmd.exe

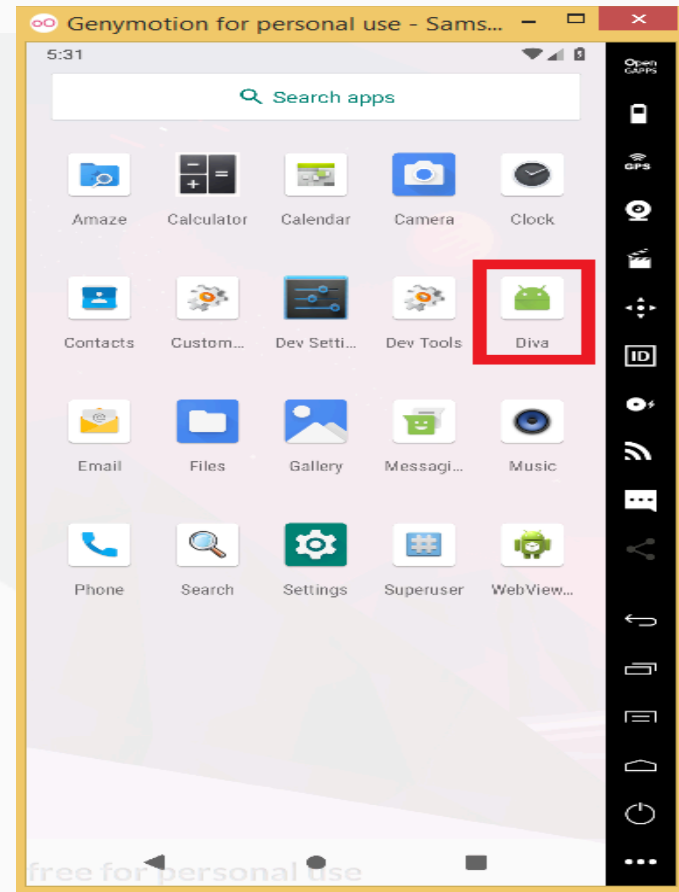
C:\Users\Solomon\Desktop\Android Labs>adb devices
List of devices attached
192.168.219.102:5555    device

C:\Users\Solomon\Desktop\Android Labs>adb install diva-beta.apk
Performing Streamed Install
Success

C:\Users\Solomon\Desktop\Android Labs>
```

DIVA

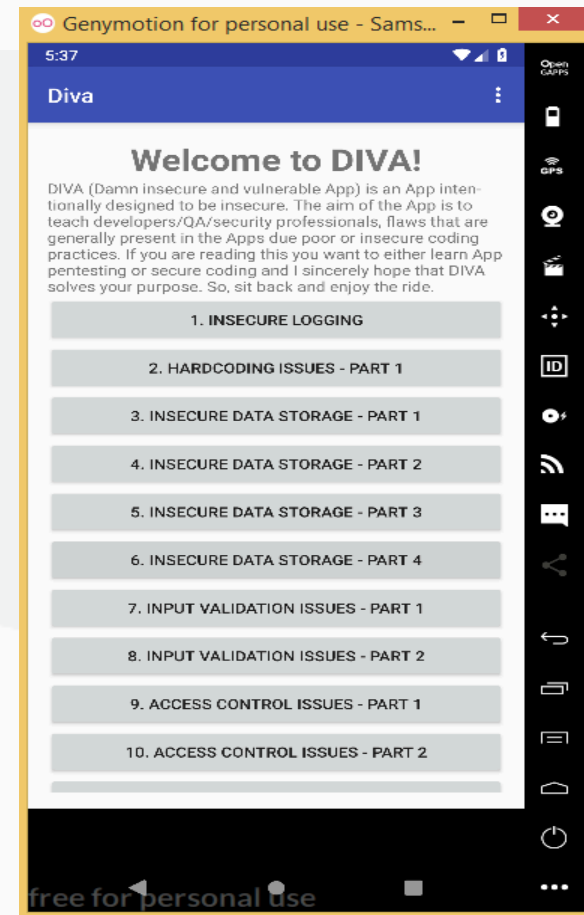
- Icon of DIVA app will also appear on your VM as shown in figure.





DIVA

- Tap (Click) on the DIVA app Icon to launch the application.



× ○ DIGITAL LEARNING CONTENT



Parul[®] University



www.paruluniversity.ac.in

