Windows, Kali Linux and Android Password Cracker

Sucheta Suresh Patil

CS6899|Winter 2017

Department of Computer Networks

California State University, East Bay

Project Advisor

Dr. Levent Ertaul

CONTENT

Introduction

The project is aimed at learning and exploring various techniques that would help to crack passwords or pins of different operating systems. The project also involves exploring new advanced penetration testing Linux distributions like Kali and Santoku. For the scope of this project, I have tried password cracking or skipping for Windows, Kali Linux and Android operating systems. The Report mentions information to get started with using the tools provided by Kali and Santoku Linux. It also mentions brief description of tools like John the Ripper and Hashcat used extensively for this project. Also all screenshots involving installing the operating systems, tool and cracking process are included in report for understanding.

I would like to thank Dr. Levent Ertaul for giving me this opportunity to work on this project and help me in learning new areas of security and penetration testing tools.

1. Steps to install VirtualBox on Ubuntu

Following are the steps used to install VirtualBox on a server running Ubuntu as its operation system.

VirtualBox version: 5.1
Ubuntu version: 14.04

Step 1) Find your system distribution codename by using following command on the terminal.

$ lsb_release –c

(here, Operating System : Ubuntu 14.04, so codename is : trusty)

Step 2) Edit /etc/apt/sources.list file and add the following line according to your distribution of the system.

deb http://download.virtualbox.org/virtualbox/debian trusty contrib

Step 3) Once you have added required apt repository in your system, download and import Oracle Public key using following commands:

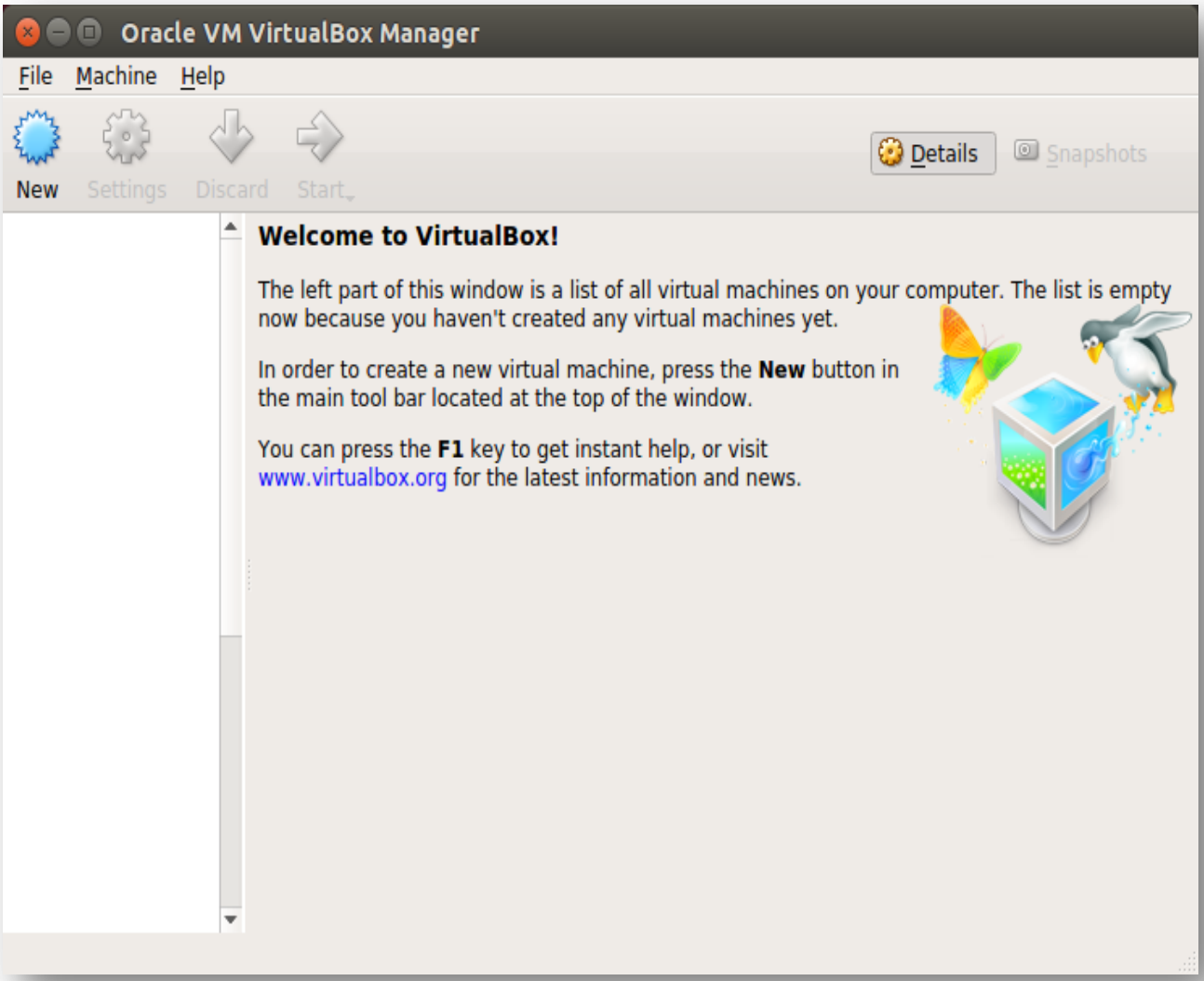
$ wget -q https://www.virtualbox.org/download/oracle_vbox_2016.asc -O- | sudo apt-key add -
$ wget -q https://www.virtualbox.org/download/oracle_vbox.asc -O- | sudo apt-key add -

Step 4) After completing above steps, install VirtualBox using following command on the terminal.

$ sudo apt-get update
$ sudo apt-get install virtualbox-5.1

Step 5) To open VirtualBox, use following command on the terminal.

$ virtualbox



Now, VirtualBox is installed, we will see the steps to install Kali Linux VM on it.

2. Kali Linux

2.1 About Kali Linux

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.

What's Different about Kali Linux?

Kali Linux is specifically geared to meet the requirements of professional penetration testing and security auditing. To achieve this, several core changes have been implemented in Kali Linux which reflects these needs:

1) **Single user, root access by design:** Due to the nature of security audits, Kali Linux is designed to be used in a "single, root user" scenario. Many of the tools used in penetration testing require escalated privileges, and while it's generally sound policy to only enable root privileges when necessary, in the use cases that Kali Linux is aimed at, this approach would be a burden.

2) **Network services disabled by default:** Kali Linux contains system hooks that disable network services by default. These hooks allow us to install various services on Kali Linux, while ensuring that our distribution remains secure by default, no matter what packages are installed. Additional services such as Bluetooth are also blacklisted by default.

3) **Custom Linux kernel:** Kali Linux uses an upstream kernel, patched for wireless injection.

4) **A *minimal* and *trusted* set of repositories**: given the aims and goals of Kali Linux, maintaining the integrity of the system as a whole is absolutely key. With that goal in mind, the set of upstream software sources which Kali uses is kept to absolute minimum. Many new Kali users are tempted to add additional repositories to their sources.list, but doing so runs a *very serious risk* of breaking your Kali Linux installation.

2.2 Kali Linux Tools

Kali Linux contains a large amount of penetration testing tools from various different niches of the security and forensics field.

Kali Linux offers tools for information gathering, vulnerability analysis, wireless attacks, web applications, forensic tools, stress testing, sniffing and spoofing, password attacks, hardware hacking and many more. For this project we have more interest in tools for password attacks.

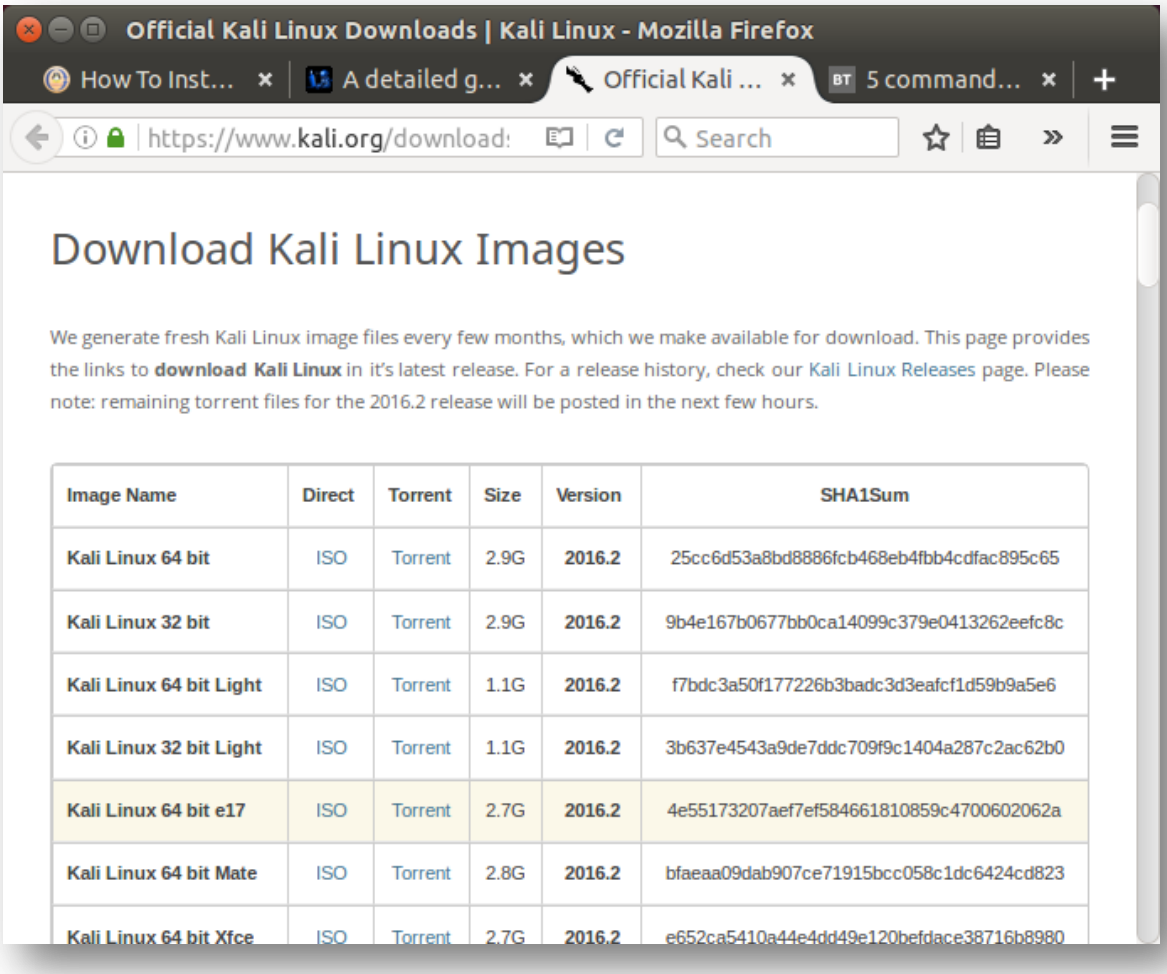
List of Kali Linux tools for Password Attacks

- acccheck
- Burp Suite
- CeWL
- chntpw
- cisco-auditing-tool
- CmosPwd
- creddump
- crunch
- DBPwAudit
- findmyhash
- gpp-decrypt
- hash-identifier
- HexorBase
- THC-Hydra
- **John the Ripper**
- Johnny
- keimpx
- Maltego Teeth
- Maskprocessor
- multiforcer
- Ncrack
- oclgausscrack
- PACK
- patator
- phrasendrescher
- polenum
- RainbowCrack
- rcracki-mt
- RSMangler
- SQLdict
- Statsprocessor
- THC-pptp-bruter
- TrueCrack
- WebScarab
- wordlists
- zaproxy

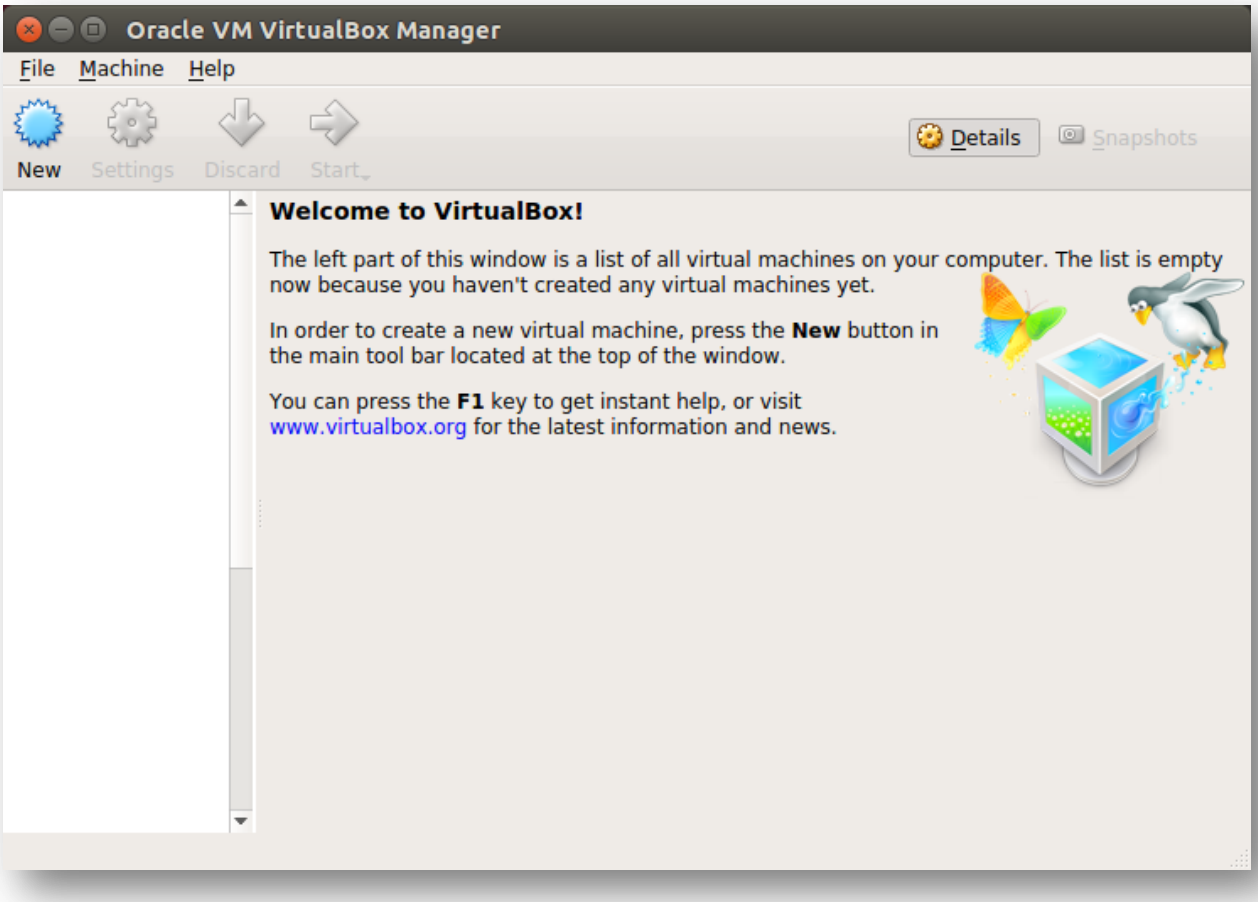
We are going to use “John the Ripper” for password cracking on Windows and Kali Linux.

2.3 Steps to install Kali Linux on VirtualBox

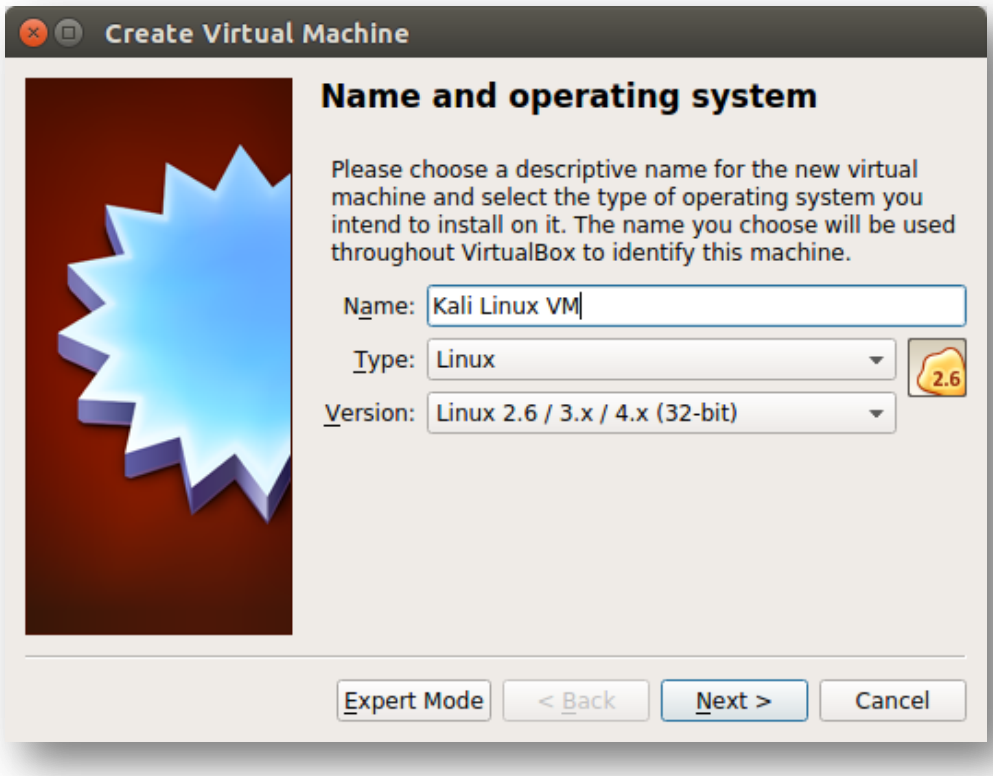
Step 1) First, download the Kali Linux ISO file from https://www.kali.org/downloads/



Step 2) To create new Virtual Machine click on "New":

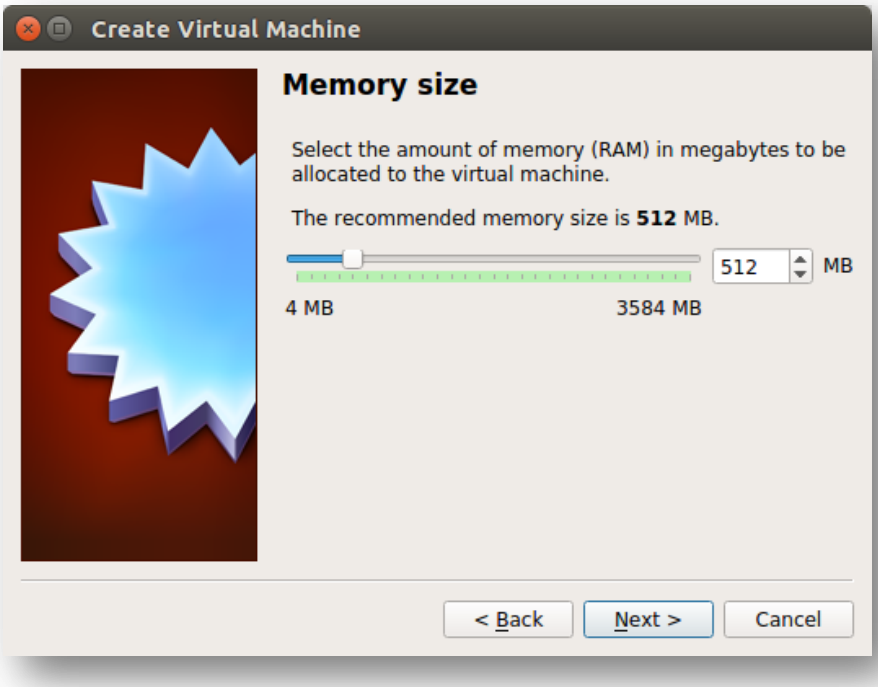


Step 3) Enter Kali Linux VM as a name. Type and version will be automatically set to Linux and Linux 2.6/3.x/4.x(32-bit) respectively.

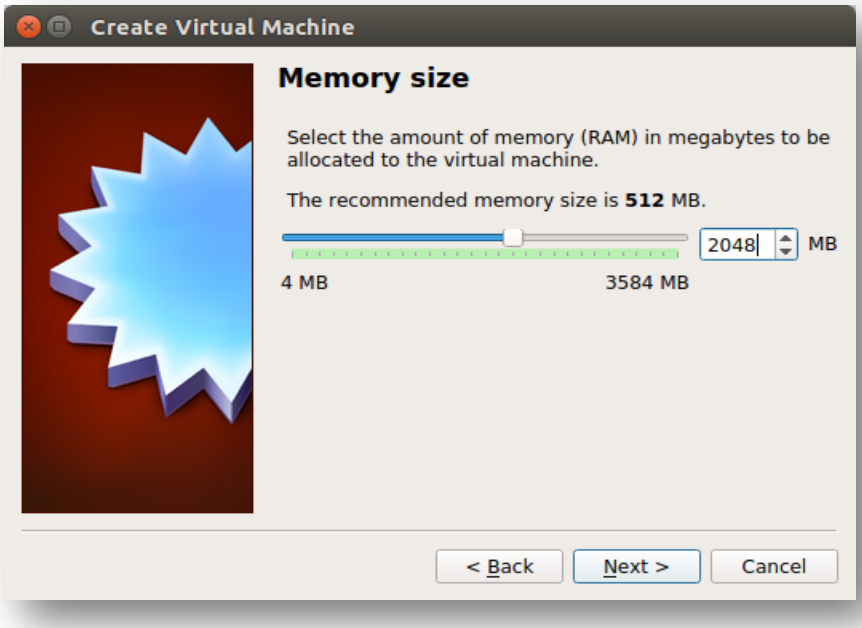


Step 4) Allocate RAM:

Default RAM size is 512 MB



Change it to 2048 MB.

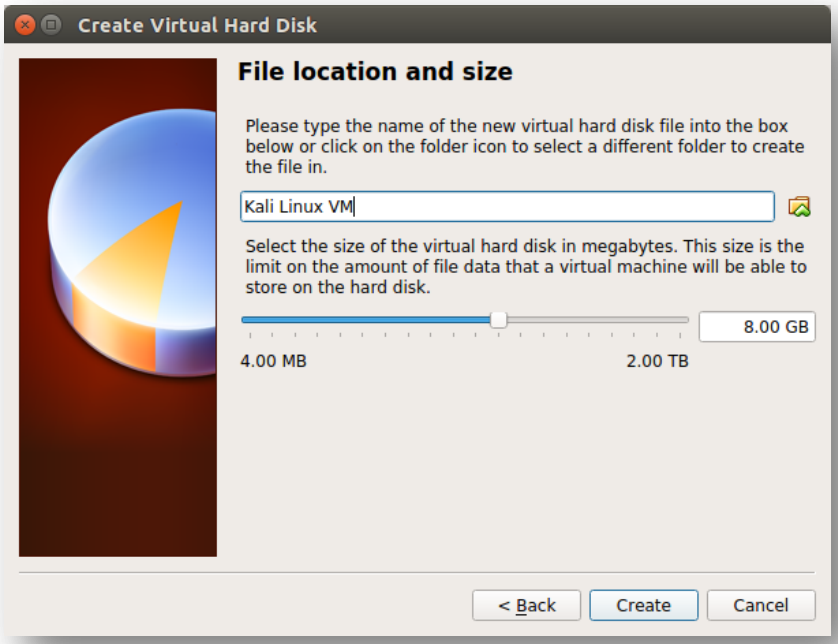


Step 5) On the screen select "Create a virtual hard disk now" and click "Create".

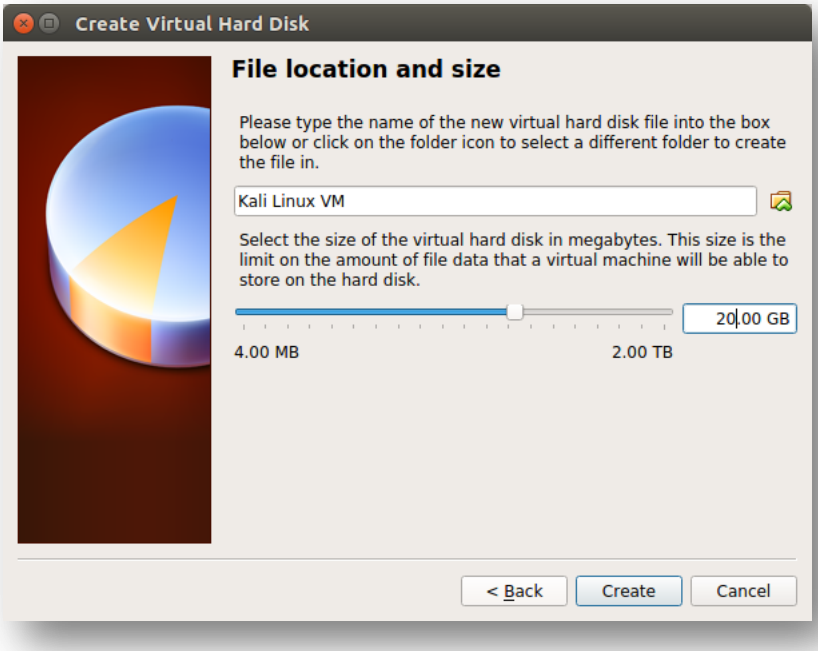
Step 6) On the screen select "VDI (VirtualBox Disk Image)" and click on "Next".

Step 7) Select "Dynamically allocated" option and click "Next".

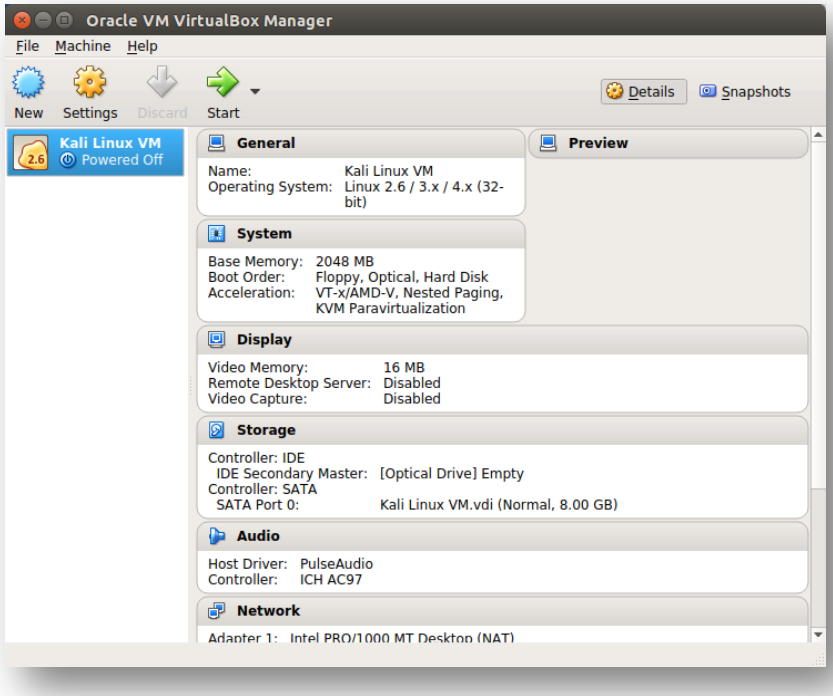
Step 8) Default disk size is 8GB.



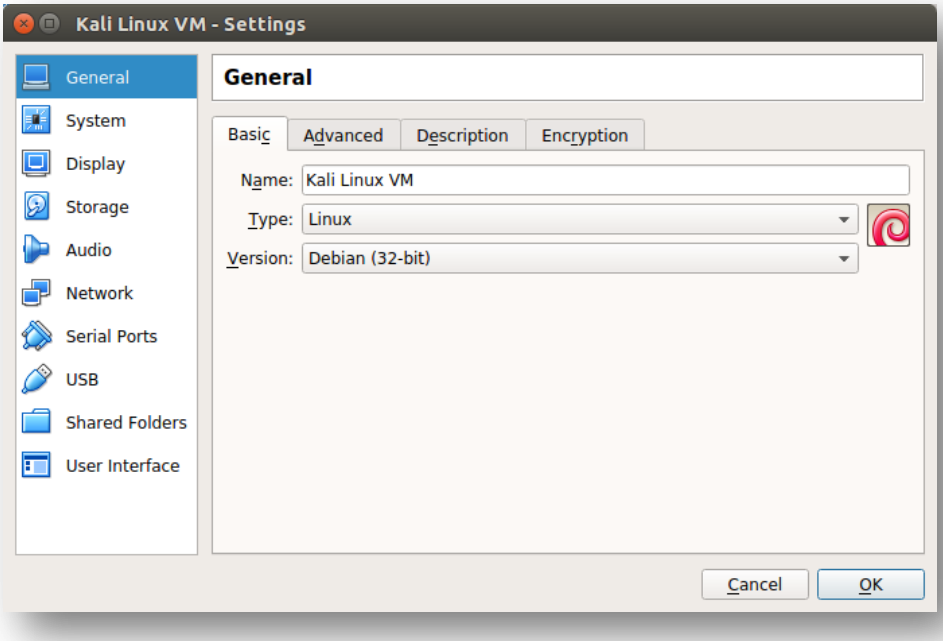
Change it to 20GB.



Step 9) Now, you can see new virtual machine named "Kali Linux VM" is created.

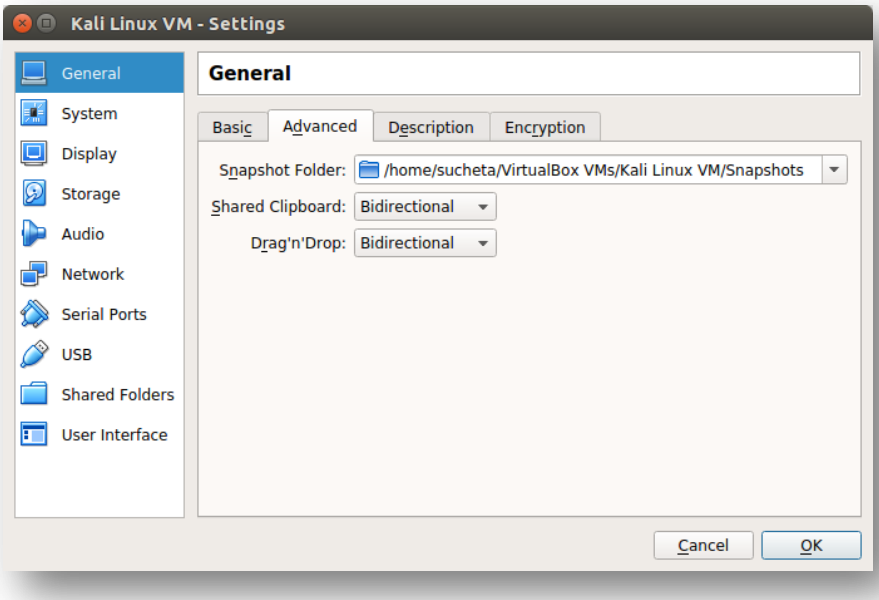


Step10) Select "Kali Linux VM" and click on "Settings":

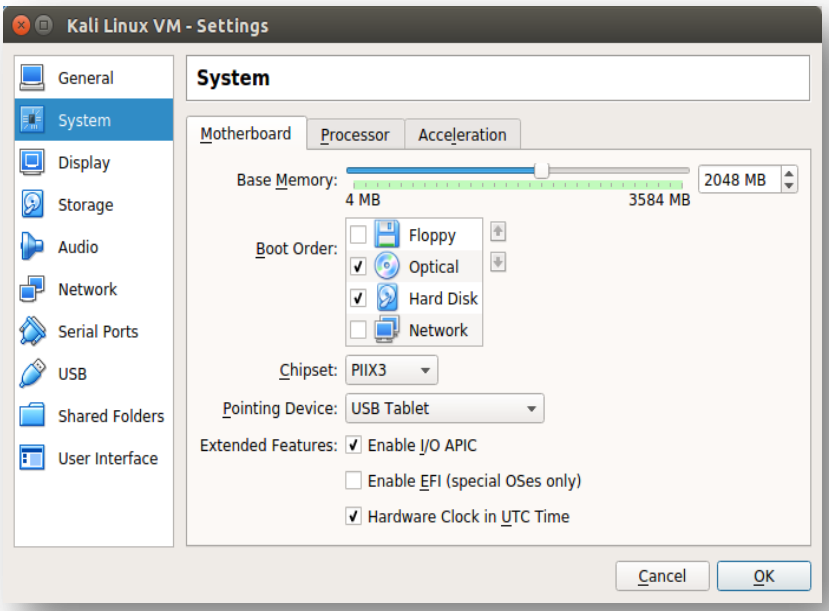


As shown in above screen shot, In "General" -> "Basic" select version based on your ISO file. As I am using 32 bit ISO file so I have selected "Debian (32-bit)" version.

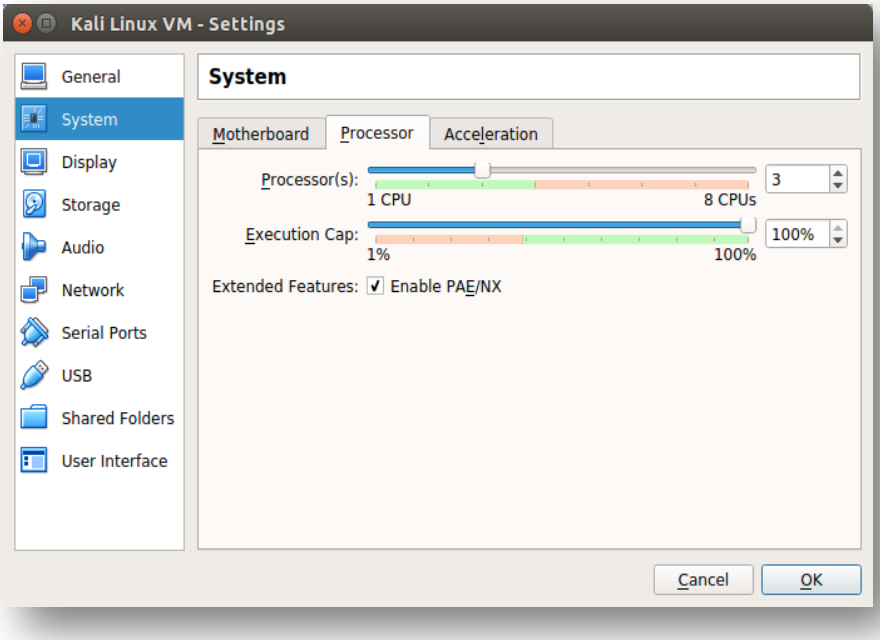
Step11) In "General" -> "Advanced" tab change "Shared Clipboard" and "Drag'n'Drop" to Bidirectional.



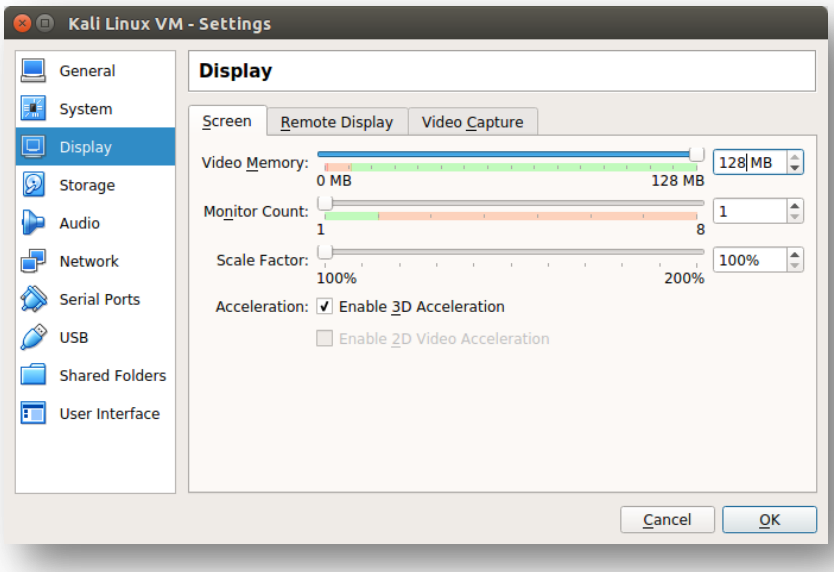
Step 12) In "System" -> "Motherboard" tab uncheck "Floppy" and check the box for "Enable I/O APIC.



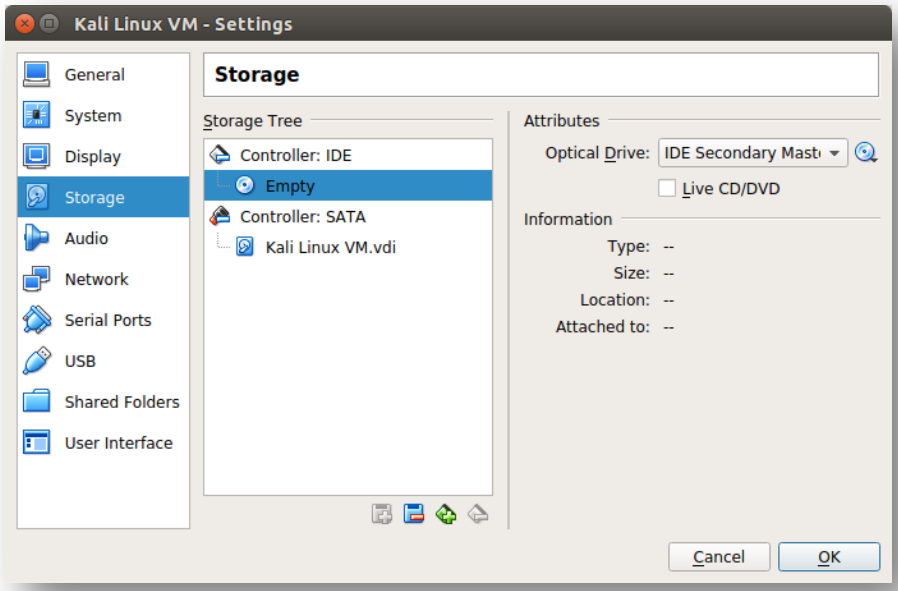
Step 13) In "System" -> "Processor" tab select number of processors. Here, I have selected 3.



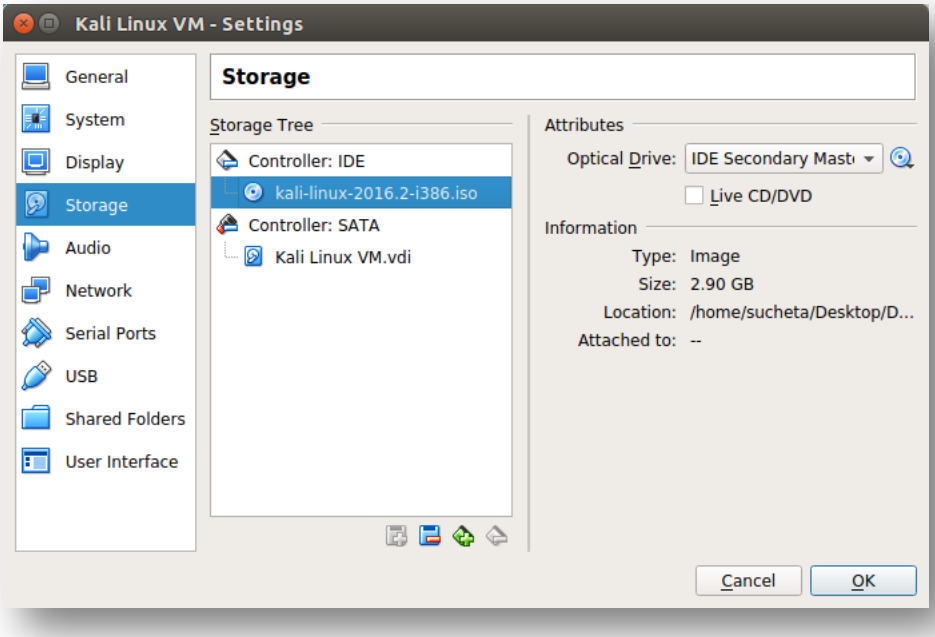
Step 14) In "Display" -> "Screen" tab select 128MB Video memory.



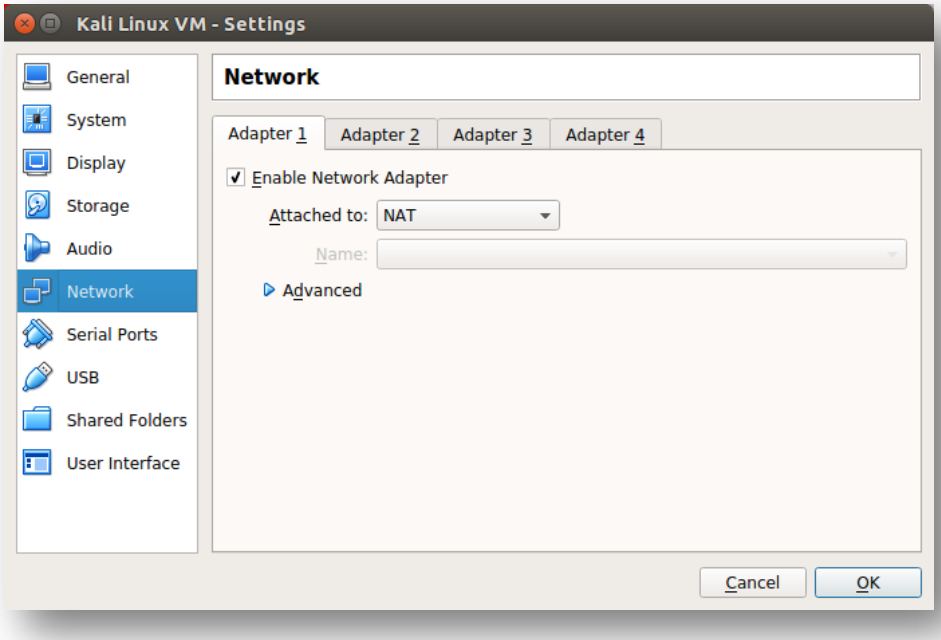
Step15) Select "Storage" -> "Controller: IDE" -> "Empty". Now, on right side click on the cd icon and browse your Kali Linux ISO file.



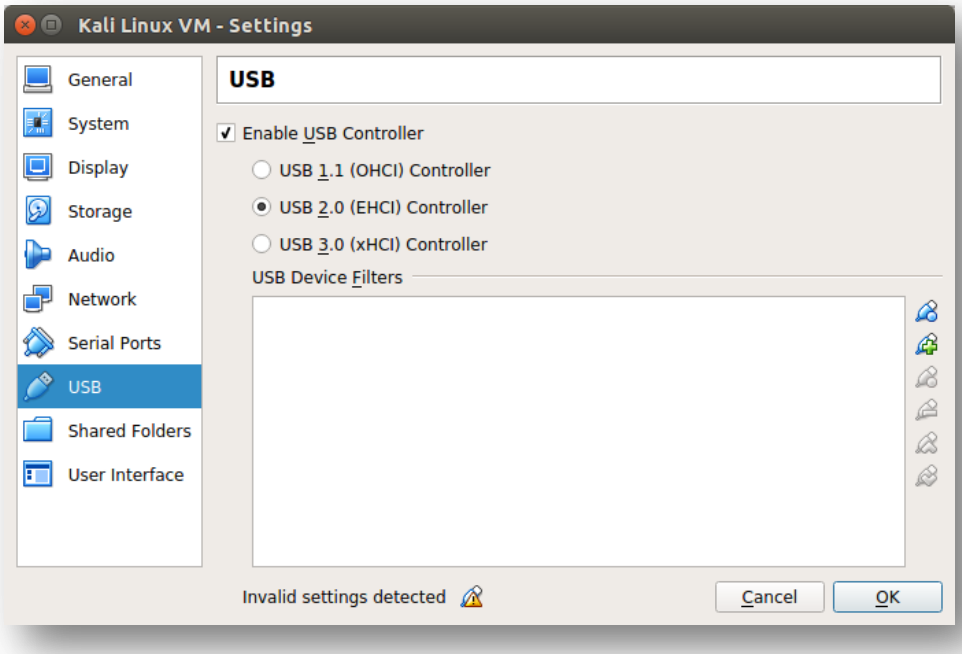
When you select the ISO file, you can see the changes in the Information.



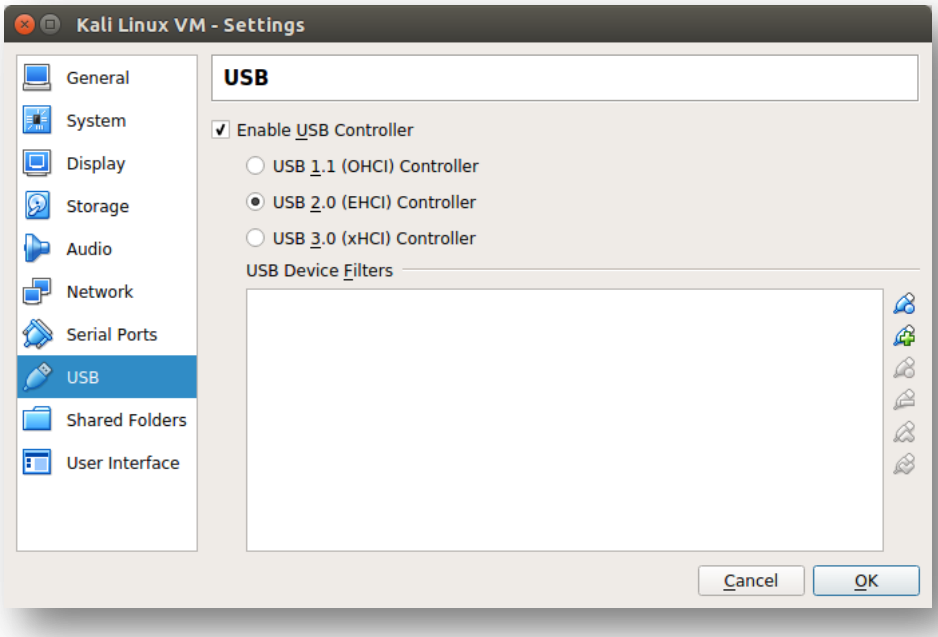
Step16) Select "NAT" in "Network" -> "Adapter 1" if your computer is connected to internet.



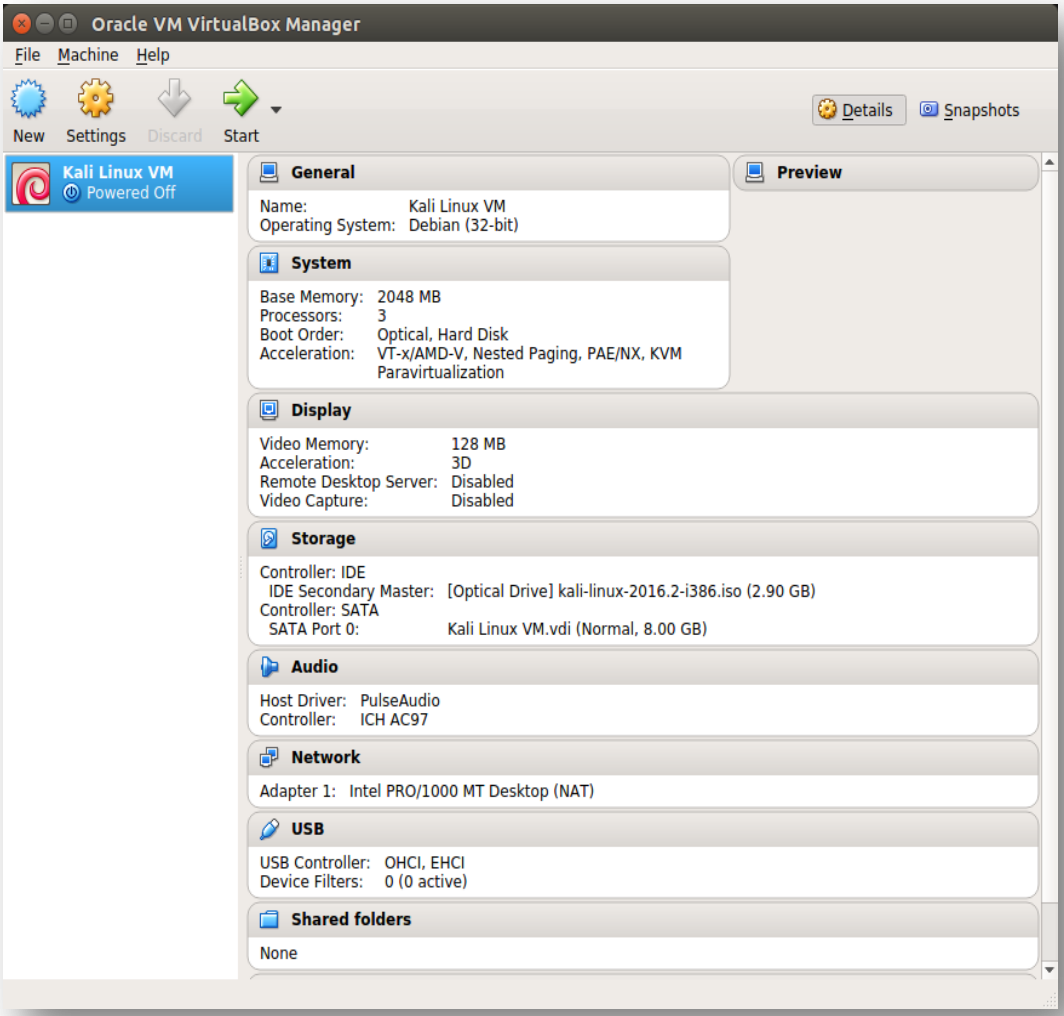
Step17) In "USB" -> "Enable USB Controller" select USB 2.0(EHCI) Controller. There will be "Invalid settings detected" error at the bottom line. To remove this error, install Virtual Box Extension Pack.



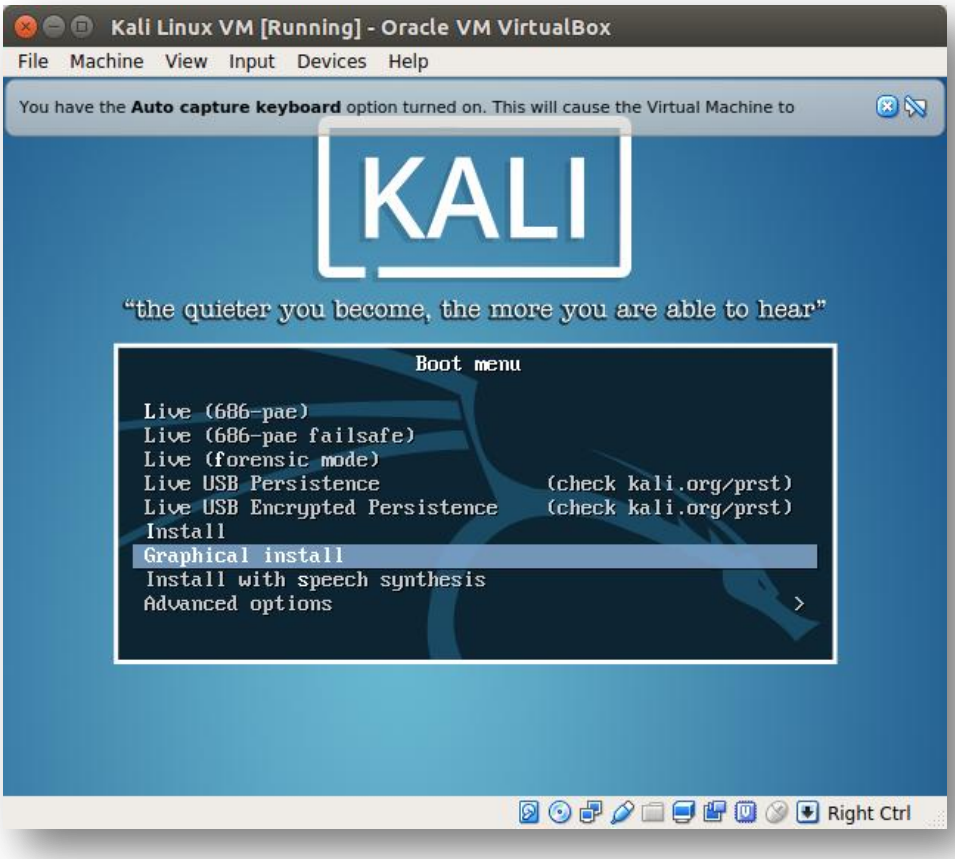
Once you install Virtual Box Extension Pack, you will see that error is gone.



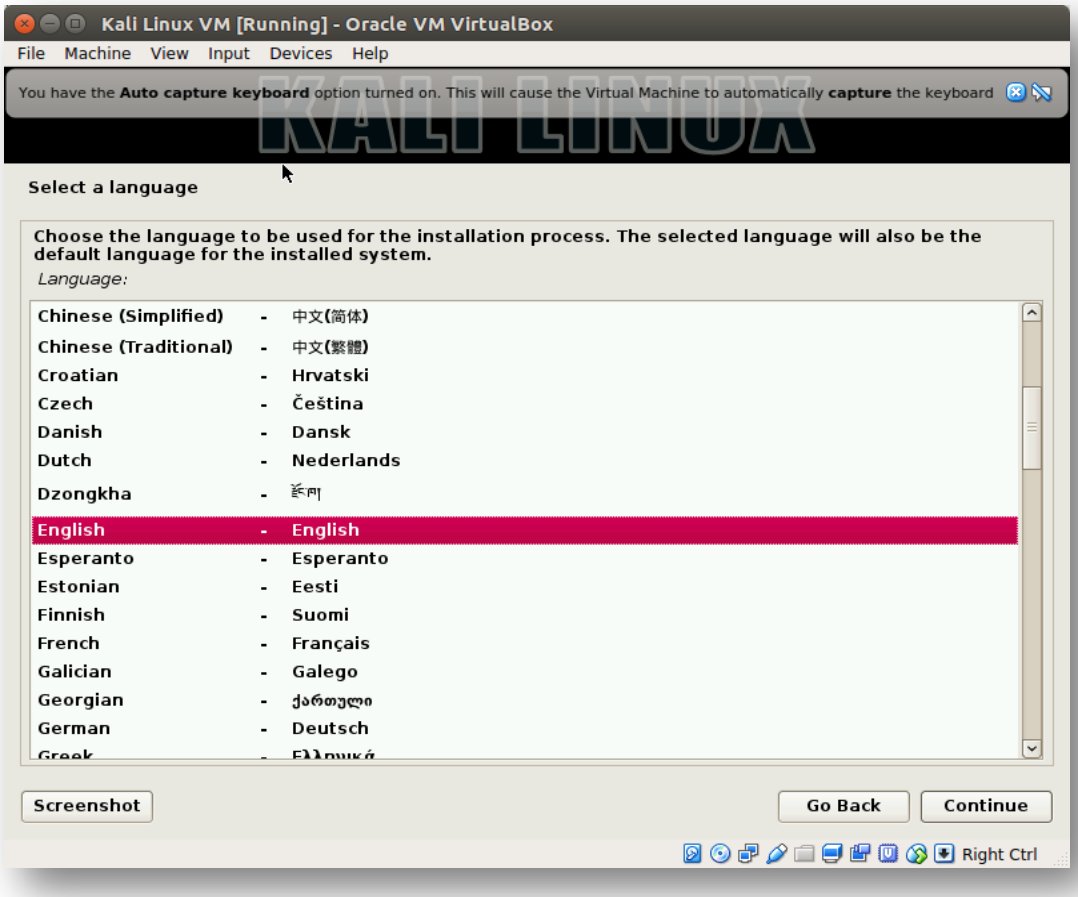
Step 18) You will see the following setting information on the right side.



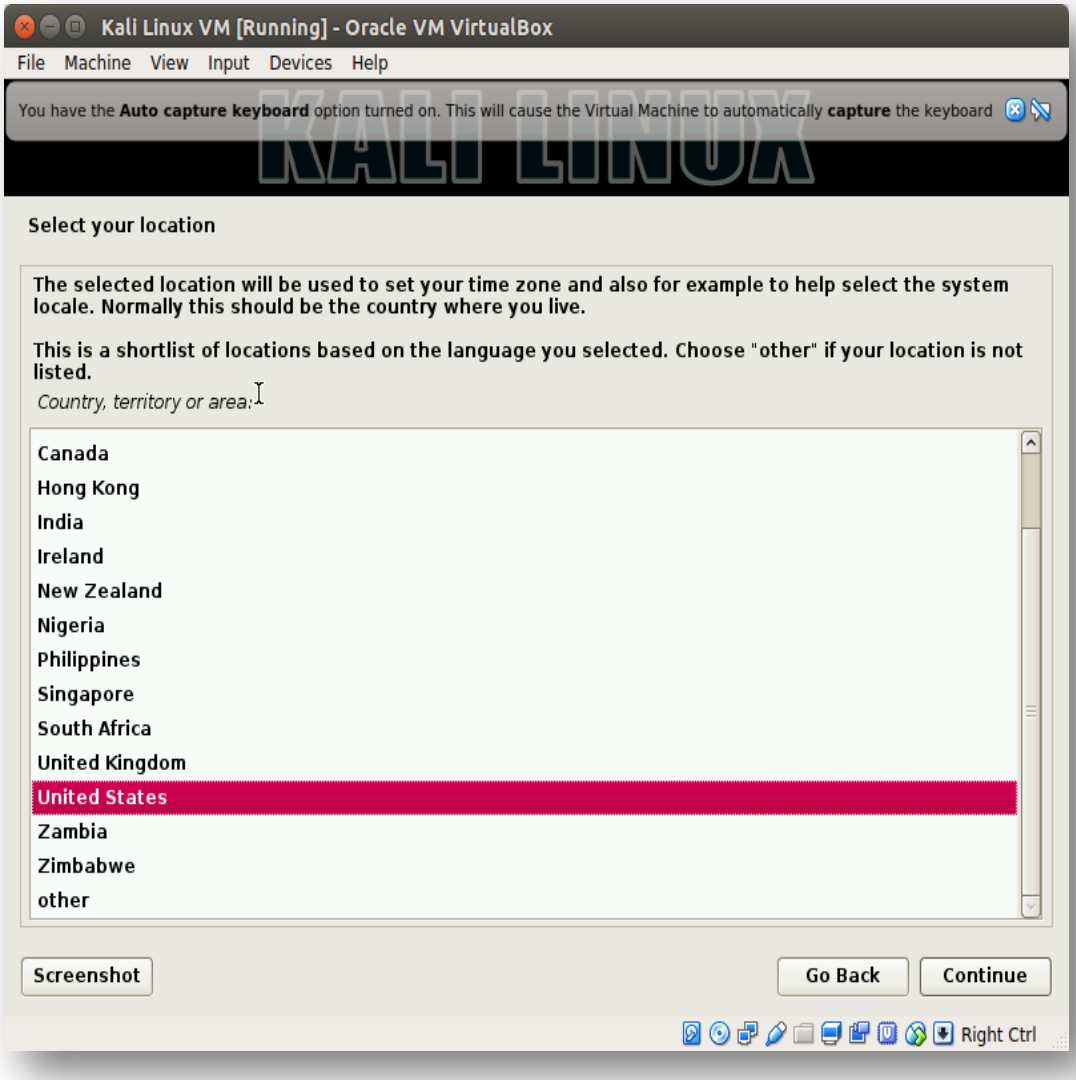
Step19) Select "Kali Linux VM" and click on "Start".
Select "Graphical install" option and press "Enter".



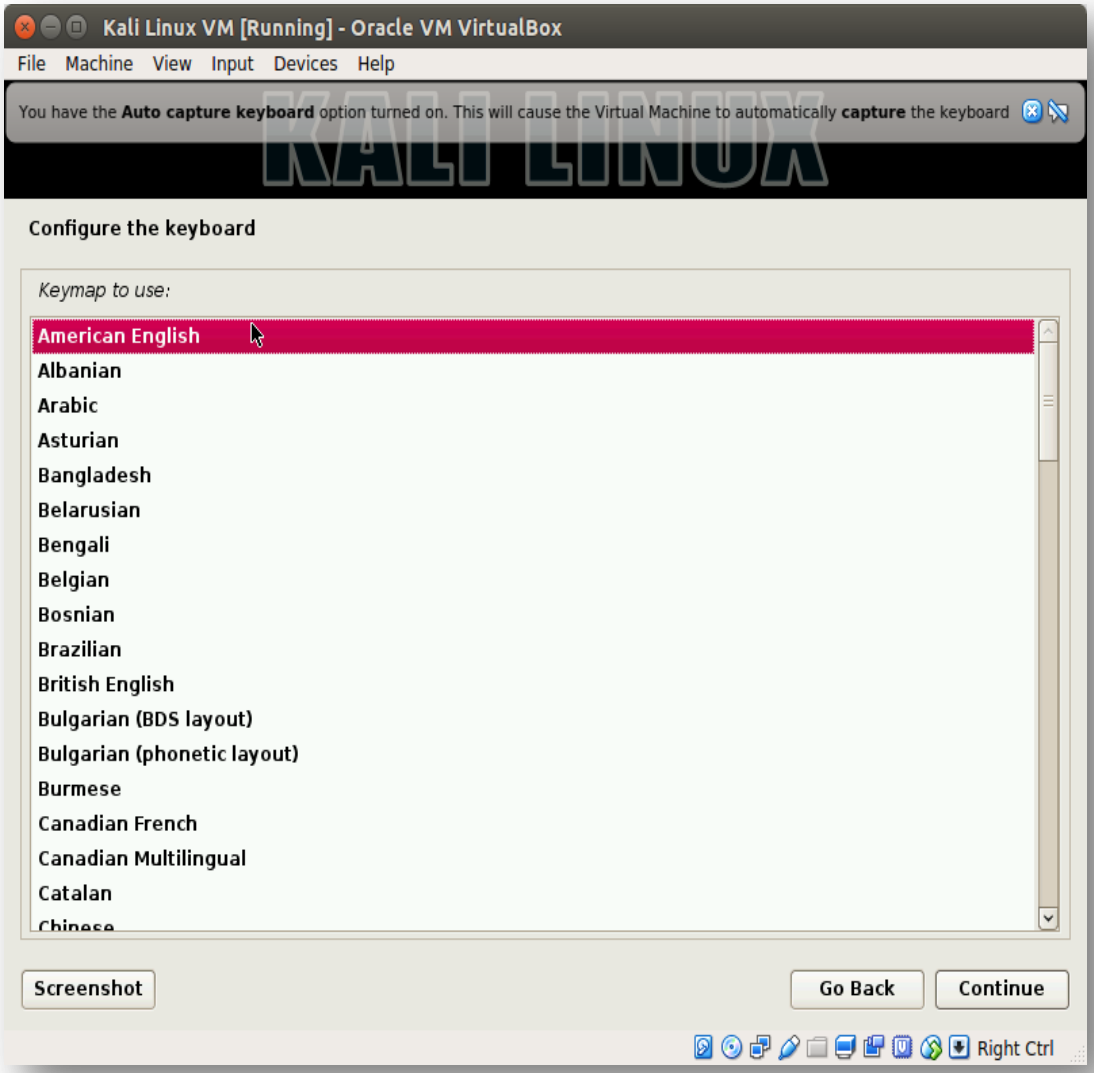
Step 20) Select your language and click on "Continue".



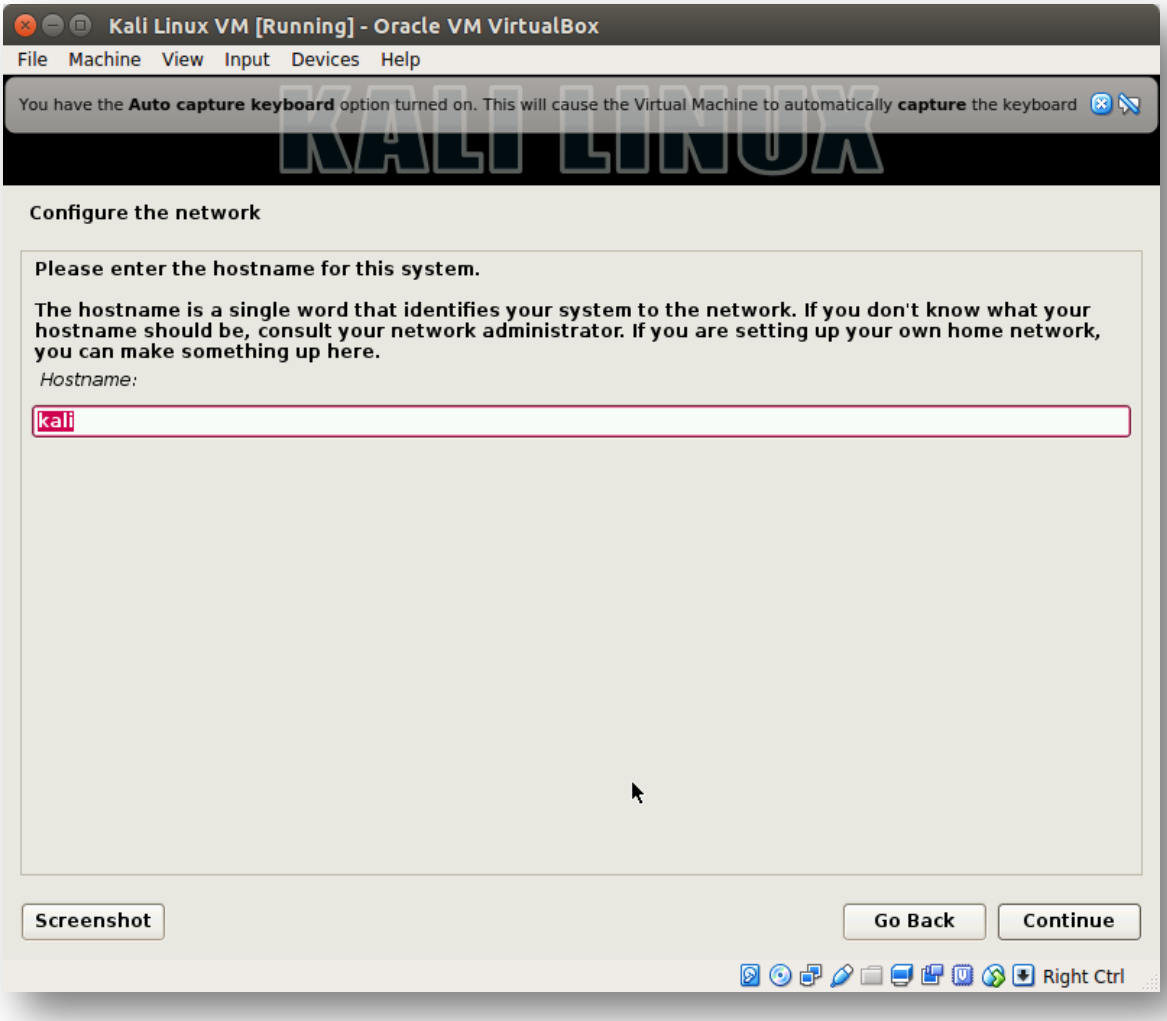
Step21) Select your location and click "Continue"



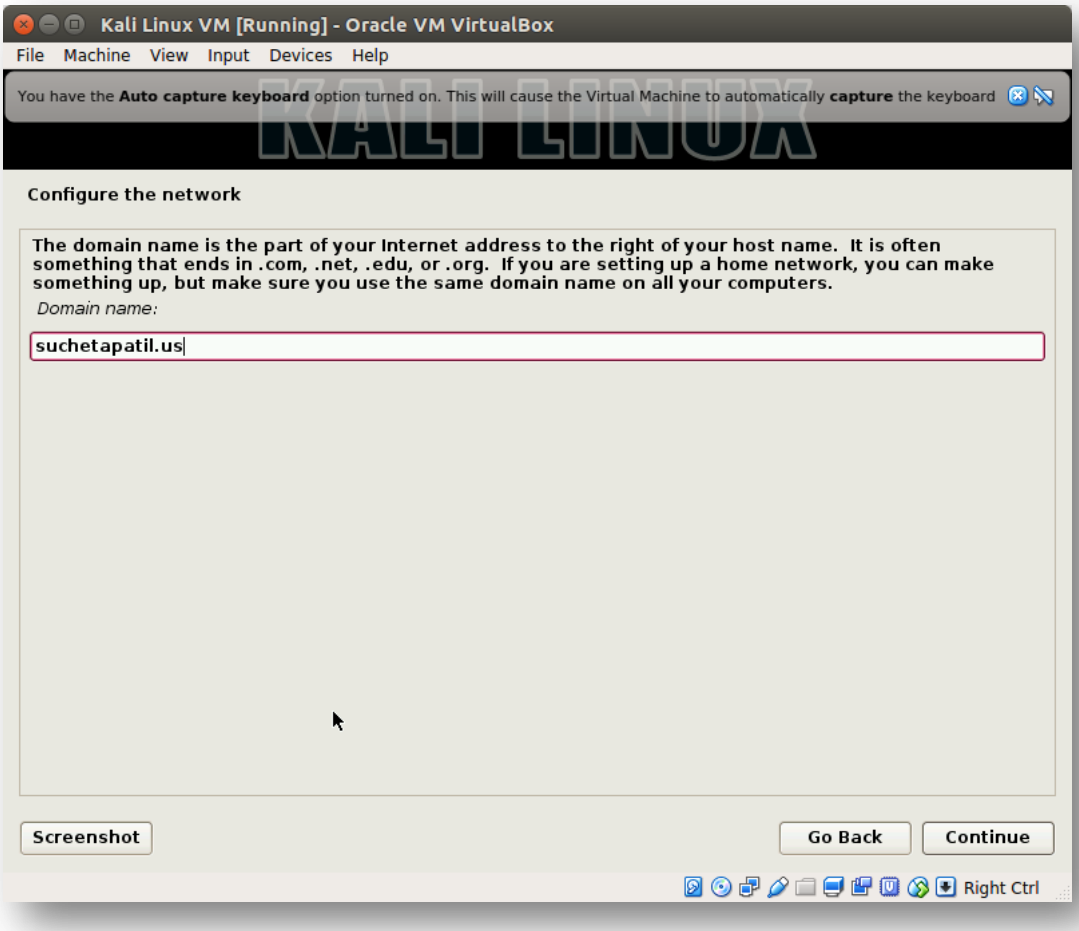
Step 22) Configure the keyboard and click "Continue"



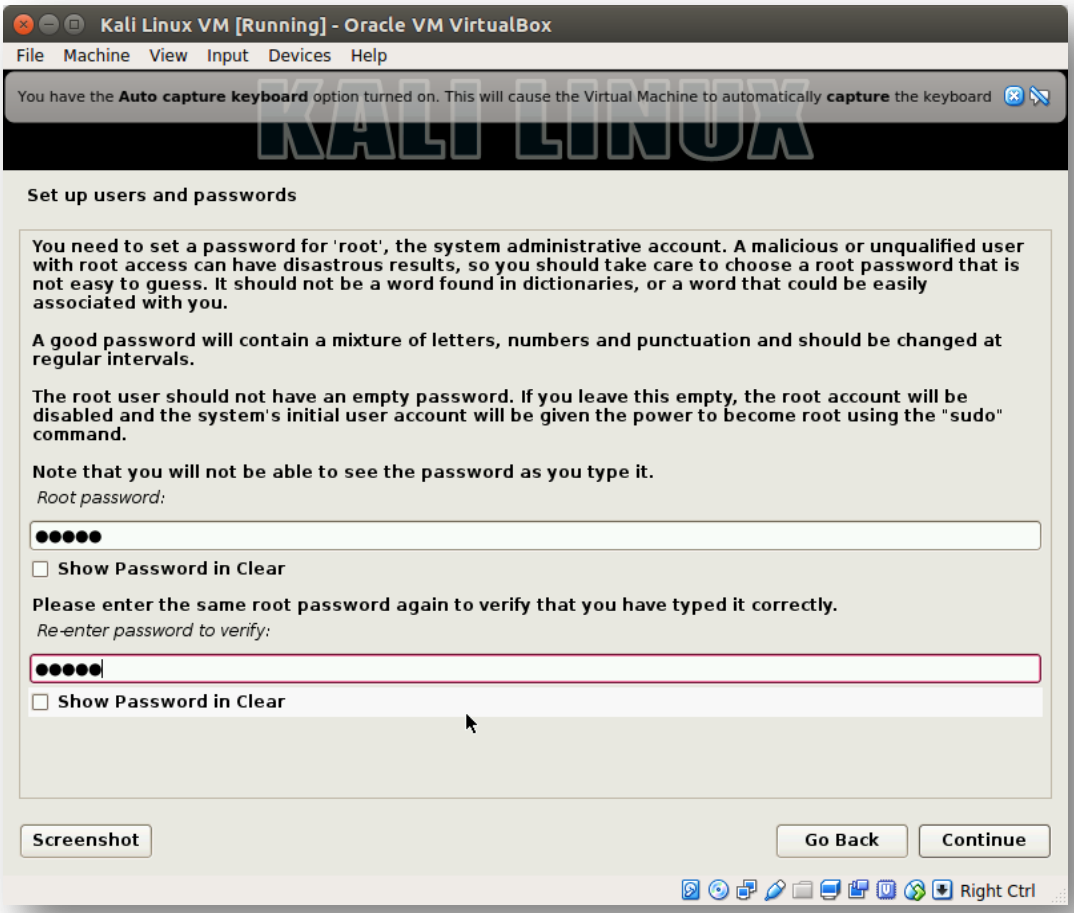
Step23) Enter the host name for the system and click "Continue".



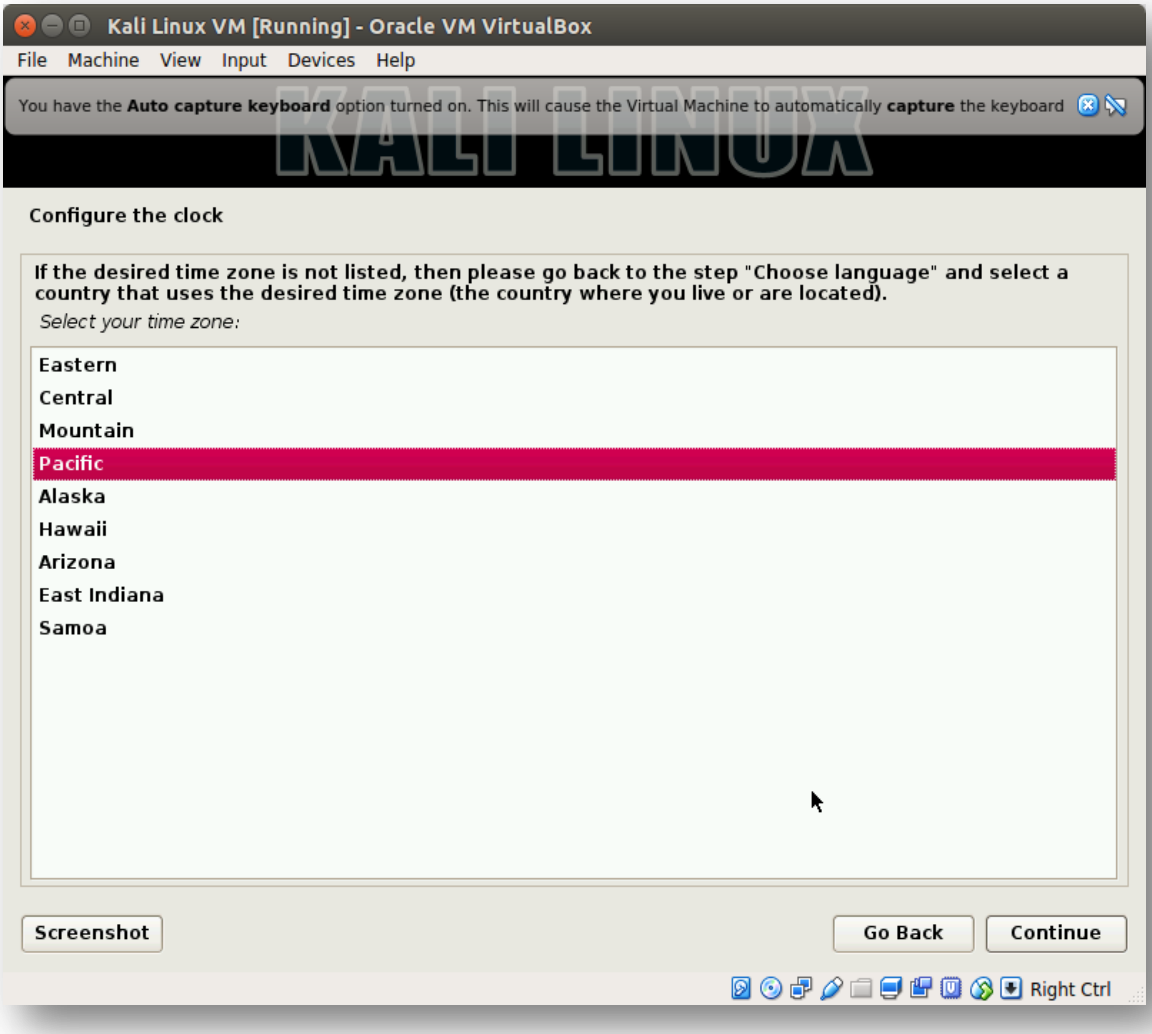
Step24) Enter the domain name and click on "Continue".



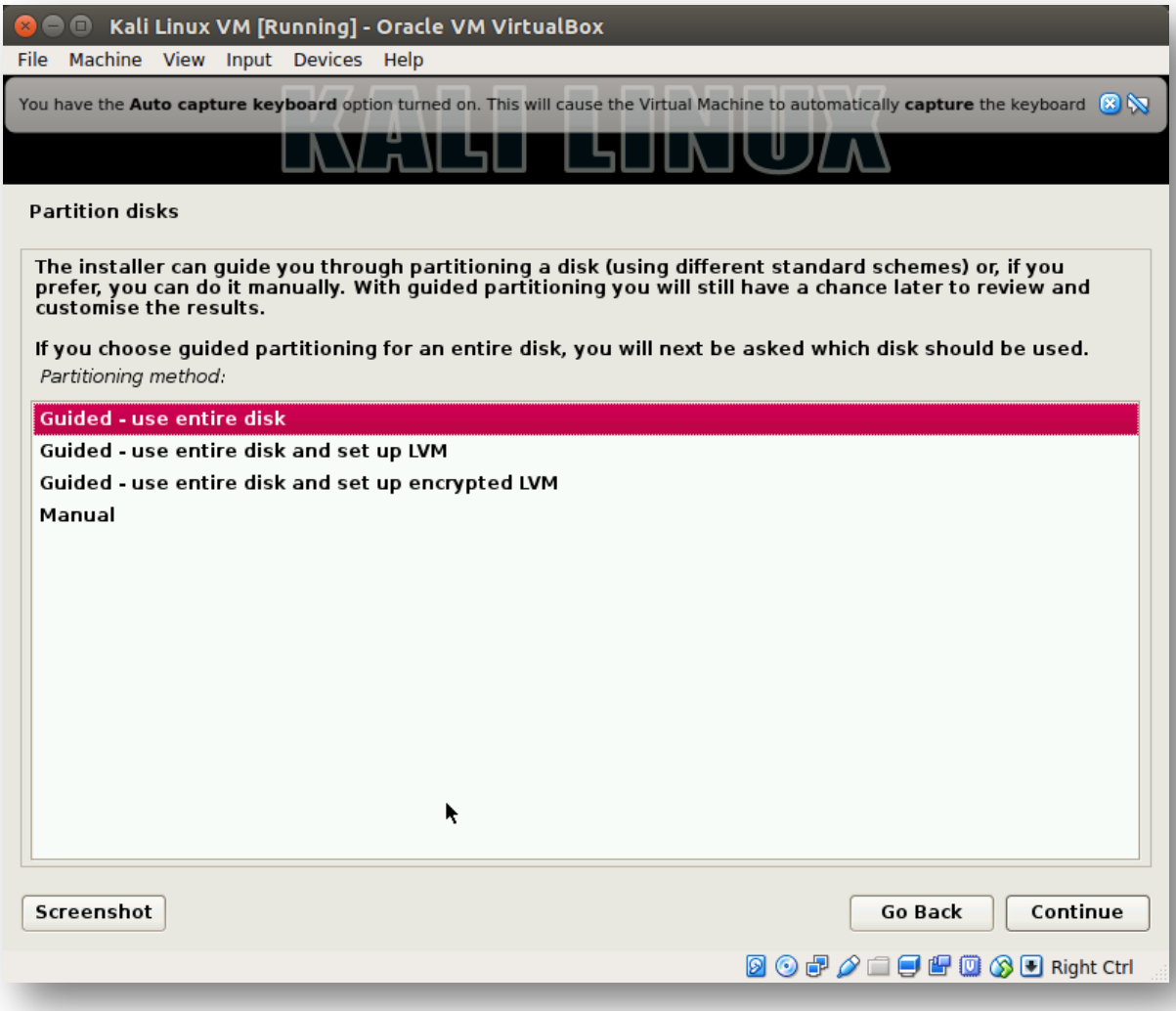
Step 25) Enter the root password and click "Continue".



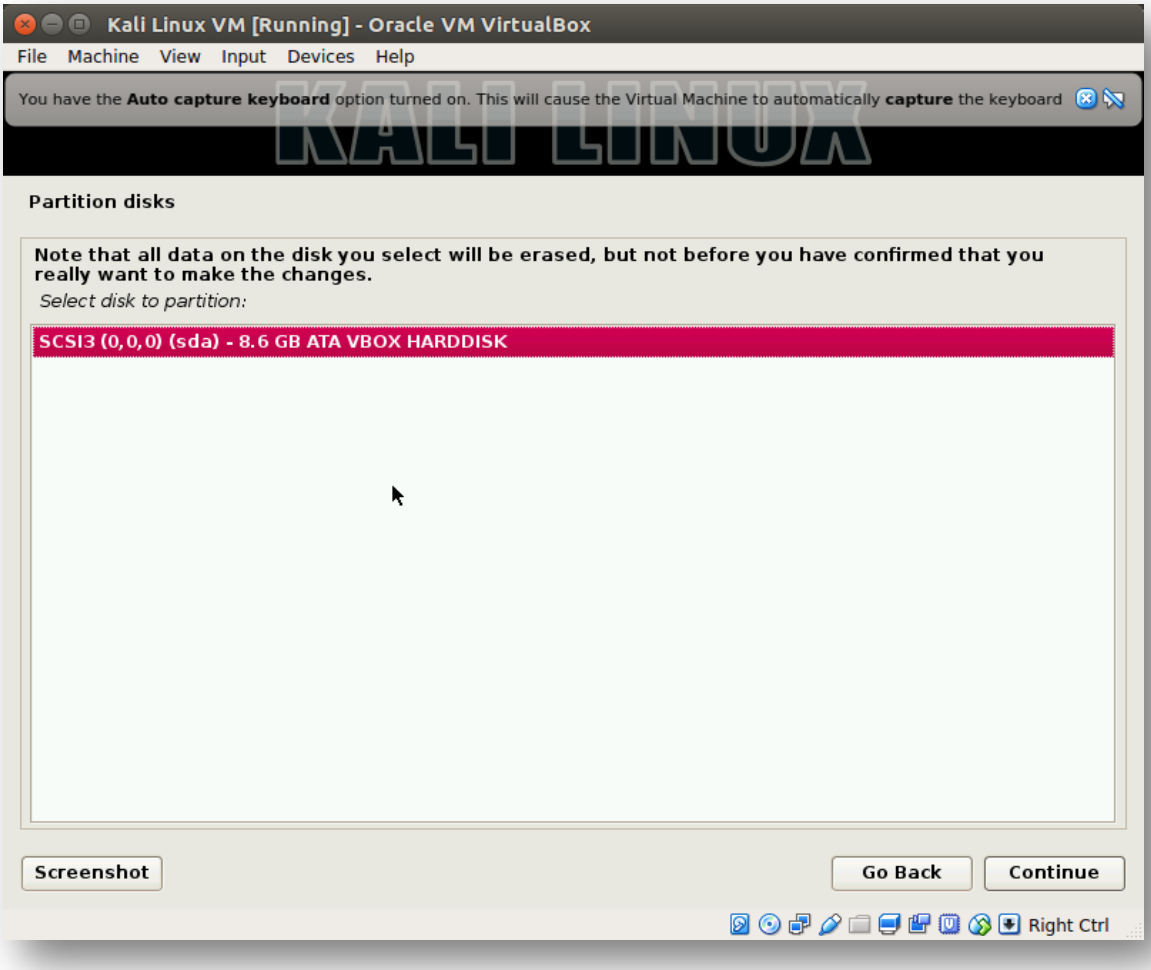
Step 26) Configure the clock and click "Continue".



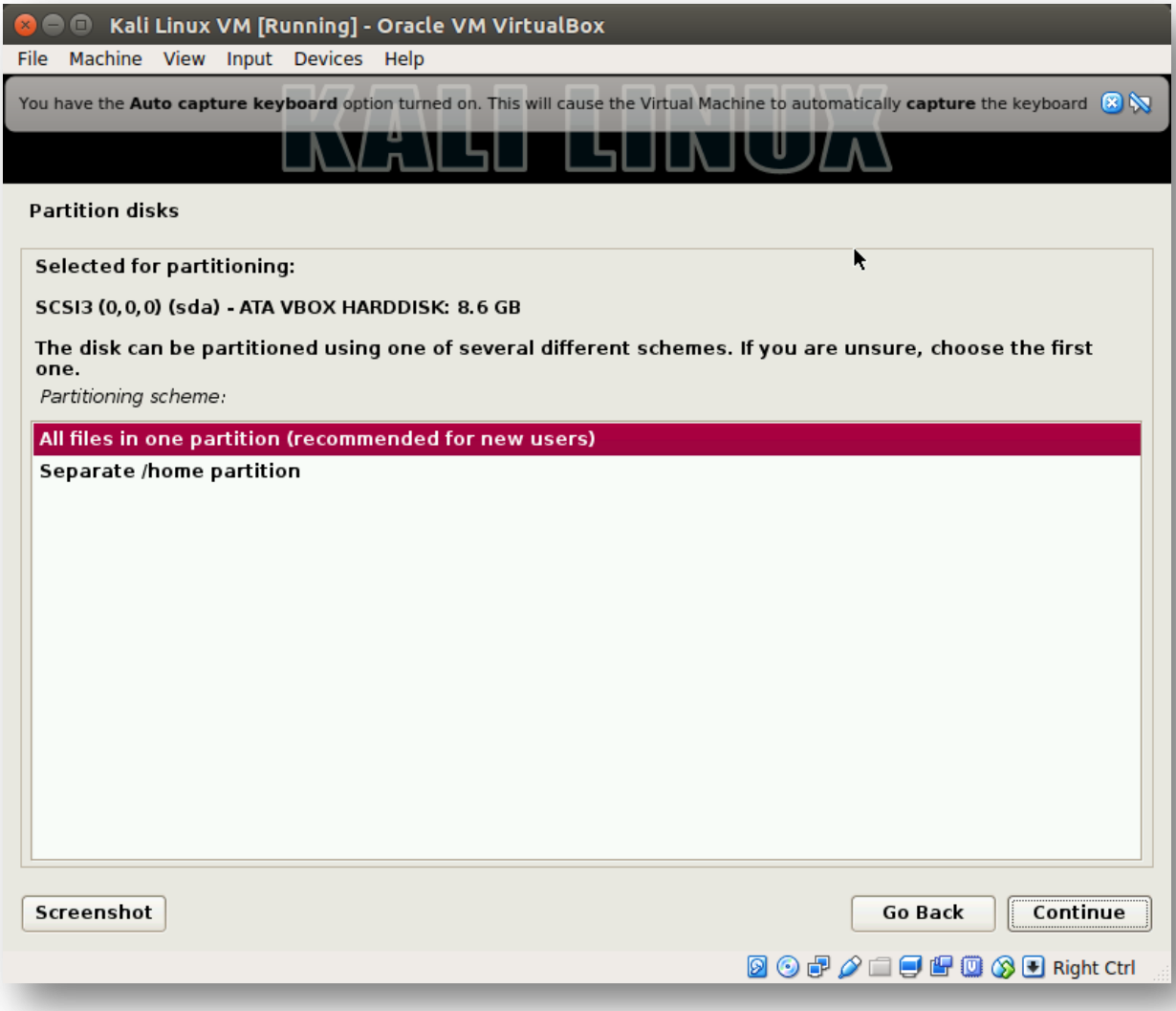
Step 27) Select "Guided- use entire disk" option and click "Continue".



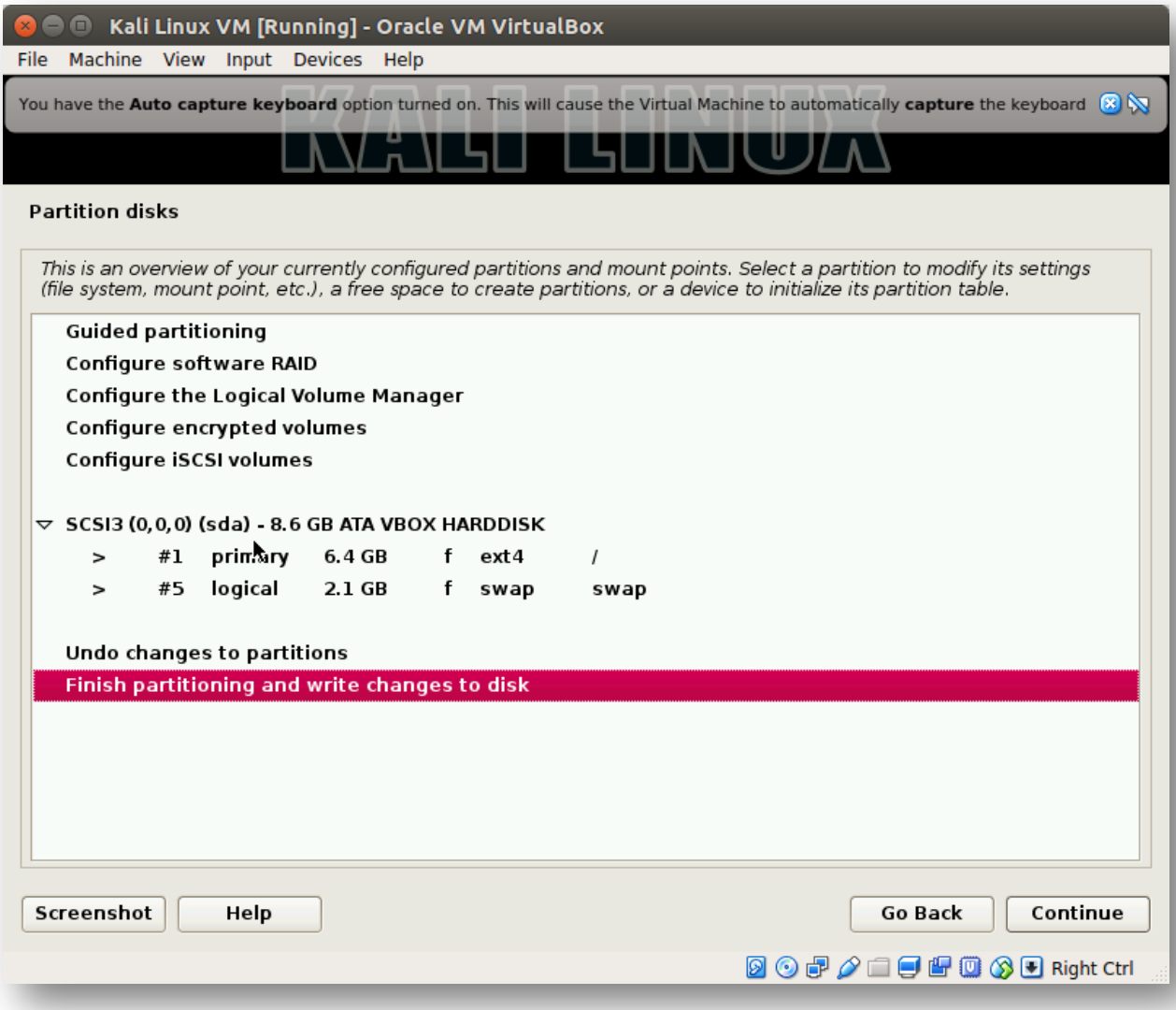
Step 28) You will have one highlighted disk name on screen and click "Continue".



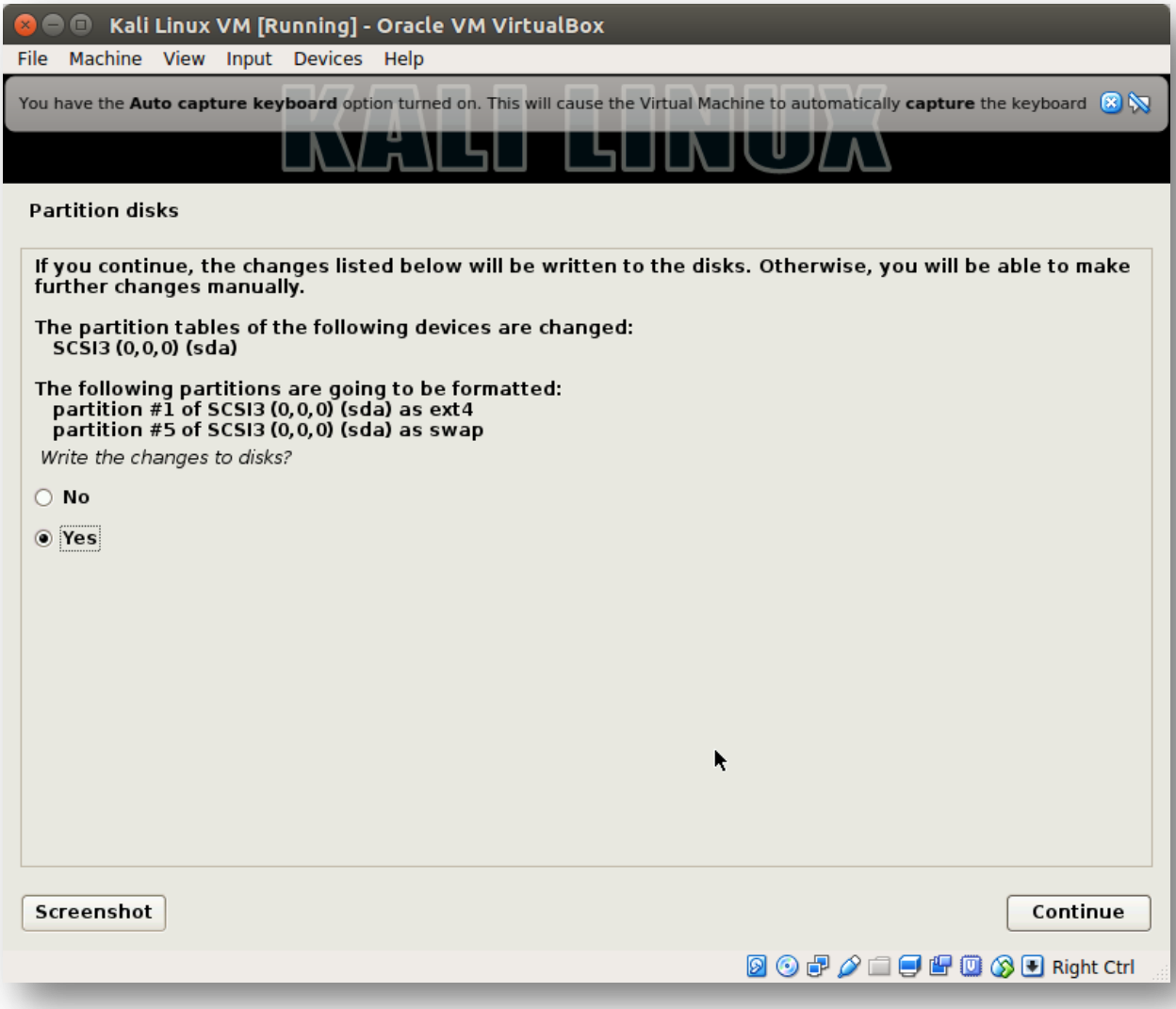
Step 29) Select "All files in one partition" option and click "Continue".



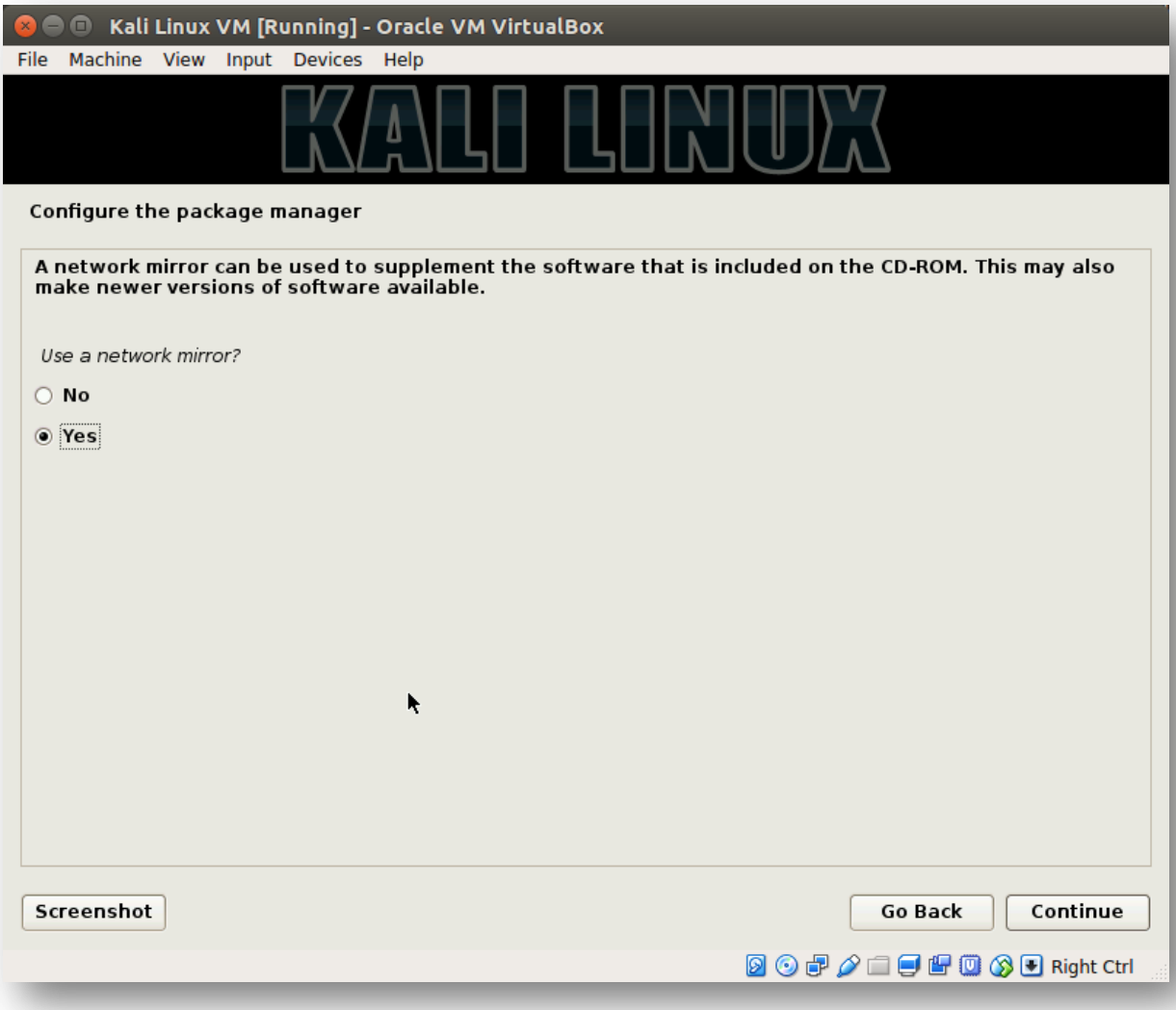
30) Select "Finish partitioning and write changes to disk" option and click "Continue".



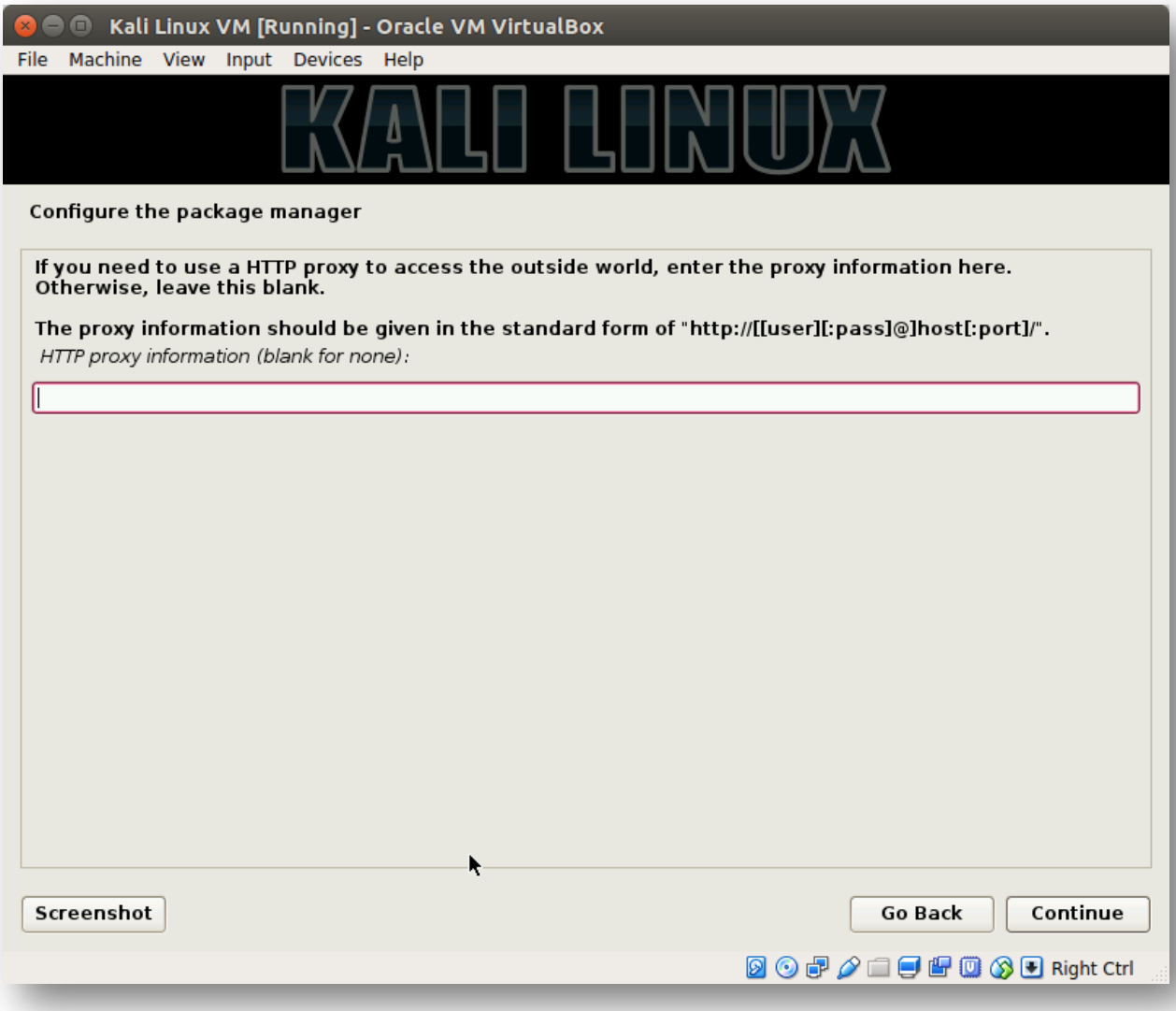
Step 31) Select "Yes" and Click "Continue".



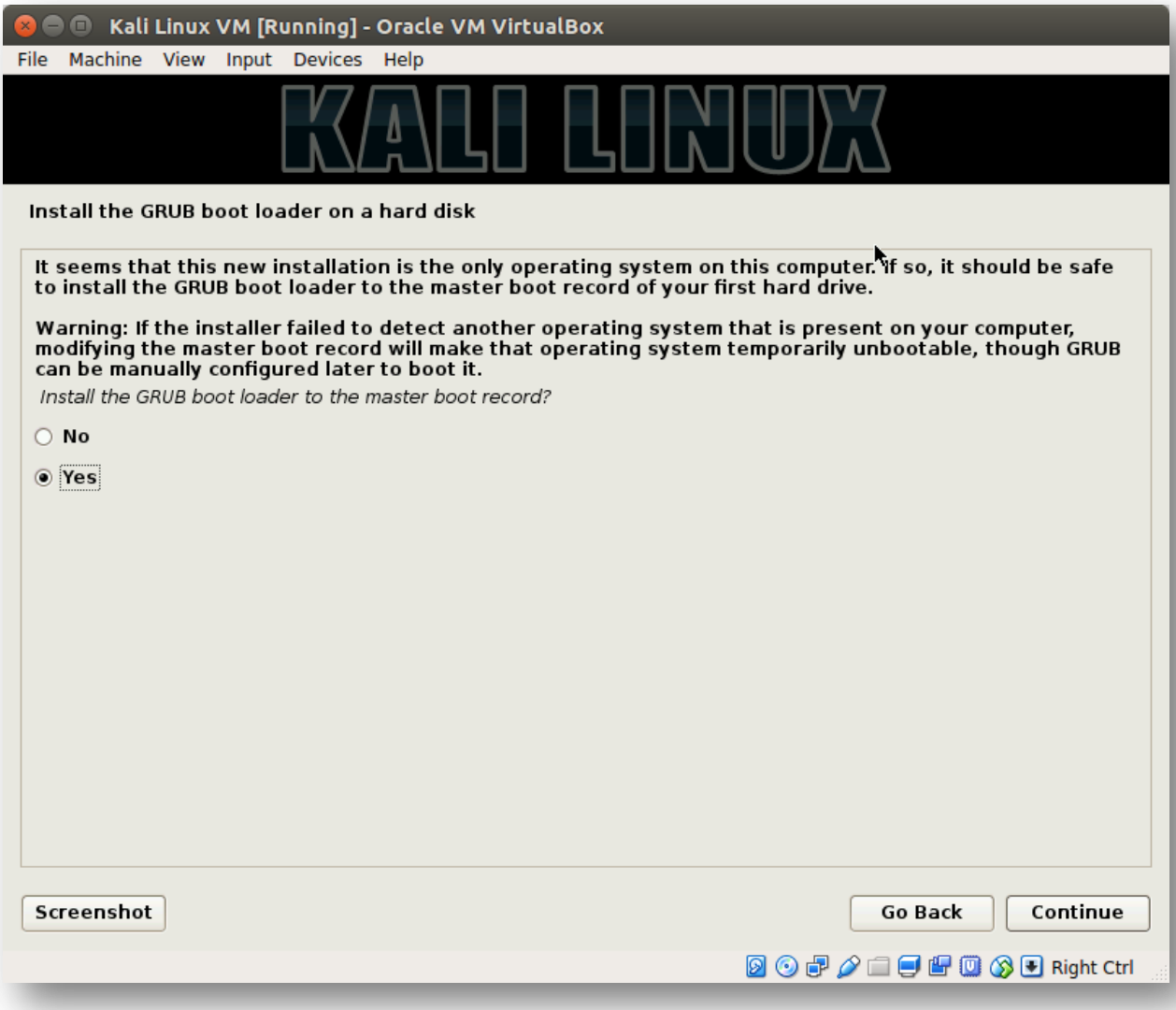
Step 32) Select "Yes" and Click "Continue".



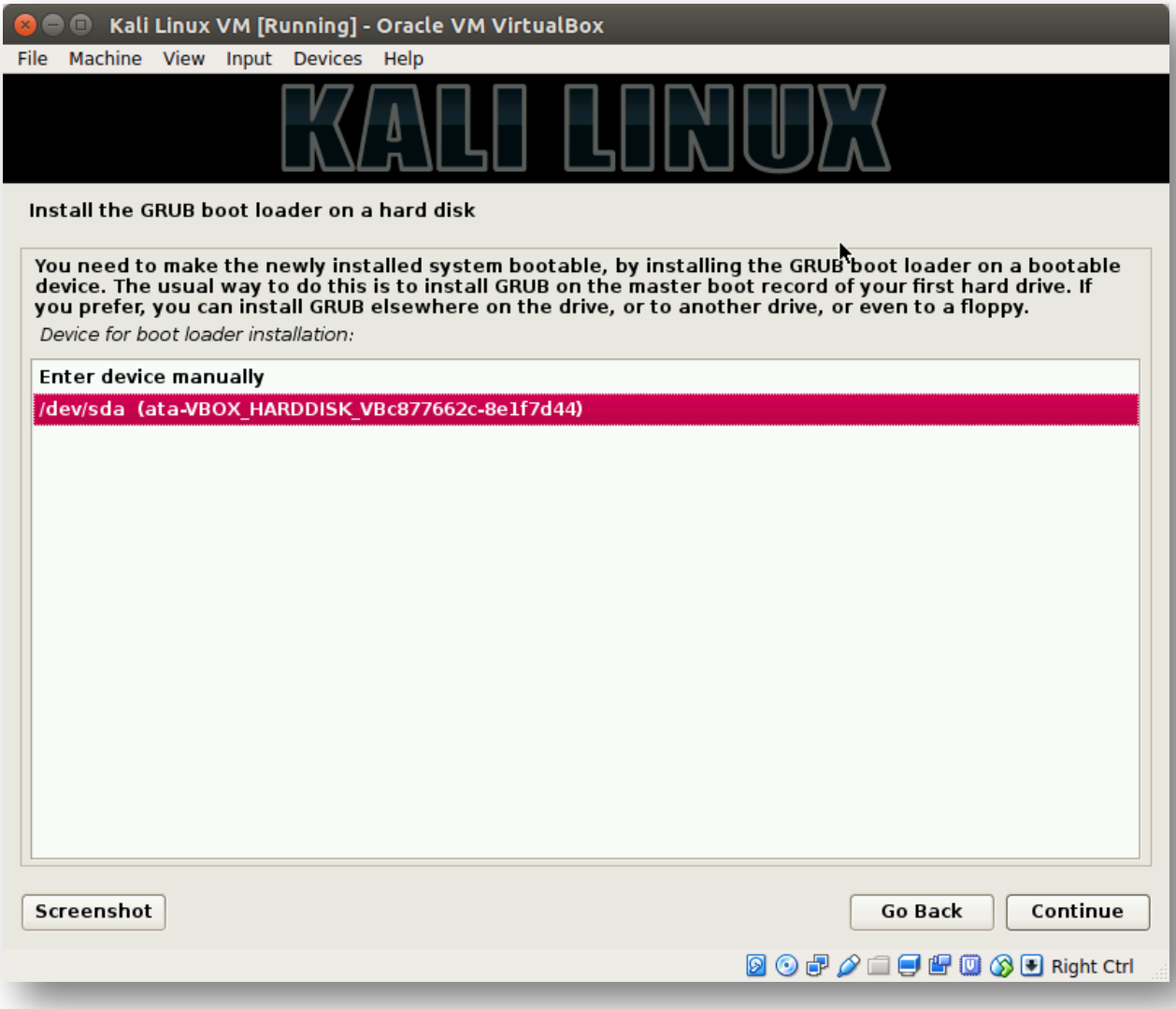
Step 33) Leave it blank if you are directly connected to internet.



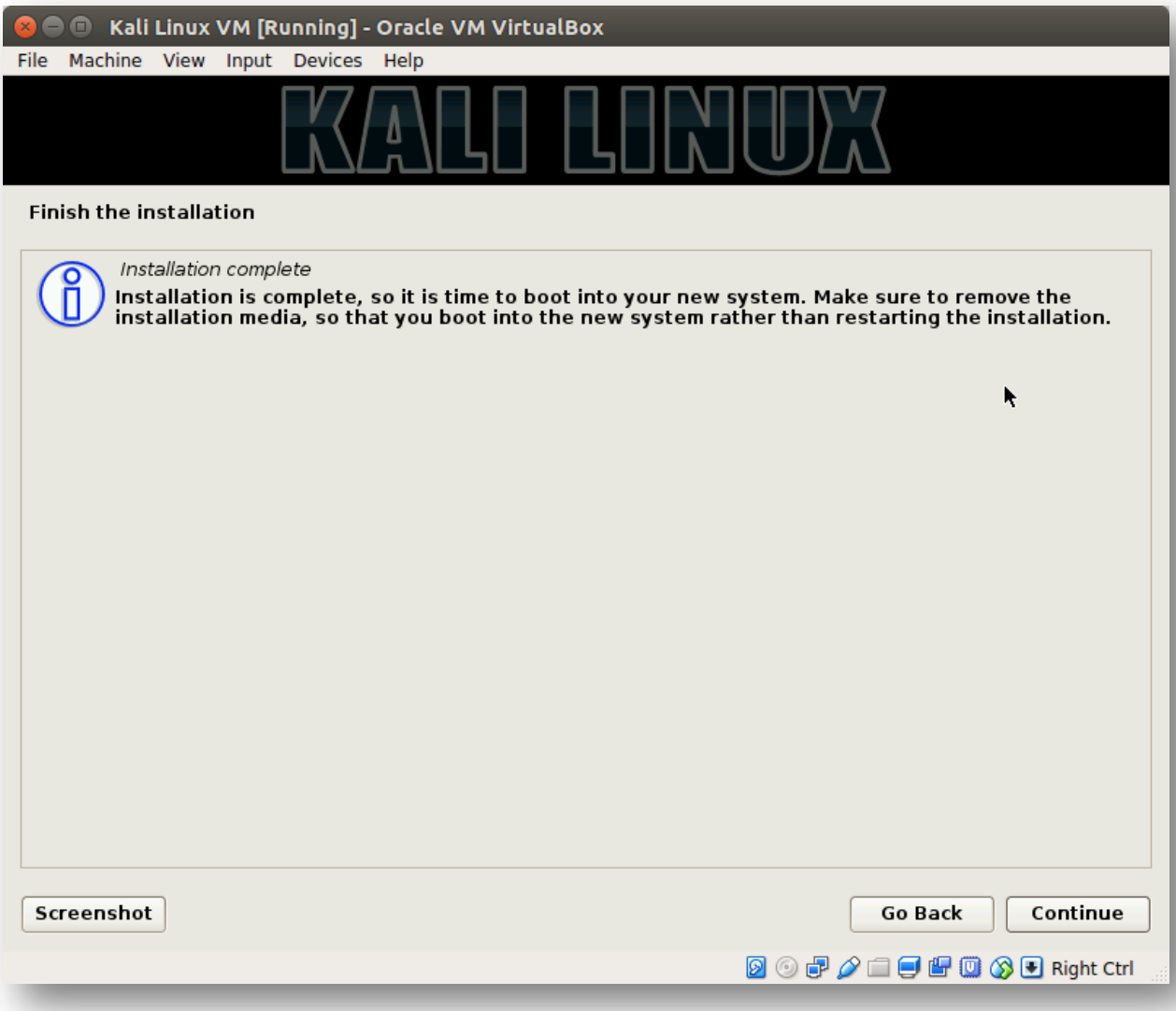
Step34) Select "yes" to install GRUB boot loader.



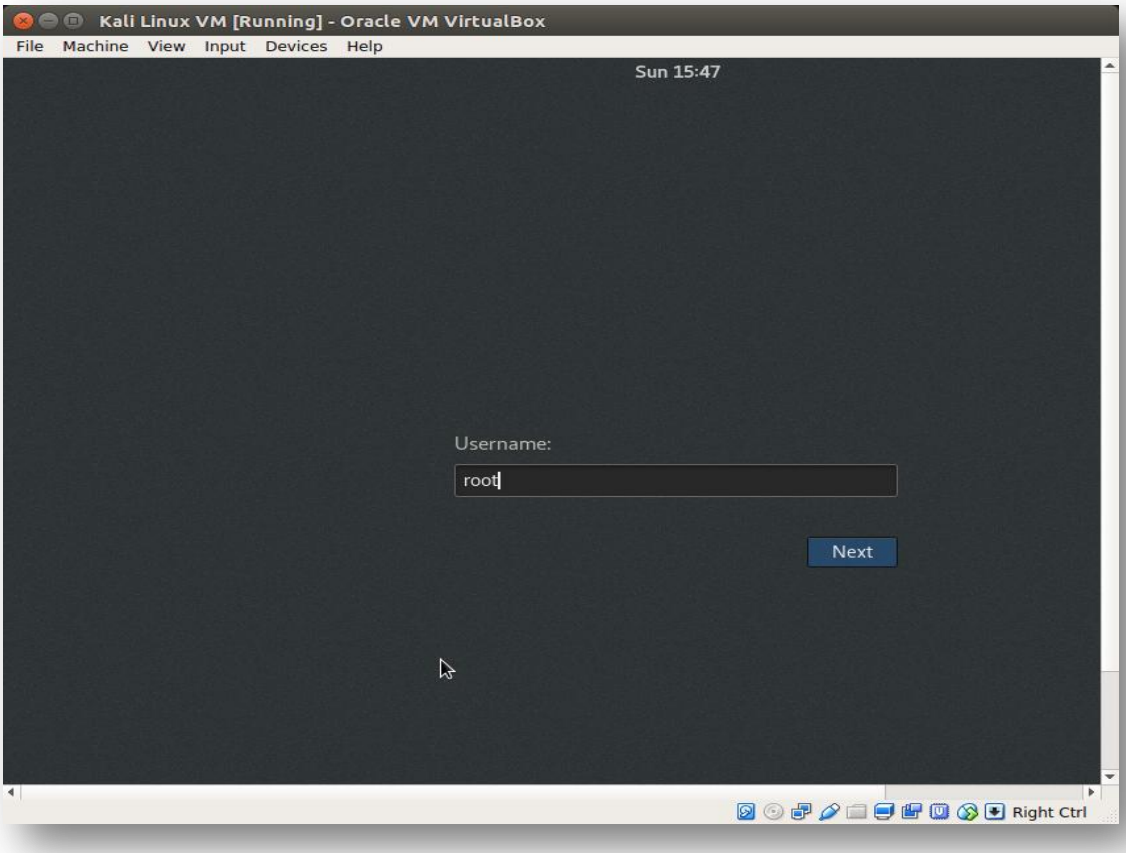
Step35) Select disk and click "Continue".



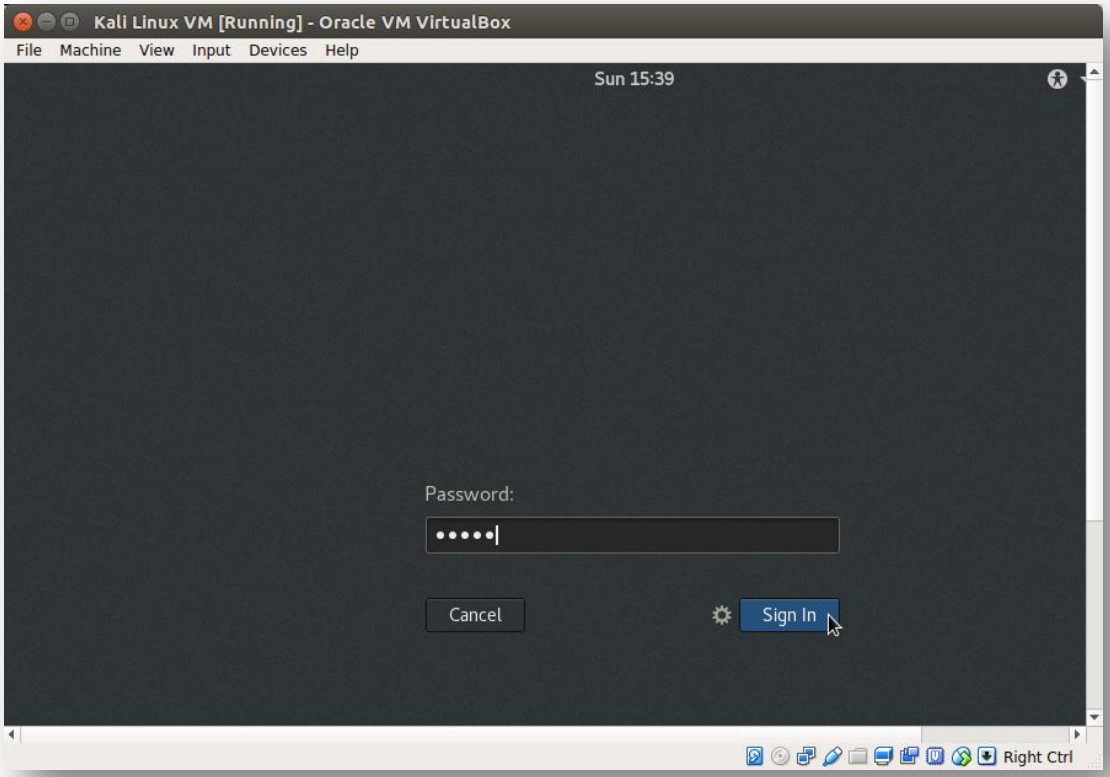
Step 36) Once installation is complete, click "Continue".



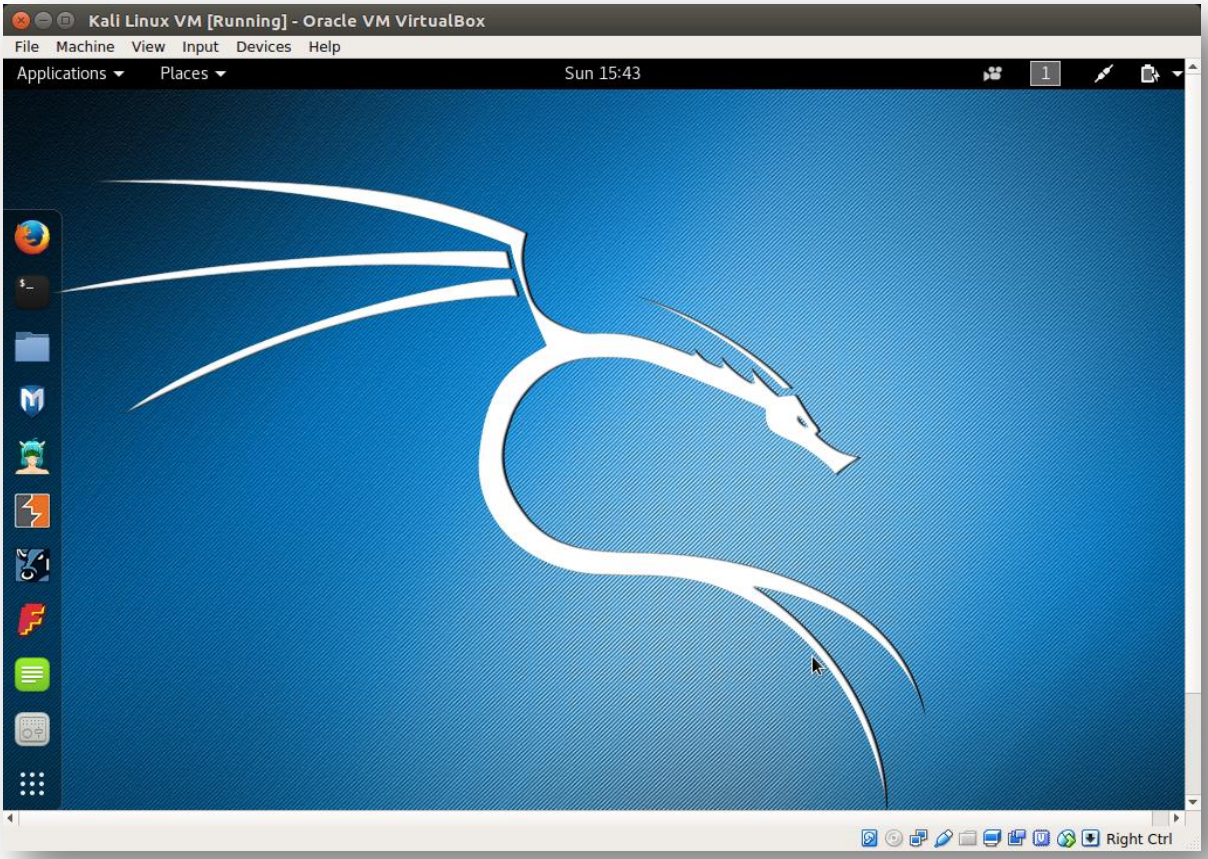
Step 37) Enter the "root" as a username, click "Next".



Step 38) Enter the password which we gave in previous step.



Step 39) You are successfully logged in to the system. You will see the following screen of Kali Linux.



3. John the Ripper Tool

3.1 About John the Ripper Tool

John the Ripper is a free password cracking software tool. Initially developed for the Unix operating system, it now runs on fifteen different platforms (eleven of which are architecture-specific versions of Unix, DOS, Win32, BeOS, and OpenVMS). It is one of the most popular password testing and breaking programs as it combines a number of password crackers into one package, auto detects password hash types, and includes a customizable cracker. It can be run against various encrypted password formats including several crypt password hash types most commonly found on various Unix versions (based on DES, MD5, or Blowfish), Kerberos AFS, and Windows NT/2000/XP/2003 LM hash. Additional modules have extended its ability to include MD4-based password hashes and passwords stored in LDAP, MySQL, and others.

3.2 Using John the Ripper Tool

3.2.1 Windows Password Cracking

Goal: To crack the password of Windows using John the Ripper.

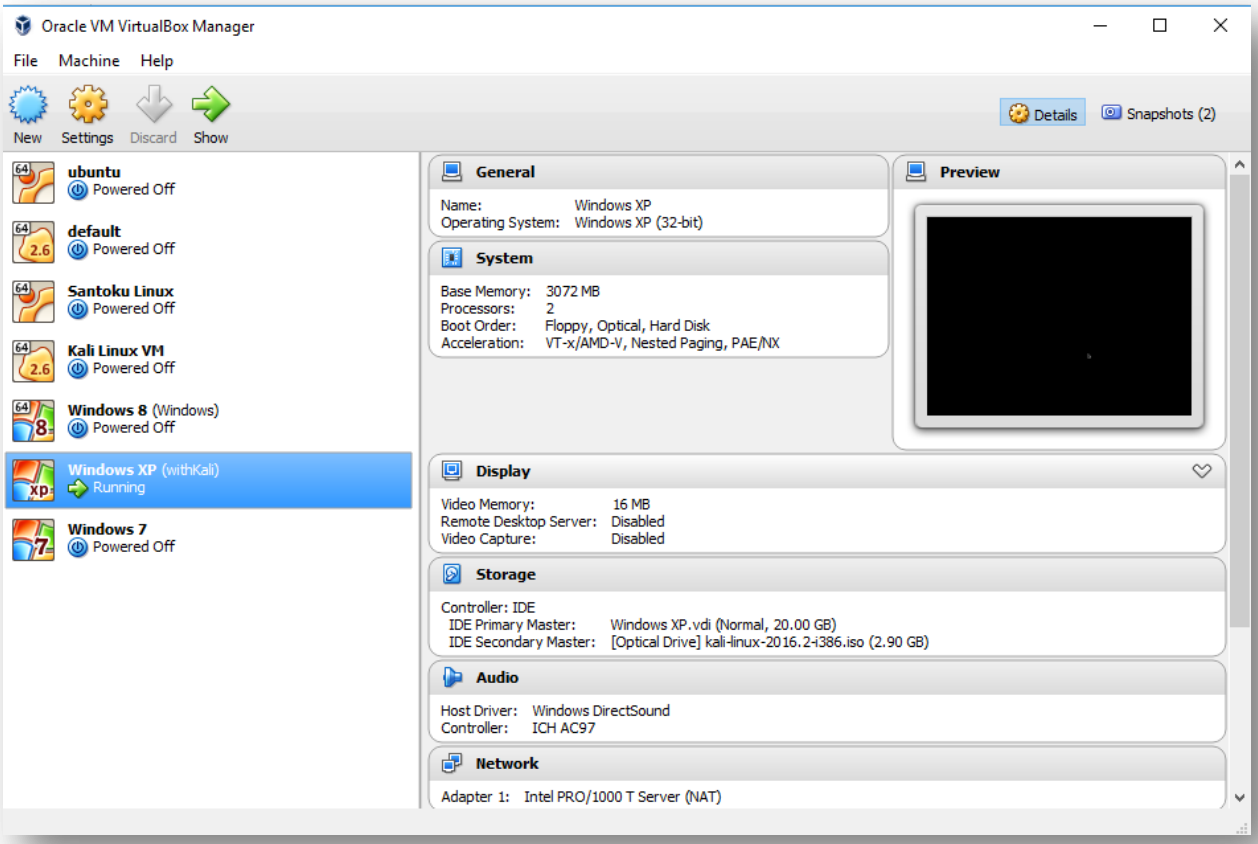
Approach followed:

a) Boot Windows into Kali Linux.
b) Use Kali Linux to mount the Windows disk which contains the SAM database
c) Use bkhive and samdump2 to extract password hashes for users
d) Use John the Ripper to crack the password

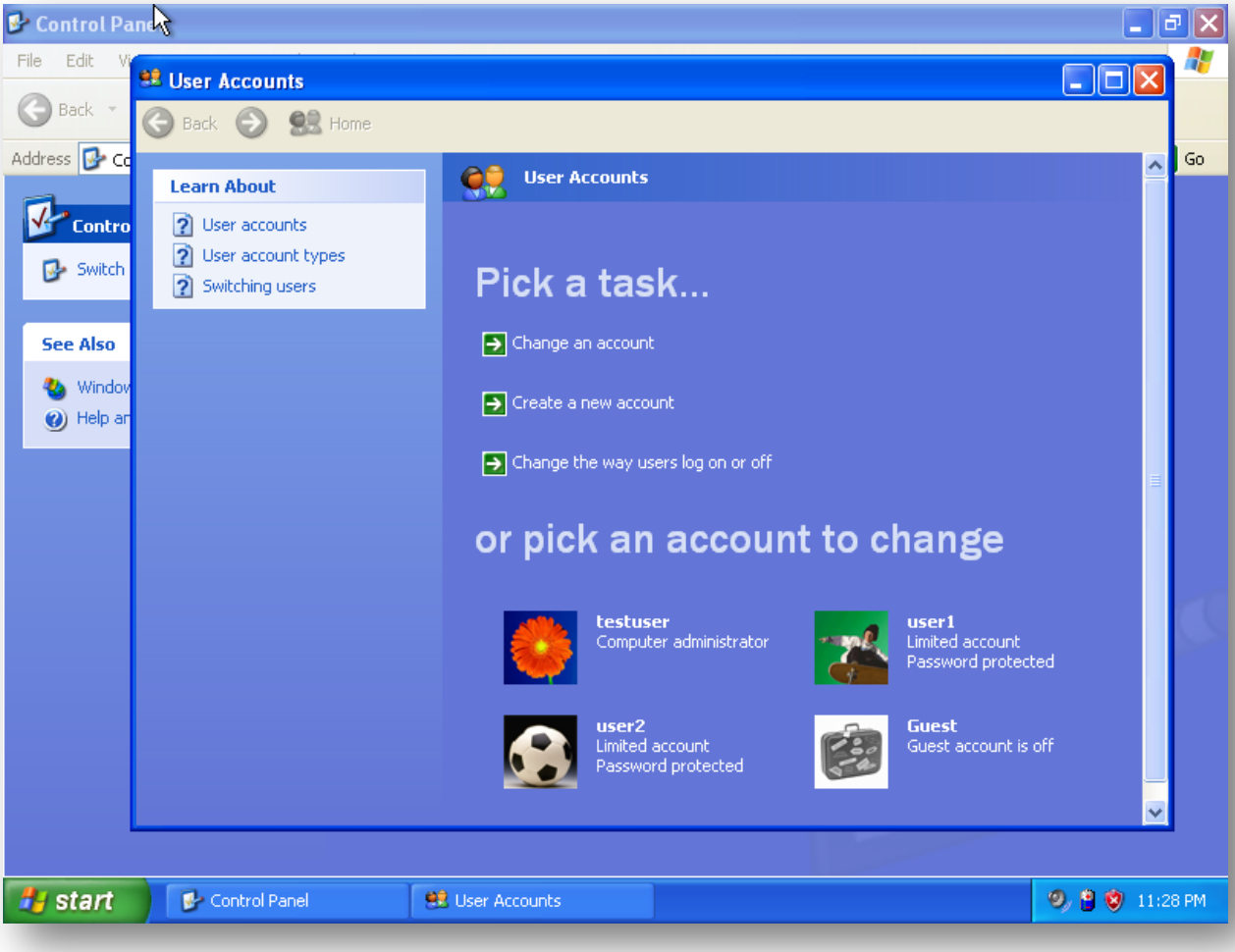
Requirements:

a) Oracle Virtual Box Manager
b) Windows XP ISO file (Used 32 bit ISO file)
c) Kali linux ISO file (Used 32 bit Kali Linux ISO file)
d) bkhive
e) samdump2
f) John the Ripper

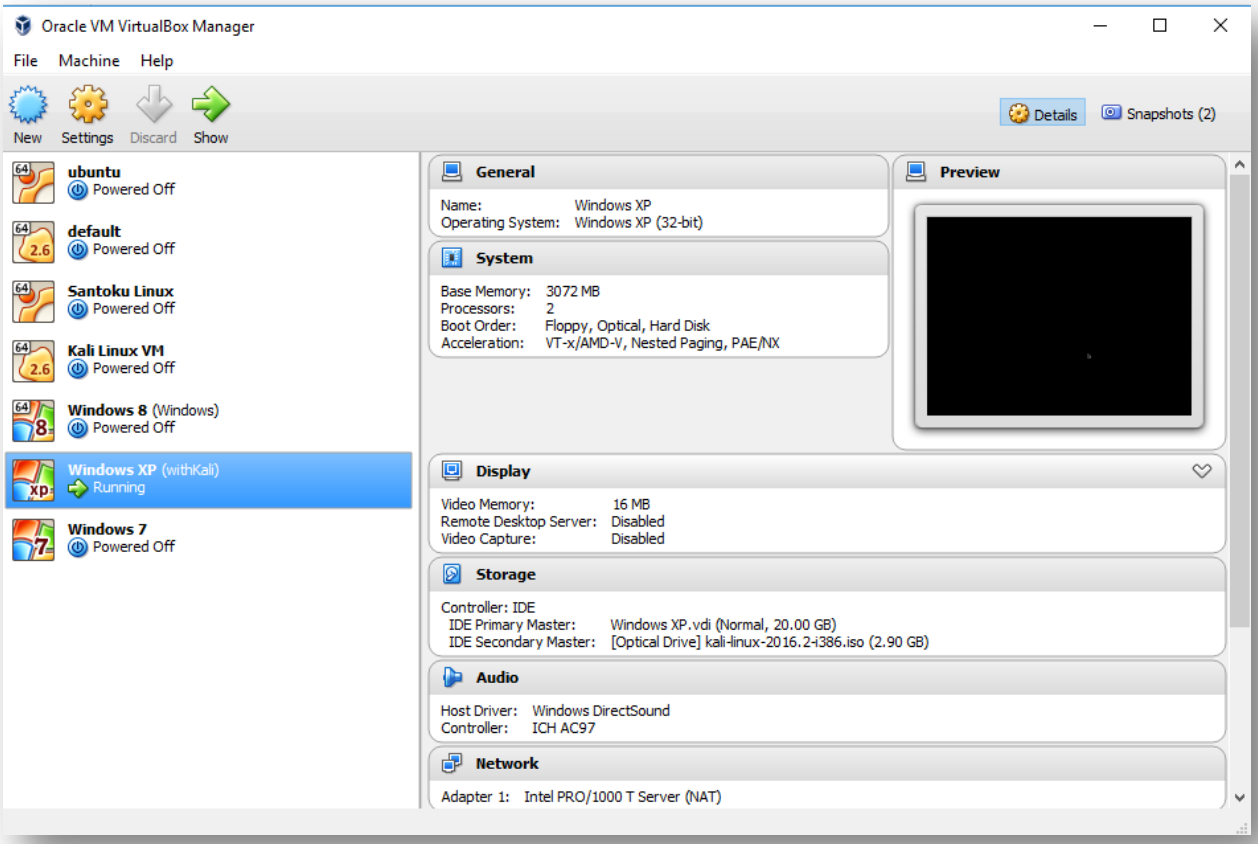
Step1) For this task, I created virtual machine of Windows XP(using 32 bit iso file) on Oracle Virtual Box Manager.



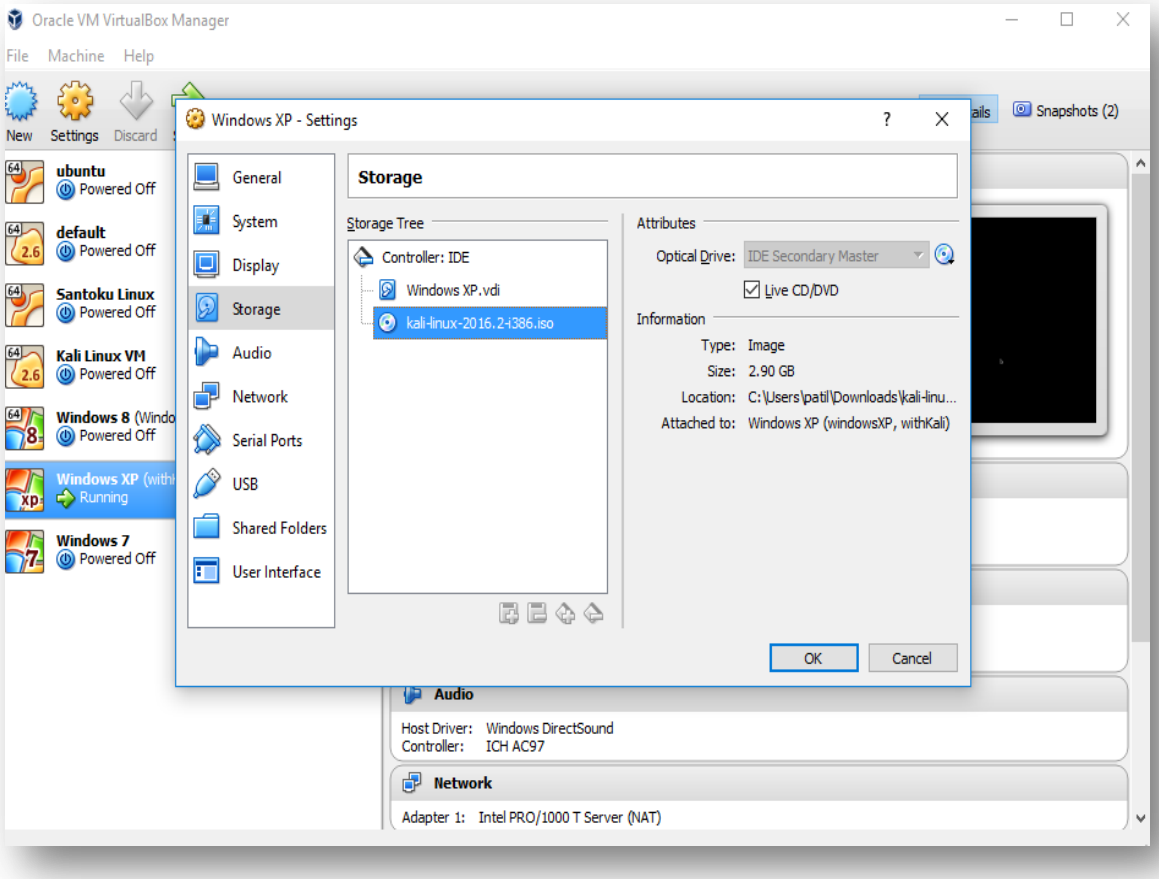
Step 2) For demo purpose, on Windows XP VM, I created different user accounts like user1, user2 with passwords ‘pass’ and ‘east’ respectively.



Step 3) Now, highlight the “Windows XP” virtual machine and click on the “Settings” tab.

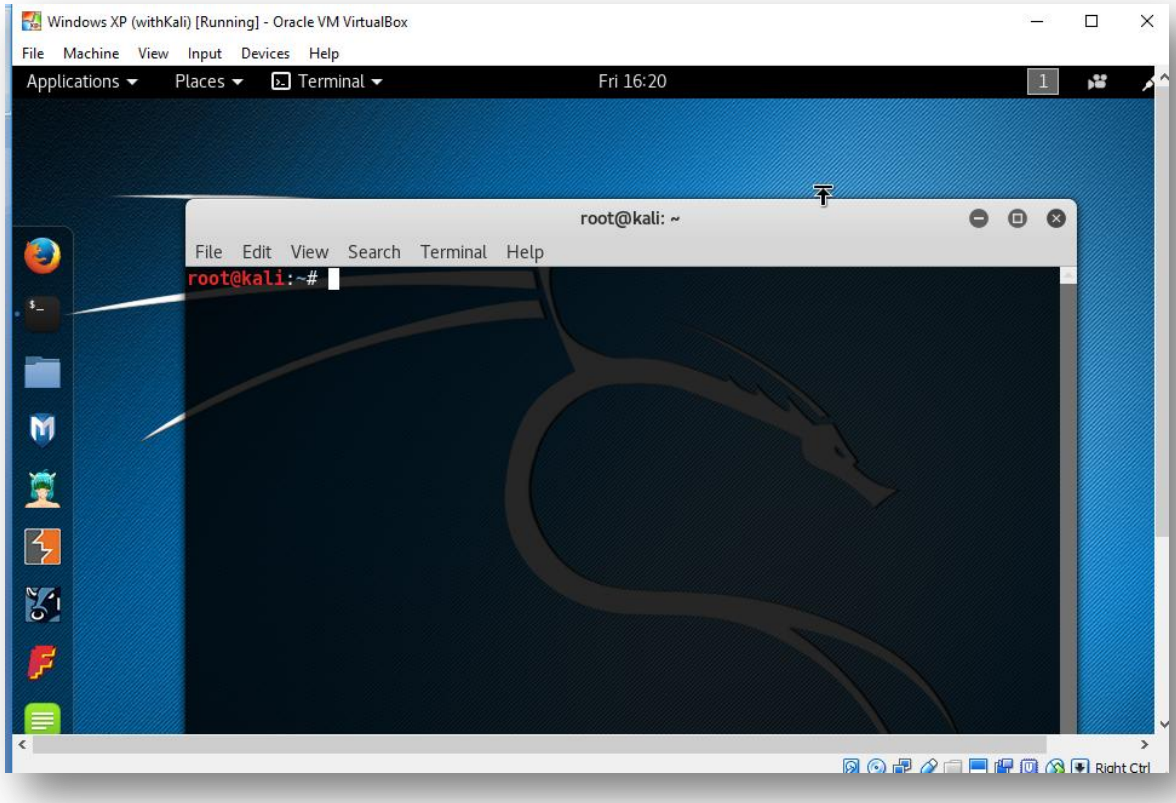


Step 4) Select "Storage" -> "Controller: IDE" .Now, on right side click on the cd icon and browse your Kali Linux ISO file. Check the “Live CD/DVD” option and click on “OK”.



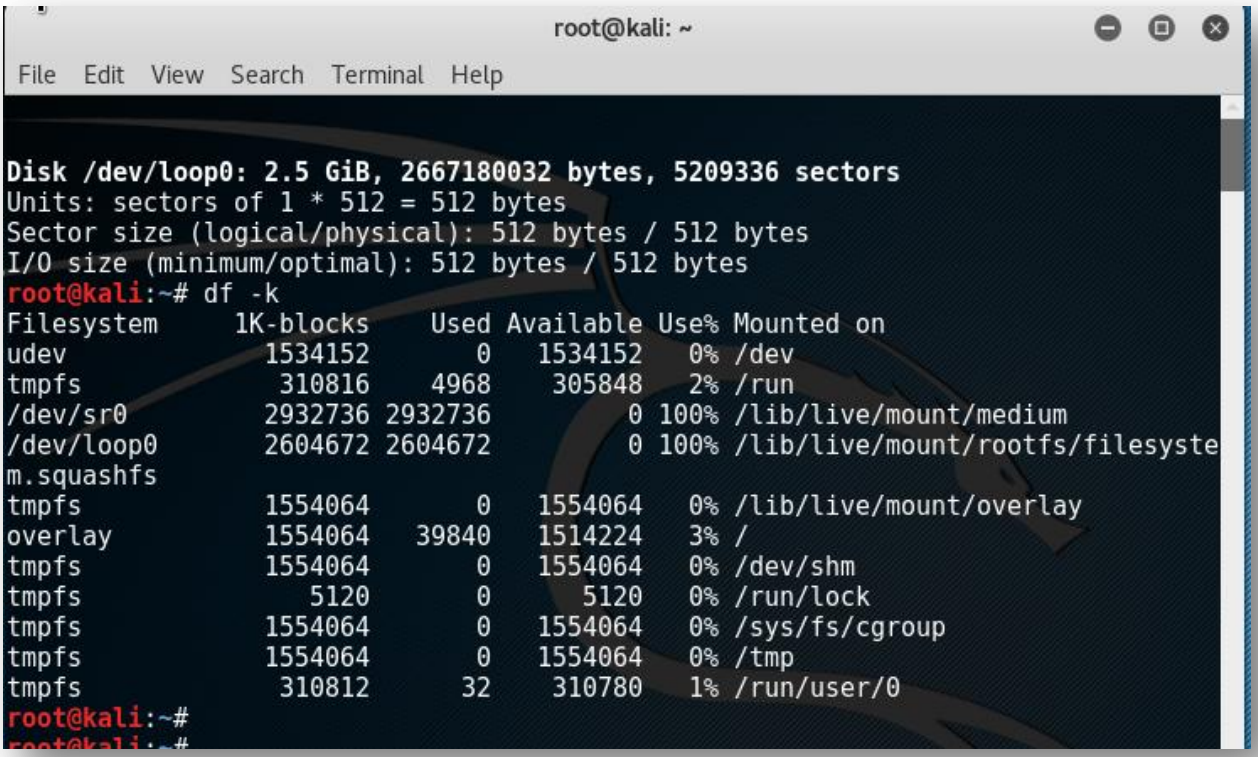
Step 5) Now, start the “Windows XP” VM and then in Kali Linux Boot menu select “Live (686 - pae)” and press ENTER.

Step 6) Now, open the terminal on Kali Linux.



Step7) To see the mount point, type following command on terminal

df –k

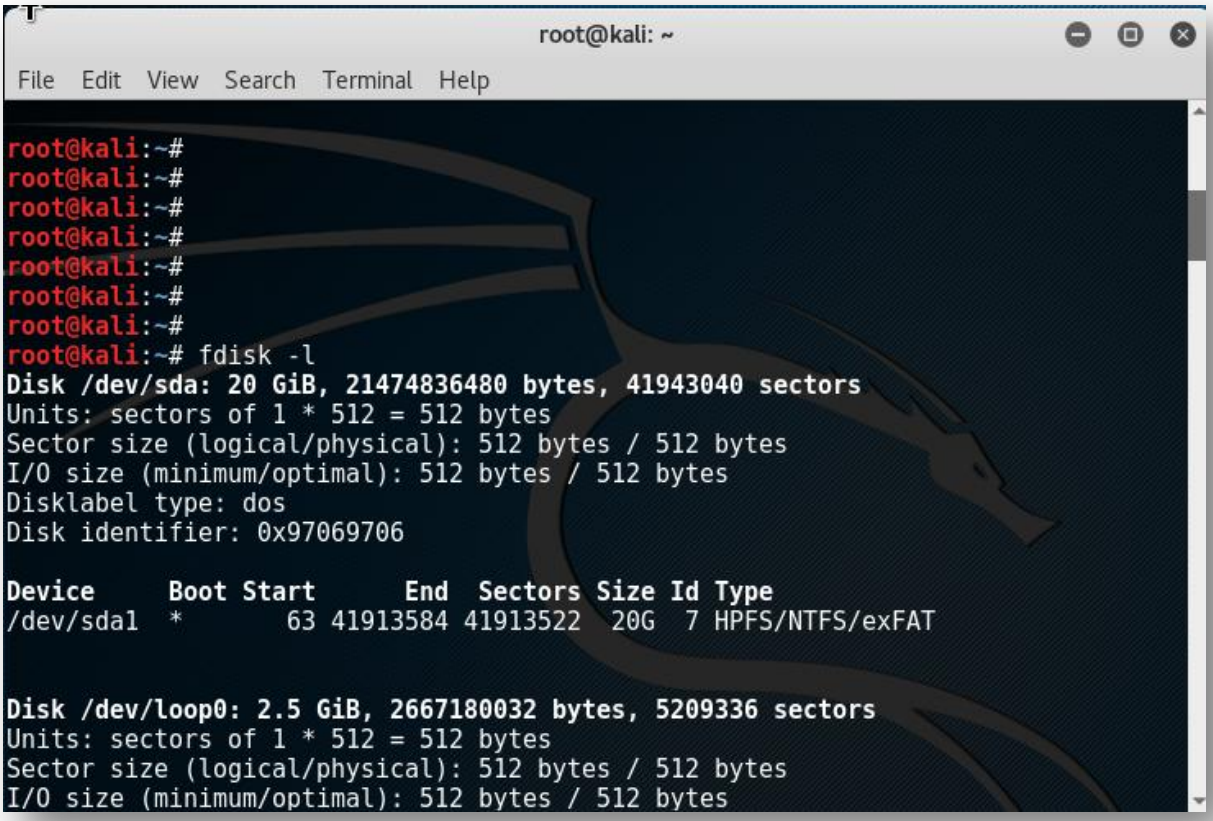


Step 8) On terminal type the following command:

fdisk –l

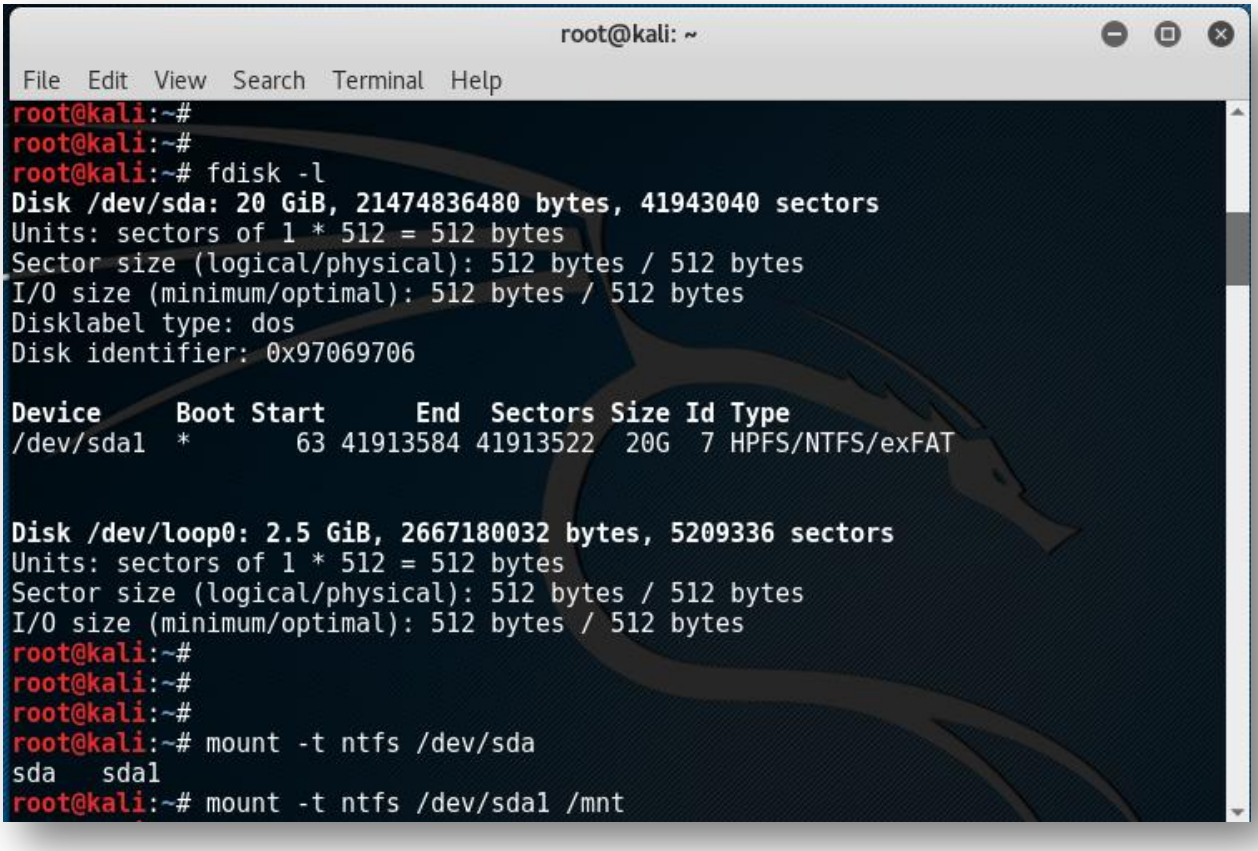
The “fdisk-l” command allows you to see the partition table for disk(s). As you can see, “/dev/sda1” is the disk which contains the SAM database.

The SAM database is the Security Accounts Manager database, used by Windows that manages user accounts and other things. It is implemented as a registry file that is locked for exclusive use while the OS is running.



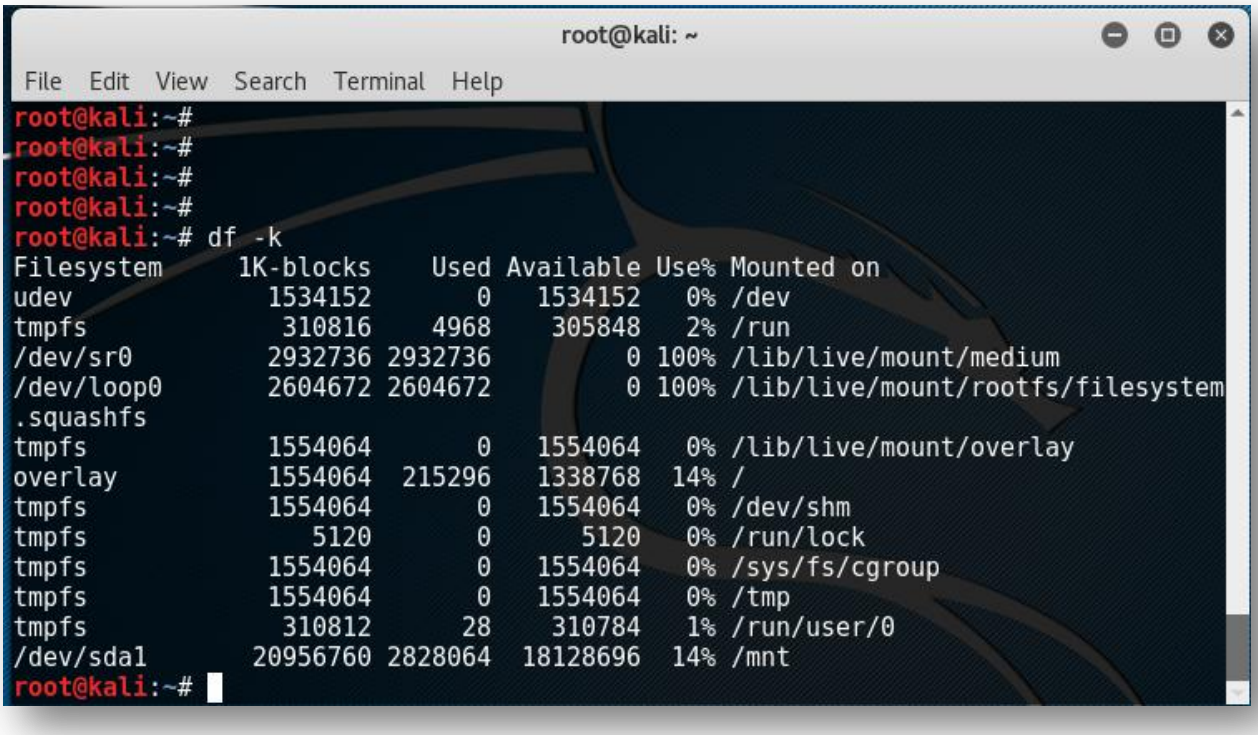
Step 9) Now, we will mount the Windows disk. To do this, type following command on the terminal:

mount –t ntfs /dev/sda1 /mnt



Step 10) Again type the following command on the terminal to make sure that the Windows disk is mounted correctly.

df -k

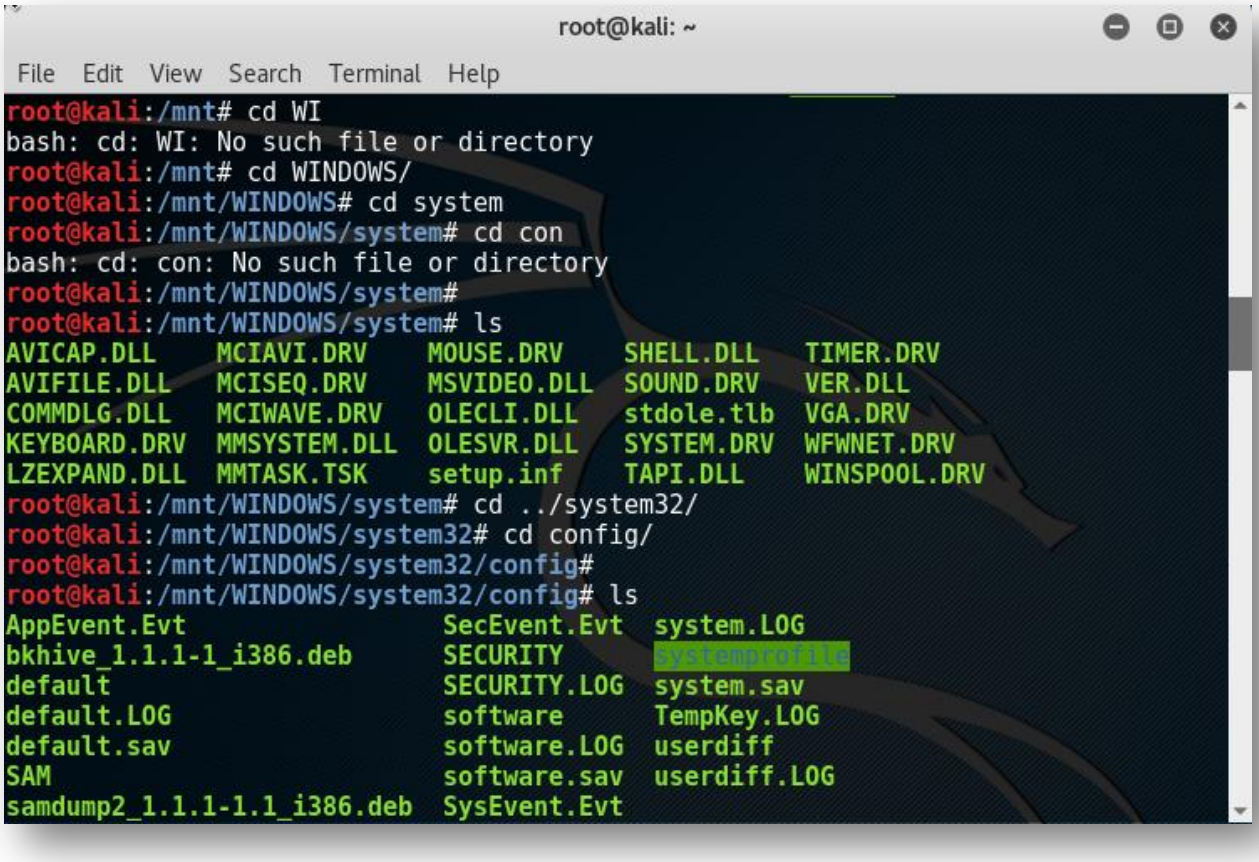


Step 11) To view the Windows disk contents type command on the terminal:

cd /mnt

As, the SAM database is in /mnt/WINDOWS/system32/config directory, type following command on the terminal:

cd /WINDOWS/system32/config



As you can see in the screen shot that:

"SAM" database is in the /mnt/WINDOWS/system32/config directory.

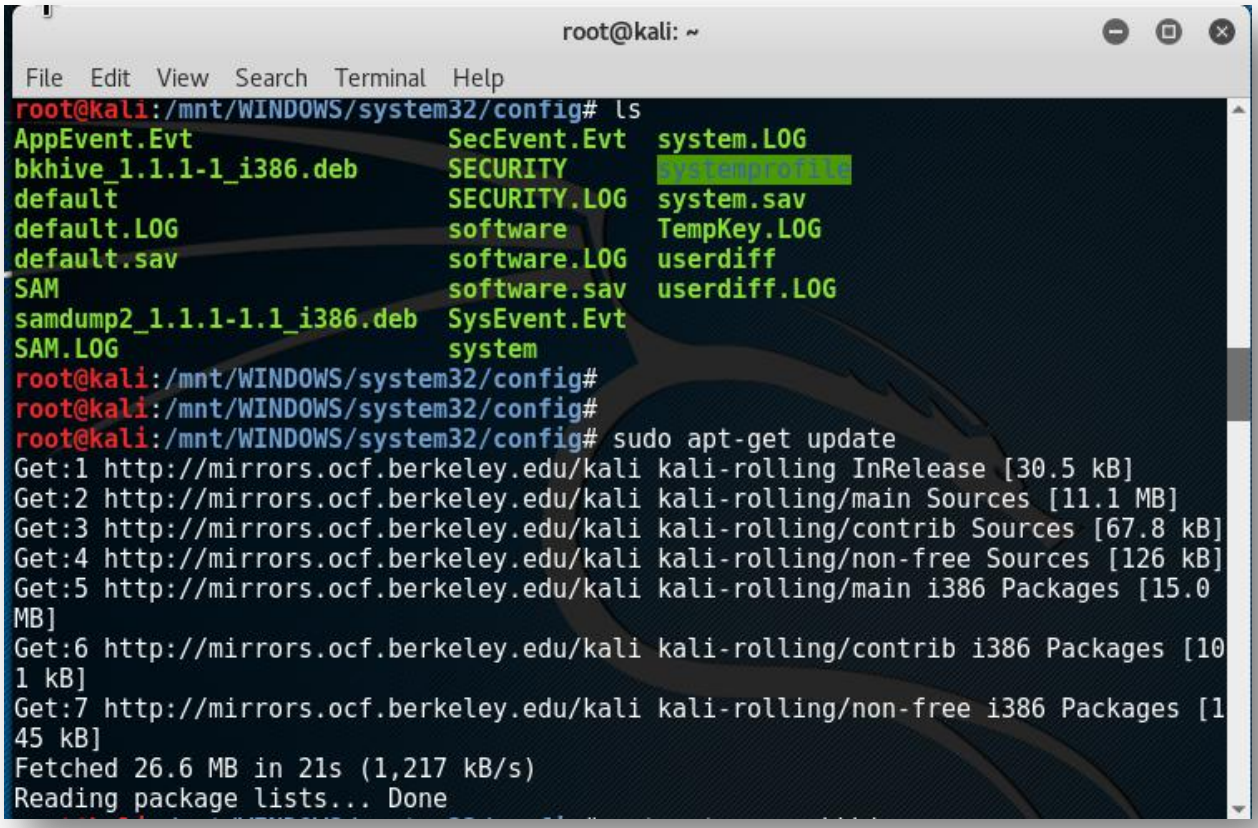
Step 12) In “config” directory, there is not bkhive or samdump2. To install bkhive type following commands:

sudo apt-get update
#sudo apt-get install bkhive

bkhive dumps the syskey bootkey from Windows NT/2K/XP/Vista system hive.

samdump2 dumps the Windows NT/2K/XP/Vista password hashes.

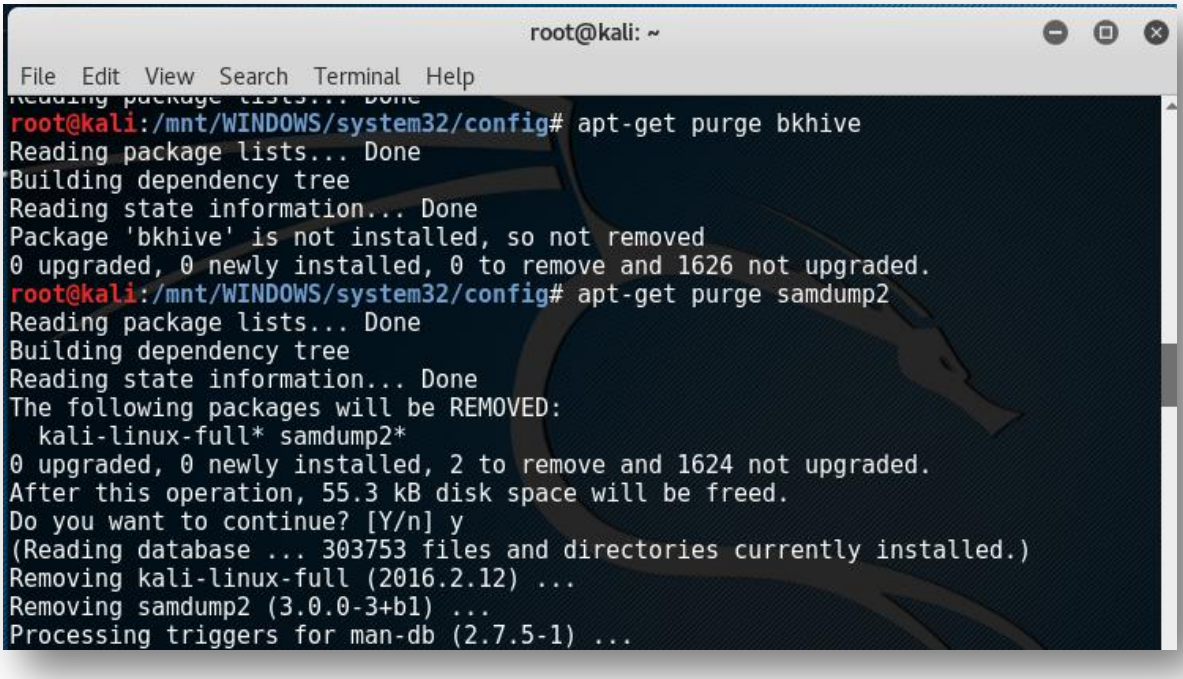
In my case, when I tried to install bkhive, it was not installed. So, to solve this issue I followed the approach explained in the next step.



Step 13) I downgrade the previous versions of bkhive and samdump2. To do that type following commands:

apt-get purge bkhive
#apt-get purge samdump2

These two commands will remove the bkhive and samdump2 packges.



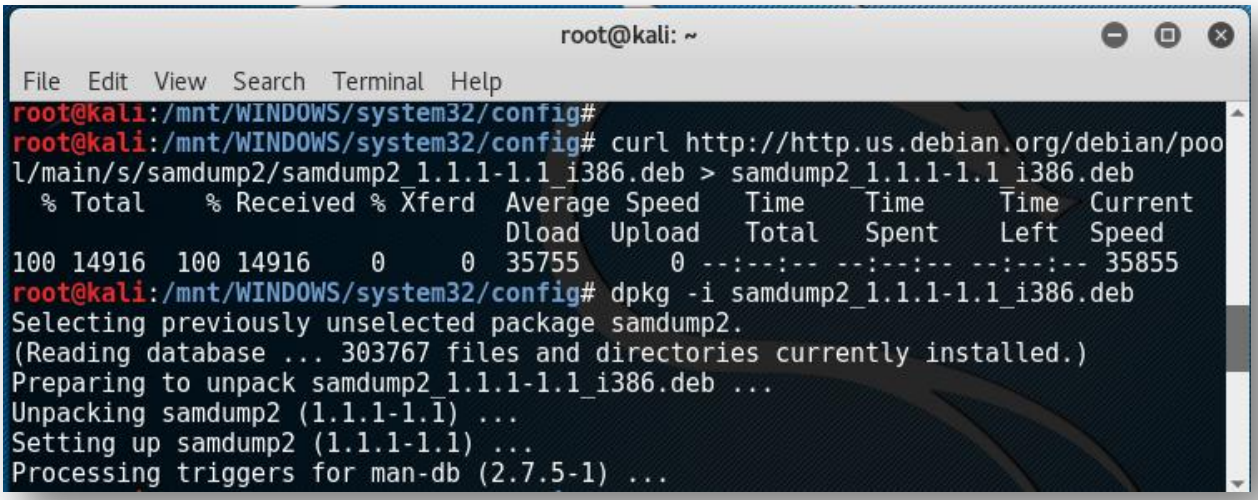
Step 14) Type following command to download samdump2:

curl http://http.us.debian.org/debian/pool/main/s/smdump2/samdump2_1.1.1-1.1_i386.deb> samdump2_1.1.1-1.1_i386.deb

Now, to install the samdump2 type the following command on the terminal:

dpkg –i samdump2_1.1.1-1.1_i386.deb

For me, after running this command I got the error saying that samdump2 has the dependency on the file named “libssl1.0.0”.

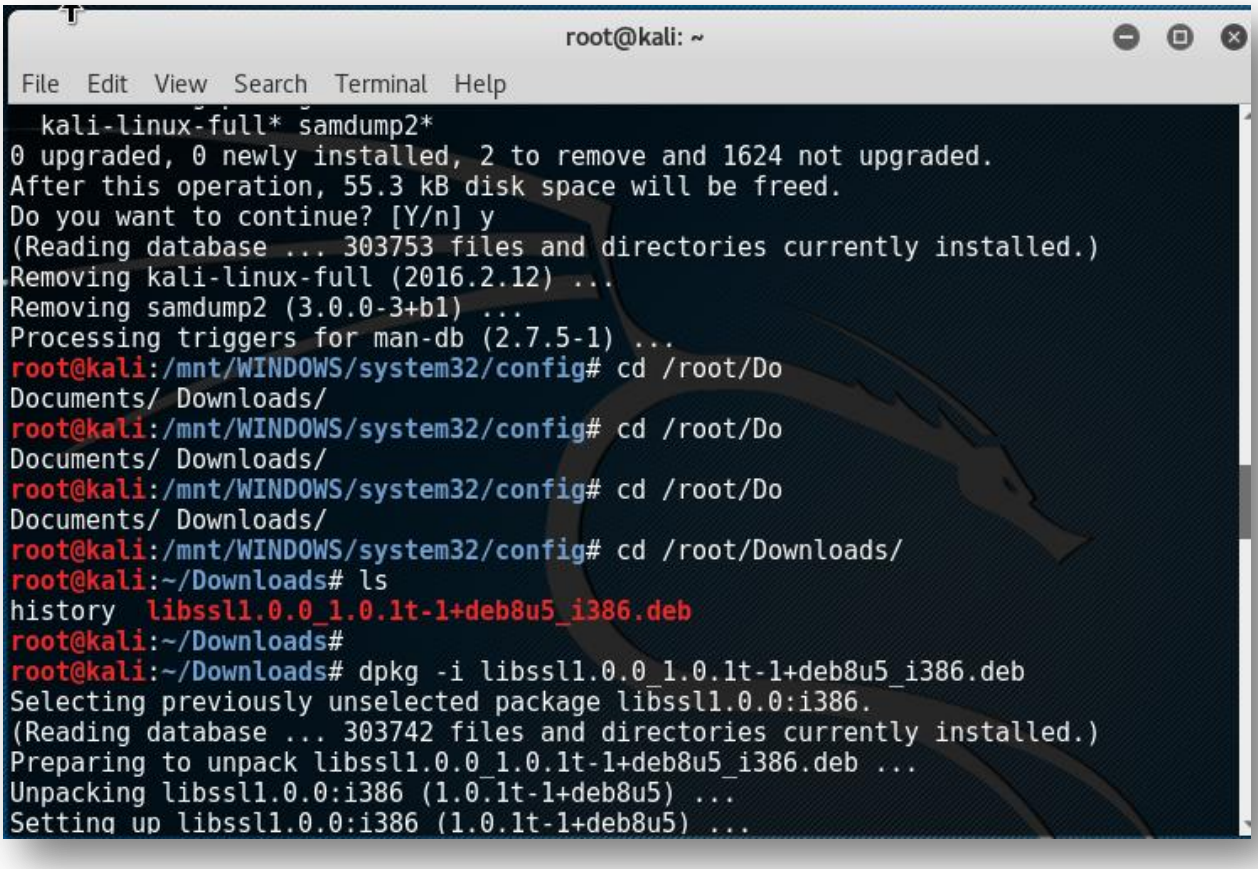


To solve this issue, I downloaded it from: https://packages.debian.org/jessie/libssl1.0.0 and then typed following commands on the terminal:

cd /root/Downloads/

dpkg –i libssl1.0.0_1.0.1t-1+deb8u5_i386.deb

Then try to install samdump2 using above command.

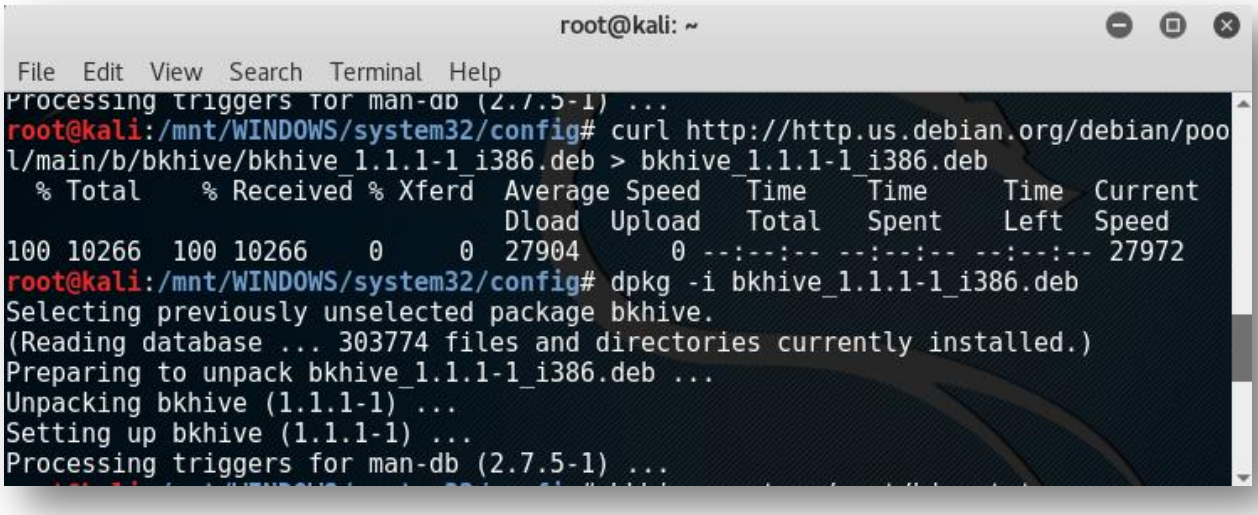


Step 15) Type following command to download bkhive:

curl http://http.us.debian.org/debian/pool/main/b/bkhive/bkhive_1.1.1-1_i386.deb> bkhive_1.1.1-1_i386.deb

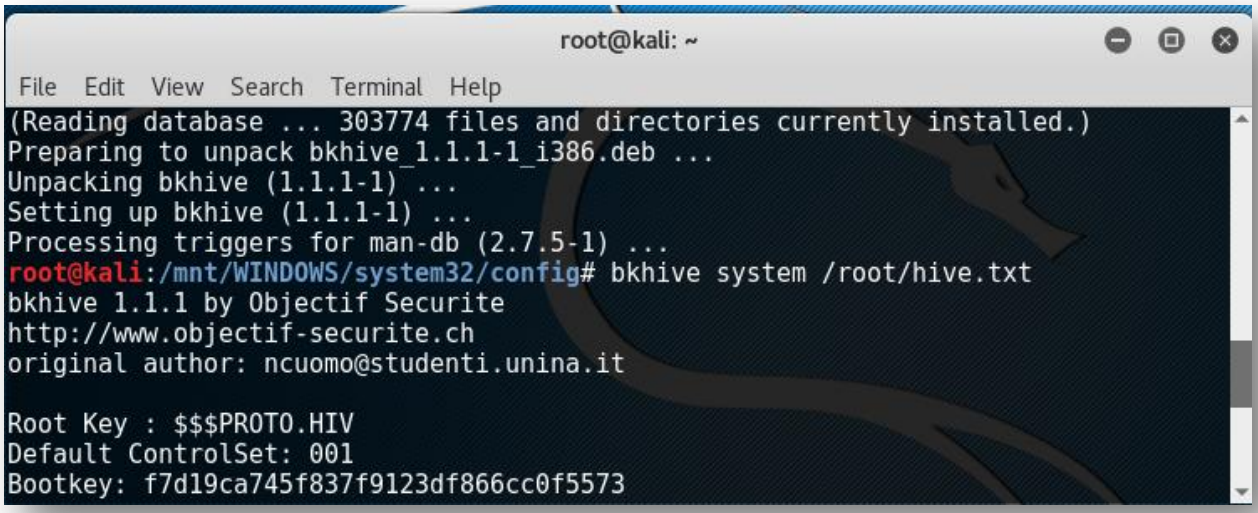
Now, to install the samdump2 type the following command on the terminal:

dpkg –i bkhive_1.1.1-1_i386.deb



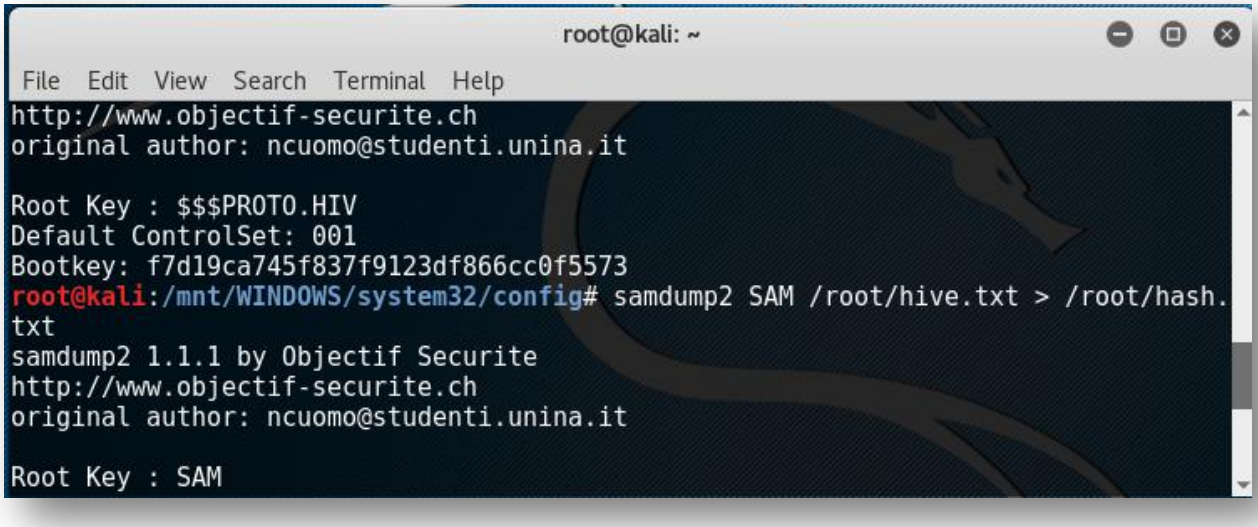
Step 16) “bkhive” dumps the syskey bootkey from Windows NT/2k/XP/Vista system hive. So, to use bkhive type following command on the terminal:

```
# bkhive system /root/hive.txt
```



Step 17) “samdump2” dumps the Windows NT/2k/XP/Vista password hashes. To use samdump2, type following command on the terminal:

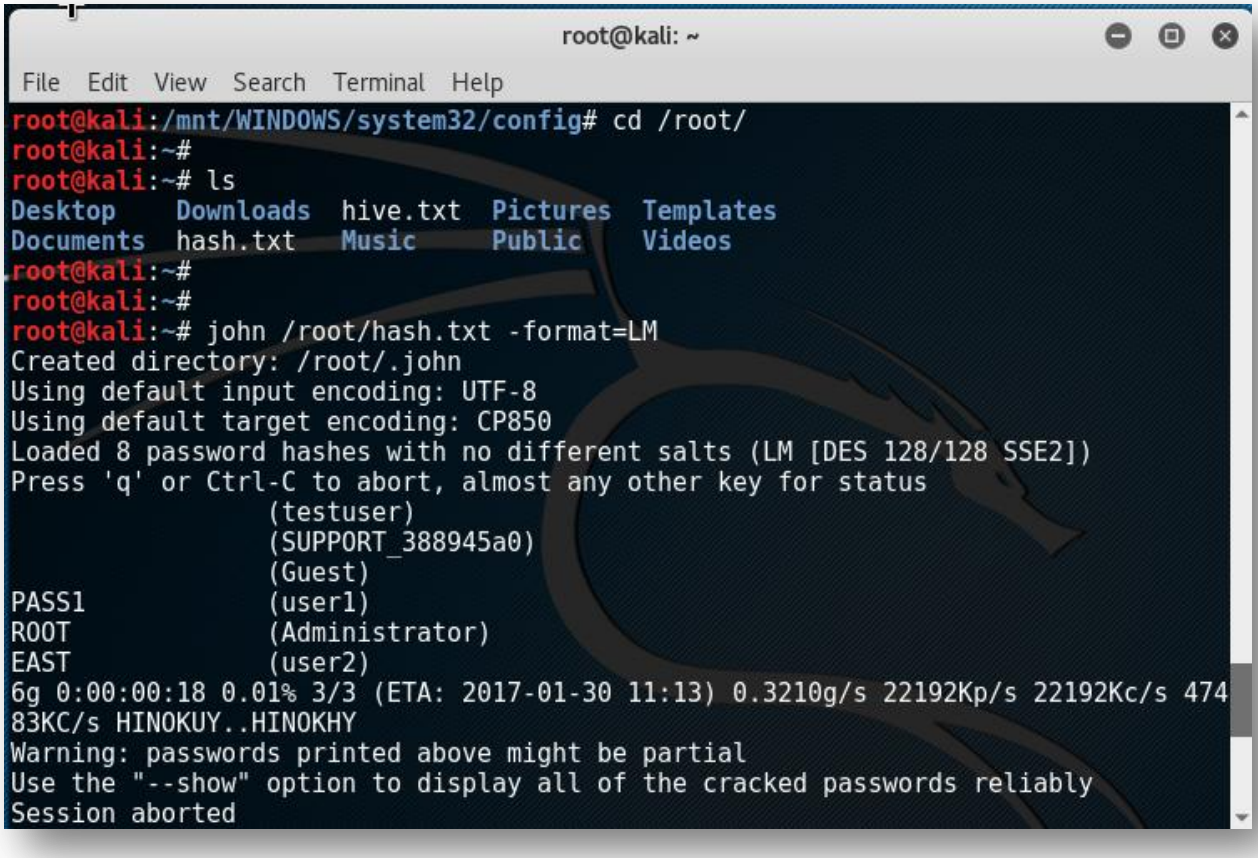
```
# samdump2 SAM /root/hive.txt > /root/hash.txt
```



Step 18) Now, we will use password cracking tool called, “John the Ripper”. To use John the Ripper type following command on the terminal:

john /root/hash.txt –format=LM

Now, you can see that on the right side part of window there are the users in the Windows system (user1, Administrator, user2) and on the left side their corresponding passwords (PASS1, ROOT, EAST).



After you ran the above command, it stores the results into .john directory under the current user’s home directory.

To see the cracked passwords stored in file john.pot, type the following command:

cd /root/.john

cat john.pot

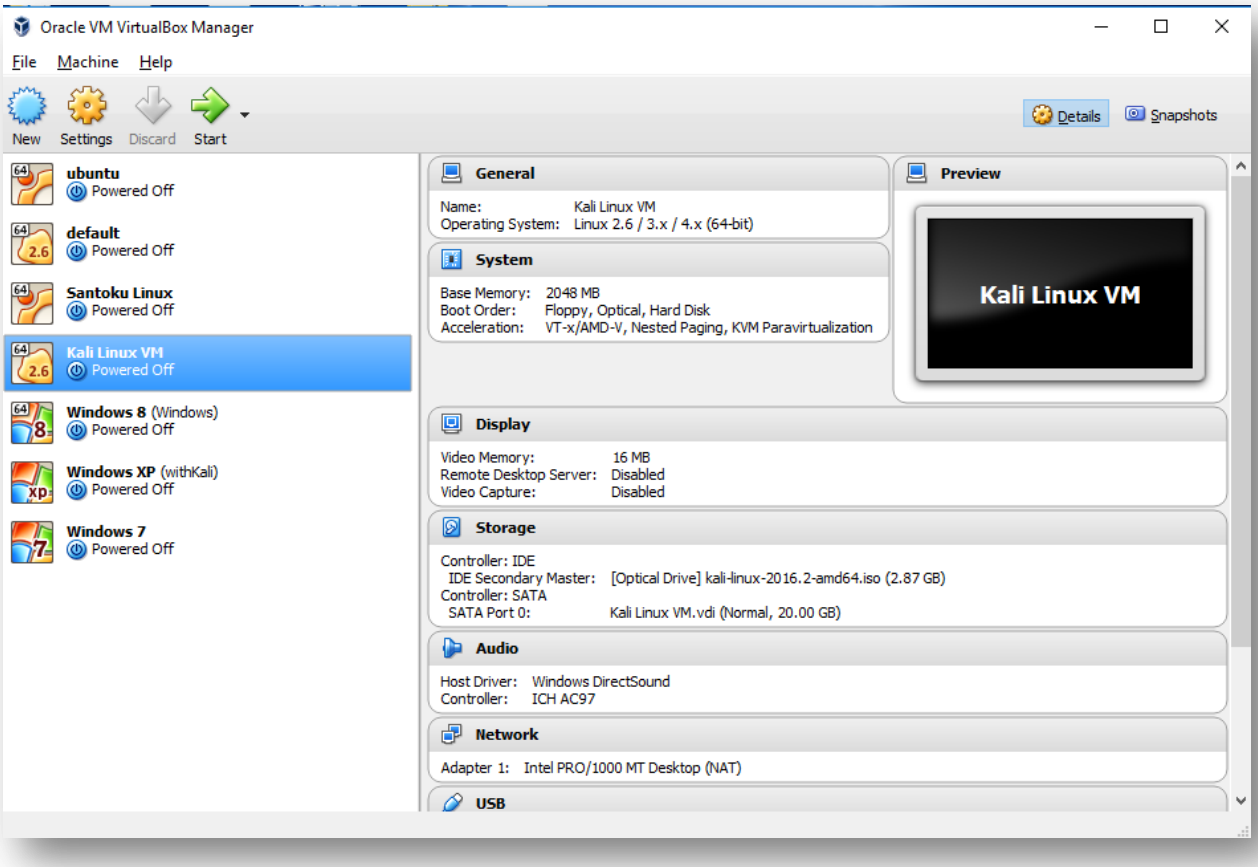
3.2.2 Kali Linux Password Cracking

John the Ripper is a free password cracking tool. One of the modes John the Ripper can use is the dictionary attack. It takes text string samples (called wordlist), encrypting it in the same format as the password being examined and then comparing the output to the encrypted string. Here we are going to use this **dictionary attack.**

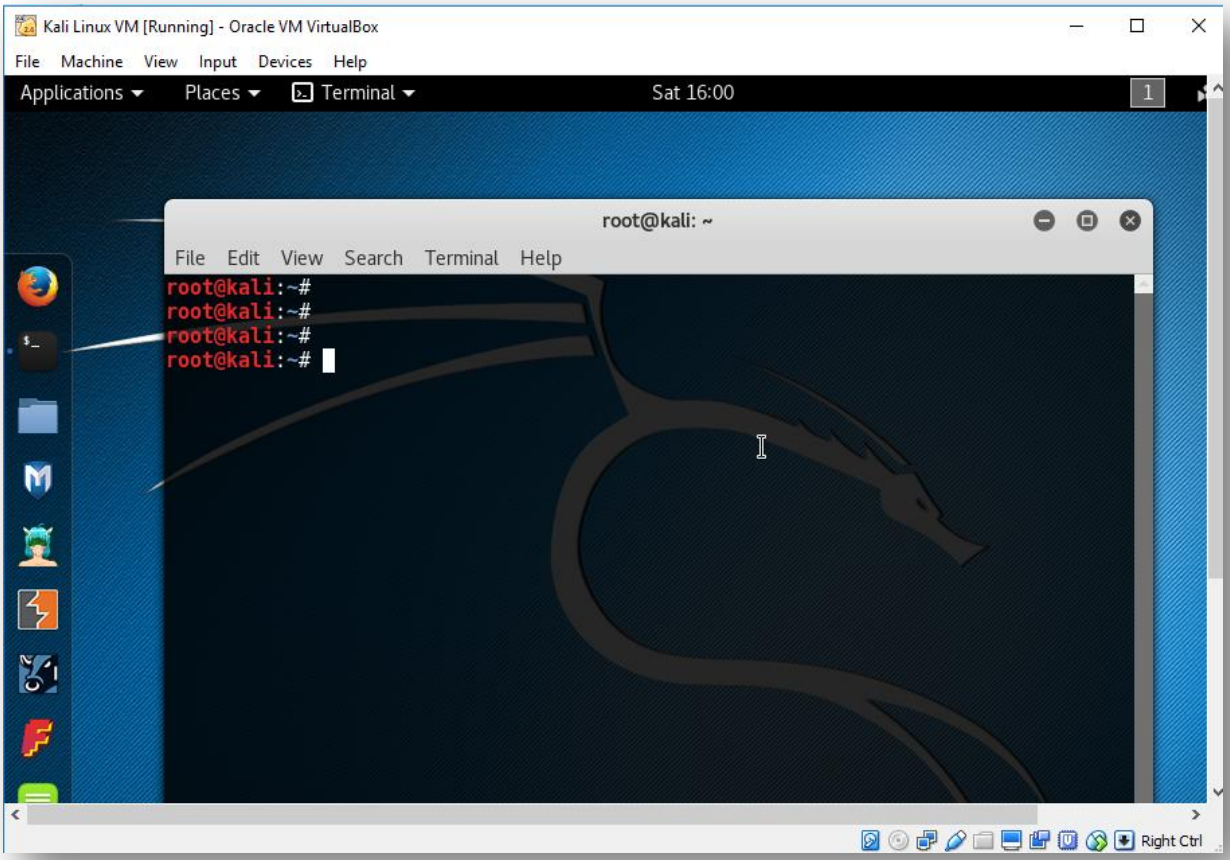
John the Ripper uses two step processes for cracking the password. It uses **passwd** and **shadow** file to create an output file. Then, use the dictionary attack against that file to crack the password.

Steps to follow to crack the Kali Linux password using John the Ripper:

Step 1) On Oracle VM VirtualBox, highlight the Kali Linux VM and then click on the "Start" button.



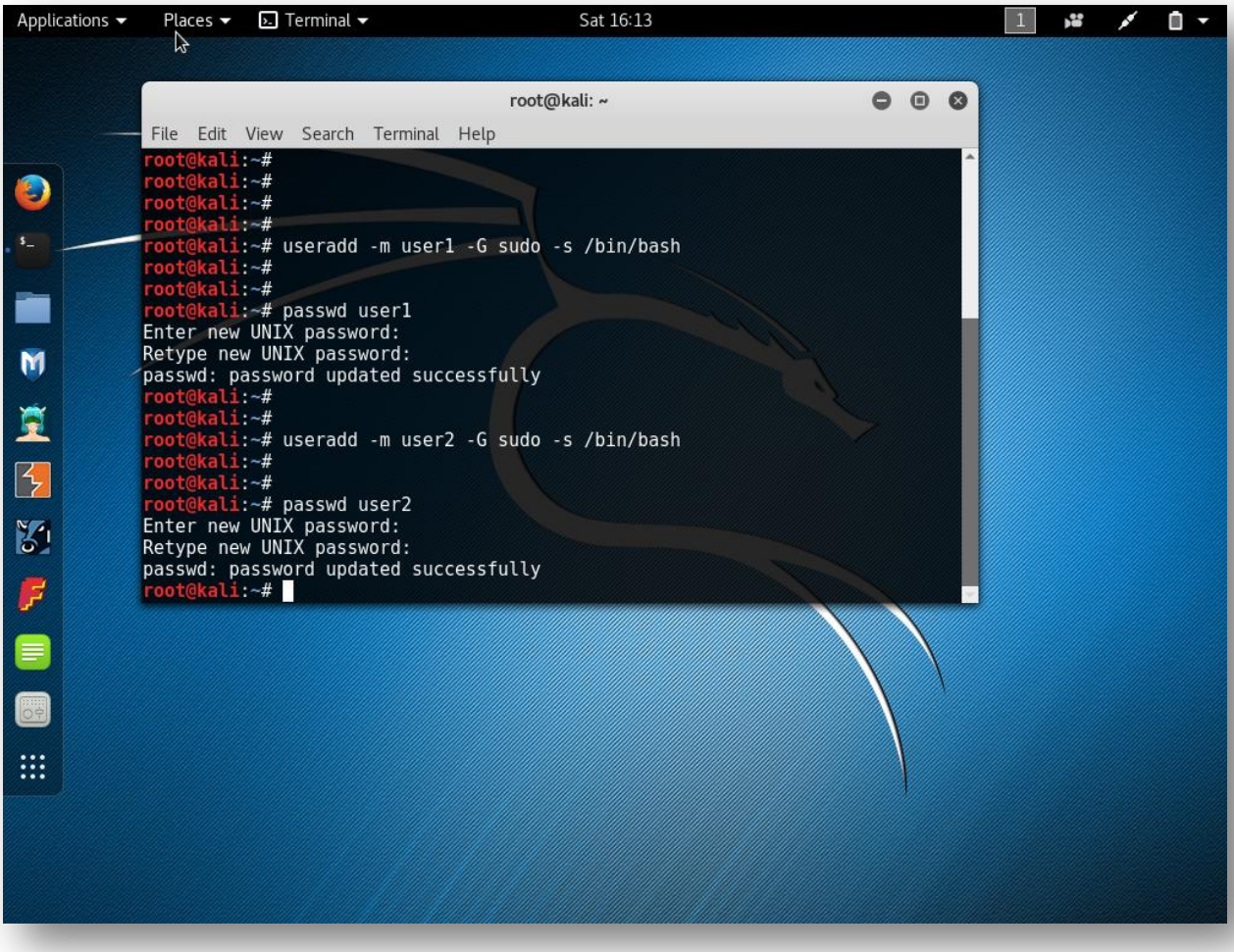
Step 2) On Kali Linux, click on the “Terminal” and then it will open the Kali Linux command prompt as shown bellow.



Step 3) Now, we will create two users namely user1 and user2 with passwords “pass” and “east” respectively. To do this type the following command on the terminal.

useradd –m user1 –G sudo –s /bin/bash

useradd –m user2 –G sudo –s /bin/bash



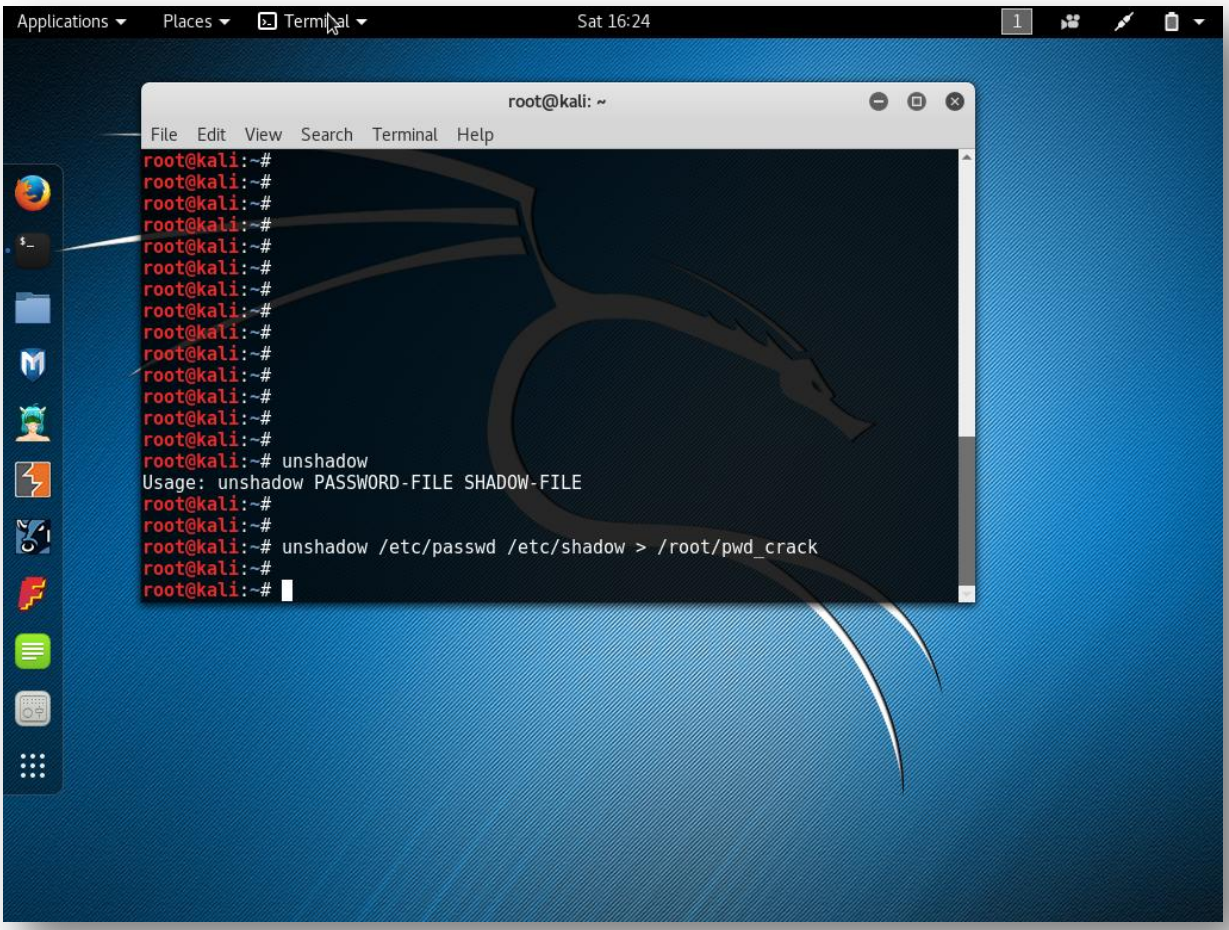
Above commands will add user1 and user2 to sudo group and assign /bin/bash as its shell. Now we have following users and their respective passwords:

User	Password
Administrator	test
user1	pass
user2	east

Step 4) Unshadowing the password :

The unshadow command will combine the extries of /etc/passwd and /etc/shadow into one file which contains usernames and passwords information.

unshadow /etc/passwd /etc/shadow > /root/pwd_crack

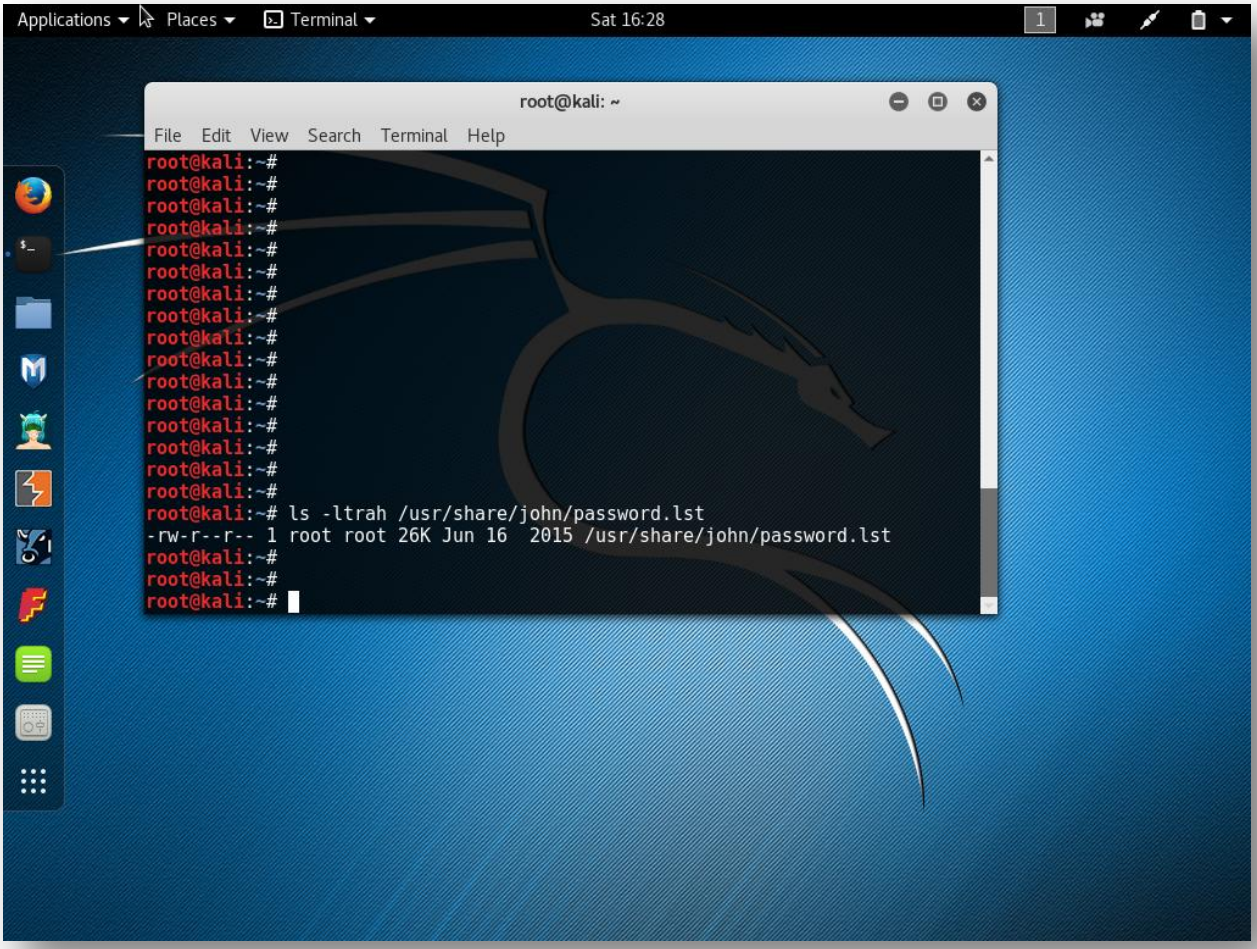


Step 5) Cracking the password with John the Ripper:

John the Ripper comes with password file which is located in /usr/share/john/password.lst

To see the size of that file, type following command on the terminal:

ls –ltrah /usr/share/john/password.lst



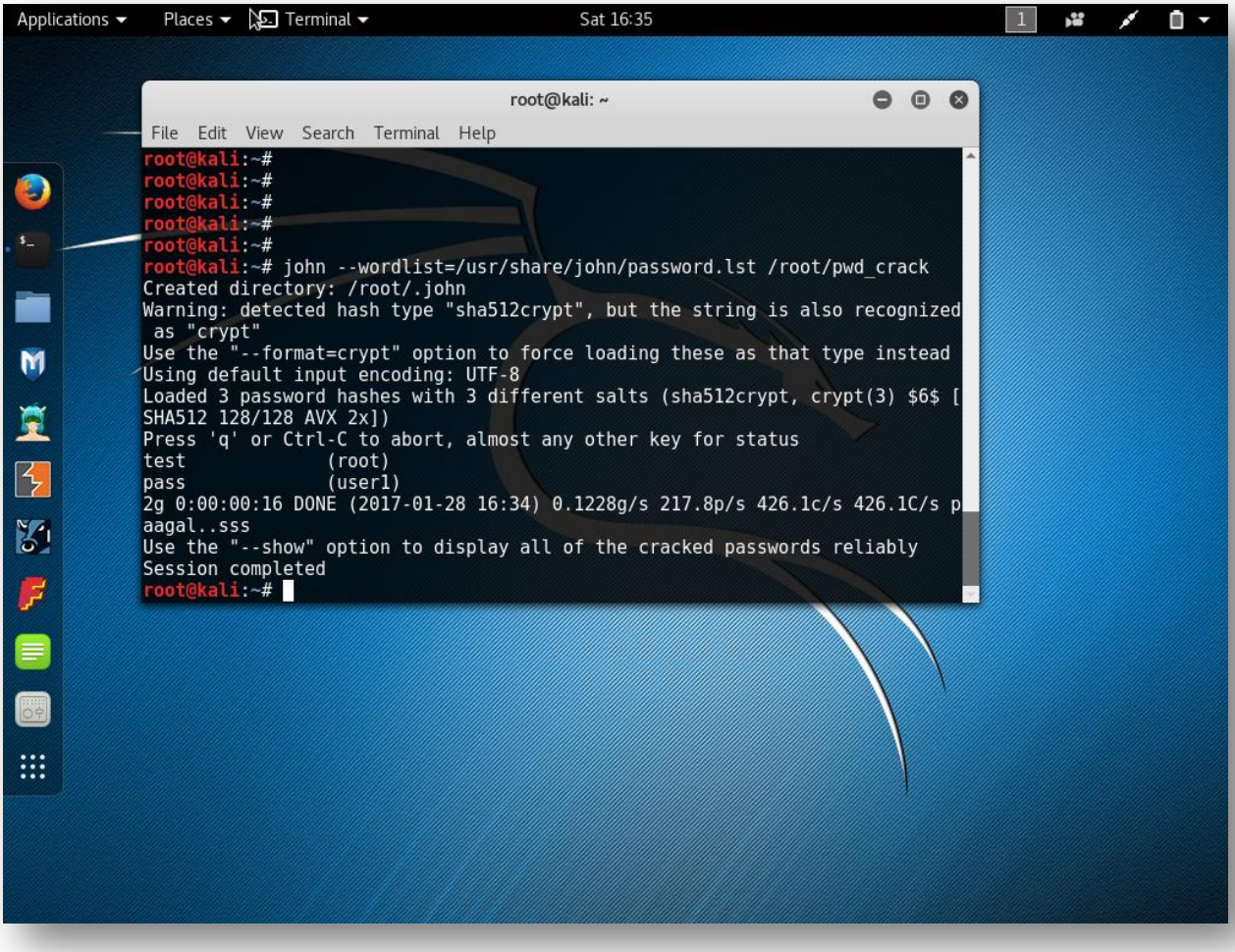
Step 6) To use this dictionary for cracking of the password, type following command on the terminal:

john –wordlist=/usr/share/john/password.lst /root/pwd_crack

This command uses two files password.lst (dictionary file) and pwd_crack (created in step4)

After you ran this command, you can see that password for root user (which is administrator) and user1 are cracked successfully by John the Ripper.

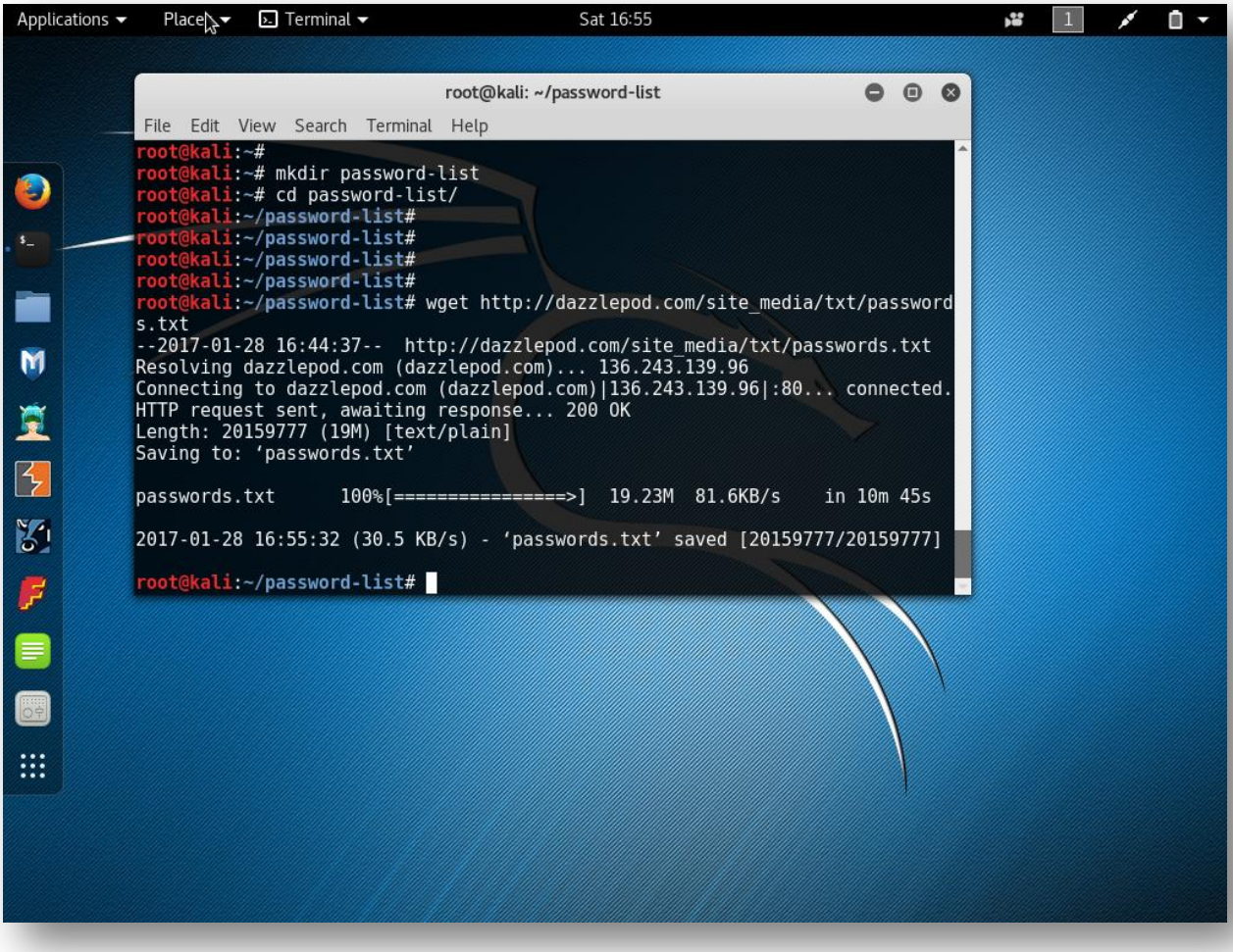
For root: password is “test”
For user1: password is “pass”



Step 7) However, we are not able to recover the password for user2. So, to solve this problem, I downloaded another dictionary from internet. If passwords are more complex, we can use bigger dictionary available on internet.

To download dictionary type following command:

wget http://dazzlepod.com/site_media/txt/passwords.txt

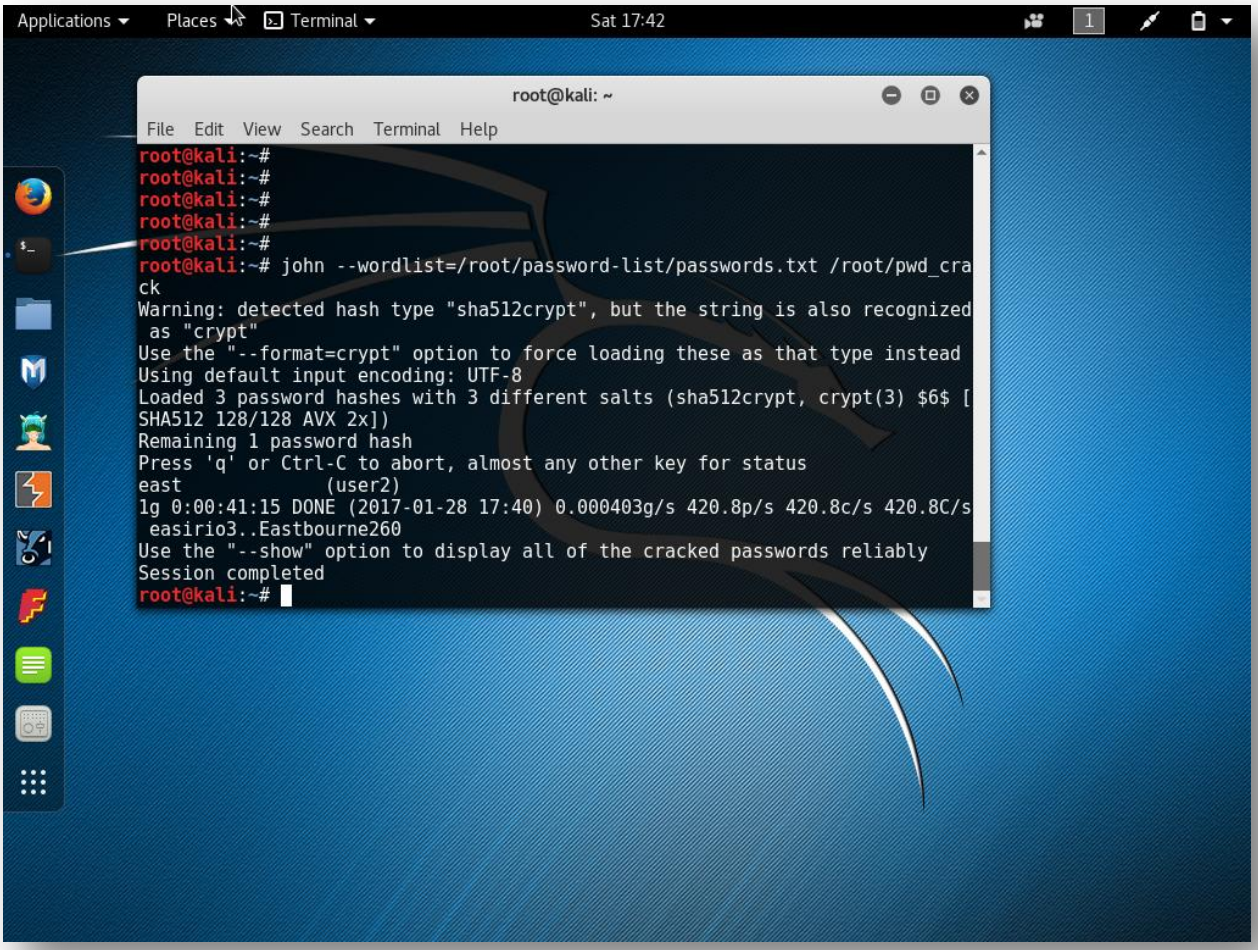


Step 8) Now, again try to crack the password using passwords.txt dictionary. Type following command on the terminal.

john –wordlist=/root/password-list/passwords.txt /root/pwd_crack

After you ran this command, you can see that the password for user2 is cracked.

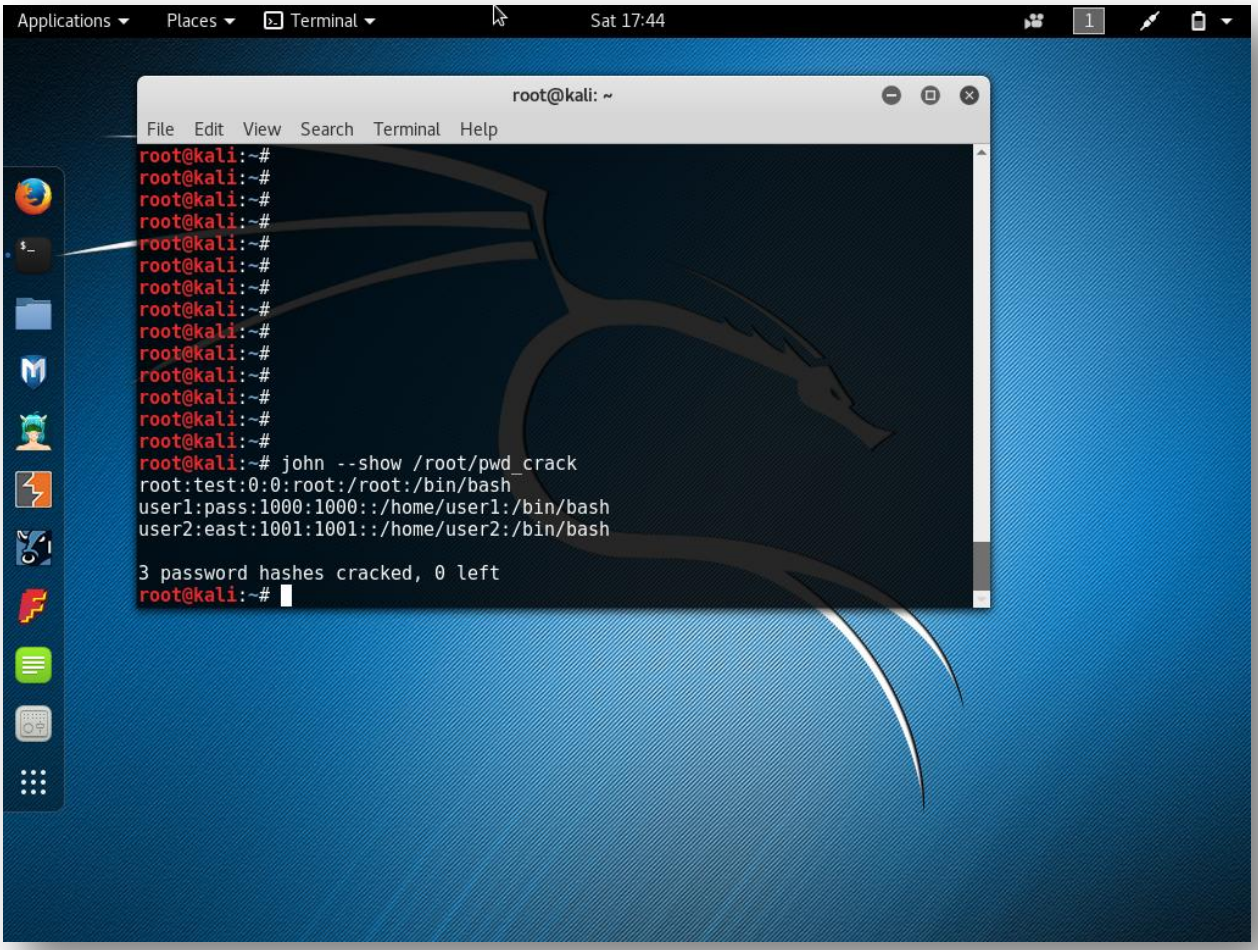
For user2: password is “east”



Step 9) We can use john - - show option to see the list of cracked passwords. Type following command:

john - -show /root/pwd_crack

As you can see, it will give you the list of passwords cracked along with their users.



4. Santoku Linux

4.1 About Santoku Linux

Santoku is dedicated to mobile forensics, analysis, and security, and packaged in an easy to use, Open Source platform.

Santoku includes a number of open source tools dedicated to helping you in every aspect of your mobile forensics, malware analysis, and security testing needs, including:

Development Tools:

- Android SDK Manager
- AXMLPrinter2
- Fastboot
- Heimdall
- Heimdall (GUI)
- SBF Flash

Penetration Testing:

- Burp Suite
- Ettercap
- Mercury
- Nmap
- OWASP ZAP
- SSL Strip
- w3af (Console)
- w3af (GUI)
- Zenmap (As Root)

Wireless Analyzers:

- Chaosreader
- Dnschef
- DSniff
- TCPDUMP
- Wireshark
- Wireshark (As Root)

Wireless Analyzers:

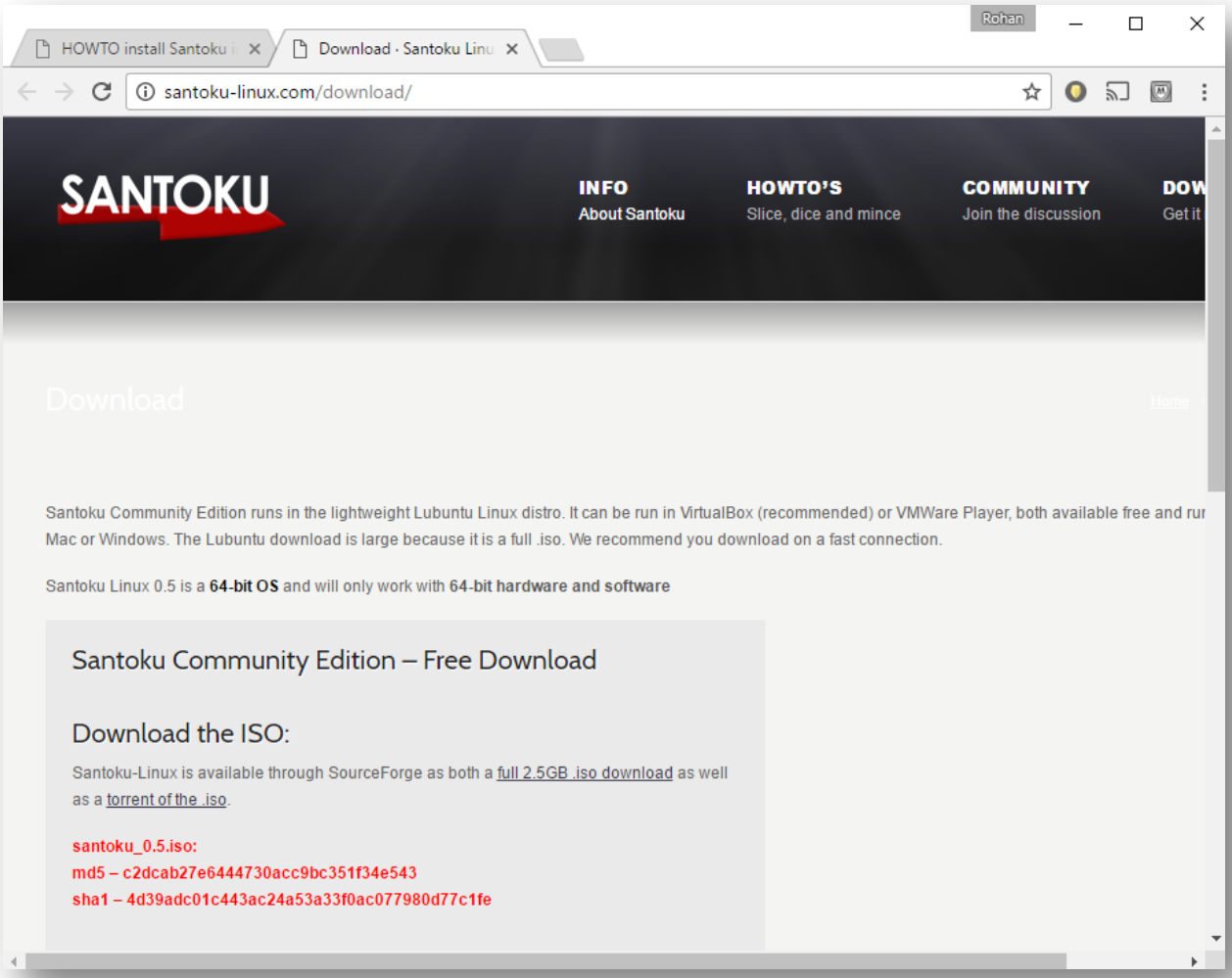
- AFLogical Open Source Edition
- Android Brute Force Encryption
- ExifTool
- iPhone Backup Analyzer (GUI)
- libimobiledevice
- scalpel
- Sleuth Kit

Reverse Engineering:

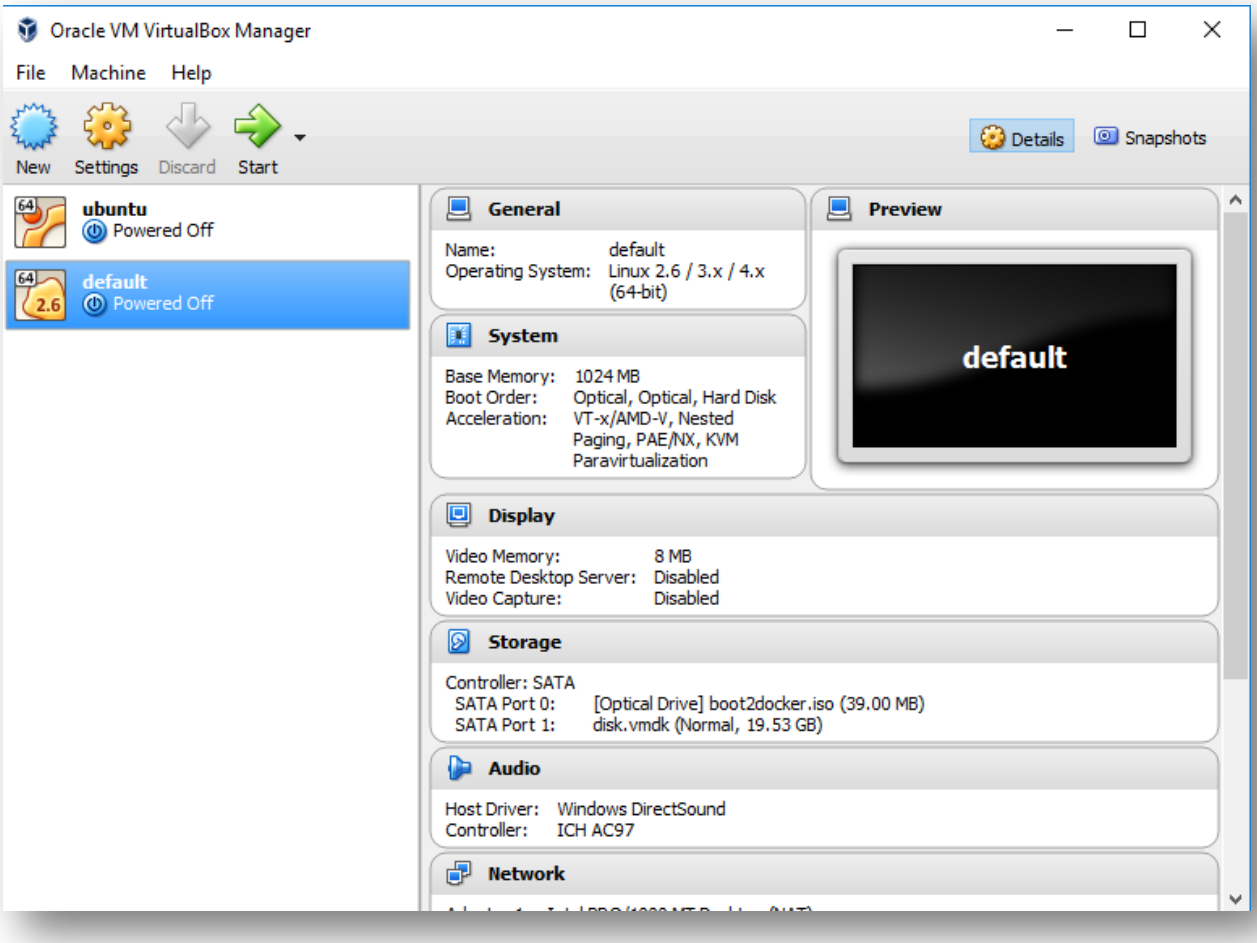
- Androguard
- Antilvl
- APK Tool
- Baksmali
- Dex2Jar
- Jasmin
- JD-GUI
- Mercury
- Radare2
- Smali

4.2 Steps to install Santoku Linux 0.5 on VirtualBox

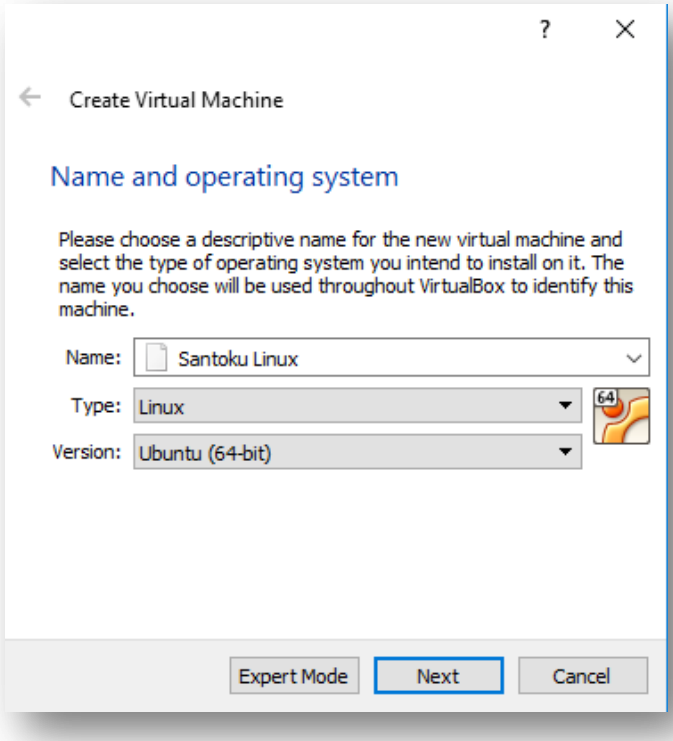
Step 1) First, download the ISO file at http://santoku-linux.com/download/



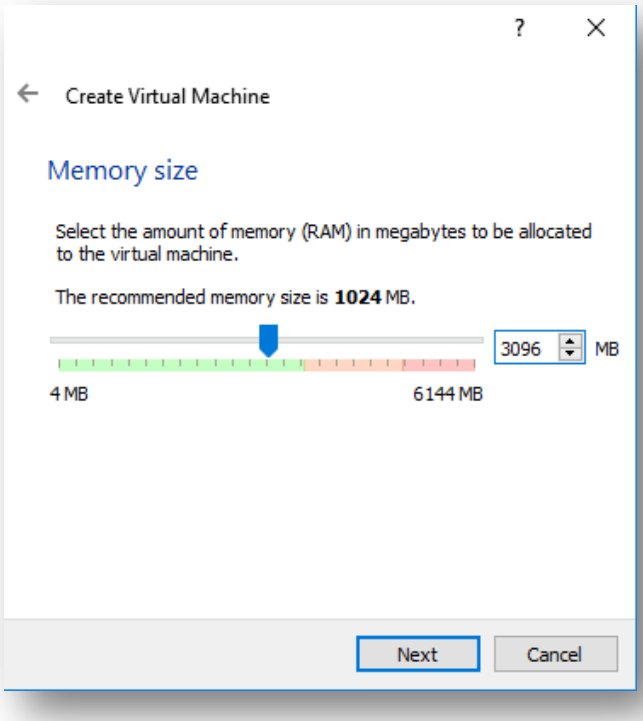
Step 2) To create new Virtual Machine click on "New":



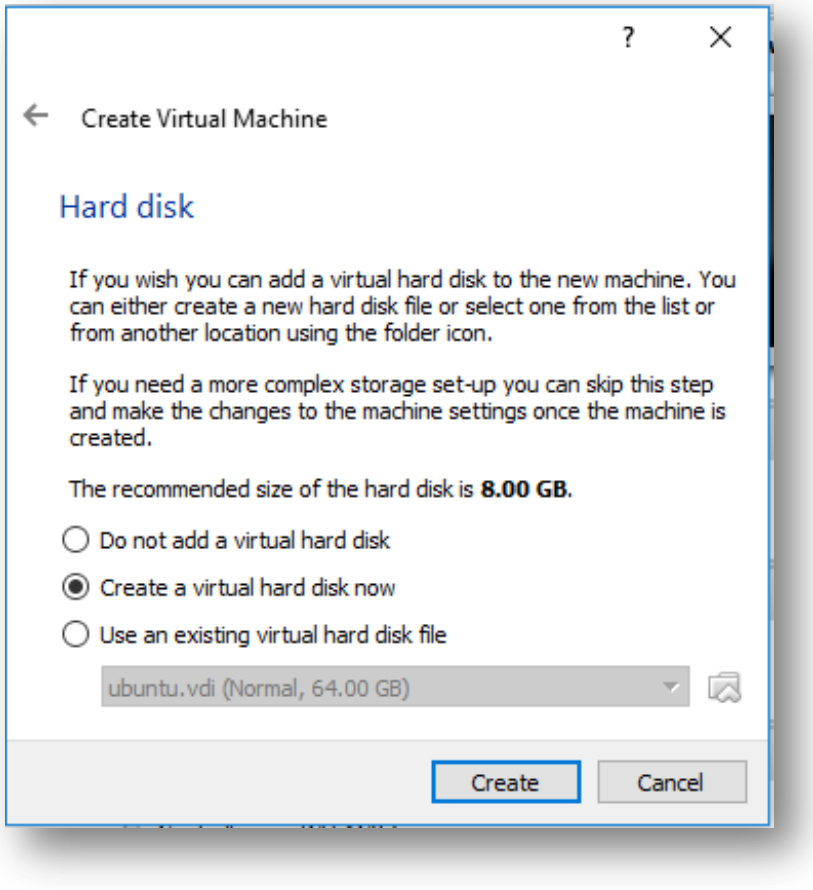
Step 3) Enter Santoku Linux as a name. Type: Linux/Debian and Version: Ubuntu(64-bit) for Santoku Linux 0.4 and later.



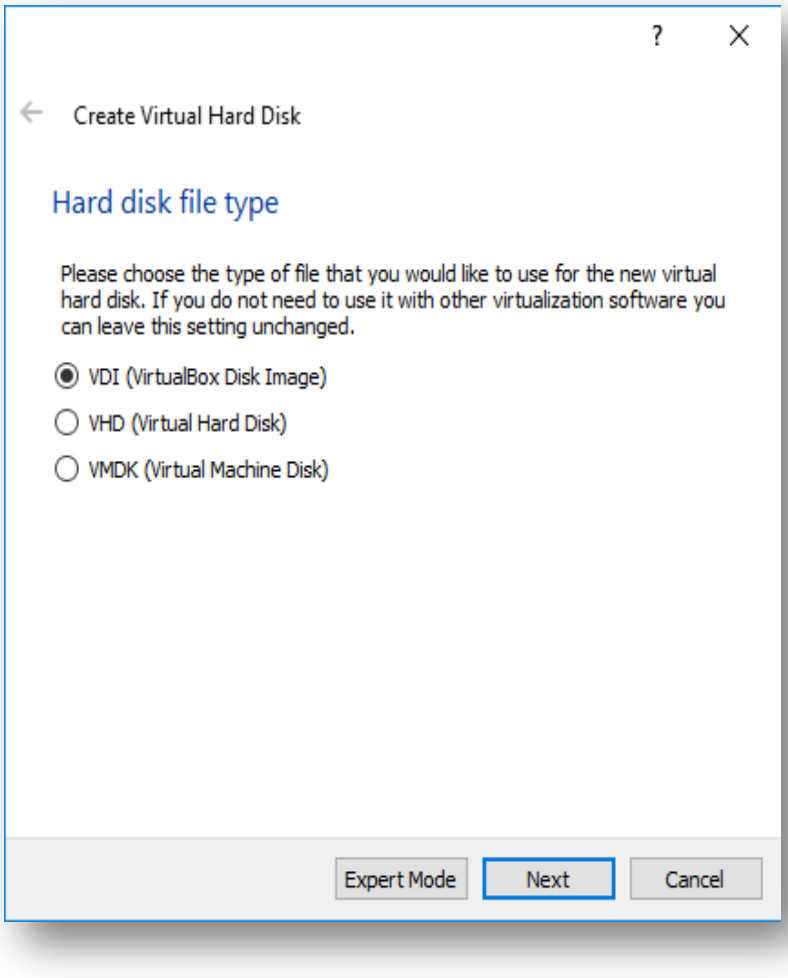
Step 4) Allocate RAM: Default RAM size is 1024 MB. Change it to 3096 MB.



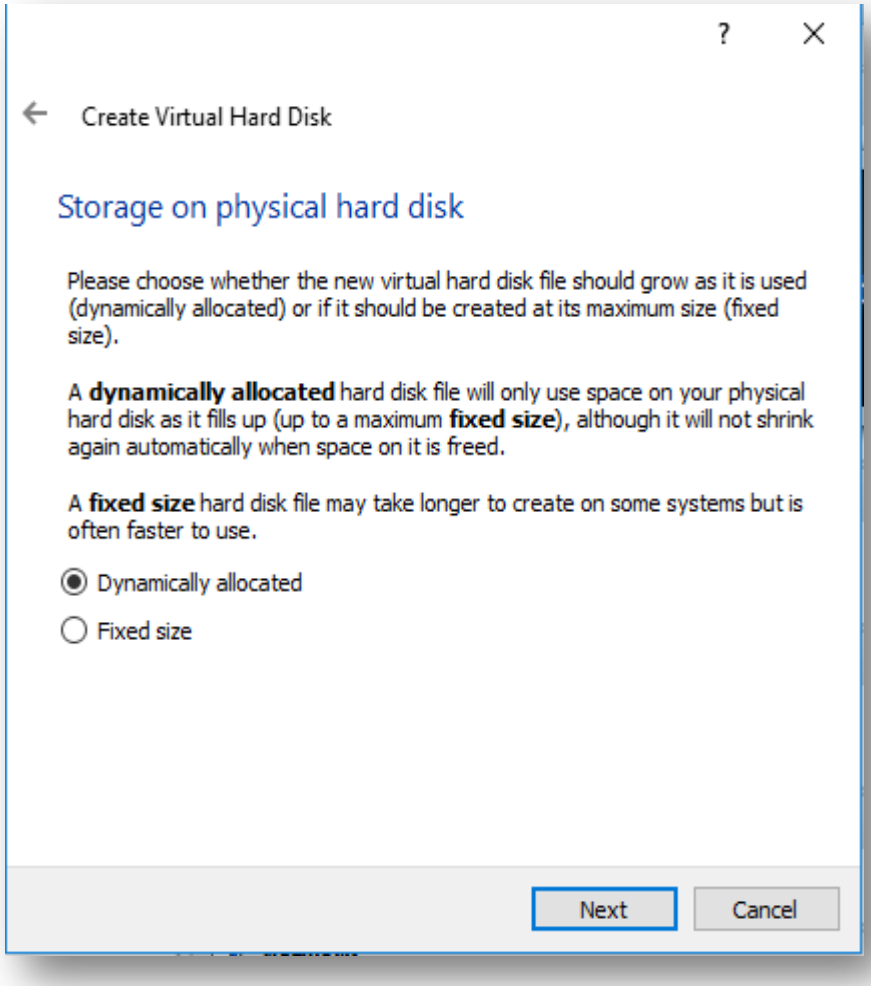
Step 5) On the screen select "Create a virtual hard disk now" and click "Create".



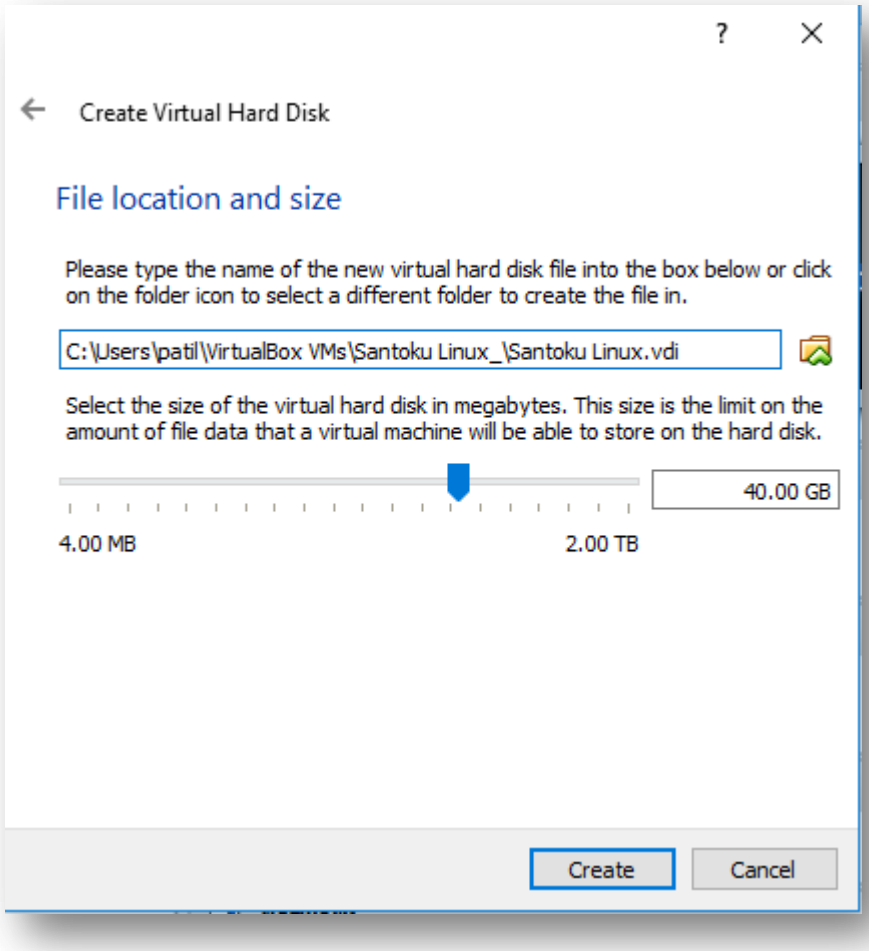
Step 6) On the screen select "VDI (VirtualBox Disk Image)" and click on "Next".



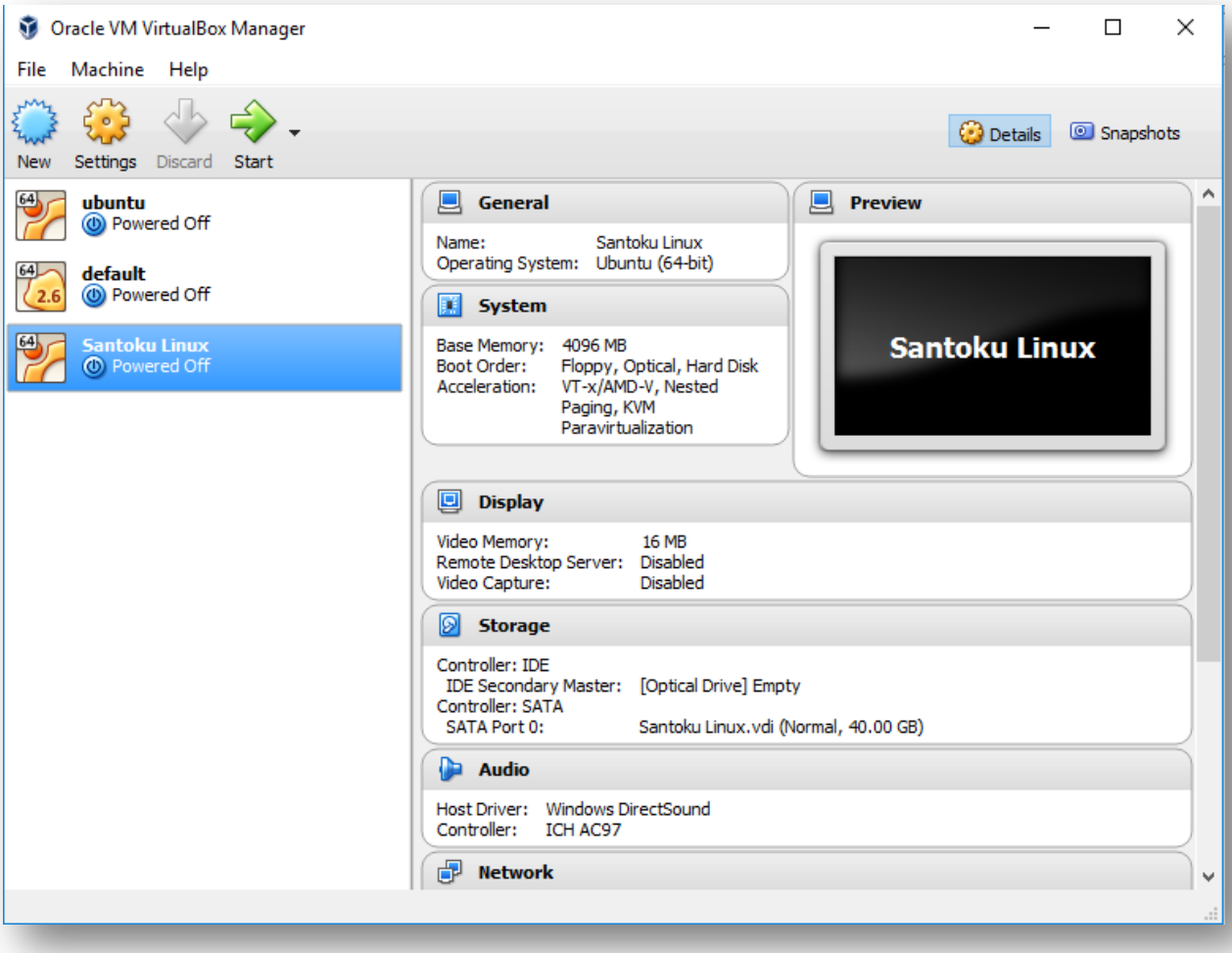
Step7) Select "Dynamically allocated" option and click "Next".



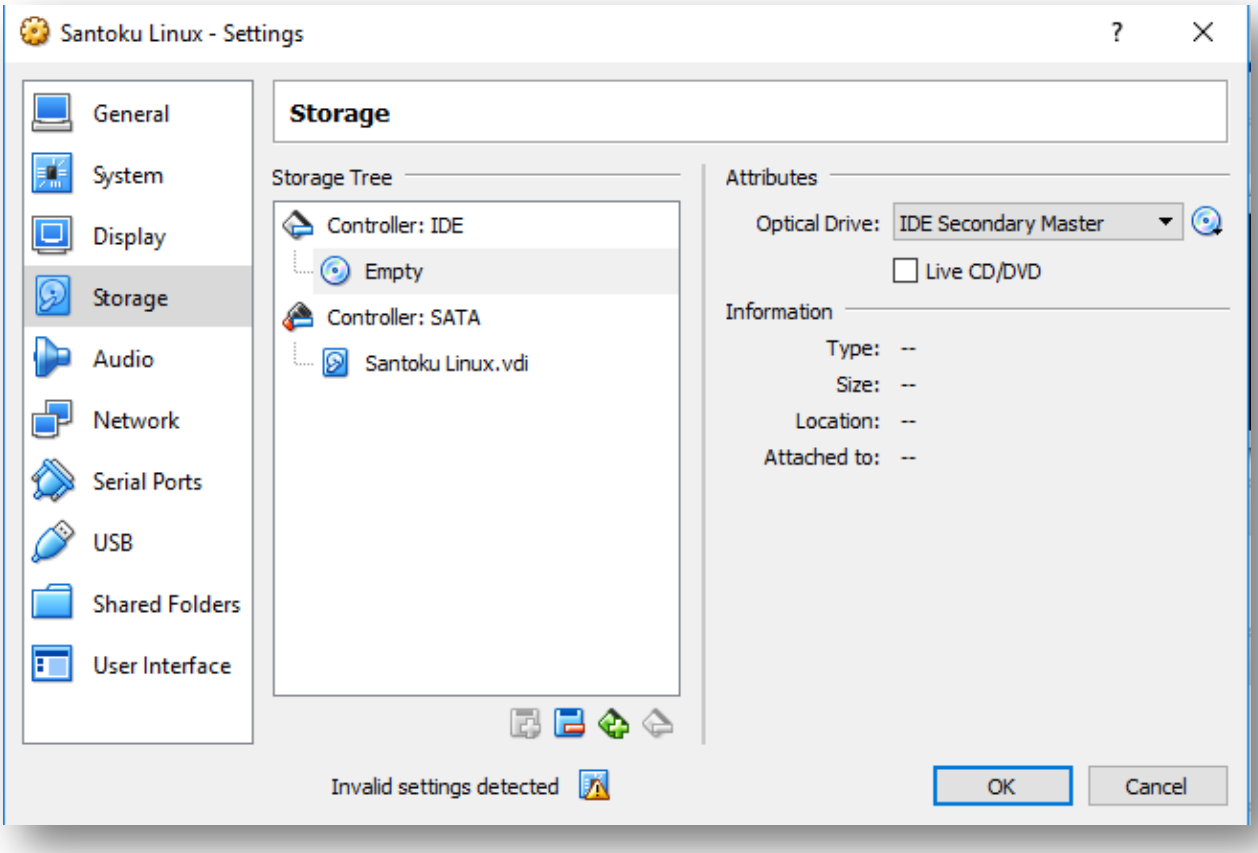
Step 8) Default disk size is 8GB. Change it to 40GB and click "Create".



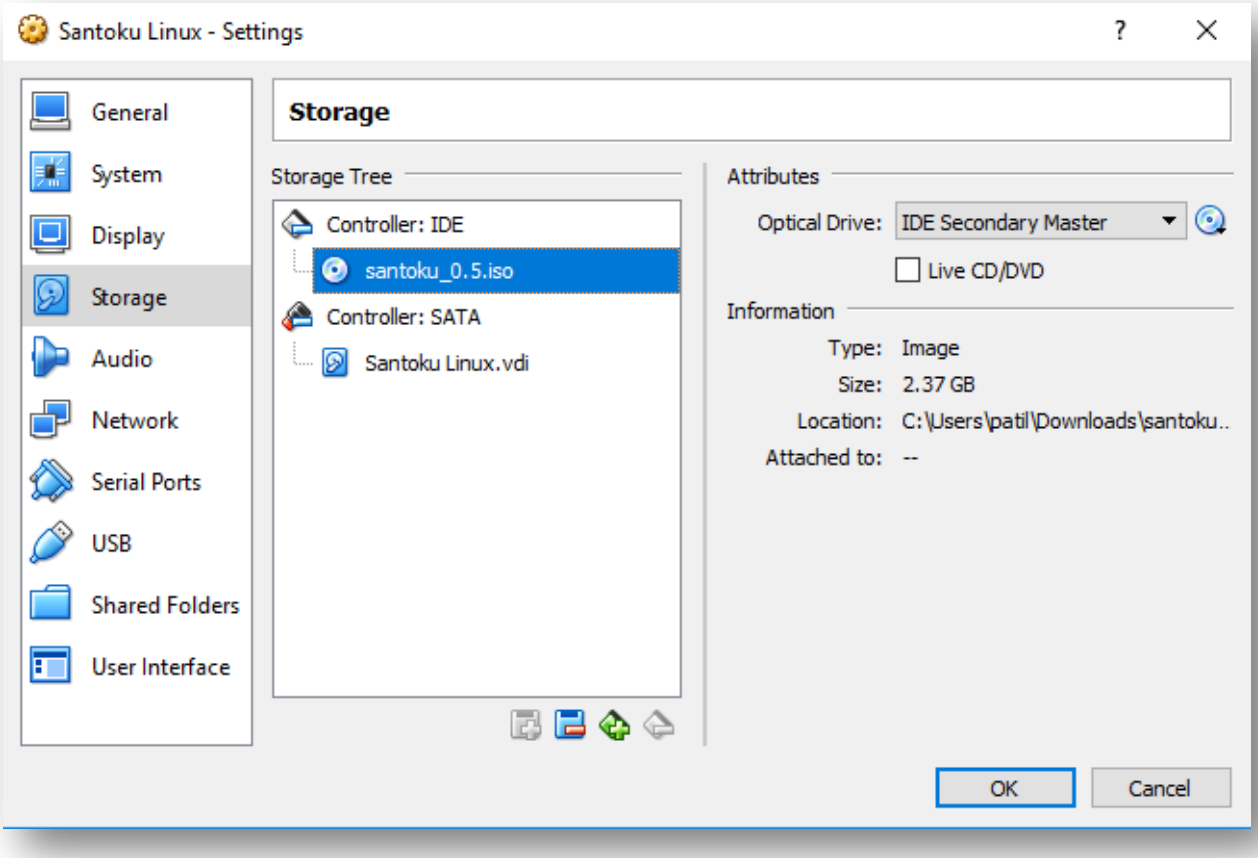
Step 9) Now, you can see new virtual machine named "Santoku Linux" is created.



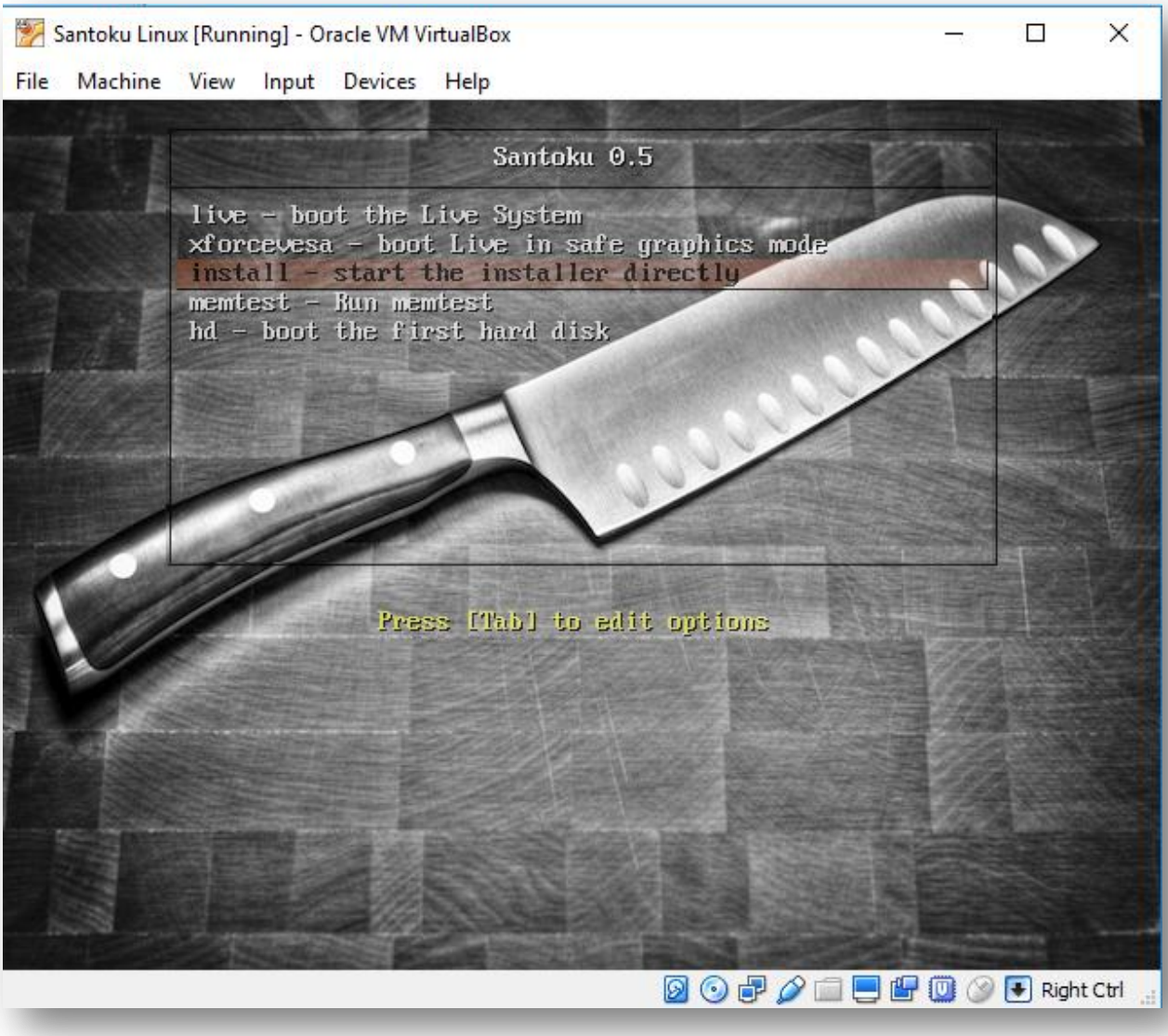
Step 10) Select "Santoku Linux" and click on "Settings". Select "Storage" -> "Controller: IDE" -> "Empty". Now, on right side click on the cd icon and browse your Santoku Linux ISO file.



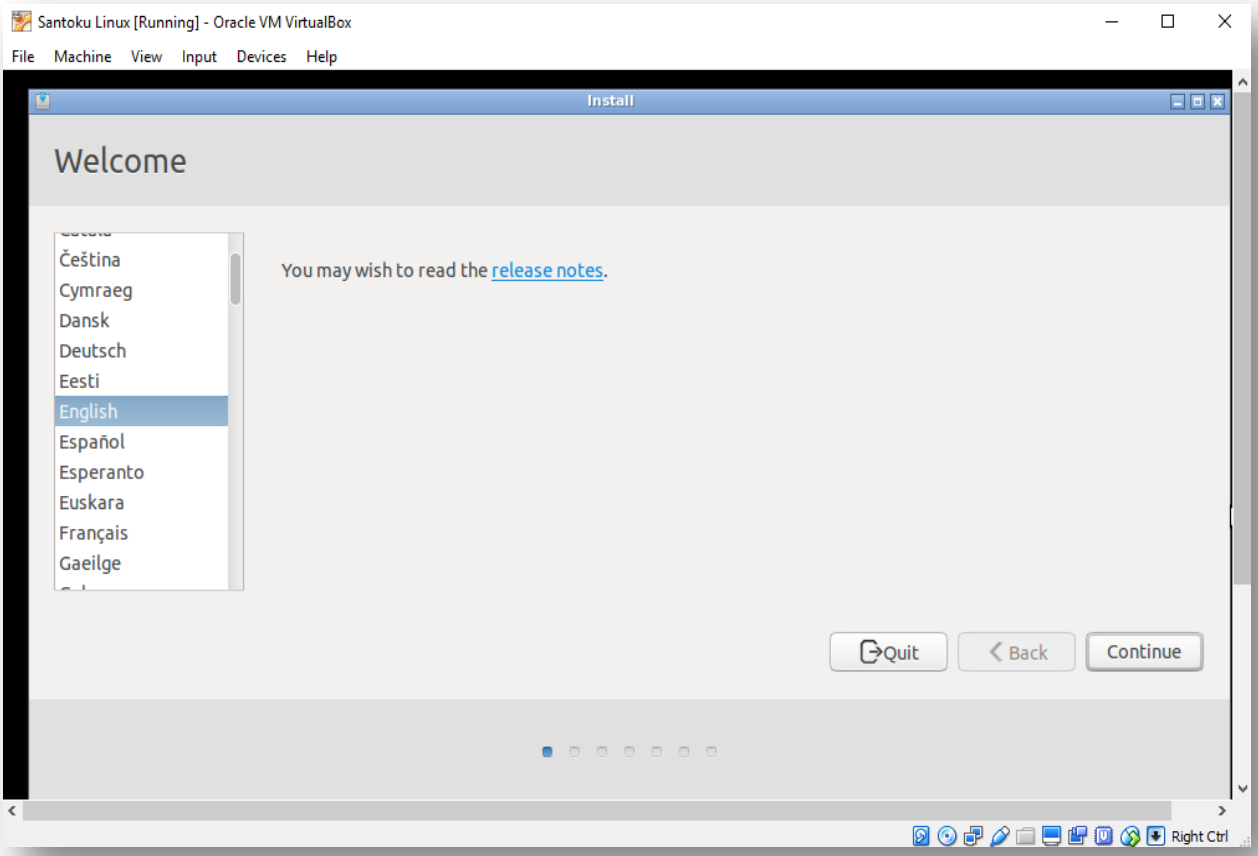
After selecting ISO file you can see the changes as shown in the screenshot:



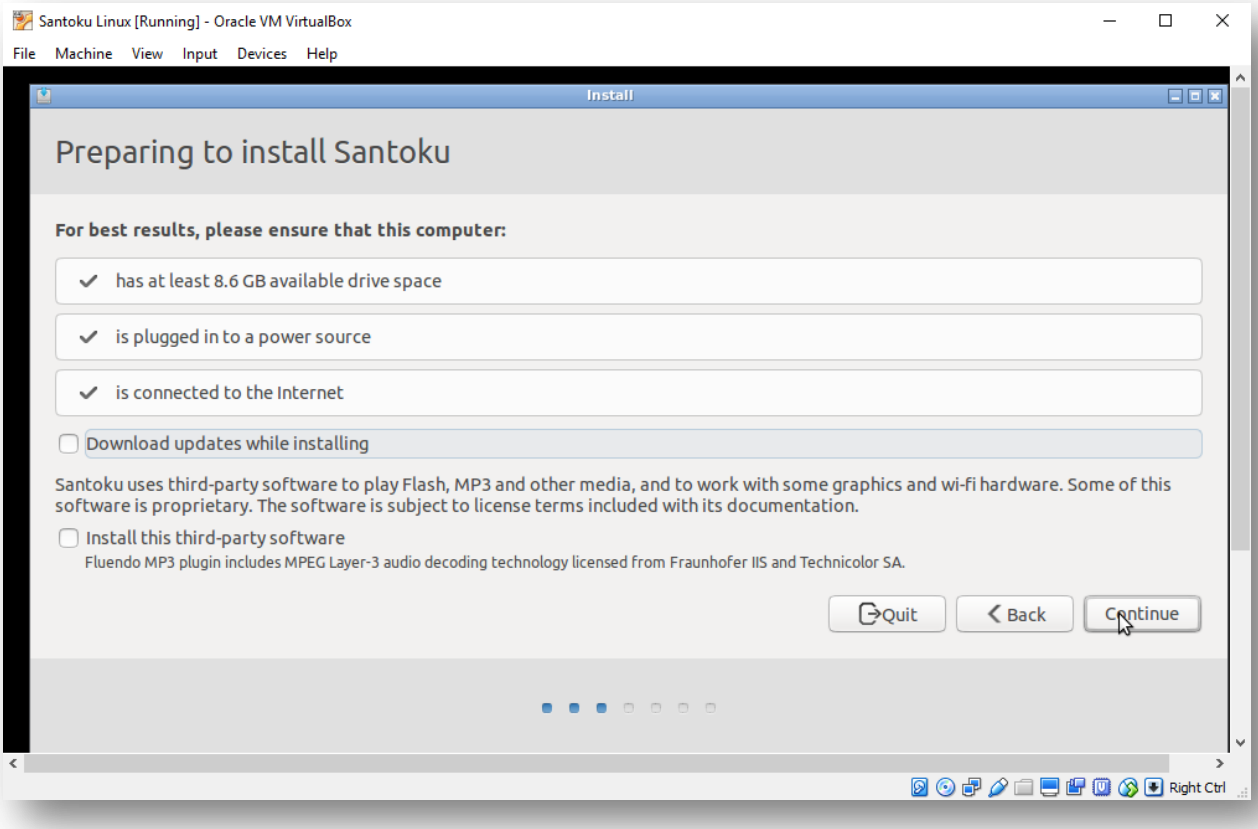
Step 11) Select "Santoku Linux VM" and click on "Start".
Select "install – start the installer directly" option and press "Enter".



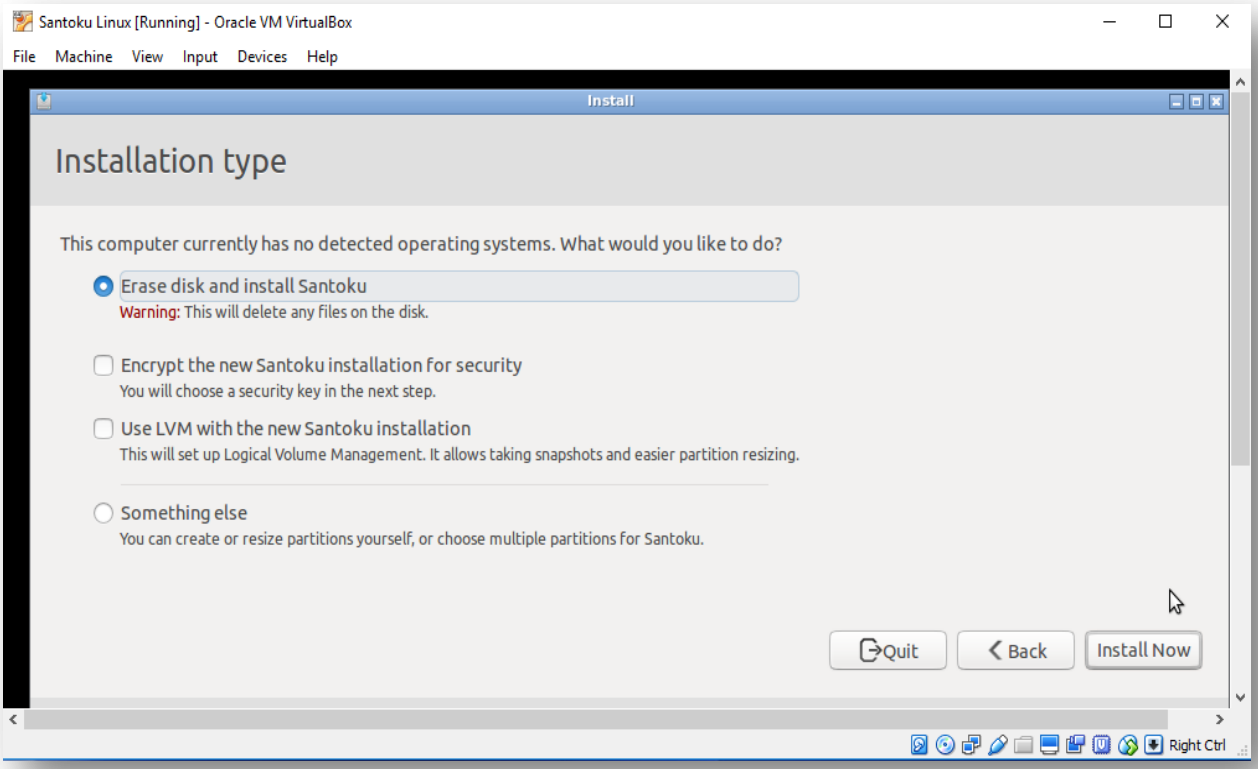
Step 12) Select your language and click on "Continue".



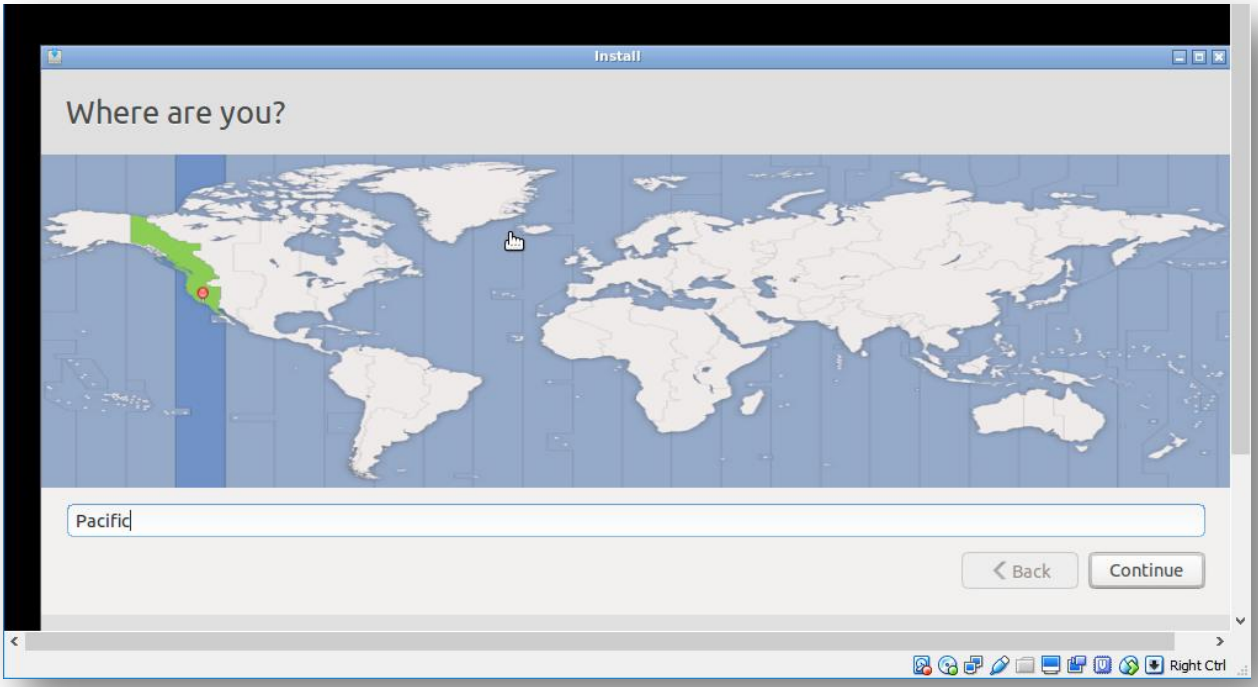
Step13) Click "Continue".



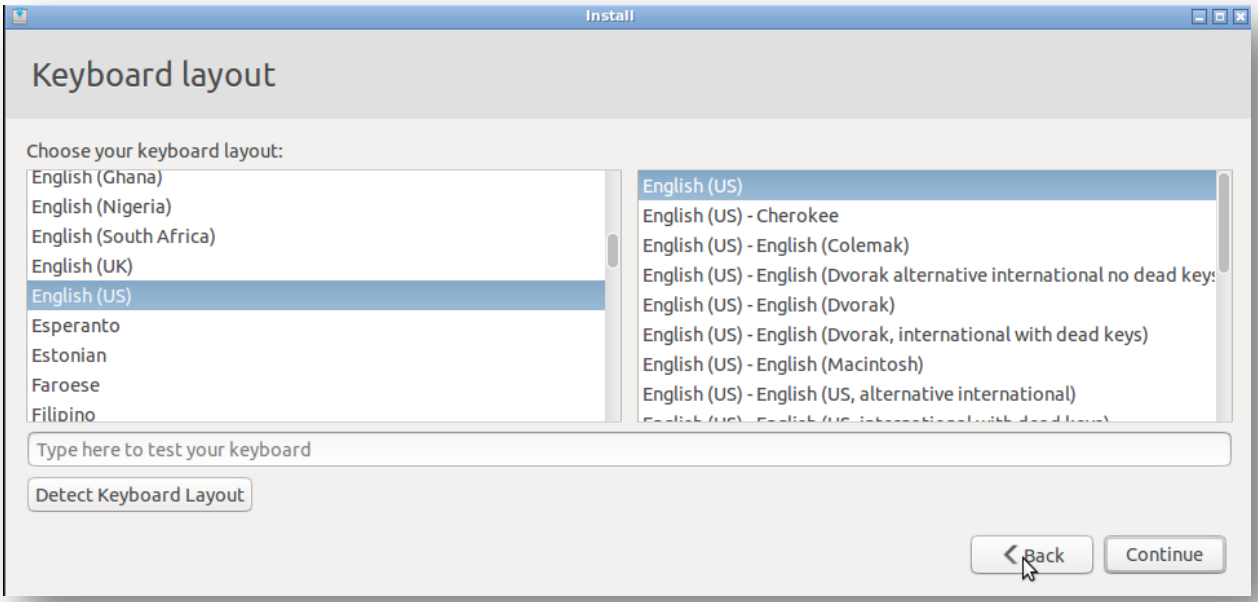
Step 14) Select option "Erase disk and install Santoku" and click "Install now".



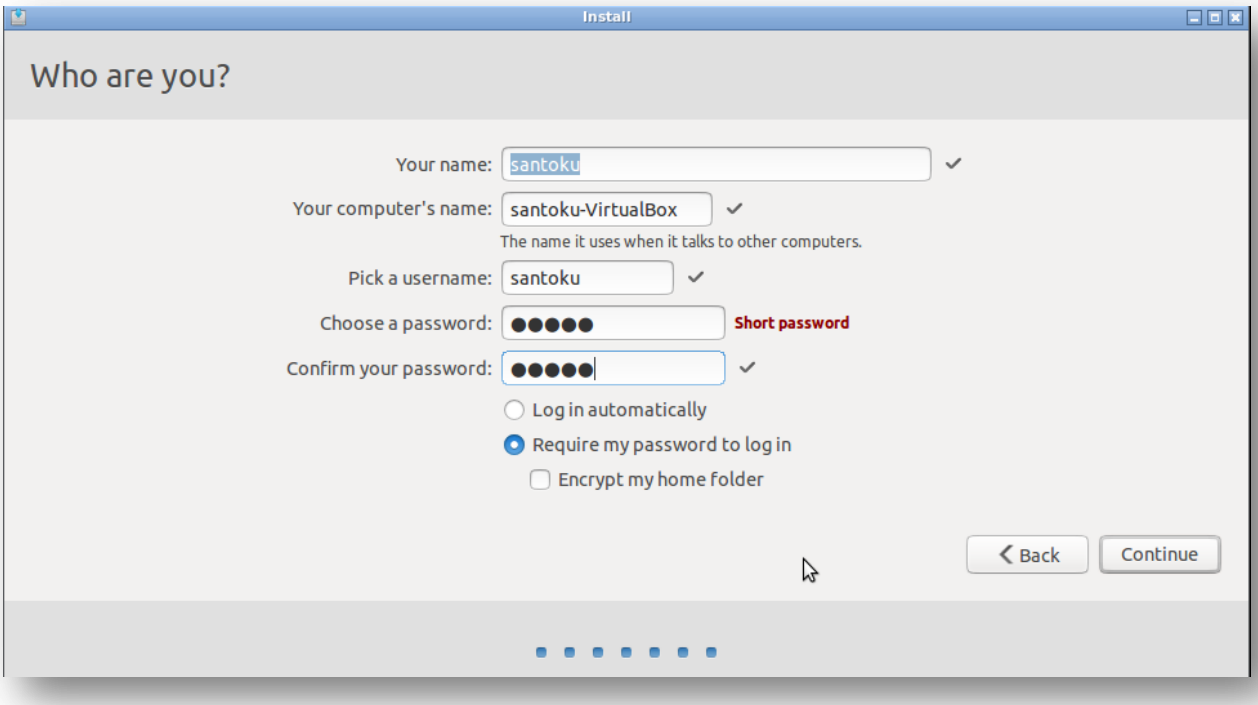
Step 15) Select the location and click "Continue".



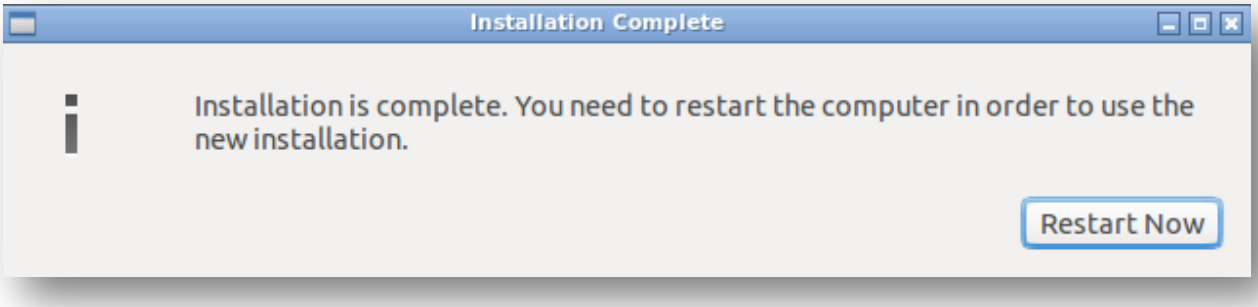
Step 16) Select keyboard layout and click "Continue".



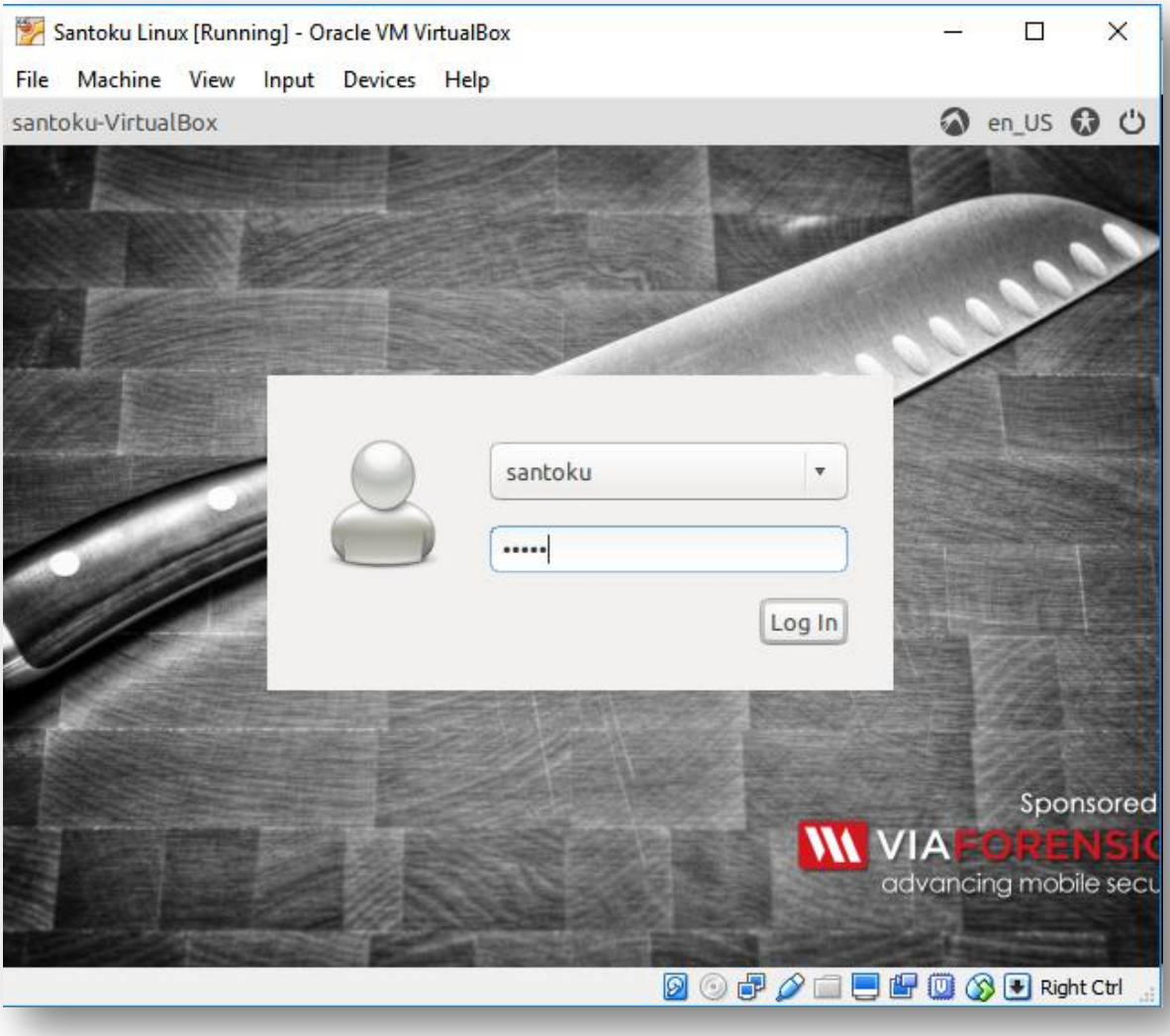
Step 17) Select your name and password and click "Continue".



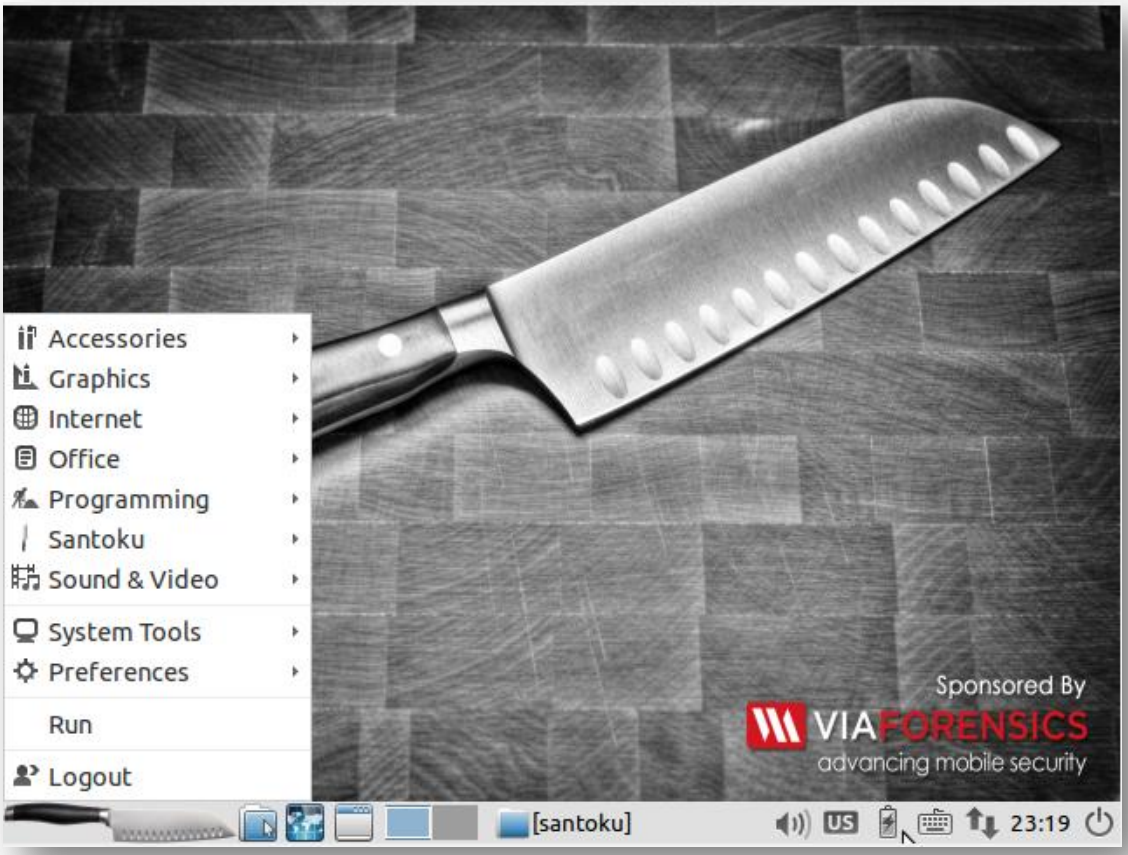
Step 18) Once installation complete, you will see the following message.



Step 19) Enter the user name and password which we choose earlier.



Step 20) After you are successfully logged into the system, you will see the Santoku Linux desktop.



4.3.1 Android Password and Pattern Skipping

We can bypass Password Pin or Pattern security from android phone by finding the correct files on system.

Goal: To skip/bypass the pin (password) or pattern of Android phone using Santoku Linux.

Approach followed:

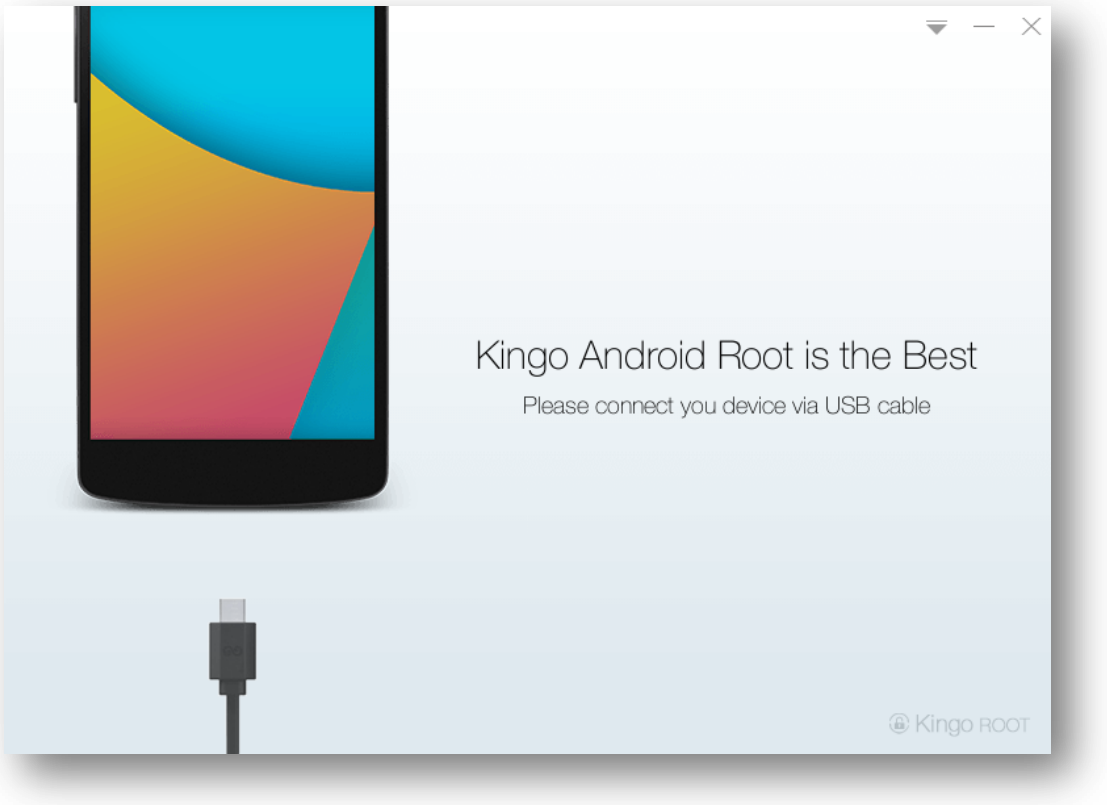
a) Enable root access on phone using Kingo ROOT application.
b) Enable USB debugging on phone
c) Connect phone to Santoku Linux (running in VM environment)
d) Run adb commands
e) Get rooted access
f) Detect password.key or gesture.key file and delete them

Requirements:

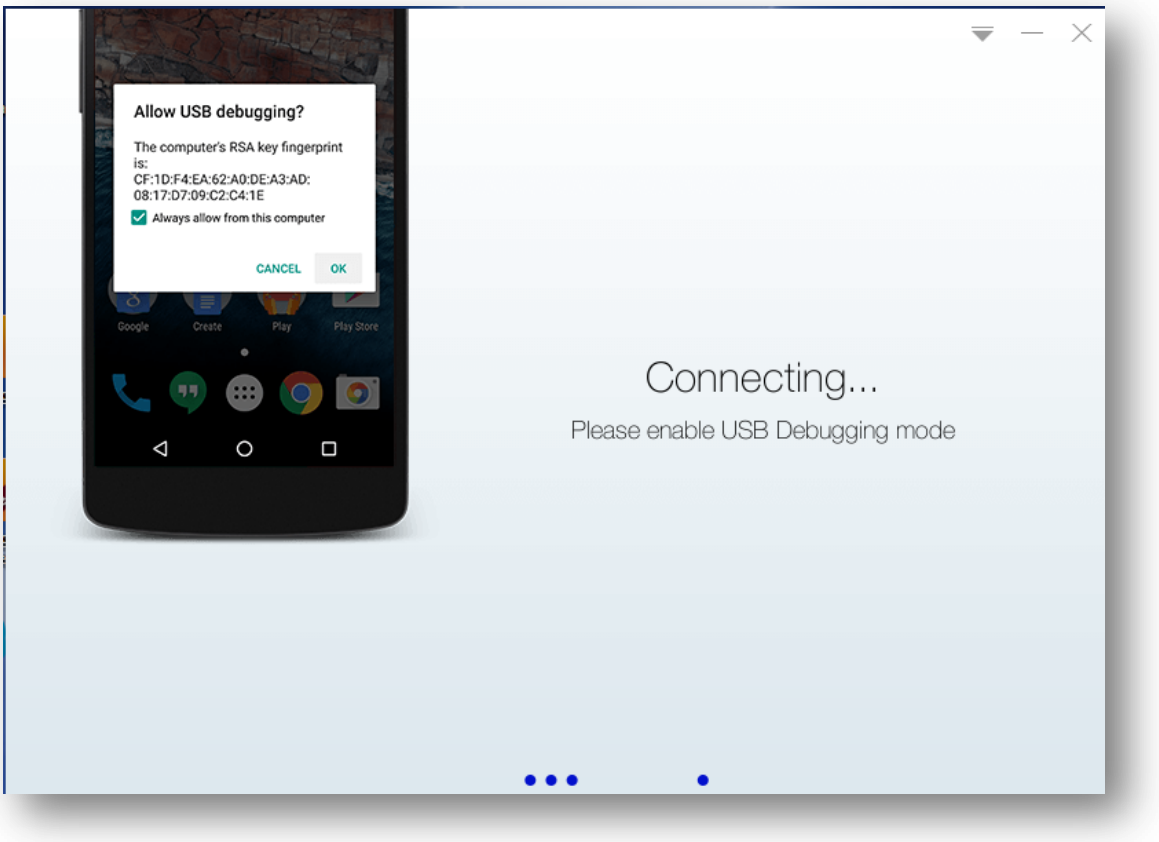
a) Oracle Virtual Box Manager
b) Santoku Linux Virtual Machine
c) Android Brute Force Encryption tool (bundled)
d) Android phone (HTC one PG86100 Android version: 4.0.3)
e) Kingo ROOT application on your desktop

A) Enable root access on phone using Kingo ROOT application.

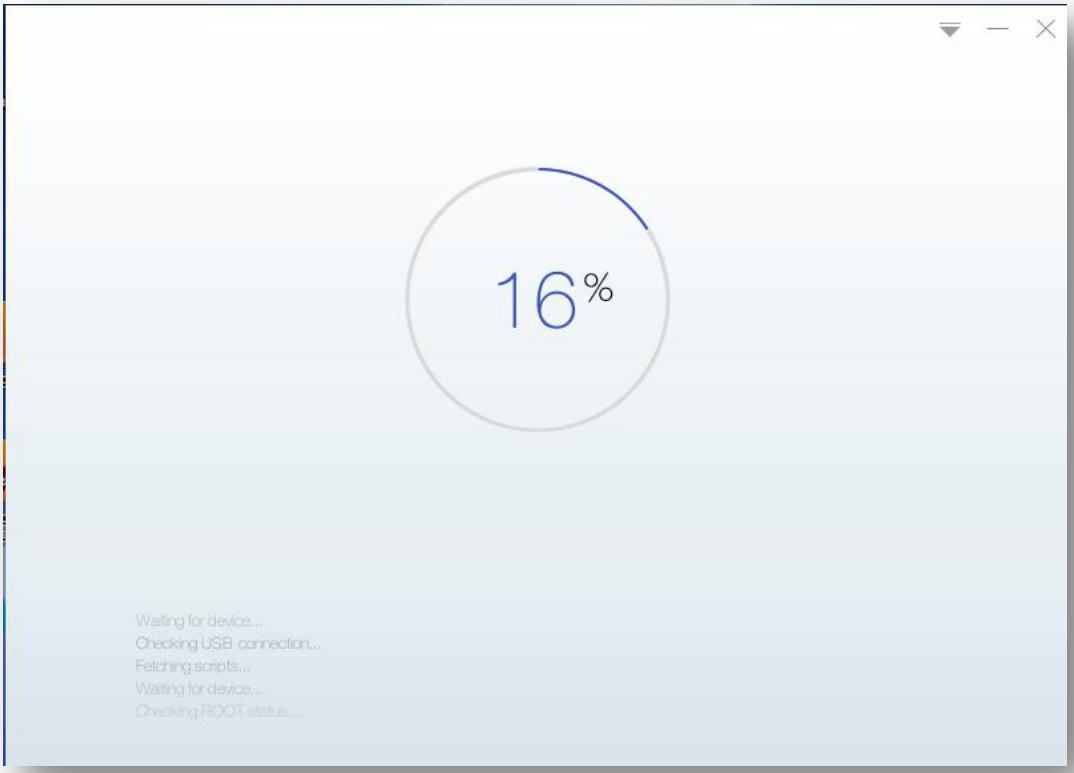
Step 1) Download and install Kingo ROOT application on your desktop. Once installed, run the application and connect your phone (one to be rooted). If your phone is already rooted you can skip this step.



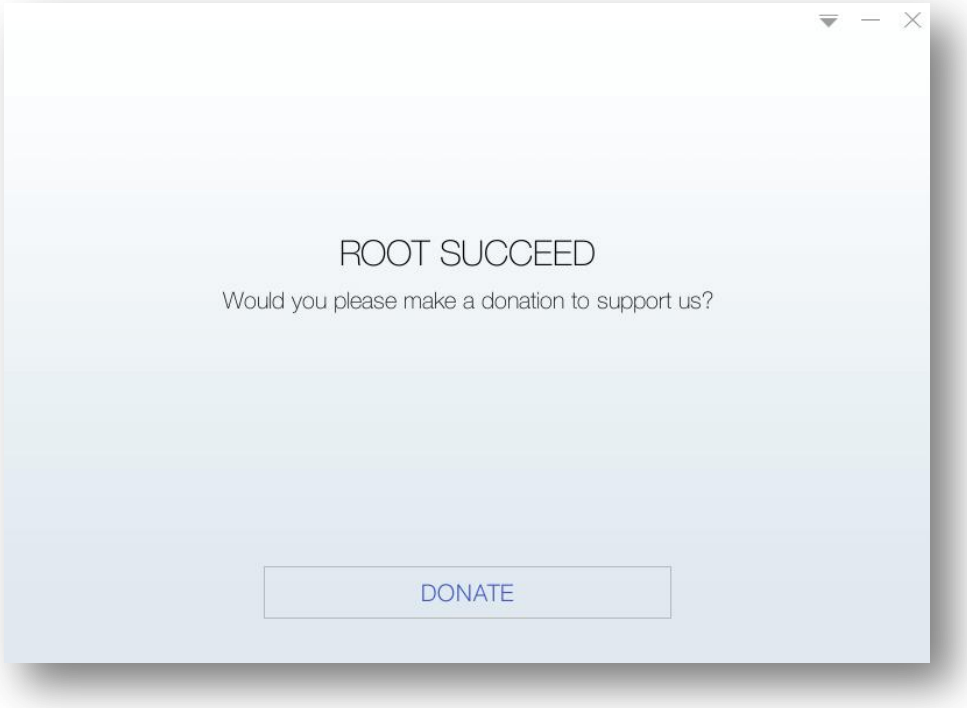
Step 2) Make sure to enable USB debugging on your phone and connect your phone via USB cable.



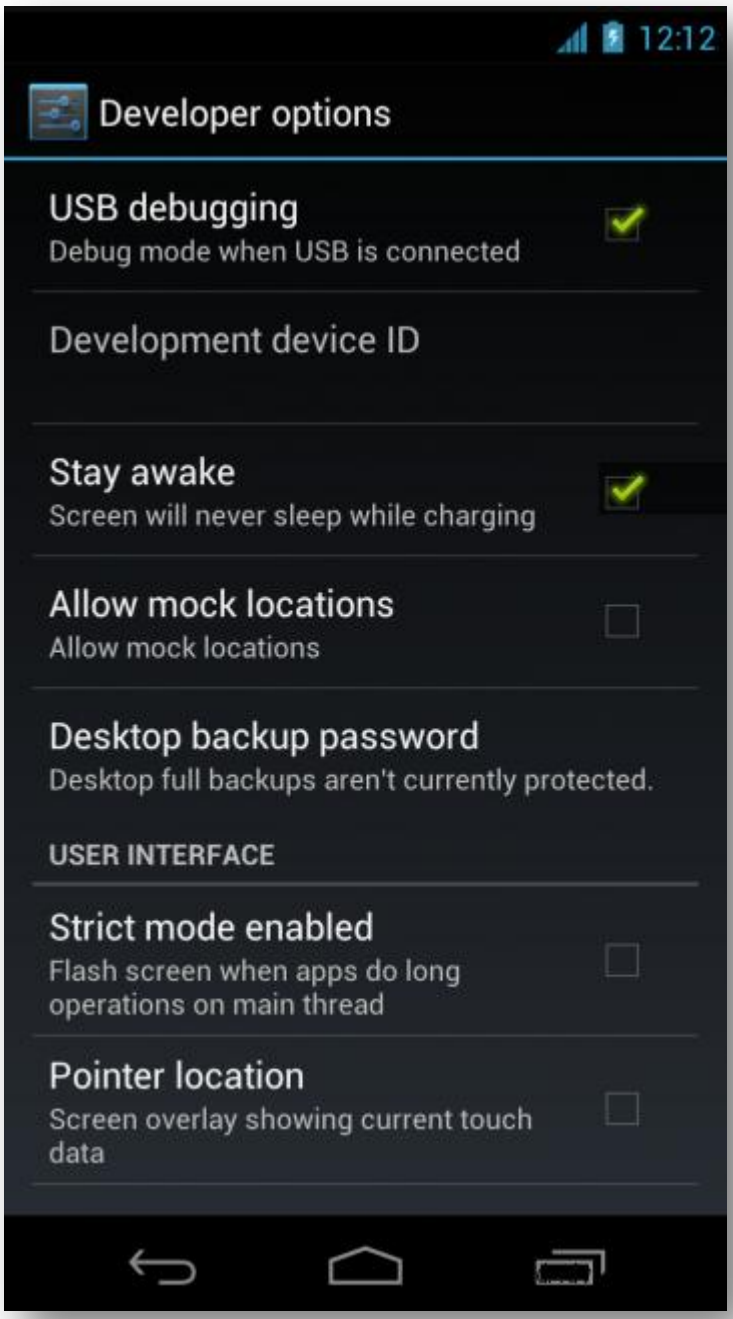
Step 3) Once the Kingo ROOT application detects the phone we can click ROOT and wait for the application to finish.



Step 4) After completion we would see the following screen denoting that the phone is rooted.



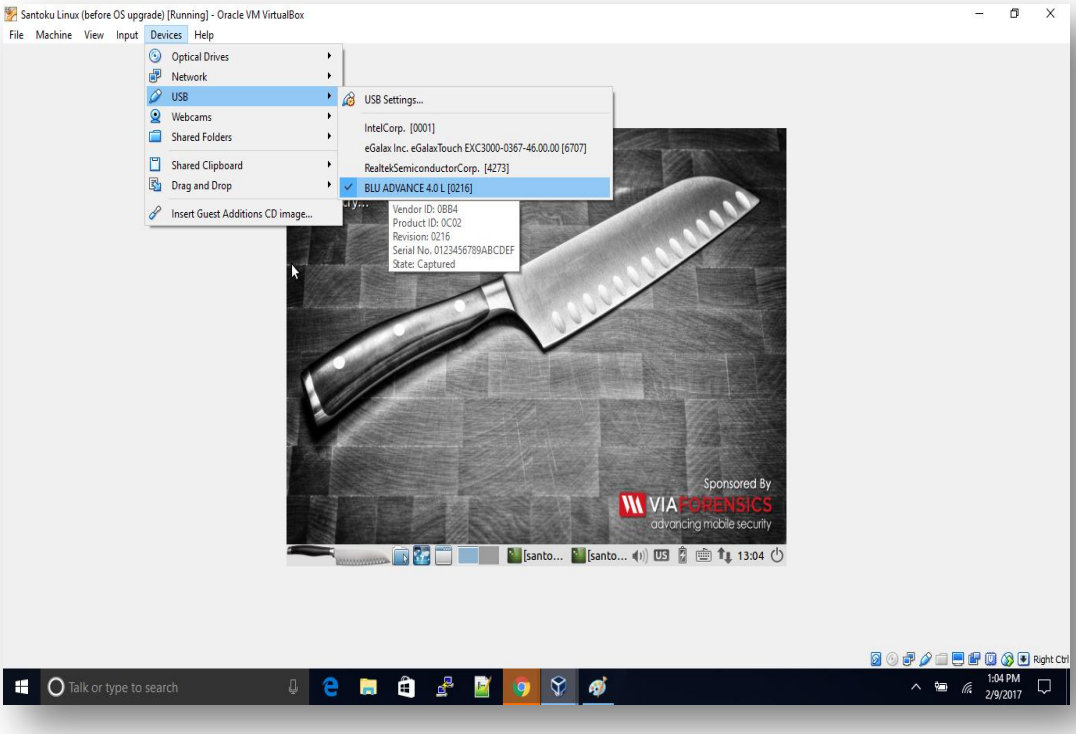
B) Enable USB debugging on phone



C) Connect phone to Santoku Linux (running in VM environment)

On your Oracle VirtalBox Manager, select your Santoku Linux VM and click on “start” button. Connect your phone to the laptop. To make your phone detectable by the laptop, click on “Devices” -> “USB” -> “USB Settings” and click on your device name.

As shown in the screen shot, it shows “BLU ADVANCE 4.0 L” as a device name.

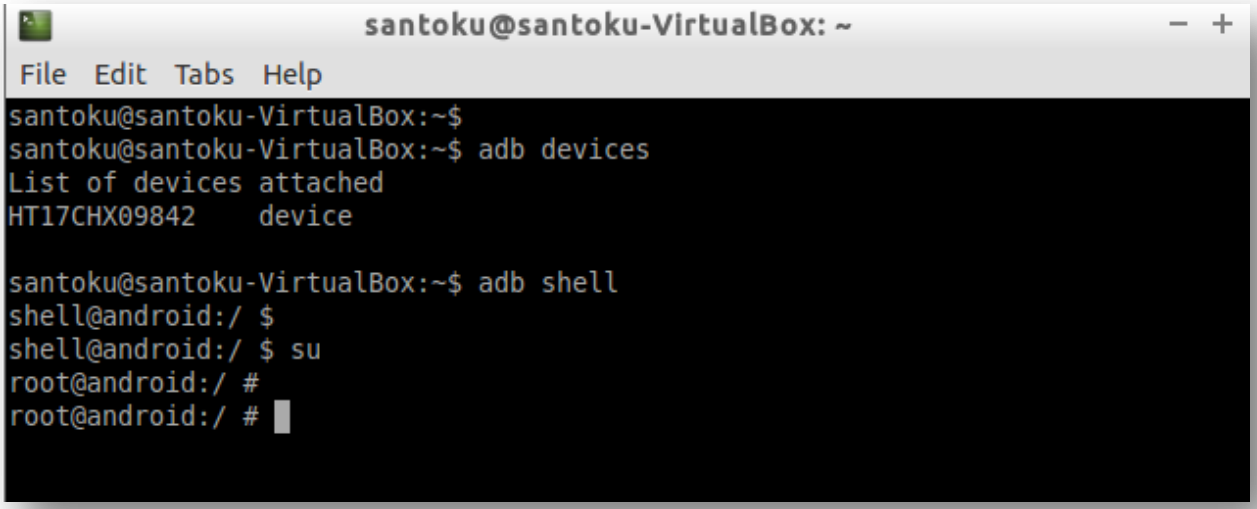


D) Run adb commands

Detect the connected device by using “adb devices” command on terminal. Once detected get shell access to the android phone using adb shell.

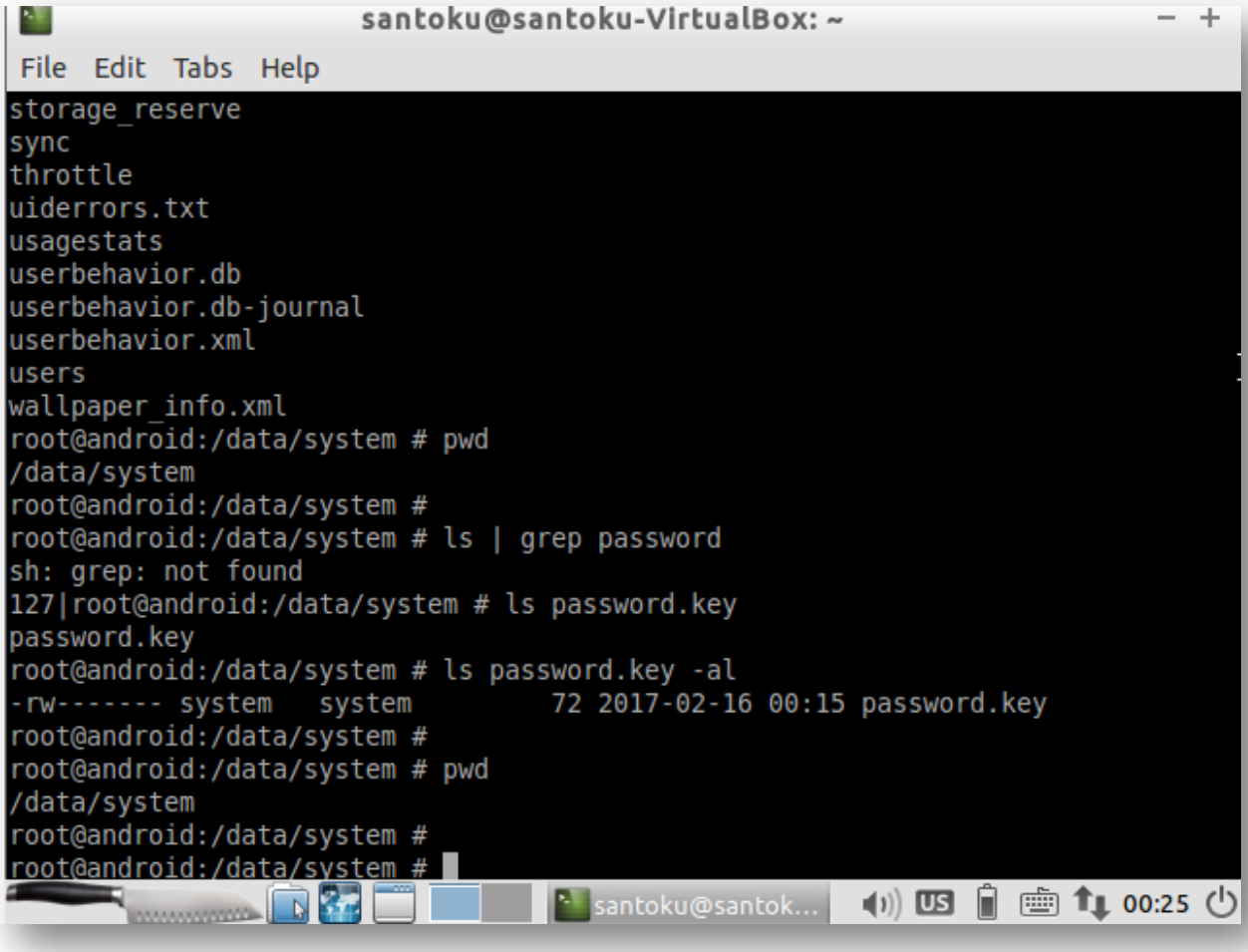
E) Get rooted access

To run commands as a root user, type “su” command on the terminal.



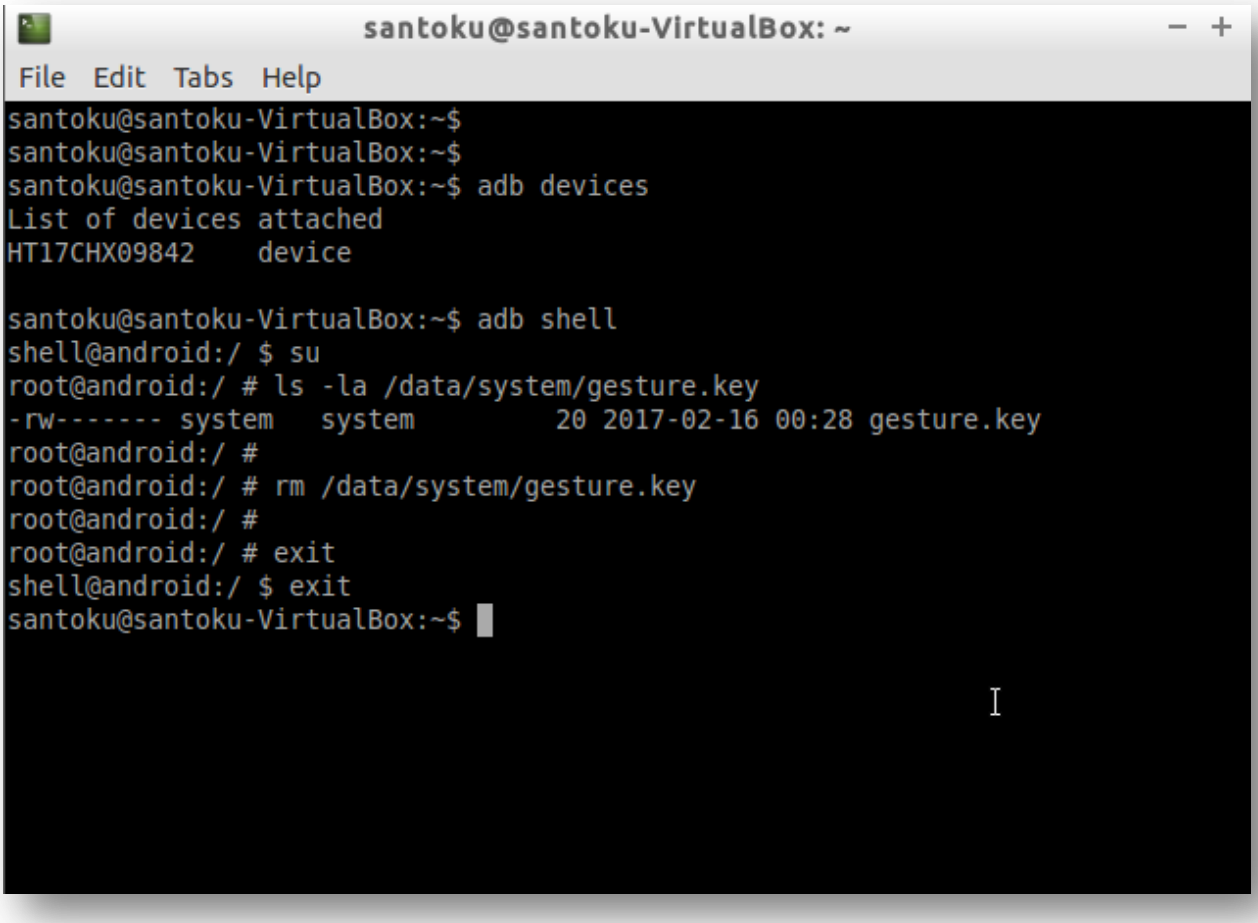
F) Detect password.key or gesture.key file and delete them

Step 1) Detect password file. For HTC one, the location is /data/system/password.key file



Step 2) Remove the password.key file

Step 3) We can also remove any Pattern lock on android phones. For HTC one phone the pattern lock information is stored in /data/system/gesture.key file



4.3.2 Android Password Cracking using Brute Force Encryption

Goal: To crack the pin (password) of Android phone using Santoku Linux.

Approach followed:

a) Enable root access on phone using Kingo ROOT application.
b) Enable USB debugging on phone
c) Connect phone to Santoku Linux (running in VM environment)
d) Run adb commands
e) Run Android Brute Force Encryption program

Requirements:

a) Oracle Virtual Box Manager
b) Santoku Linux Virtual Machine
c) Android Brute Force Encryption tool (bundled)
d) A BLU phone (BLU ADVANCE 4.0L Android version : 4.4.2) or Google Nexus (Nexus S 4G Android version: 4.1.1)
e) Kingo ROOT application on your desktop

A) Enable root access on phone using Kingo ROOT application

B) Enable USB debugging on phone

C) Connect phone to Santoku Linux (running in VM environment)

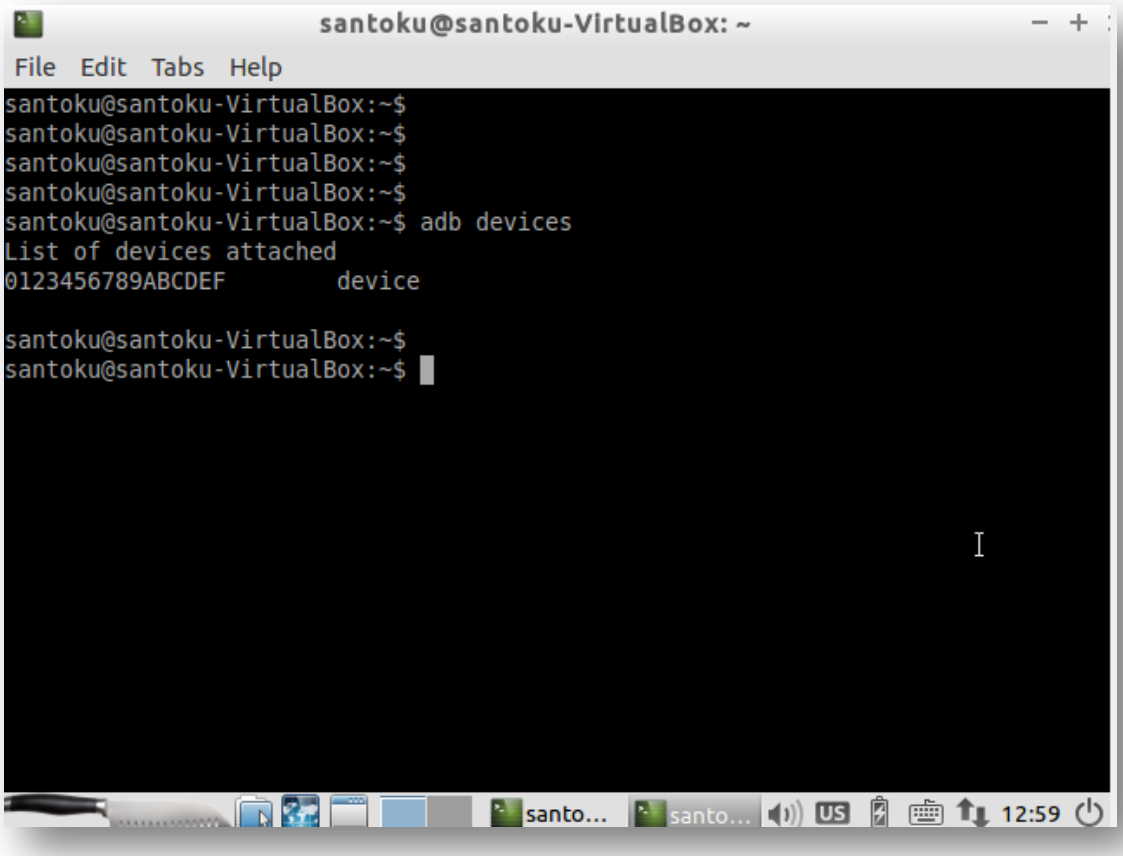
These three steps are similar to the steps A, B, and C of the document “4.3.1 Android Password and Pattern Skipping”

D) Run adb commands

Step 1) Click on “Accessories” and open LXTerminal on Santoku Linux and type following command on the terminal to check whether the device (phone) is detected or not.

$ adb devices

It will show the serial number of the device which is detected.



Step 2) Log in to phone shell using adb shell command:

$ adb shell

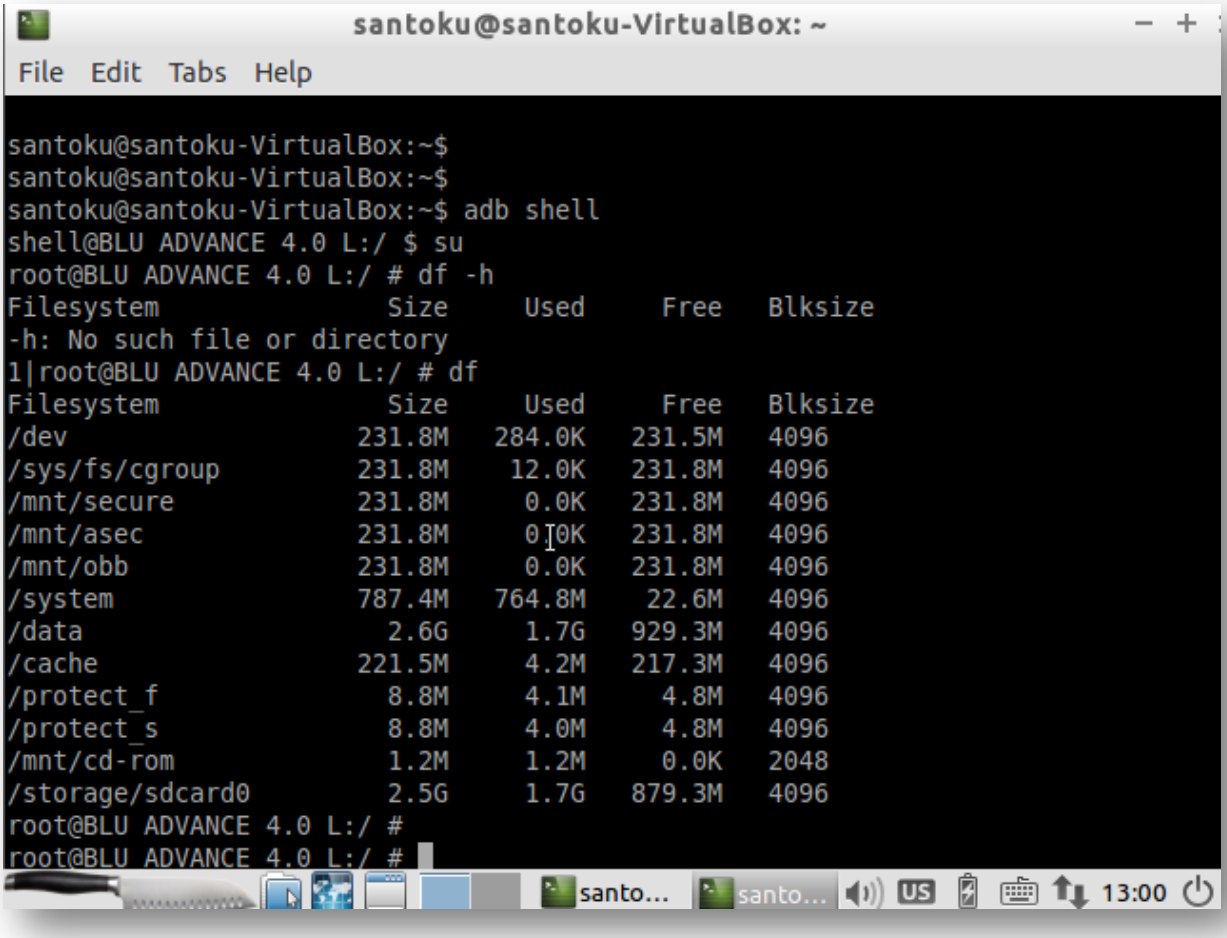
Since we have Android phone rooted, we can run commands as root user using “su” command. If phone is not rooted, then we won’t get sudo(root) access.

$ su

We can look at the disk partitions on phone using df command.

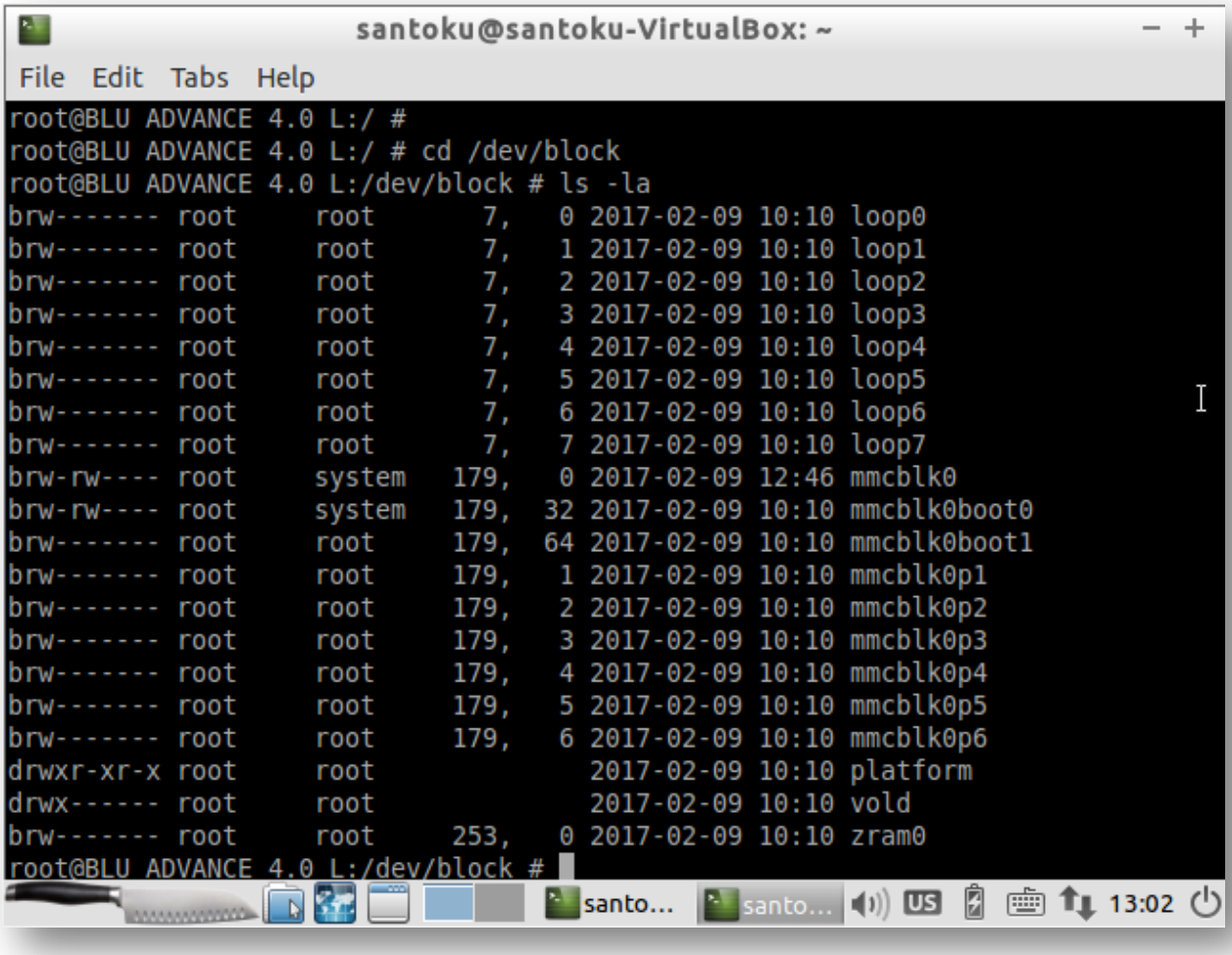
$ df

All these commands can be seen in following screenshot.



Step 3) Change directory to /dev/block/. This directory contains the blocks of data that will be used to generate header and footer information. The header and footer information we collect here will be used as input to the brute force std crypto application.

$ cd /dev/block



Step 4) Generate the header and footer information using commands

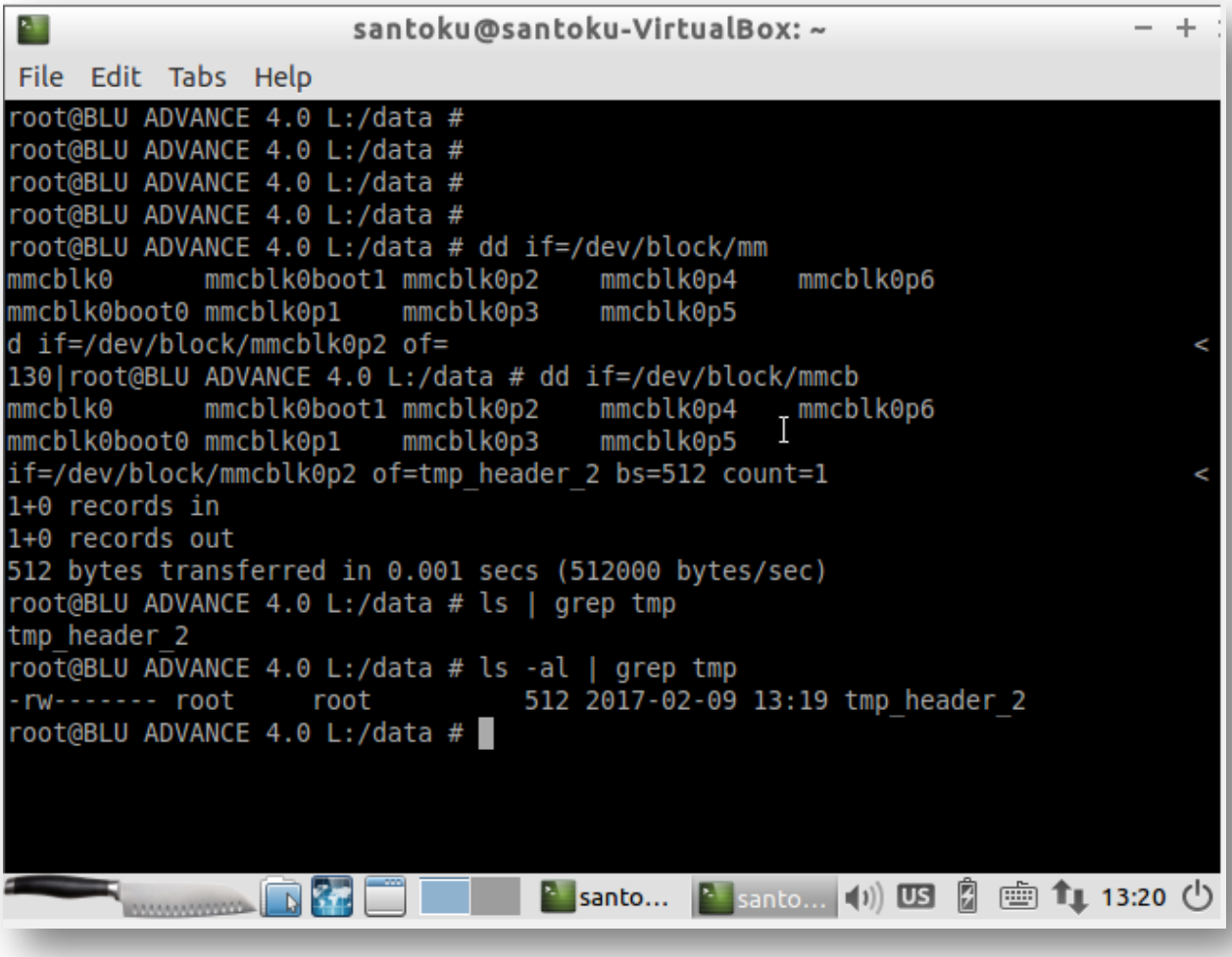
$ dd if=/dev/block/mmcblk0p2 of=tmp_header_2 bs=512 count=1

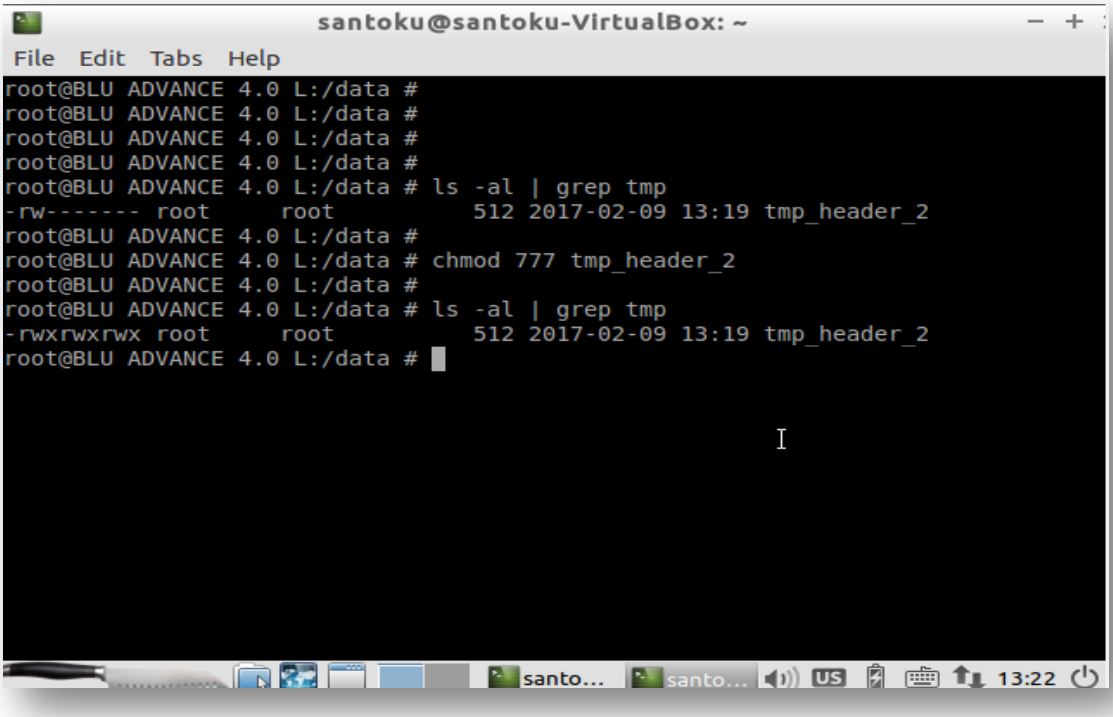
$ dd if=/dev/block/mmcblk0p6 of=tmp_footer_6

In order to be able to pull the data from Santoku Linux, we need to change the permission on the tmp_header and tmp_footer files using ‘chmod’ function.

$ chmod 777 tmp_header_2

$ chmod 777 tmp_footer_6




santoku@santoku-VirtualBox: ~
File Edit Tabs Help
root@BLU ADVANCE 4.0 L:/data #
root@BLU ADVANCE 4.0 L:/data #
root@BLU ADVANCE 4.0 L:/data #
root@BLU ADVANCE 4.0 L:/data #
root@BLU ADVANCE 4.0 L:/data # ls -al | grep tmp
-rw------- root root 512 2017-02-09 13:19 tmp_header_2
root@BLU ADVANCE 4.0 L:/data #
root@BLU ADVANCE 4.0 L:/data # chmod 777 tmp_header_2
root@BLU ADVANCE 4.0 L:/data #
root@BLU ADVANCE 4.0 L:/data # ls -al | grep tmp
-rwxrwxrwx root root 512 2017-02-09 13:19 tmp_header_2
root@BLU ADVANCE 4.0 L:/data #
santo...
santo...
US
13:22

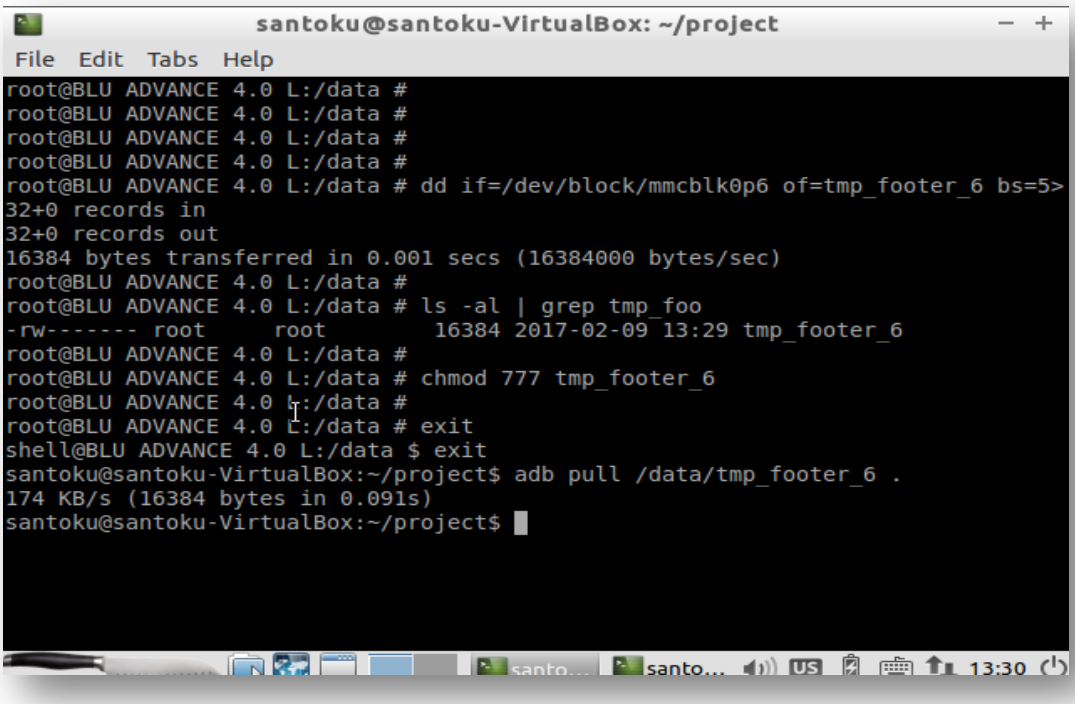
Step 5) To switch from phone to Santoku Linux, type “exit” command as shown in the screen shot.

Now, get those tmp_header and tmp_footer files using “adb pull” command.

$ adb pull /data/tmp_header_6

$ adb pull /data/tmp_footer_6

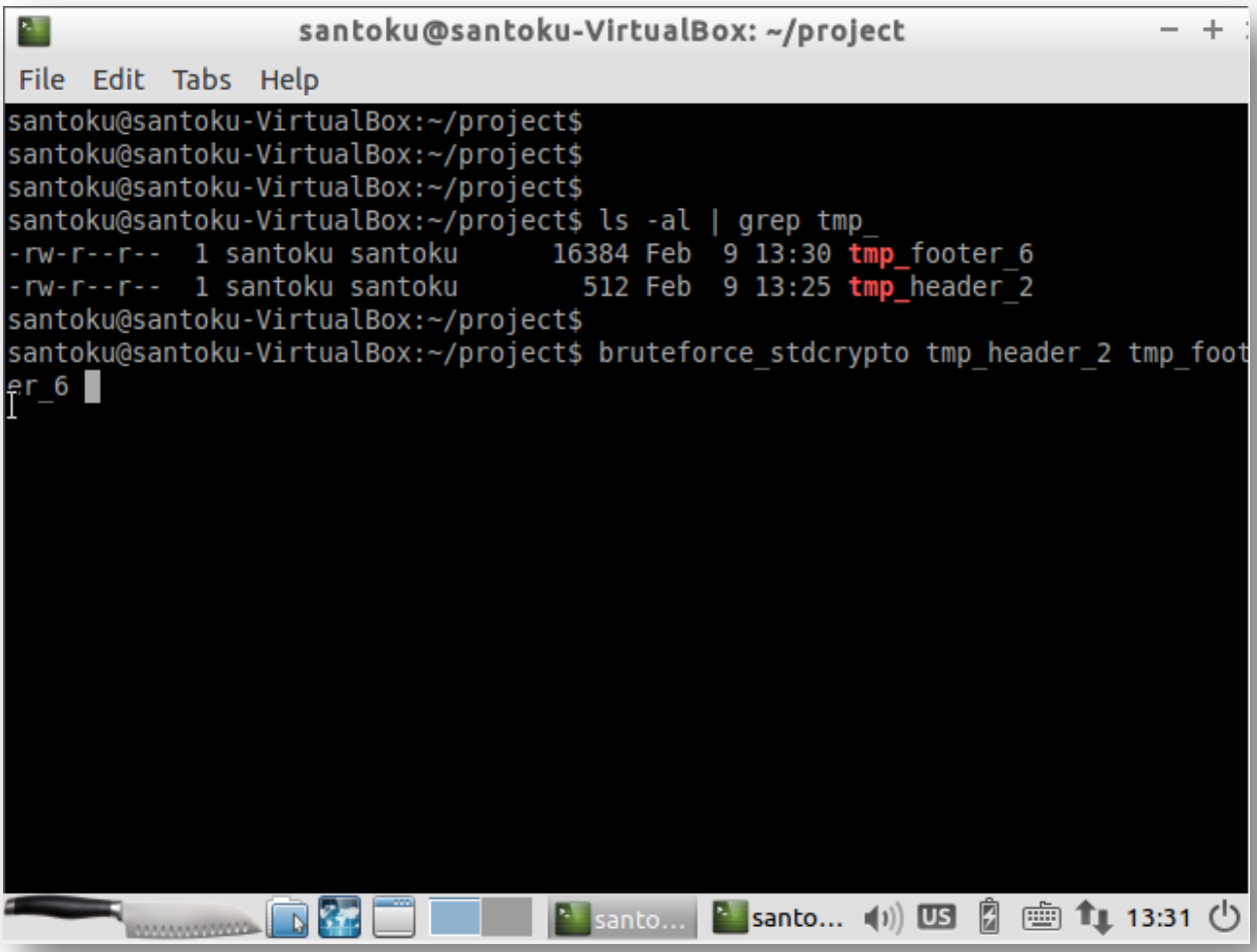
These two files now will be available on Santoku Linux.



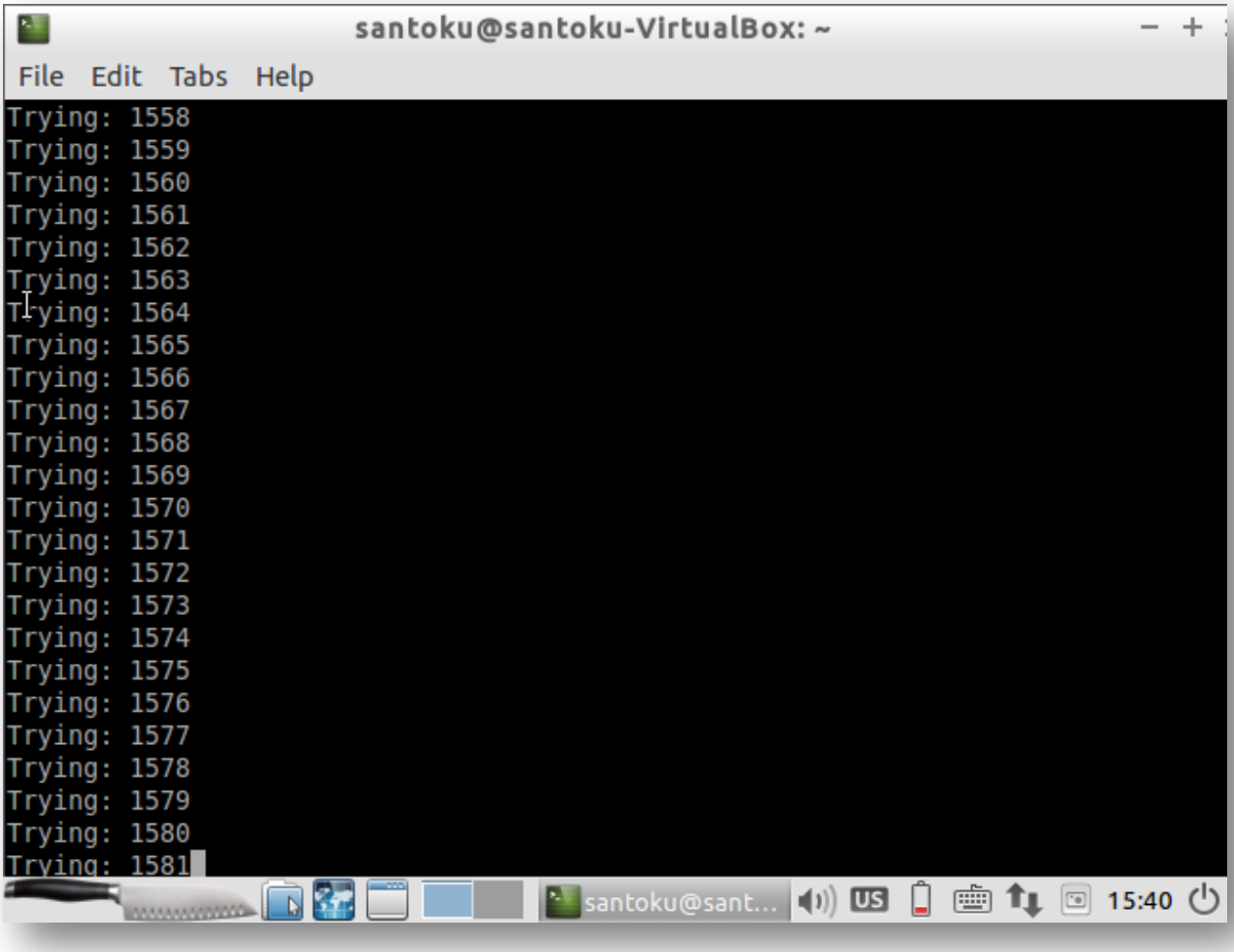
E) Run Android Brute Force Encryption program

Now you have tmp_footer_6 and tmp_header_2 files on your Santoku Linux. Run Android Brute Force Encryption program using following command on the terminal.

$ bruteforce_stdcrypto tmp-header_2 tmp_footer_6



Once you run this command, you can see that program will brute force the password.



4.3.3 Android Password Cracking Using Hashcat

Goal: To crack the pin (password) of Android phone using Hashcat.

Background:

- Hashcat is the CPU-based password recovery tool. It is released as free software. Versions are available Linux, OS X, and Windows. Examples of hashcat supported hashing algorithms are Microsoft LM hashes, MD4, MD5, SHA-family, and MySQL.
- For password cracking we need two files:
    1) /data/system/password.key : hash is stored
    2) /data/system/locksettings.db : salt is stored

Approach followed:

a) Enable root access on phone using Kingo ROOT application.
b) Enable USB debugging on phone
c) Connect phone to Santoku Linux (running in VM environment)
d) Run adb commands
e) Pull password.key and locksettings.db file
f) Install Hashcat
g) Run Hashcat

Requirements:

a) Oracle VirtualBox Manager
b) Santoku Linux VM
c) A BLU phone BLU phone (BLU ADVANCE 4.0L Android version : 4.4.2)
d) Kingo ROOT application on your desktop
e) Hashcat

A) Enable root access on phone using Kingo ROOT application.

B) Enable USB debugging on phone

C) Connect phone to Santoku Linux (running in VM environment)

These three steps are similar to the steps A, B, and C of the document "4.3.1 Android Password and Pattern Skipping"

D) Run adb commands

1) Click on "Accessories" and open LXTerminal on Santoku Linux and type following command on the terminal to check whether the device (phone) is detected or not.

   $ adb devices

   It will show the serial number of the device which is detected.

2) Log in to phone shell using adb shell command:

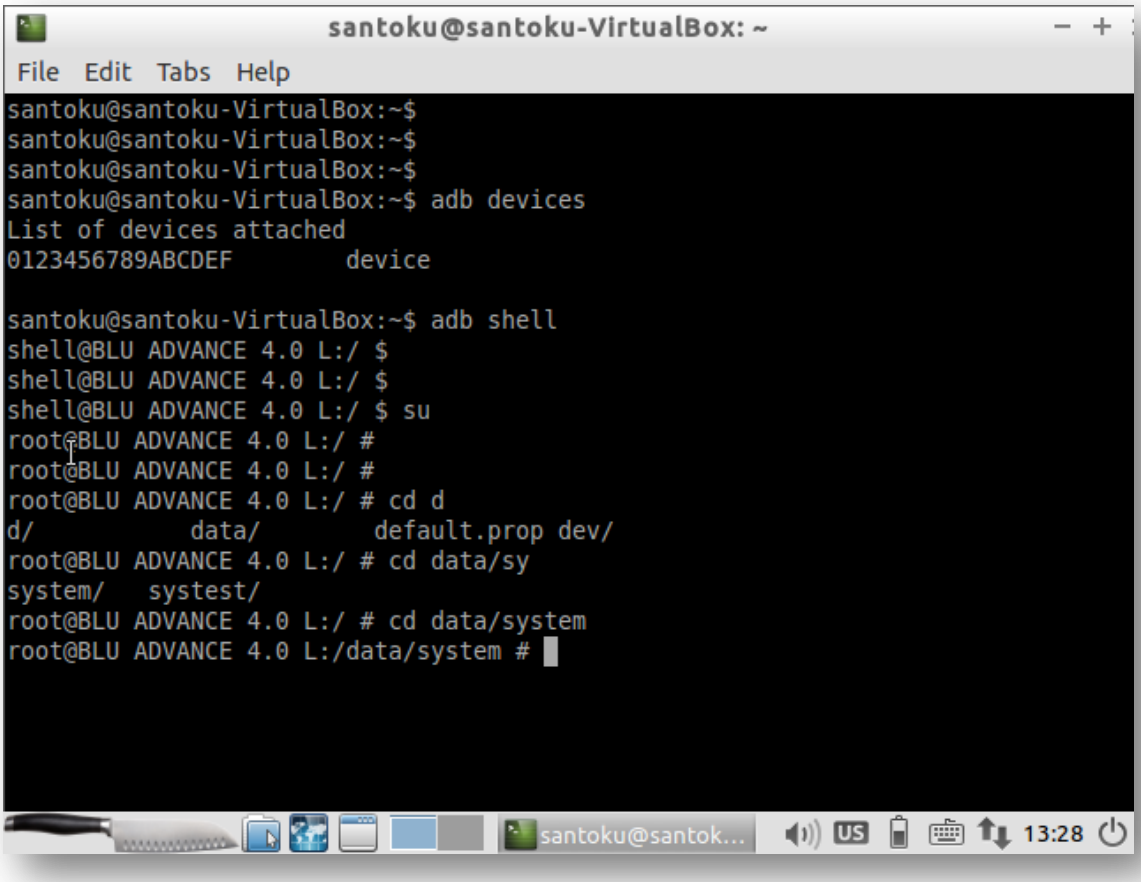
   $ adb shell

3) Since we have Android phone rooted, we can run commands as root user using "su" command. If phone is not rooted, then we won't get sudo(root) access.

   $ su

4) Change directory to /data/syatem. This directory contains files password.key and locksettings.db

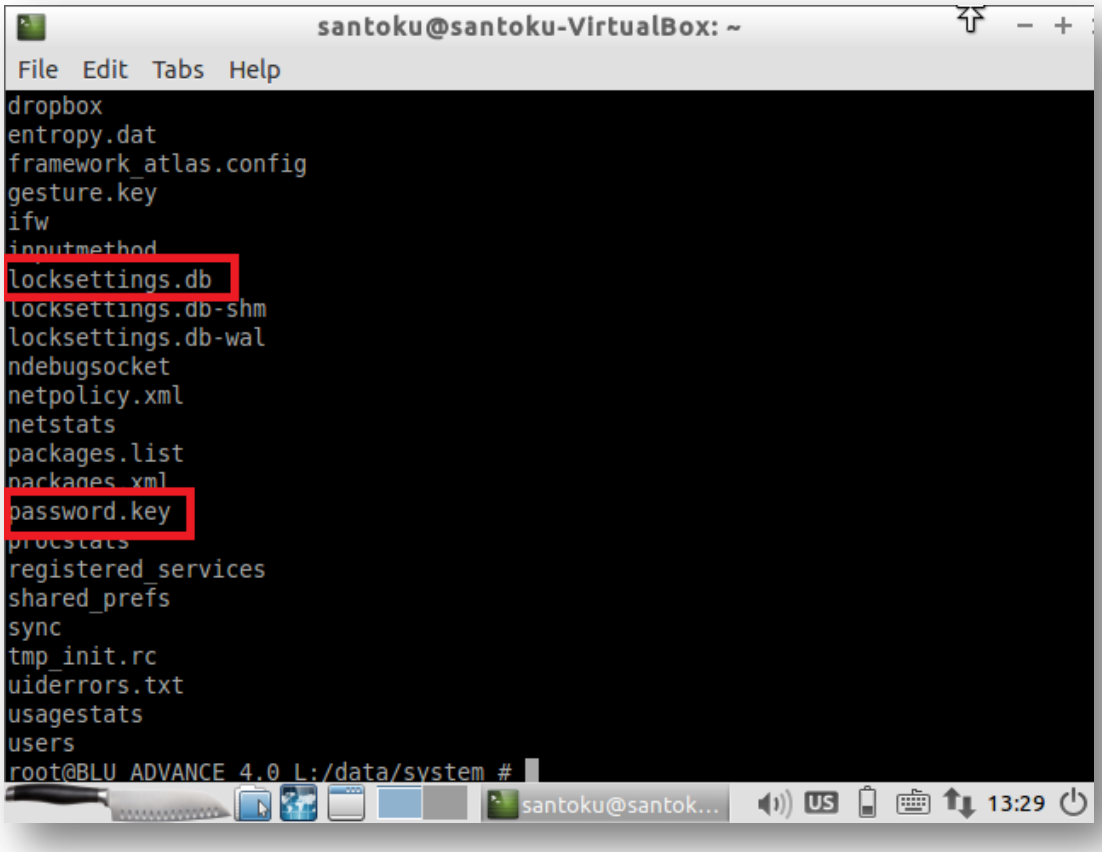
   $ cd /data/system


santoku@santoku-VirtualBox: ~
File Edit Tabs Help
santoku@santoku-VirtualBox:~$
santoku@santoku-VirtualBox:~$
santoku@santoku-VirtualBox:~$
santoku@santoku-VirtualBox:~$ adb devices
List of devices attached
0123456789ABCDEF device
santoku@santoku-VirtualBox:~$ adb shell
shell@BLU ADVANCE 4.0 L:/ $
shell@BLU ADVANCE 4.0 L:/ $
shell@BLU ADVANCE 4.0 L:/ $ su
root@BLU ADVANCE 4.0 L:/ #
root@BLU ADVANCE 4.0 L:/ #
root@BLU ADVANCE 4.0 L:/ # cd d
d/ data/ default.prop dev/
root@BLU ADVANCE 4.0 L:/ # cd data/sy
system/ systest/
root@BLU ADVANCE 4.0 L:/ # cd data/system
root@BLU ADVANCE 4.0 L:/data/system #
santoku@santok...
US
13:28

E) Pull password.key and locksettings.db file

1) Type following command on the terminal to make sure that password.key and locksettings.db files are in the /data/system directory.

$ ls



2) Now, to pull these files change their permissions using following commands on the terminal.

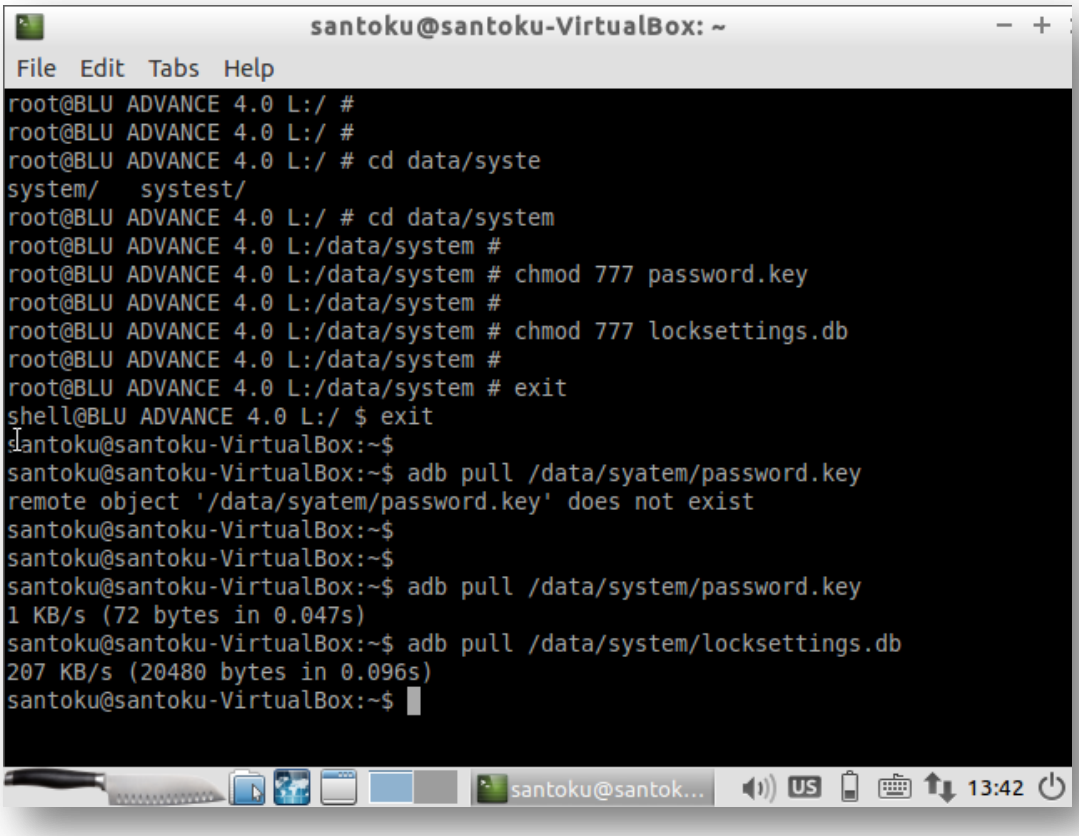
$ chmod 777 password.key

$ chmod 777 locksettings.db

Exit from the phone shell by using “exit” command on the terminal and use “adb pull” commands to pull the files into Santoku Linux.

$ adb pull /data/system/password.key

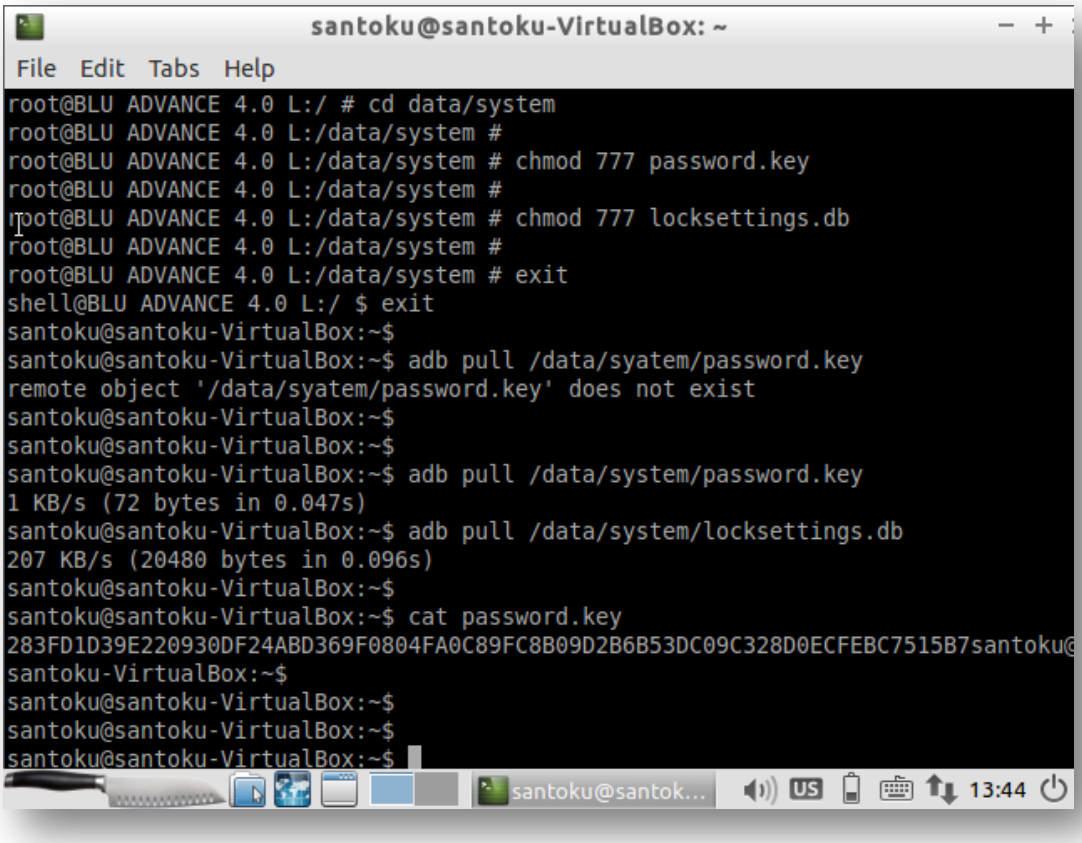
$adb pull /data/system/locksettings.db



3) To get the hex representation of the password stored in /data/system/password.key file, type following command on the terminal.

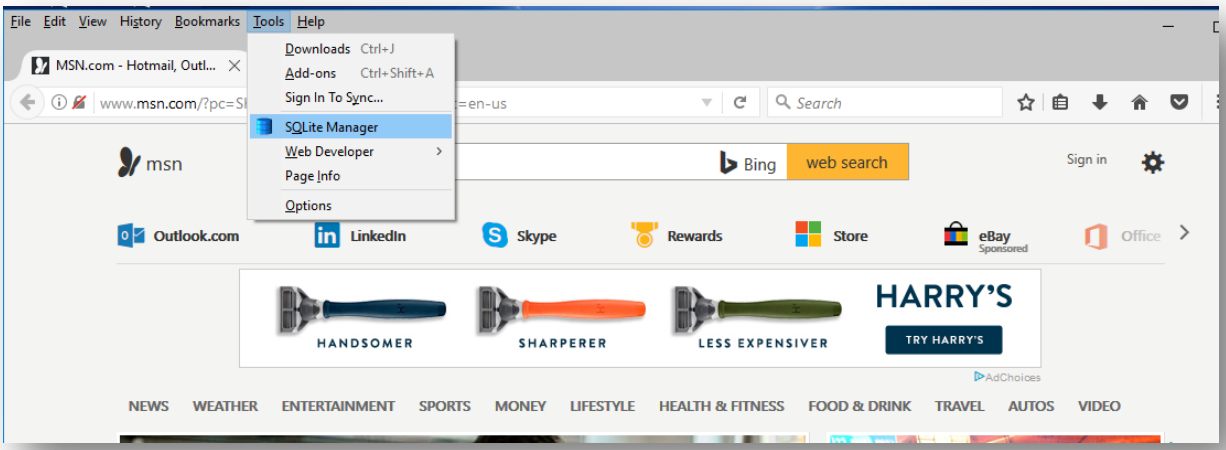
$ cat password.key

Note down this string.

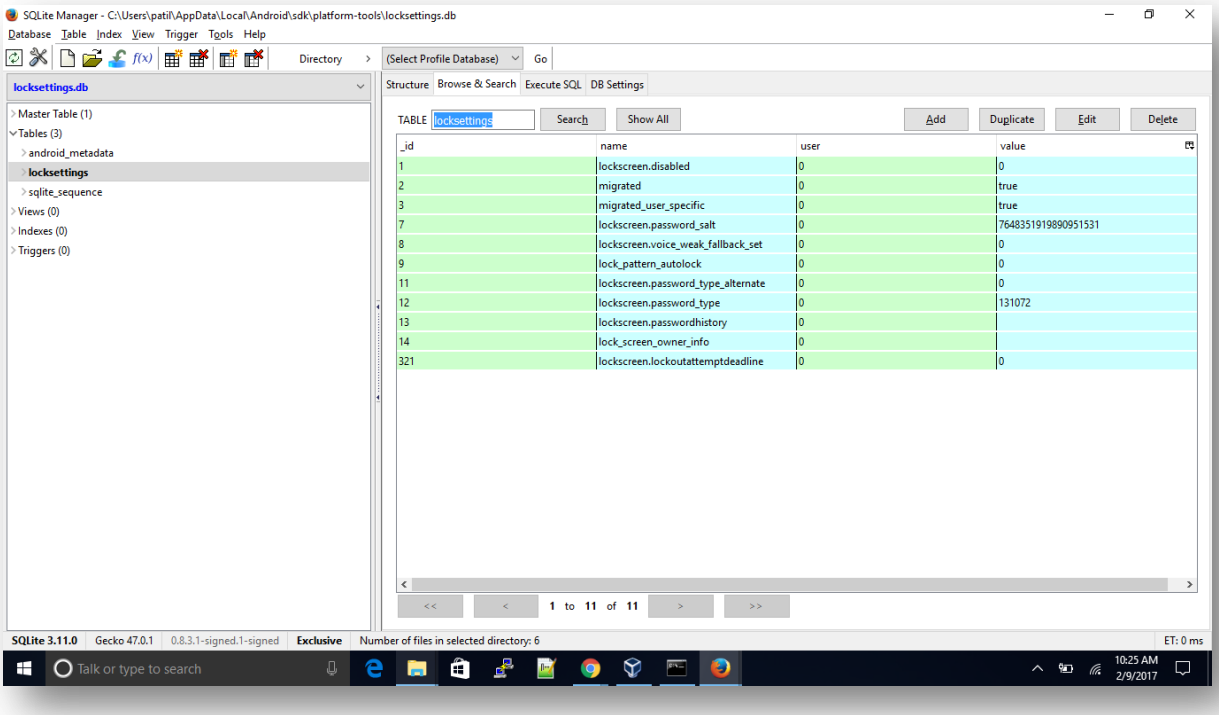


4) Now, to get the salt stored in locksettings.db file, get that file from Santoku Linux to your host operating system which is Windows here via USB. Another way of getting files from Santokku Linux VM to your host VM is by simply sending those files as attachment over E-mail.

Go to the firefox -> Tools -> SQLiteManager and give locksettings.db as input to it.



You can see the salt on the right side of the window as shown in the screen shot:



F) Install Hashcat

1) Download hashcat from https://hashcat.net/hashcat/ on your host operating system. Here, for this project I used Windows 10 (64 bit OS) as a host operating system and downloaded hashcat-3.30.7z archive.

2) Create “hashcat” folder on “C:” drive and copy that archive file to that folder. Open command prompt on Windows and change directory to “C:\hashcat” using following command:

$cd C:\hashcat

3) Now, you need to unpack that archive into hashcat folder. Type following command on the terminal

$ 7za x hashcat-3.30.7z

In hashcat-3.30 folder there are hashcat64.exe file and hashcat32.exe file. I am having 64-bit Windows 10 Operating System, so I will use hashcat64.exe file.

G) Run Hashcat

1) You already have the password in hex representation and salt with you.

String that we got from password.key file is 72 characters long. It’s actually two hashes, one SHA1 and one MD5 concatenated together. So split the above hash into two.

SHA1:

283FD1D39E220930DF24ABD369F0804FA0C89FC8

MD5:

B09D2B6B53DC09C328D0ECFEBC7515B7

2) The 64bit salt that we got is:

7648351919890951531

Convert it to hex by using online Decimal to Hex converter and then to lower case:

6A24678C6646ED6B = **6a24678c6646ed6b**

3) On Windows command prompt, change directory by using following command on the terminal:

$ cd C:\hashcat\hashcat-3.30

4) Run hashcat by using following command on the terminal

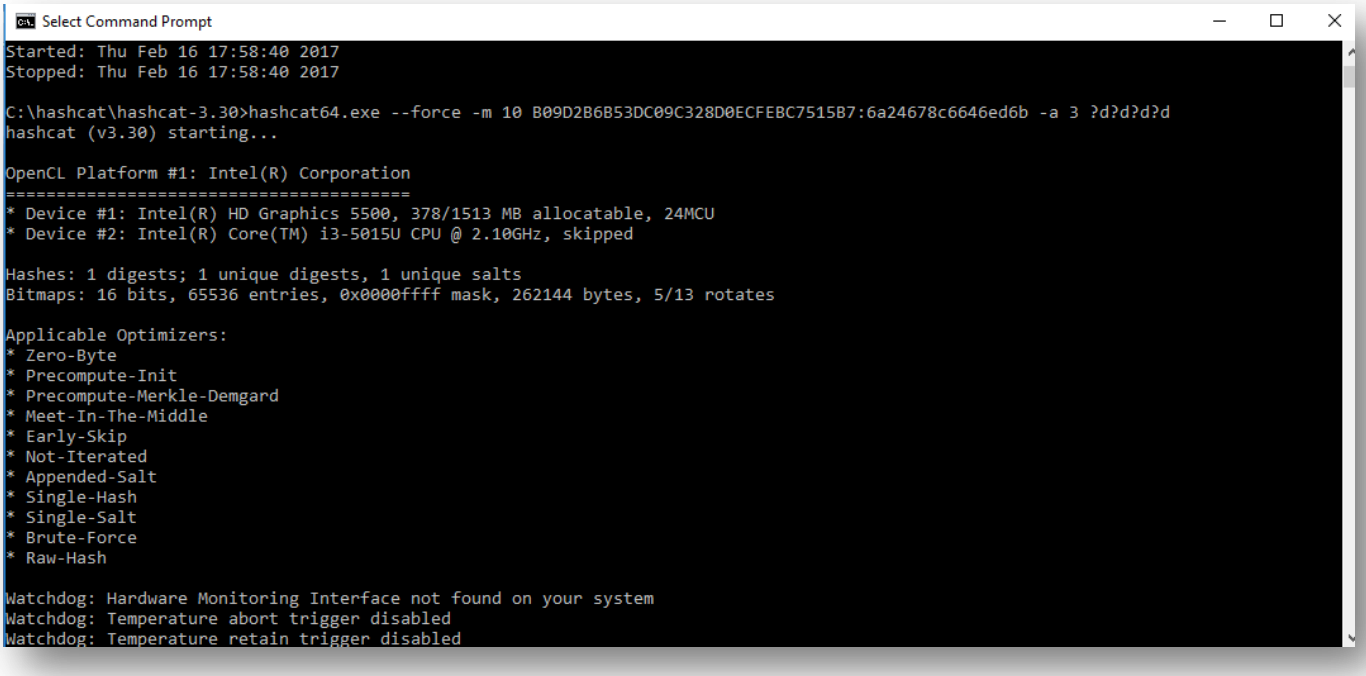
$ hashcat64.exe --force -m 10 B09D2B6B53DC09C328D0ECFEBC7515B7: 6a24678c6646ed6b -a 3 ?d?d?d?d

- --force : attribute (avoid warnings)
- -m : represent hash type
- 10 : hash mode is md5
- Note that B09D2B6B53DC09C328D0ECFEBC7515B7 and 6a24678c6646ed6b is the information which we already got in above steps.
- -a : represent attack mode
- 3 : Brute Force
- Our android phone has a pin “1234” which is 4 digit long, so we are using format: ?d?d?d?d

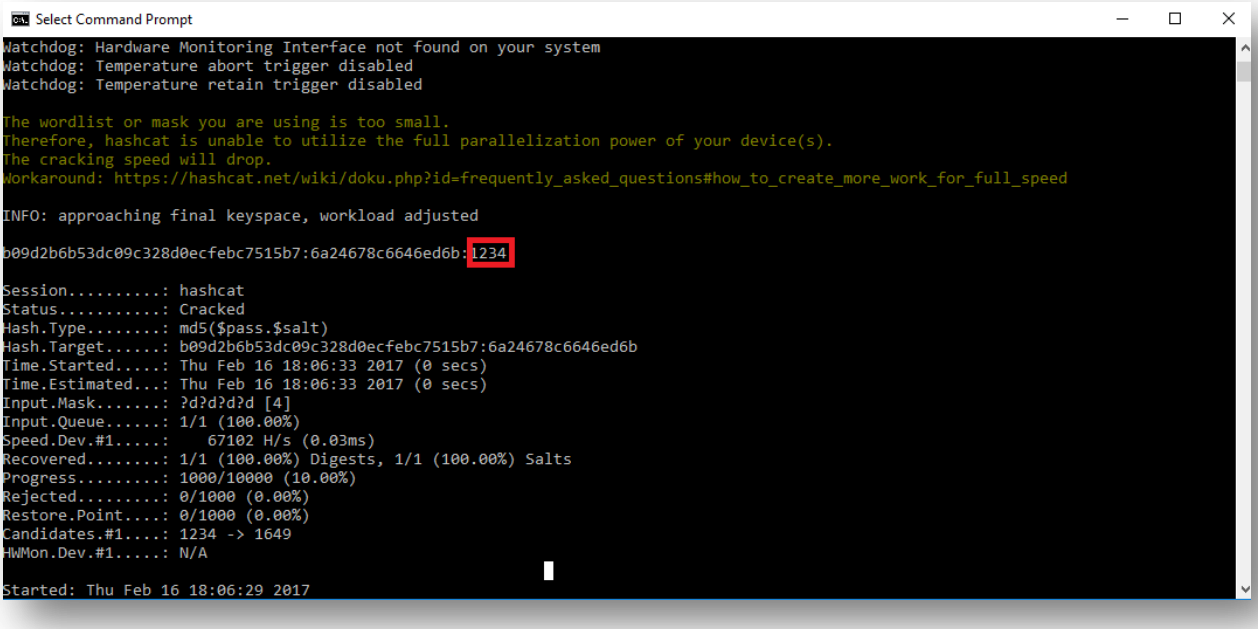
To know more about hashcat command and its options refer to the link bellow:

https://hashcat.net/wiki/doku.php?id=hashcat

5) Once you run the command, you can see that hashcat starts brute forcing the pin.



As shown in the red box, your pin “1234” is successfully cracked.



6. References

[1] R. K, "TecAdmin.net," in *Virtualization*, TecAdmin.net, 2016. [Online]. Available: http://tecadmin.net/install-oracle-virtualbox-on-ubuntu/. Accessed: Feb. 25, 2017.

[2] "Kali Linux Official Documentation,". [Online]. Available: http://docs.kali.org/introduction/what-is-kali-linux. Accessed: Jan. 20, 2017.

[3] "A detailed guide on installing Kali Linux on VirtualBox,". [Online]. Available: https://www.blackmoreops.com/2014/04/08/detailed-guide-installing-kali-linux-on-virtualbox/. Accessed: Jan. 12, 2017.

[4] "Password cracking: Lesson 2: Using kali, bkhive, samdump2, and john to crack the SAM database," 2013. [Online]. Available: http://www.computersecuritystudent.com/SECURITY_TOOLS/PASSWORD_CRACKING/lesson2/. Accessed: Feb. 11, 2017.

[5] Home and P. Policy, "Cracking password in kali Linux using john the Ripper," 2015. [Online]. Available: https://www.blackmoreops.com/2015/11/10/cracking-password-in-kali-linux-using-john-the-ripper/. Accessed: Feb. 02, 2017.

[6] "About Santoku · Santoku Linux,". [Online]. Available: http://santoku-linux.com/about-santoku/. Accessed: Jan. 23, 2017.

[7] "HOWTO install Santoku in a virtual machine · Santoku Linux,". [Online]. Available: https://santoku-linux.com/howto/installing-santoku/installing-santoku-in-a-virtual-machine/. Accessed: Jan. 20, 2017.

[8] S. Lee, "9 ways to bypass Samsung lock screen pattern, pin, Password and fingerprint,". [Online]. Available: https://drfone.wondershare.com/unlock/9-ways-to-bypass-samsung-lock-screen-pattern-pin-password-fingerprint.html#Part6. Accessed: Feb. 25, 2017.

[9] "HOWTO brute force Android Encryption on Santoku Linux · Santoku Linux,". [Online]. Available: https://santoku-linux.com/howto/mobile-forensics/how-to-brute-force-android-encryption/. Accessed: Feb. 25, 2017.

[10] D. Lodge, "Cracking Android passwords, a how-to," 2015. [Online]. Available: https://www.pentestpartners.com/blog/cracking-android-passwords-a-how-to/. Accessed: Feb. 25, 2017.