# LAPORAN

**TUGAS 11**

12 - 19 - 2020



Oleh

Demitries Baskhara Rivaldo Tolla/123180137

Program Studi Informatika

Jurusan Teknik Informatika

Fakultas Teknik Industri

Universitas Pembangunan Nasional “Veteran” Yogyakarta

2020

**COVER 1**

[**Linux adalah Sistem Operasi paling aman**](#_tjalz4p16y43) **3**

[Proses Instalasi](#_c1ou5qmh6xz9) 3

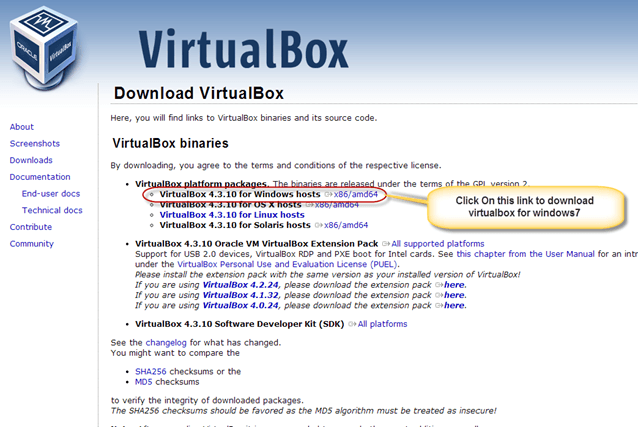
[Supaya Secure dalam pemakain Linux](#_g6aed2x7wtmt) 11

[**Digital Forensic**](#_fqi0fcrfcvdd) **13**

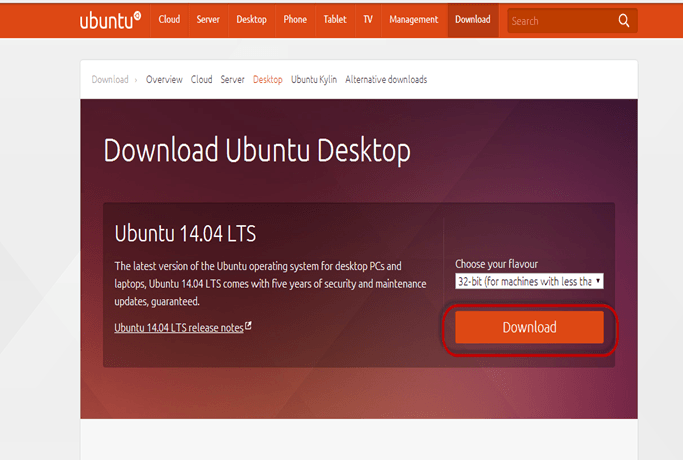
# Linux adalah Sistem Operasi paling aman

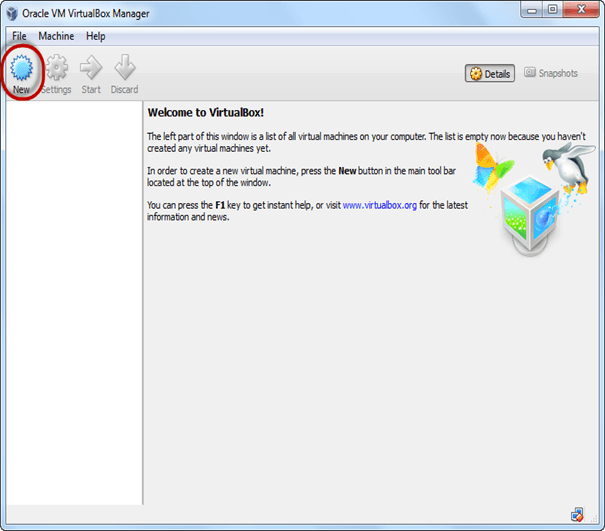
## Proses Instalasi :

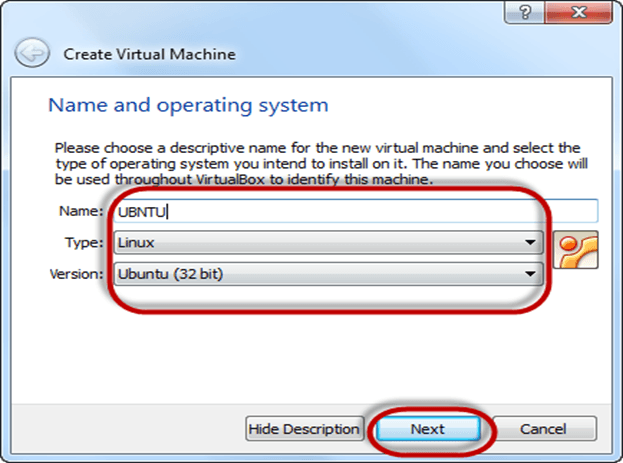
1. Download dan Install Virtual Box



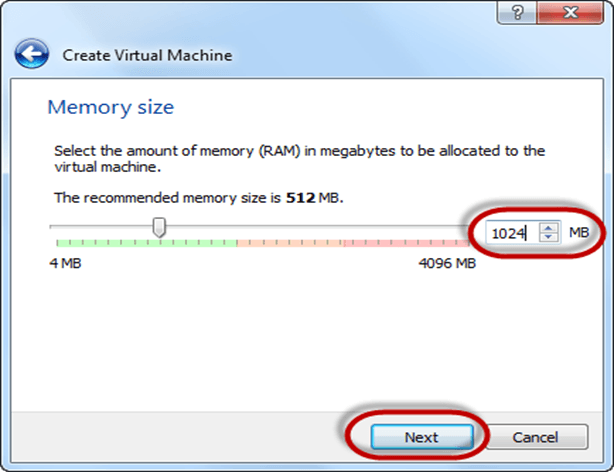
1. Download Ubuntu

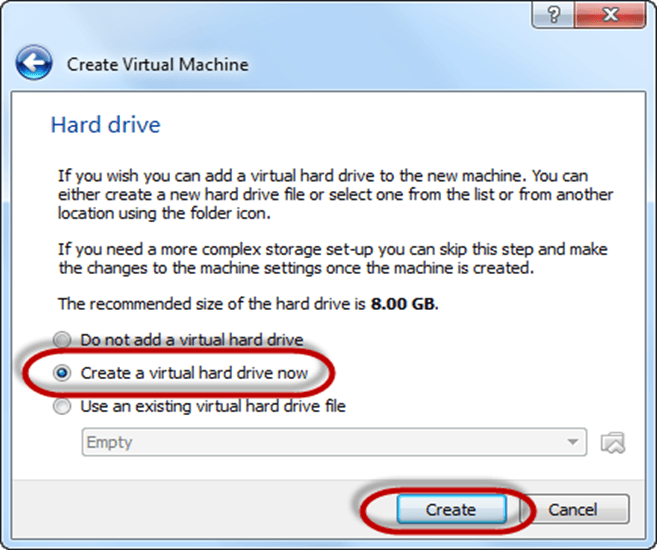


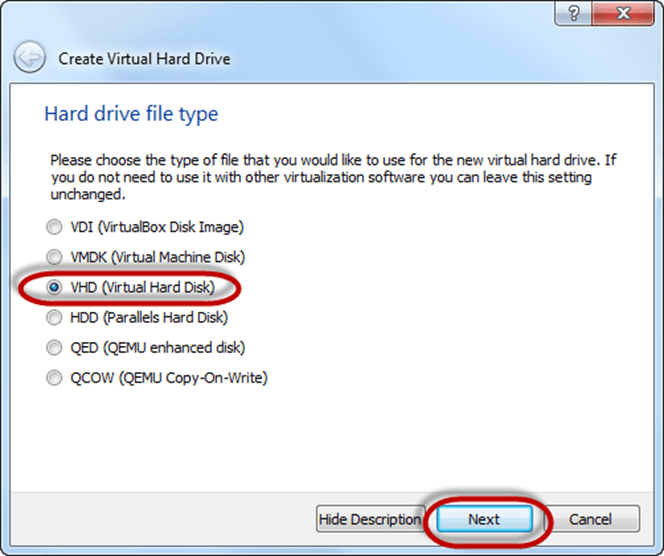
1. Buka virtual box dan tekan “New”
2. Isikan Nama , Type dan Version



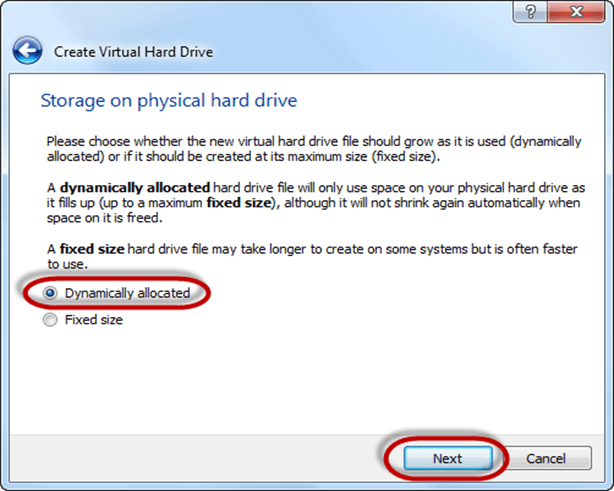
1. Alokasikan penggunaan RAM

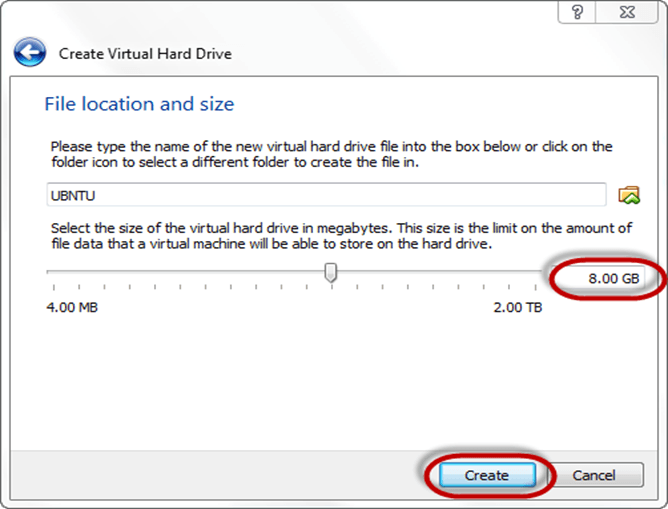


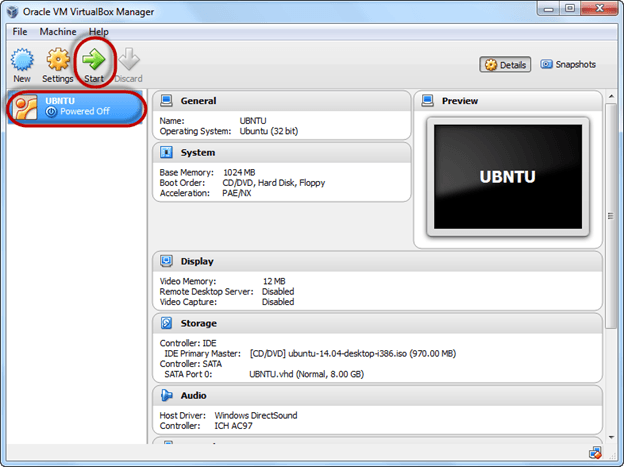
1. Buat virtual hard drive untuk tempat Linux
2. Pilih VHD

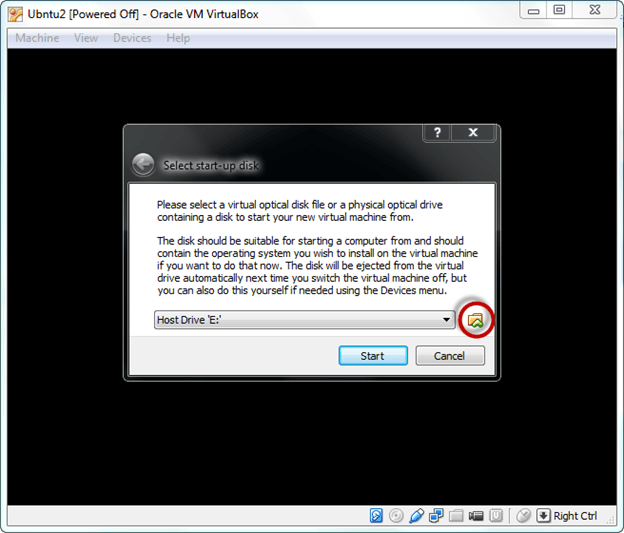


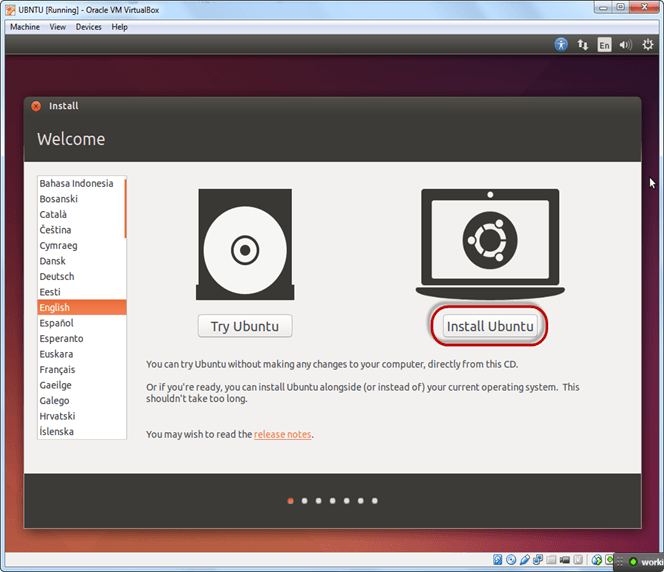
1. Pilih Dynamically allocated

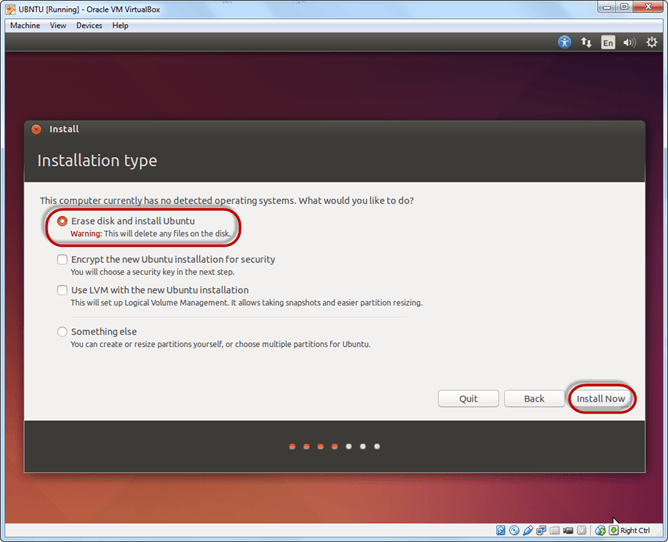


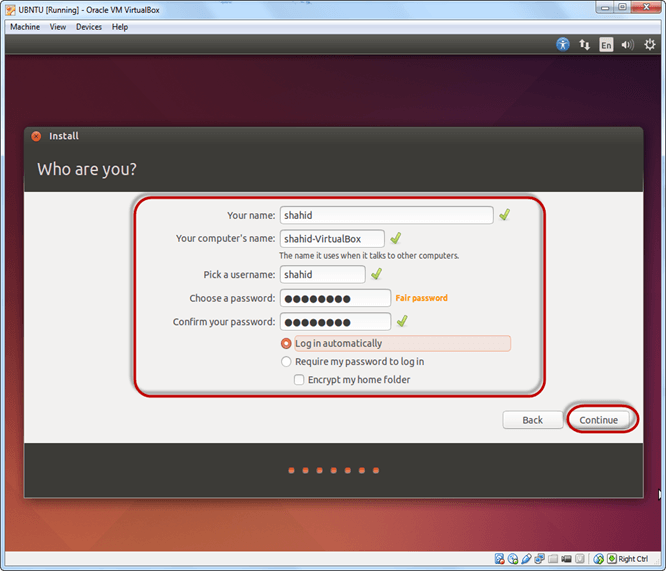
1. Alokasikan size pada hard drive
2. Pilih virtual drive yang sudah dibuat lalu start



1. Cari file ubuntu dan start
2. Pilih instal Ubuntu dan continue



1. Format disk untuk Ubuntu
2. Buat account admin untuk bisa masuk ke dalam ubuntu



## Supaya Secure dalam pemakain Linux :

1. Update server

Hal pertama adalah mengupdate file local dan mengupgrade Sistem Operasi..

→ $ sudo apt update && sudo apt upgrade -y

1. Buat akun privileged

Selanjutnya buat akun user . Jangan masuk ke server sebagai root , masuklah sebagai user.

→ $ adduser <username>

→ $ usermod -a -G sudo <username>

1. Upload SSH key

Untuk masuk ke server diperlukkan SSH key , maka dari itu upload saja SSH key sehingga bisa masuk tanpa memasukkan kunci.

→ $ ssh-copy-id <username>@ip\_address

1. Secure SSH

Selanjutnya lakukan hal ini :

* Menghilangkan kunci SSH untuk otentikasi
* Larang root dikendalikan dari luar
* Larang akses IPv6 dan IPv4

buka /etc/ssh/sshd\_config memakai text editor dan ganti :

|  |
| --- |
| PasswordAuthentication yes  PermitRootLogin yes |

menjadi

|  |
| --- |
| PasswordAuthentication no  PermitRootLogin no |

Selanjutkan berikan larangan akses untuk merubah pada AddressFamily. Untuk mengubah hanya boleh pada IPv4 lakukan perubahan:

|  |
| --- |
| AddressFamily inet |

Restart SSH untuk mendapat perubahan. Sebelumnya buat lah koneksi cadangan sebelum restart , dapat dilakukan dengan :

→ $ sudo service sshd restart

1. Gunakan firewall

Sekarang instal firewall dan jalankan dengan :

→ $ sudo apt install ufw

→ $ sudo ufw allow ssh

→ $ sudo ufw allow http

→ $ sudo ufw allow https

→ $ sudo ufw enable

1. Install Fail2ban

Aplikasi ini bekerja dengan cara mengecek apakah ada hal aneh dalam koneksi , jika ditemukan keanehan tersebut maka koneksi akan diputuskan.

→ $ sudo apt install fail2ban -y

→ $ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

→ $ sudo service fail2ban restart

# Digital Forensic

ProDiscover adalah rangkaian produk yang membahas berbagai skenario yang ditangani oleh organisasi penegak hukum dan investigasi internal perusahaan. ProDiscover menyediakan serangkaian fitur dan toolkit untuk Forensik Komputer dan Respon Insiden. Rangkaian produk juga dilengkapi dengan alat diagnostik dan pengumpulan bukti untuk investigasi kepatuhan kebijakan perusahaan dan penemuan elektronik.

## 

ProDiscover Forensics memungkinkan ahli forensik komputer menemukan semua informasi digital pada disk komputer dan kemudian melindungi bukti digital dan menghasilkan laporan pembuktian yang baik untuk digunakan dalam proses hukum. memungkinkan penyelidikan informasi digital tanpa mengubah metadata berharga seperti terakhir kali diakses.

ProDiscover Forensics dapat memulihkan HDD & file yang dihapus, Investigasi ruang kosong, Analisis Aliran Data Alternatif Windows, dan secara dinamis memungkinkan pratinjau, pencarian forensik, dan akuisisi data Area Dilindungi Perangkat Keras (HPA) dari disk. sangat sulit untuk menyembunyikan data dari ProDiscover Forensics atau ProDiscover Incident Response karena membaca disk di tingkat sektor & cluster.

ProDiscover Forensics memungkinkan pencarian forensik melalui seluruh disk untuk kata kunci di mana ekspresi dan frase reguler dengan kemampuan pencarian Boolean penuh untuk menemukan informasi digital yang diperlukan yang disimpan di perangkat digital. Fitur perbandingan hash dapat digunakan untuk menemukan file ilegal yang diketahui atau file terkenal baik, misalnya file sistem operasi standar, dengan memanfaatkan database Hashkeeper yang disertakan dari sumber eksternal. ProDiscover Forensics atau ProDiscover Incident Response memiliki kemampuan pencarian forensik terbaik & sangat cepat dan fleksibel, memungkinkan pencarian kata kunci untuk kata atau frasa di mana saja pada disk yang menyertakan ruang kosong.