

## Environment Setup

### Downloads

Download & install Virtual Box (<https://www.virtualbox.org/wiki/Downloads>)

Download Kali Linux .iso (<https://www.kali.org/downloads/>)

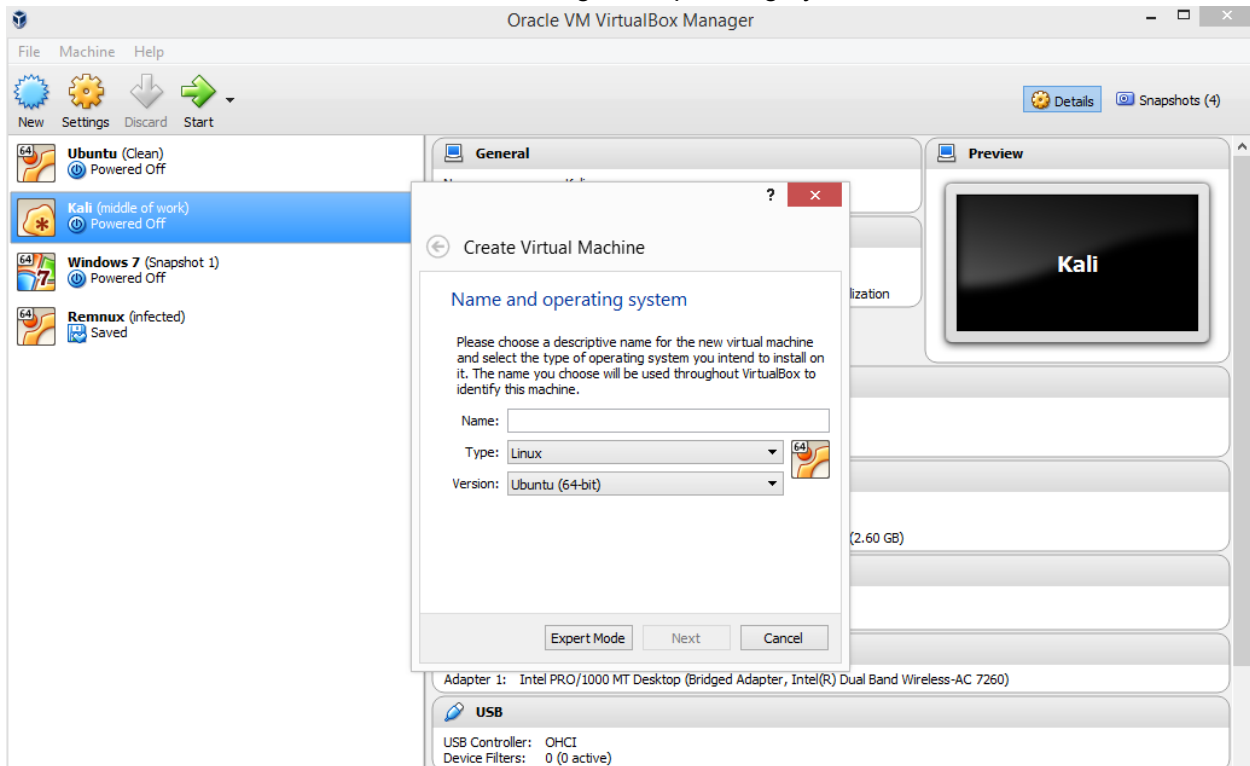
Download Remnux .ova (<https://remnux.org/docs/distro/get/>)

Download Ubuntu .iso (<https://www.ubuntu.com/download>)

### Setup Ubuntu & Kali Virtual Machines

Open Virtual Box and click on the “New” button on the top of the screen select the type and version of the operating system you are trying to install.

If there is not a Version that matches the targeted operating system choose “Linux other”.



Once your machine has been created, double click on the machine to power it on.

You will be prompted to provide a media. Browse to your download folder and pick the previously downloaded .iso files.

When installing **Kali**, you will see the following:

Choose any option you would like. Usually, you'd want to install the OS, but since we can take snapshots, it doesn't matter if you run the live version or not.

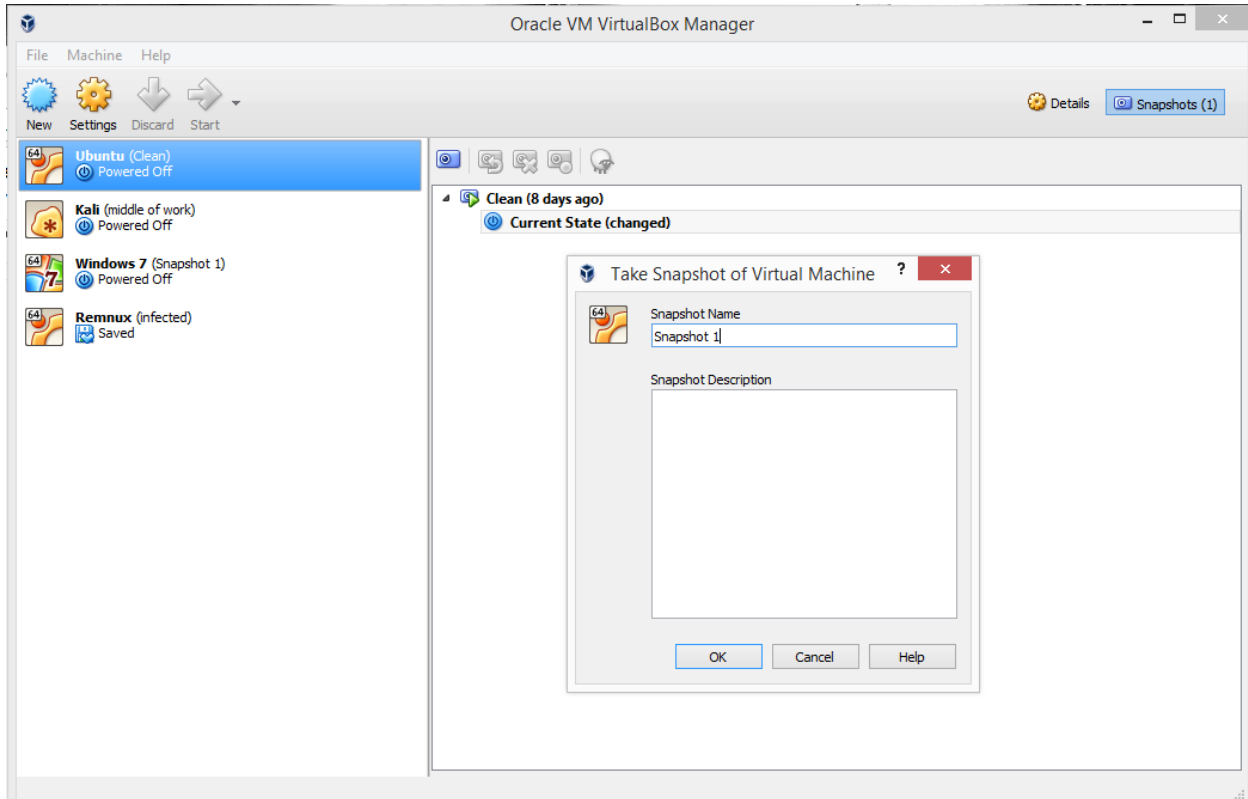
When installing **Ubuntu** you can choose to “Install” and go through the setup process.

Texas Tech University  
Spring 2017  
Digital Forensics  
Environment Setup

Once you are up and running, go back to the Virtual Box VM Manager to create a snapshot of the clean machine.

Click on the machine you would like to snapshot.

Then, up in the right hand corner, click on the button with the camera icon. It should take you to a page that looks like this:



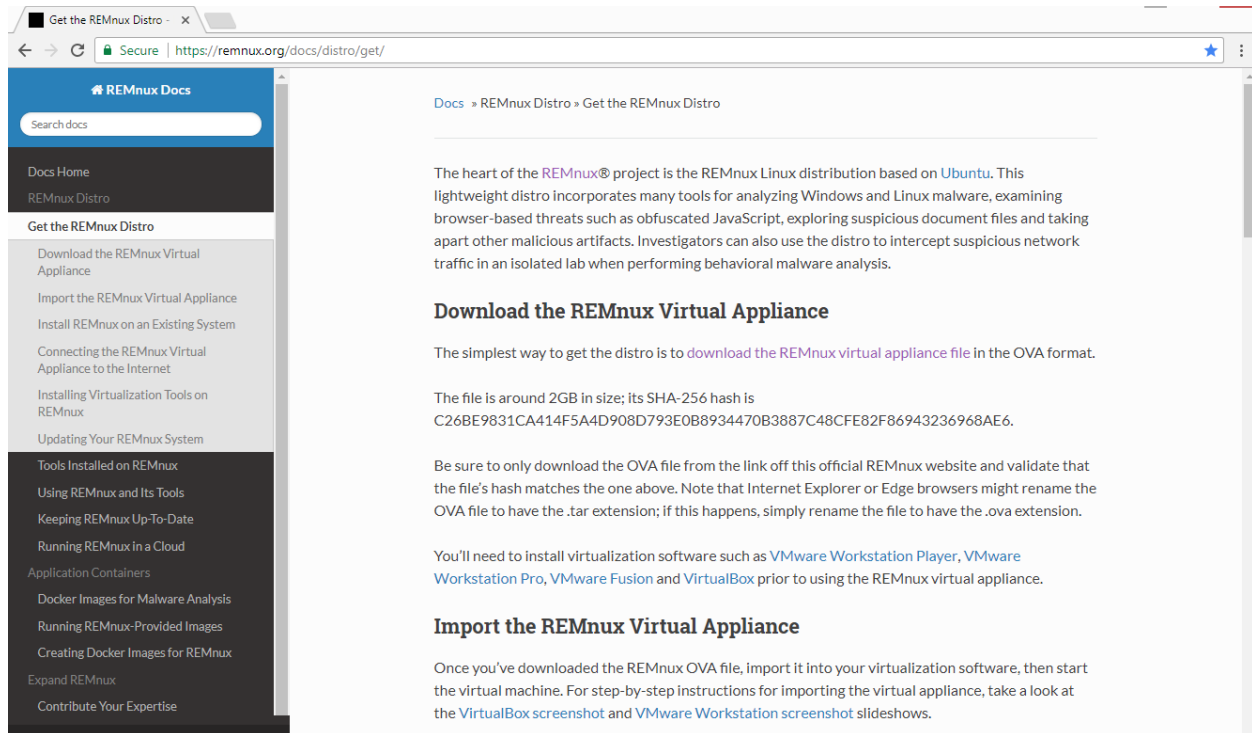
“Take snapshot” and give the snapshot a name that will let you know what state the machine is in.

At any point in your analysis, you can return to the state of the machine using this snapshot.

## Setup Remnux Virtual Machine

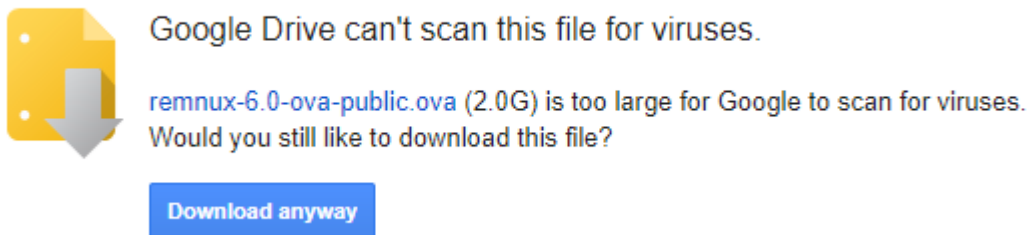
Texas Tech University  
Spring 2017  
Digital Forensics  
Environment Setup

Download the remnux .ova file.



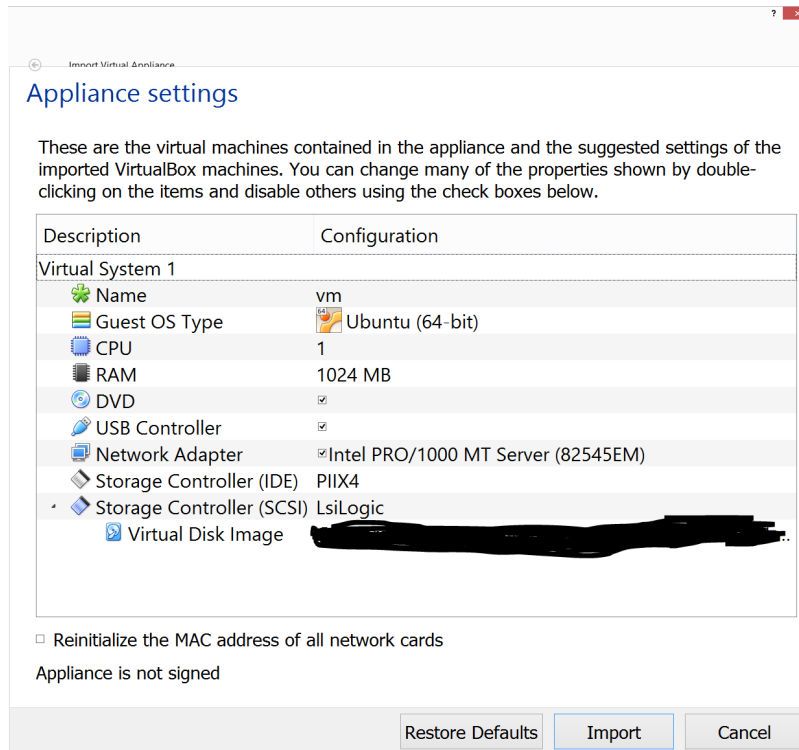
The screenshot shows a web browser window with the URL <https://remnux.org/docs/distro/get/>. The left sidebar contains a navigation menu with the following items: REMnux Docs, Search docs, Docs Home, REMnux Distro, Get the REMnux Distro (selected), Download the REMnux Virtual Appliance, Import the REMnux Virtual Appliance, Install REMnux on an Existing System, Connecting the REMnux Virtual Appliance to the Internet, Installing Virtualization Tools on REMnux, Updating Your REMnux System, Tools Installed on REMnux, Using REMnux and Its Tools, Keeping REMnux Up-To-Date, Running REMnux in a Cloud, Application Containers, Docker Images for Malware Analysis, Running REMnux-Provided Images, Creating Docker Images for REMnux, Expand REMnux, and Contribute Your Expertise. The main content area has the breadcrumb "Docs » REMnux Distro » Get the REMnux Distro". The text describes the REMnux project as a lightweight Linux distribution based on Ubuntu, designed for analyzing Windows and Linux malware. It provides instructions on how to download the virtual appliance in OVA format, including the file size (around 2GB) and its SHA-256 hash (C26BE9831CA414F5A4D908D793E0B8934470B3887C48CFE82F86943236968AE6). It also mentions that the file should be renamed from .tar to .ova and that virtualization software like VMware Workstation Player, VMware Workstation Pro, VMware Fusion, and VirtualBox must be installed before using the appliance. The section "Download the REMnux Virtual Appliance" states that the simplest way to get the distro is to download the REMnux virtual appliance file in the OVA format. The section "Import the REMnux Virtual Appliance" explains that after downloading the OVA file, it should be imported into the virtualization software, and provides links to screenshots for VirtualBox and VMware Workstation.

If you are using google chrome, you may see the following error; download anyway.

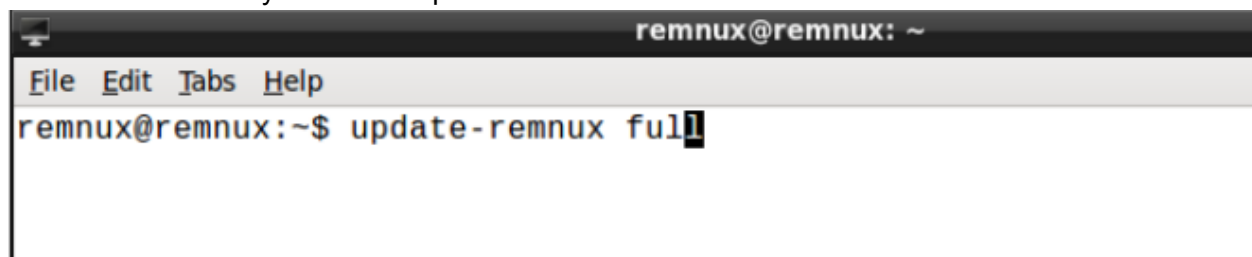


Once the file has been downloaded double click on the file. Virtual Box should open with a window to import an appliance:

Texas Tech University  
Spring 2017  
Digital Forensics  
Environment Setup



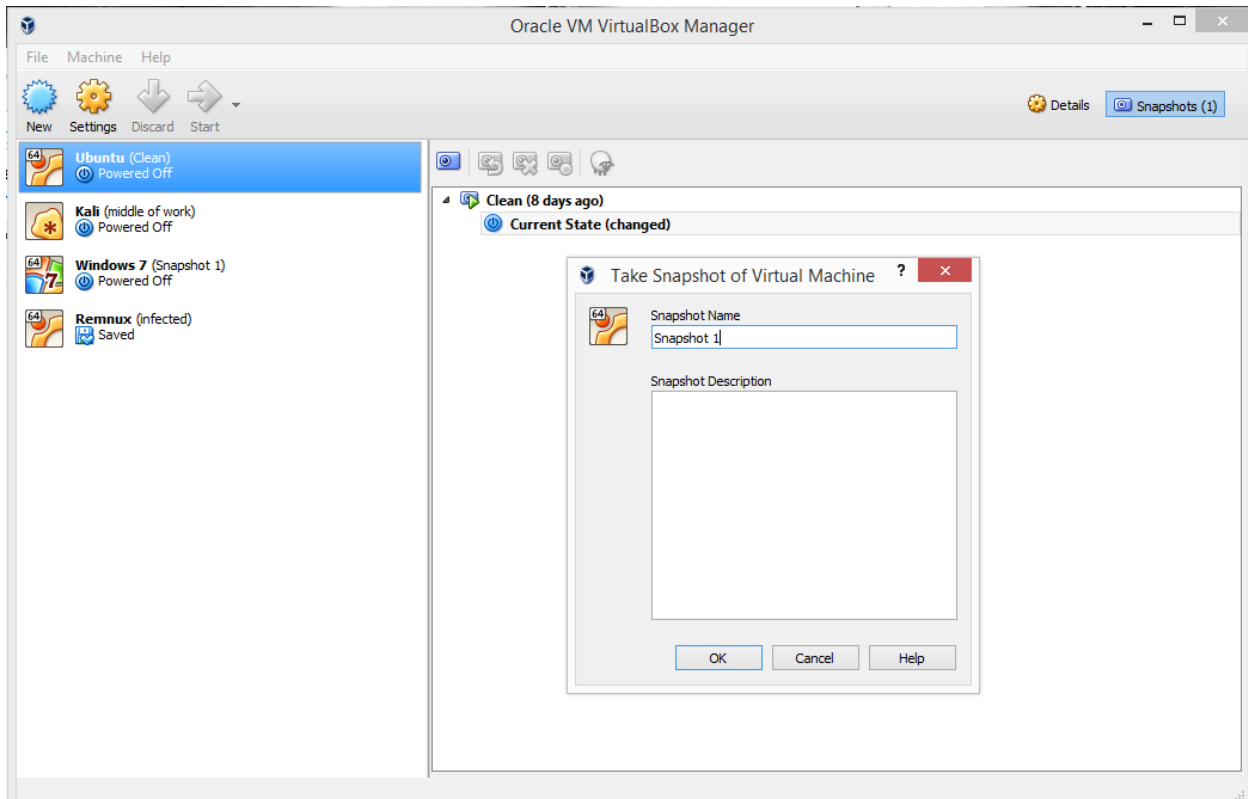
Click Import. That's all you should have to do. Once the virtual machine starts, it's recommended that you run the update command in the terminal.



Take a snapshot of the machine

Then, up in the right hand corner, click on the button with the camera icon. It should take you to a page that looks like this:

Texas Tech University  
Spring 2017  
Digital Forensics  
Environment Setup



“Take snapshot” and give the snapshot a name that will let you know what state the machine is in.

At any point in your analysis, you can return to the state of the machine using this snapshot.

### Setup Windows Virtual Machine (requires a windows key)

TTU offers operating systems to students. To retrieve your key and setup a Windows VM, follow the instructions below:


- Go to the ttu software page (<http://www.depts.ttu.edu/itts/software/>)

Texas Tech University  
Spring 2017  
Digital Forensics  
Environment Setup

Software/Site License | T X

www.depts.ttu.edu/itts/software/


IT Technology Support
About ITTS
All Services
Computing Labs
ShortCourses & Training
Software
Web Development



load


s, Faculty and Staff

JAWS



Statistical Discovery™ From SAS.


JMP



Mathematics • Modeling • Simulation

A CUBERT GROUP COMPANY


Maple



MATLAB

and Staff

MATLAB




Microsoft Imagine

der download for educational

ents, Faculty and Staff

Microsoft Imagine



Office


s, Faculty and Staff

Microsoft Office 365

TTU Price: Free via Office 365

Eligibility: TTU, Students, Faculty and Staff

OS: PC and Mac




sas

load

lty and Staff

www.depts.ttu.edu/itts/software/jmp.php



symantec™

lty and Staff

Microsoft Campus Agree X

www.depts.ttu.edu/itts/software/ms/index.php

IT Technology Support
About ITTS
All Services
Computing Labs
ShortCourses & Training
Software
Web Development

Click on any of the software titles below to view more information.

Microsoft Office 365

Microsoft Imagine

**Name:** Microsoft Imagine

**Eligible Users:** TTU, Students, Faculty and Staff


**Operating System(s):** PC, Mac

**TTU Price:** Free

Learn more at the [official website](#)

Imagine is a Microsoft Program that supports technical education by providing access to Microsoft software for learning, teaching and research purposes. It includes the following software:

- Visual Studio
- Virtual PC
- Windows

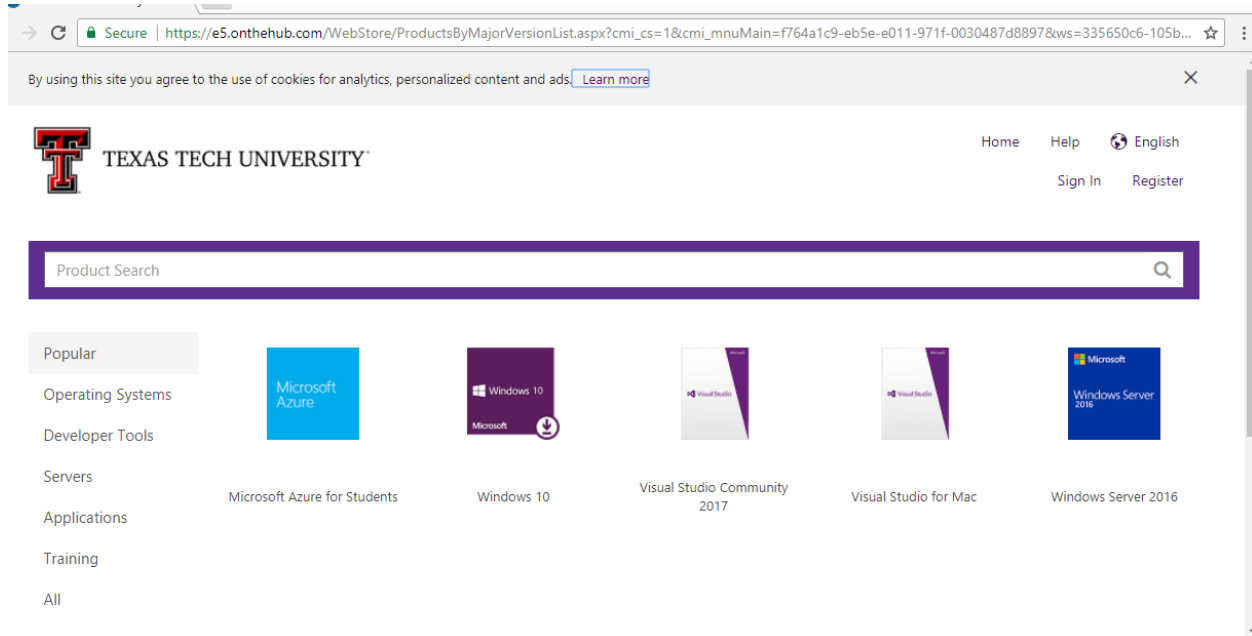


### Related Links

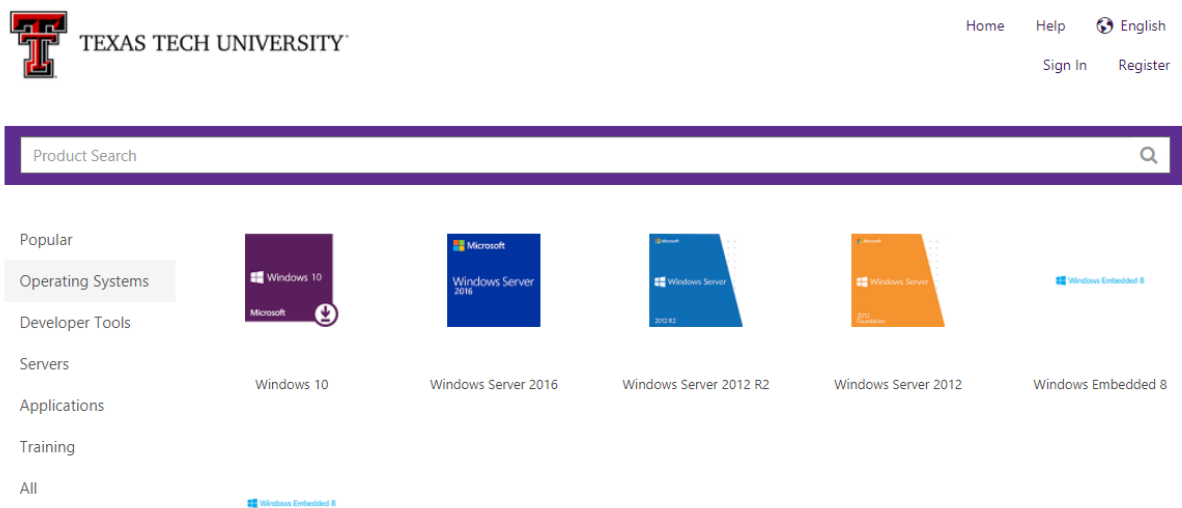
- View Full Software List
- Find a Computer Lab
- Attend a ShortCourse

- Go to microsoft imagine

Texas Tech University  
Spring 2017  
Digital Forensics  
Environment Setup



- Register
- Search for operating systems



- Add to cart, and checkout. Follow the instructions about creating an image.

— Windows 10 IoT Core, Version 1703 (Update March 2017)



Windows 10 IoT Core brings the power of Windows to your device and makes it easy to integrate richer experiences with your devices such as natural user interfaces, searching, online storage and cloud based services.

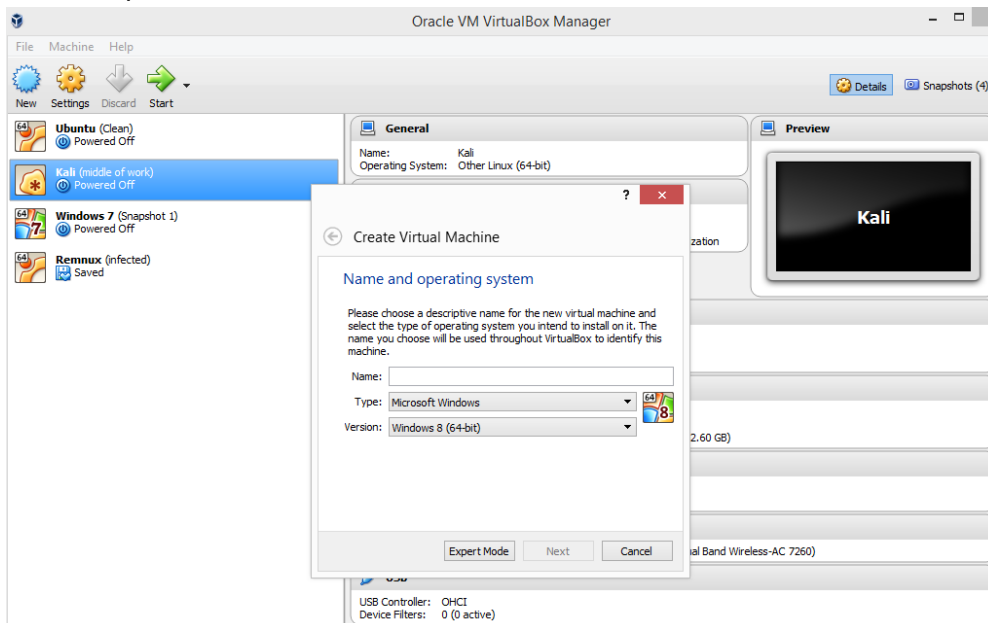
Windows 10 IoT Core, Version 1703 (Update March 2017) (ARM, x86, x64) (English) - Microsoft Imagine

Available to: Students/Faculty/Staff

Free

Add to Cart

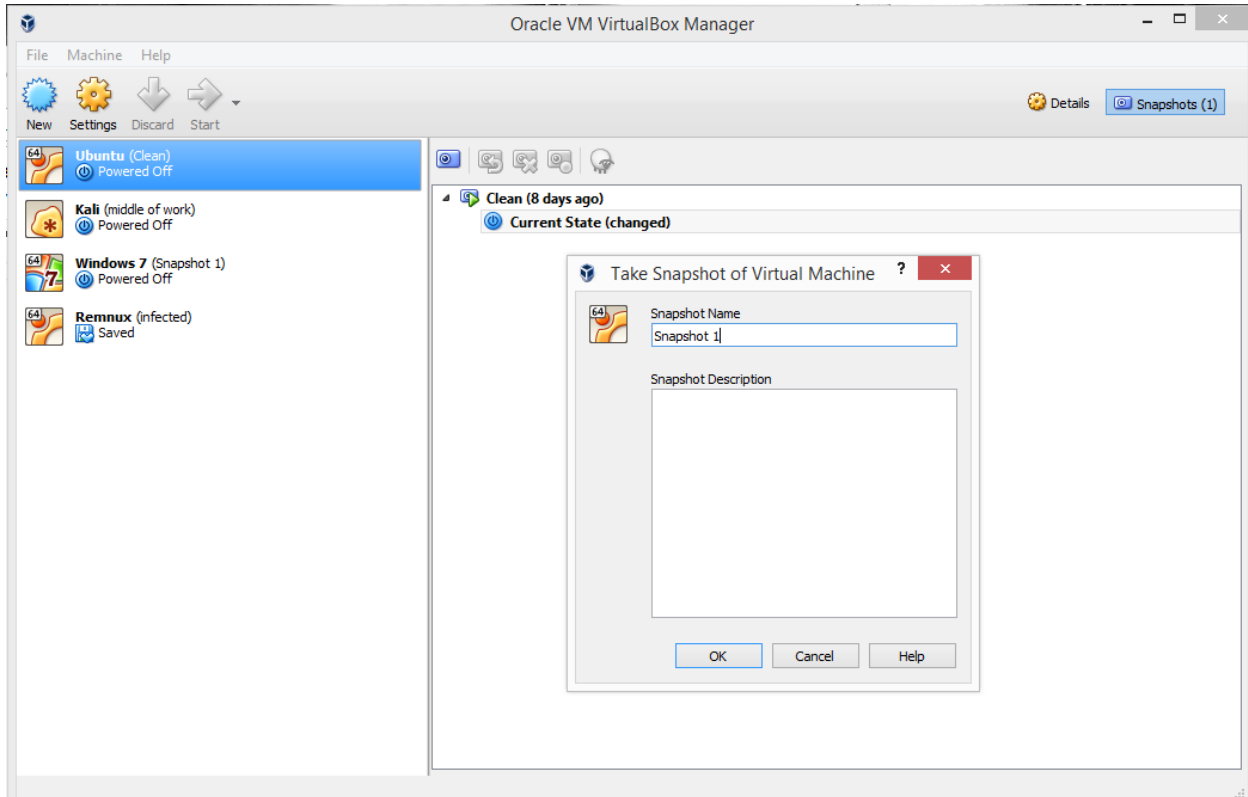
- Create the .iso ([ftp://ftp.kivuto.com/pub/docs/Working\\_with\\_Image\\_Files.pdf](ftp://ftp.kivuto.com/pub/docs/Working_with_Image_Files.pdf))
- Open virtual box & create a new machine



Take a snapshot of the machine; in the right hand corner, click on the button with the camera icon. It should take you to a page that looks like this:



Texas Tech University  
Spring 2017  
Digital Forensics  
Environment Setup



“Take snapshot” and give the snapshot a name that will let you know what state the machine is in.

At any point in your analysis, you can return to the state of the machine using this snapshot.

## Troubleshooting

### **I only see 32-bit operating systems in the dropdown list. What now?**

- If you are in VirtualBox trying to create a new machine and only see options for 32-bit machines you will likely need to change settings in the BIOS.
  - If you don't already know, look up the key on the keyboard that allows you to navigate the the BIOS. The key combination varies depending on the manufacturer.
  - Restart your computer and press the key combination to enter BIOS
  - When you get to the BIOS you will need to enable virtualization. Again, this looks different for each computer manufacturer, but you are looking for a setting that will allow you to enable virtualization.
- After the BIOS settings have been changed, you should see the 64-bit options in the virtual box dropdown. From there, you can create virtual machines with operating systems of your choice.

Texas Tech University  
Spring 2017  
Digital Forensics  
Environment Setup

?

×

←

Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.


If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **25.00 GB**.


☐ Do not add a virtual hard disk

☒ Create a virtual hard disk now

☐ Use an existing virtual hard disk file

 Windows 7.vdi (Normal, 25.00 GB)

▼



Create

Cancel

?

×

←

Create Virtual Hard Disk

Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

☒ VDI (VirtualBox Disk Image)

☐ VHD (Virtual Hard Disk)

☐ VMDK (Virtual Machine Disk)

Expert Mode

Next

Cancel

Texas Tech University  
Spring 2017  
Digital Forensics  
Environment Setup

?

← Create Virtual Hard Disk

Storage on physical hard disk

Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

☒ Dynamically allocated

☐ Fixed size


Next Cancel

?


← Create Virtual Hard Disk

File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

Windows 8 

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

 25.00 GB

4.00 MB 2.00 TB

Create Cancel

Texas Tech University  
Spring 2017  
Digital Forensics  
Environment Setup

