# Digital Forensics (IFS4102) Lab 1: Setting up Your Forensic Workstations

## Lab Objectives

In this first lab, you will prepare and set up your own **forensic workstations**. For more exposure with various available forensic tools and software, you should set up both **Windows** and **Linux-based** forensic workstations. Additionally, for the next 2 labs on data acquisition, **USB storage-device requirements** for your practices are also mentioned.

## Task 1-A: Installing a Virtualization Software

Note that you will need to install various third-party forensic tools into your forensic workstations. As such, if you do ***not*** want to use your personal notebook/ computer as your forensic workstation, you will need to install a hypervisor or VMM software so that you can then run your forensic workstations as VMs instead. For this, you can use either **VirtualBox** or **VMware**. Slides on installing and using VirtualBox, as well as a VirtualBox documentation PDF file, have been uploaded to LumiNUS for your reference.

## Task 1-B: Setting up a Linux-Based Forensic Workstation

For your Linux-based forensic workstation, you can install **Kali Linux**, which comes with various forensic tools pre-installed. Slides on installing and configuring Kali Linux, as well as a Kali Linux documentation PDF file, have been uploaded to LumiNUS for your reference.

Alternatively, you are welcome to set up other Linux-based forensic workstations. One example is **SANS Investigative Forensic Toolkit (SIFT)** workstation, whose information is given at https://www.sans.org/tools/sift-workstation/.

## Task 1-C: Setting up a Windows-Based Forensic Workstation

Additionally, you should also set up a **Windows**-based forensic workstation since many available forensic tools are Windows-based tools for easy and convenient usage by Digital Forensics practitioners. You can download **your preferred VM** version from https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/. Note that the available VMs expire after 90 days. As such, you may want to set a snapshot when you first install the WM which you can then roll back to later.

## Task 1-D: Obtaining USB Storage Devices for Labs 2 & 3

In your Lab 2, you will perform **a static (non-volatile) data acquisition**.
More specifically, you will create a forensic disk image of a target storage drive.
For this, please get a **USB thumb drive** with a **relatively small capacity**
(e.g. 1-4GB) for a fast imaging. Please put some sample files into the drive before the lab.

In your Lab 3, you will also perform **a live (volatile) data acquisition** to create the memory/RAM image file of a target computer. For this, you will need an **external storage drive** to store the created memory image file, and the drive's free space must be larger than the size of the RAM of your target machine/VM. Hence, please prepare a **USB thumb drive** or a USB-connected **external hard drive** with enough free space (e.g. >8GB) for the exercise. (Note that you can't use your target machine's hard drive since you do not want to modify the evidence drive!)