**Download software for the Windows environment**

# Get Windows 10

1. Go the following link: **https://portal.azure.com**
2. Click the sign-in link
3. Use your SAIT Credentials:
   1. <firstname>.<lastname>@edu.sait.ca
   2. Same password used to access your O365 account
4. Once logged in, browse to **Software** section using the **Navigation** Links on the left side of the page.
   1. Access student benefits
   2. Explore button
   3. Software link on the left
5. Filter the results to assist in finding what you are searching for. You can choose Product Category (**Operating System**), Operating System (**Windows**), System type (**64bit**)
6. All components of the lab were built with Windows 7; possible to use Windows 10 – 64 bits for the labs with a few tweaks.

**NOTE:** The Windows Update can’t be disabled therefore, snapshot the OS so that it possible to rollback if necessary.

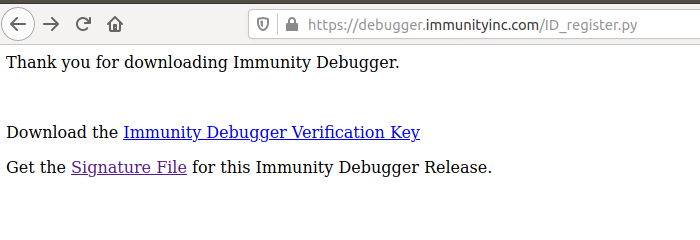
* 1. Pick one of the links that starts with **Windows 10**

1. Ensure that for whatever OS chosen, you will need to Click the **View Key** button to get a license. Get the license to avoid the annoying reminders.
2. You should only need a license if you use the product longer than the grace period time provided by Microsoft. 90 – 180 days in most cases
3. Install the Windows OS as a VM. Give it a minimum of **40-50GB** of space, so that you can install more software later.
4. After installation boot it up and follow the rest of the installation steps below. Snapshot the VM so that you can rollback to an earlier time when things were functioning.

# Get Python

1. You will need two versions of python from the website: **https://www.python.org/downloads/windows/**
2. Download Python **2.7.14:** **https://www.python.org/downloads/release/python-2714rc1/**
3. Download Python **3.8.3:** **https://www.python.org/ftp/python/3.8.3/python-3.8.3.exe**
4. Install the versions on your Windows VM.

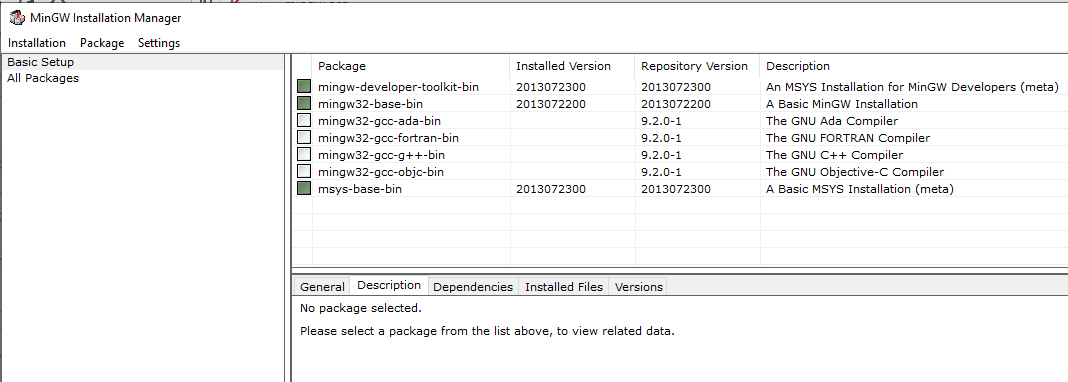
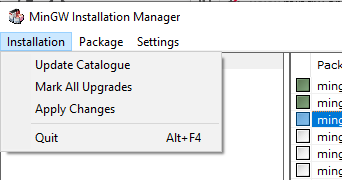
# Get Immunity Debugger

1. Go to the following link: **https://www.immunityinc.com/products/debugger/**
2. Find the download link “**Download Immunity Debugger Here**!”
3. You will be asked to register, you can enter random information here, as it does not go through a strict registration process.
4. It is always a good idea to validate the image downloaded by using the signature file or verification key.

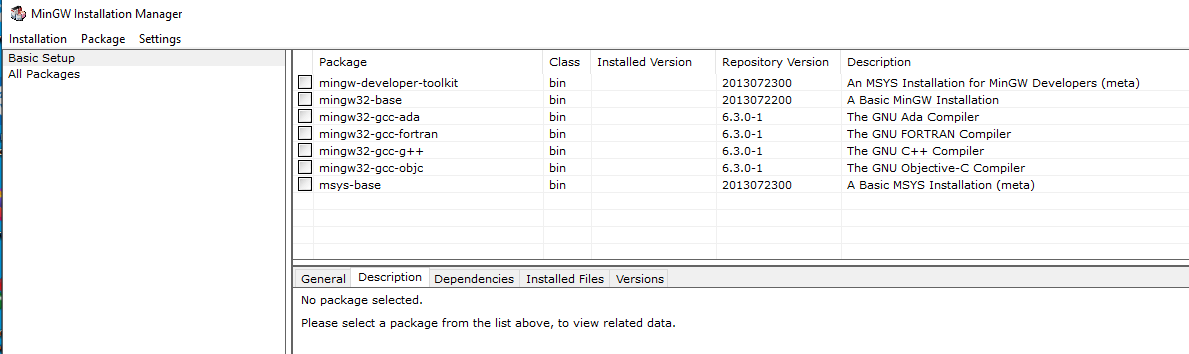
# Get Java JDK 1.8u241 (required if installing PyCharms)

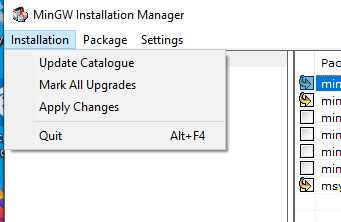
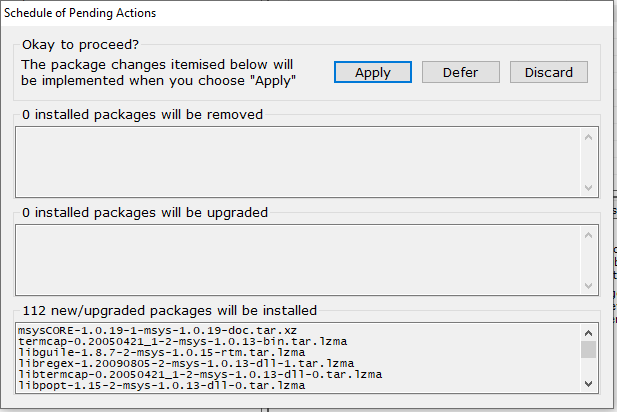
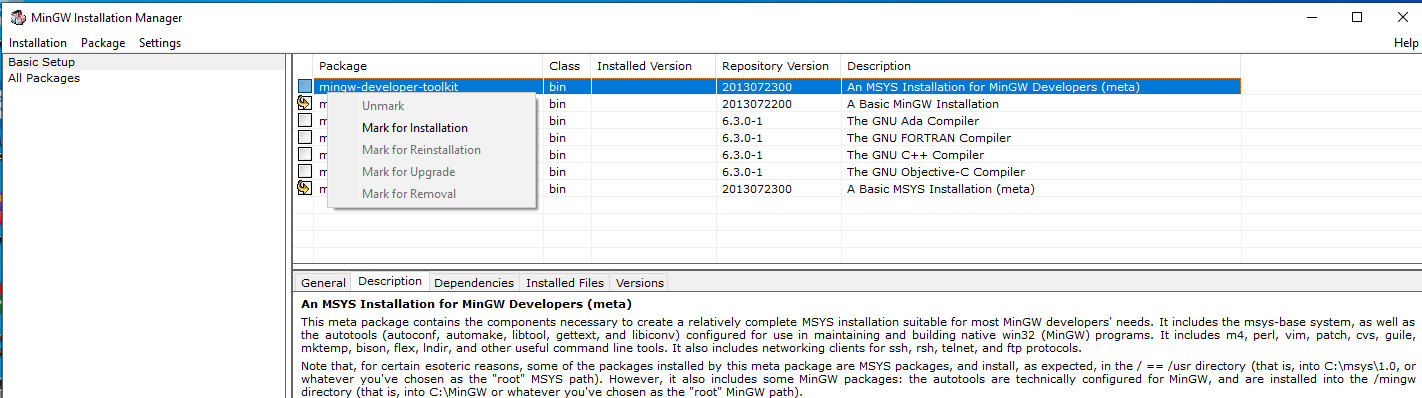
1. Go to the following link: **https://www.oracle.com/java/technologies/javase/javase-jdk8-downloads.html**
2. Find the section for Windows x86 and download jdk-8u251-windows-i586.exe
3. Unfortunately, you will need to register to get a copy of the file.
4. If you find an alternative, trusted link to get this content, share this will the class.d

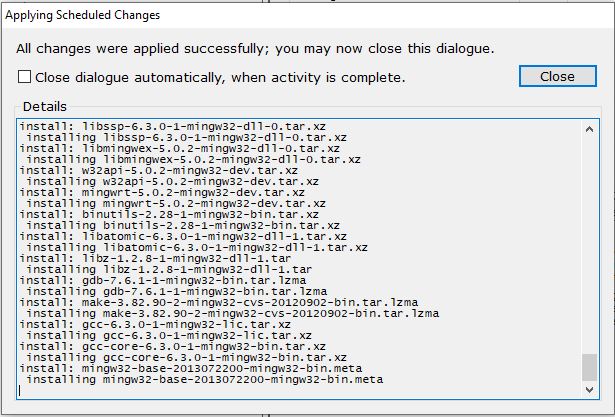
# Get MINGW (GCC compiler) – abbreviated setup steps

1. Go to the following website: **https://sourceforge.net/projects/mingw/**
2. This should start the auto download process.
3. Run the installer once download has completed.
4. Once installed, click Continue, you will see a screen like the following:
5. Choose the Basic Setup
6. Select the ming-developer-toolkit-bin, mingw32-base-bin and msys-base-bin
   1. Choose Mark …
7. Once you have selected your packages to install, click the Installation menu item and choose **Apply Changes**.
8. The installation should take some time and once completed you will have the gcc compiler for windows installed.

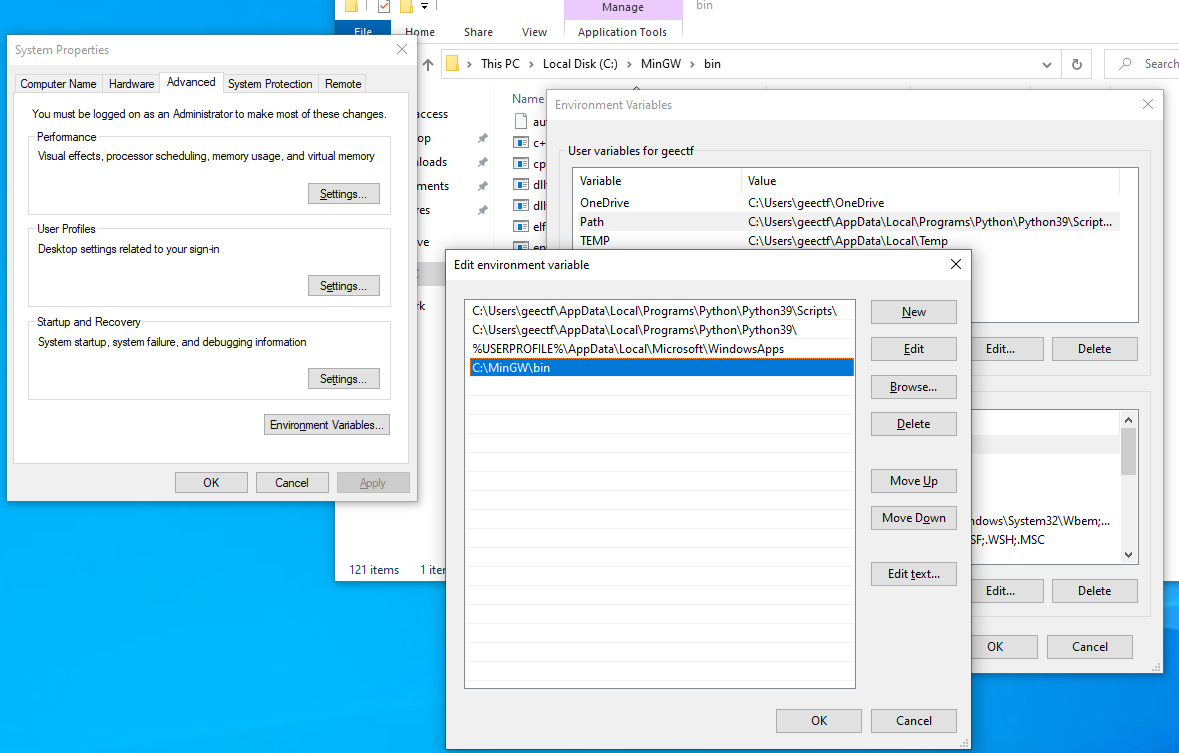
# DETAILED MINGW SETUP







1. Find the path of the MinGW directory
2. Go to the environment variable settings
3. Double click Path
4. Double click empty slot
5. Add path for MINGW bin directory



**1**

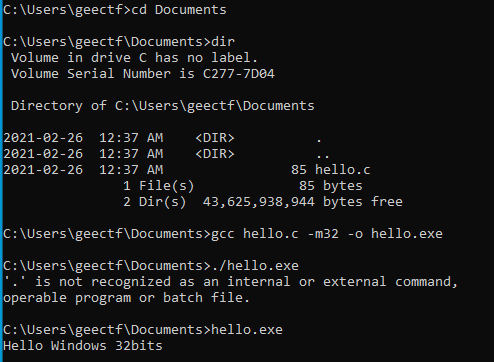
**2**

**3**

**4**

Create a C file with your favorite editor.

See sample execution below:



# Configure your Path Environment Variable

1. Set the environment variable by adding a few more entries.
   1. C:\Python27\
   2. C:\Python27\Scripts
   3. C:\MinGW\bin
2. Note that you may not have to do this for Python if you choose to include the path during the installation of the interpreter.

# Get Book Code

1. Download the code from the book by following the link: **https://nostarch.com/download/ghpython\_src.zip**
2. Check the following link for errata and updates: **https://nostarch.com/ghpython.htm#updates**

# Get PyCharm

1. Install PyCharm if you would like to have an IDE to assist with ease of programming.
2. Go to the following site: https://www.jetbrains.com/pycharm/download/other.html
3. Choose a version that will work on x86 such as 2018.2.8 for Windows (exe): **https://www.jetbrains.com/pycharm/download/other.html**

# Alternate VM setup

**The following is not necessary** but I think that it will provide you with some interesting tools to work with in the windows environment.

There are some tools that you can install on windows to provide with an excellent environment to perform some analysis (Forensic and Malware). Here are a couple of **IMPORTANT** notes:

1. You will need about **90-100** GB for this VM
2. It will take about 2+hrs to complete the installation process.
3. You will need to disable manually the Windows Defender Antivirus Tools (if you don’t it will uninstall some features).
4. You will need to update your VM prior to starting (Note that updating the VM will cause some features that make malware analysis difficult). Therefore, you will need to exclude some folders from inspection when the Defender Tools run.
5. Make sure to snapshot your VM often.

To learn about and setup your VM to use **FlareVM**:

1. Go to the following URL and read a bit about it:

https://www.fireeye.com/blog/threat-research/2018/11/flare-vm-update.html

1. Then you can go to the following URL and read about how to install it: <https://github.com/fireeye/flare-vm>