# Setup

This course will focus on 64 bit Windows, but we will talk about 32 bit and Linux as well. Note: x32 and x86 are the same.

## Operating System

You will need a 64 bit Windows OS. You can use a virtual machine (VM) if you want, but there is no need to. It's typically best to use a VM for security reasons, but we won't need to worry about that in this course. If you plan on making reverse engineering part of your life then you will probably want to set up a reversing VM. Having a VM will allow you to better isolate the software you are reversing. This can be extremely helpful if you are analyzing the network traffic. Also, if you mess anything up you can revert the VM. Again, you don't need one for this course but in the future, I would recommend you get one.

## Reversing Tools:

Most of the software can be replaced with anything you like. The software I will be using is listed (all of it's free):

**Required:**

- **Ghidra** (Needs Java JRE and JDK).
- **x64dbg** (Comes with x32dbg as well). I will also use the xAnalyzer plugin, you don't need this but I would recommend it.
- **dnSpy** (preferred) or ILSpy (Used for .NET reversing towards the end).
- **Visual Studio** with "Desktop development with C++" installed. I would also recommend installing ".NET desktop development."

**Optional:**

The software listed here won't be used in the course, but you might want it in the future.

- **HxD** (Hex editor)
- **Sysinternals Suite** (Various tools to analyze Windows).
- **Dependency Walker** (Can be used as a GUI alternative of "DUMPBIN" which comes with Visual Studio).

**You can choose when to install this software. You will start using it in 0x300.**

As you can see there is no IDA Pro! With the release of Ghidra, there isn't really a reason to use IDA Freeware or Pro. Although IDA Pro is better (in my opinion), it's not free like Ghidra is. In fact, it's quite expensive. If you prefer IDA you can use it. I'm cheap so I won't be using it.

Some other good software you may want to take a look at some time is Hopper, Radare, and Binary Ninja. Of those, only Radare is free. Hopper has a free version but you can only use it for a certain amount of time.

## Target Software:

All files we will be reversing are in FilesNeeded. I'm unable to distribute all software due to legal reasons. Any programs that I didn't provide directly are listed in FilesNeeded/@ExternalResources.txt.

**Warning: The files may change over time. I will try to update the course as needed.**