[Section 0 Install a Linux Desktop on Your PC 2](#_Toc5350070)

[Section 1 Write and Run a Short Program: *first* 2](#_Toc5350071)

[Section 2 Concepts explanation: Terminal, Assembler, Linker and Emulator 3](#_Toc5350072)

[Section 3 Programs explanation: apt, as, ld and qemu 4](#_Toc5350073)

[Section 4 8086 Assembly Language 6](#_Toc5350074)

[Appendix A Installing Ubuntu Desktop 7](#_Toc5350075)

[References 7](#_Toc5350076)

[Resources 7](#_Toc5350077)

## Section 0 Install a Linux Desktop on Your PC

A Linux operating system is to be used as the platform for the experiments in this book. Please move to the next section if you currently have any distribution of Linux installed on your personal computer, it can be running on a virtual machine or alongside with Windows or macOS.

For these who do not currently have a Linux system in hand, or these who are even new to Linux system, Ubuntu desktop is recommended. Ubuntu is a free and open-source Linux distribution. It can be installed either on a virtual machine which is running on your current operating system or alongside with your current operating system. Please refer to appendix A for more information if you encounter some difficulties in installing Ubuntu desktop. It might take several hours if it’s your first time to install a system. Be patient and keep searching the answer whenever something confuses you.

## Section 1 Write and Run a Short Program: *first*

The best way to learn is by doing. Please note I am using Ubuntu 18.04.2 LTS, the commands or operations can be different from these given in this book if you are using any other distribution of Linux. In this case, I suppose you know how to probably change the commands or operations as you are an experienced Linux user. Log into Ubuntu desktop and do the following steps:

1. Write the first program. Find the **Documents** folder and click into it. Create a text file and name it with **first.s**. Open it, copy and paste the following lines into it then save and close.

.code16

.global \_start

\_start:

mov $26, %cx

mov $0x0903, %dx

mov $0x000c, %bx

mov $msg, %bp

mov $0x1301, %ax

int $0x10

loop: jmp loop

msg: .ascii "My first computer program!"

.org 510

.word 0xAA55

Congratulations! We have finished the hardest part of the whole chapter. Do not worry at the moment if you have no idea on what you have pasted, all these will be explained in the following sections. Please move to the next chapter if you understand fully what the code does.

1. Open a terminal. Right click on the blank area inside of **Documents** folder and then click **Open Terminal** in the context menu.
2. Install **binutils** tool. Key in **sudo apt install binutils** and press Enter button. Input your password when asked.
3. Assemble the program: **first.s**. Inside of the terminal, input the following command and press Enter button:

**as -o first.o first.s**

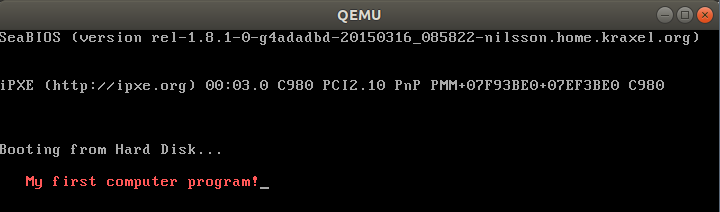
1. Generate the **first.img**. Input or copy the following command and press Enter key :

**ld -Ttext=0x7c00 -o first.img --oformat=binary first.o**

1. Install **Qemu** emulator. Key in **sudo apt install qemu**. Input **Y** and press Entre key when asked “Do you want to continue? [Y/n]”.
2. Run your program. Input or copy the following command and press Entre key:

**sudo qemu-system-x86\_64 -cpu max -drive format=raw,file=first.img**

1. We will see the following window if everything has gone well so far. The light red words My first computer program! on the screen is what the program does.



1. We have finished first program and had it run. Again please move to the next chapter if you understand what we have done by now. Otherwise see the next sections for the explanations.

## Section 2 Concepts explanation: Terminal, Assembler, Linker and Emulator

We go though some basic concepts before we explain what exactly we have done in the last section.

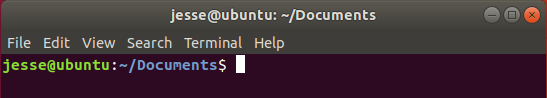
* Familiar yourself with **Ubuntu desktop environment**. New to Linux? Give yourself a quarter to click each icon or button you can find in Ubuntu desktop to see what they are. Refer to the guide below or just search any topic you are interested in if necessary.

Ubuntu desktop guide: <https://help.ubuntu.com/stable/ubuntu-help/>

* **Terminal, command-line** and **shell**. On Linux desktop, the Terminal is a program where command is used to interact with computer. Most people are familiar with GUI or graphical user interface. Instead of using mouse heavily to interact with all kinds of windows, we will use command-line interface or CLI to talk to computer. In case you are new to CLI, you may want to quickly go through chapter 2~4 of this book ***The Linux Command Line*** (<http://linuxcommand.org/tlcl.php>) written by Willian Shotts. Or search something like the most used 10 Linux commands and play with these commands for an hour.
* **Binutils**, **as** and **ld**. GNU Binutils are a collection of binary tools. The main ones are **as** and **ld**. The GNU Assembler, commonly known as **gas** or simply **as**. Assembler is a computer program which assembles assembly language to machine language. Assembly language is a more readable interpretation of a processor’s machine code, allowing easier understanding and programming by human [2]. Machine code is a computer program written in machine language [instructions](https://en.wikipedia.org/wiki/Instruction_set) that can be executed directly by a [computer](https://en.wikipedia.org/wiki/Computer)'s [central processing unit](https://en.wikipedia.org/wiki/Central_processing_unit) or CPU. Each instruction causes the CPU to perform a very specific task [3]. CPUs can only understand machine code. Machine code is some combination of statuses which only use two symbols: typically, “0” and “1”. The **ld** is another program, called linker, that takes one or more object files generated by the assembler and combines them into a single executable file, library file, or another object file [4].
* **Qemu emulator**. QEMU is a generic and open source machine emulator and virtualizer.

## Section 3 Programs explanation: apt, as, ld and qemu

* In step 1 of section 1, we composed a text file using assembly language. It’s OK for now if we do not really understand what the code means. We will examine these assembly code in the next sections. All we need to understand now is we wrote some assembly code and saved it as **first.s**, we call this file **source file** as it contains the source code. The suffix **s** stands for source file.
* In step 2, we opened a terminal window. The window will look like the below picture where **jesse** and **ubuntu** are the user name and computer name. **~** indicate the current user’s home folder which is **/home/yourUserName**. **Documents** is a folder under your home folder. We are now under **Document** folder because we right clicked in the blank area of this folder in the GUI. Believe you already tried to navigate to different folders following some books or web pages which tell the basic Linux commands usage. The place where the cursor flashes is where we key in the commands to interact with computer, just after the **$** sign.



* Advanced package tool or apt is a program that handles the installation and removal of software Ubuntu and related Linux distributions. **sudo** is short for superuser do, which is a program allows us to run programs with the security privileges of another user, by default the superuser. We use **sudo apt install binutils** when installing the tool collection **binutils**. Program **as** and **ld** which are part of the **binutils** will be used to translate the source file **first.s** to a runnable or executable file.
* Let’s see the command in step 4 **as -o first.o first.s.** **as** is the program name of GNU assembler. Except for ‘--’ any command-line argument that begins with a hyphen (‘-’) is an option. The **-o** in **as -o first.o first.s** means we want to give the output file which is generated by the assembler the name **first.o**. Number of options can be zero or many. Anything that is not an option will be treated as a source file, like the **first.s** here. After the execution of this command, we get an object file **first.o** which is the input file the **ld**.
* In Step 5, the **option -Ttext=0x7c00** tells the linker to locate the text section in the output file at the absolute address **0x7c00**. 0x7c00 is a magic number, this is where the computer loads the data from the external storage like hard disk or USB flash drive into main memory. I understand this explanation might still confuse you. We will explain this in the following sections. Similarly, **-o** **first.img** tells the linker to generate the output file with the name **first.img**. Option **–oformat=binary** specifies the binary format for the output object file. Finally after the execution of this command we get the runnable file **first.img**.
* With this runnable file **first.img**, we would like to find a way to run it now. For now we can image that the Qemu emulator, which has been installed in step 6, is our brand new machine which has exactly the function as the PC you buy from the shopping centre! But it’s not a real machine, it is only an emulator running on your Linux. We imagine it equips with one of the latest Intel or AMD CPUs (Intel and AMD are the companies who produce CPUs, probably not only CPUs). The difference is the PC you buy from the shop comes with an operating system, usually Windows. While this machine does not come with any operating system. We will load the **first.img** file into the Qemu machine. We image the **first.img** file is equivalent to the files which are located on the hard disk of your real PC. I see this analogy might be not accurate enough from a computer scientist’ view, but I wish this is good enough for us to understand the relationship between the **first.img** file and the Qemu emulator for now.
* For the command in Step 7, **sudo qemu-system-x86\_64 -cpu max -drive format=raw,file=first.img, qemu-sysem-x86\_64** is our brand new computer but without the operating system installed. Option **-cpu max** is used to enables all features supported by the accelerator in the current host machine. Option **-drive format=raw,file=first.img** is used to tell Linux to write the **first.img** into the disk of our brand new computer Qemu and then press the Power button. Specifying **format=raw** avoids Qemu detecting the format and believe it’s a trusted fromat. **file=first.img** obviously tells Qemu which file to be loaded into the hard disk. You may have noticed the new term **x86\_64**, also known as **x64**, **x86-64**, **AMD64** and **Intel 64**, is the 64-bit version of the x86 instruction set architecture. We have mentioned the smallest unit the CPU can execute is called instruction. The set of all the instructions the CPU can understand is some kind of abstract model of a computer. Almost all the PC and all kinds of Mac available in the shop in nowadays (in 2019) are using **x86\_64** CPUs. Refer to the below link if you are interested in more information on **x86\_64** and its family: <https://en.wikipedia.org/wiki/X86>

By now we have explained everything regarding the program and the commands we used so far but the most important part: what does the code in the text file mean. That’s the task for the following secitons.

## Section 4 Explanation of program first.s

In this section we will overally explain the program wrote in setion 1.

What is real mode and the legacy bios boot process.

Register and CPU, memory mode.

Heximal, binary, decimal

Line 1 .code16 is a directive which instructs the assemler, GNU as or GAS the one we use here, to generate runnable file in 16-bit mode. As defautly GAS generates 32-bit or 64-bit depending on the configuration. The reason why we need 16-bit runnable file is at the time this of the program runs the CPU is in 16-bit real mode. All directives have name that begin with a period (‘.’) in GAS. These directives are not translated into any machine code but only tells GAS how to orgainse or translate the code into machine code.

The second line code .global is a directive as well. The function of this directive is to make the symbol, which is \_start in this program, visiable to linker. Program first.s only has one source file, while for programs which have more than one scource file, the .global directive whille make symbol is also avaiable to other scource files. Back to the third line of the program, \_start is the default entry point. GAS makes the runnable file starts from the first instruction which is just after the symbol \_start.

In line 4 mov $26, %cx, where mov is its opcode, $26 and %cx are its two operands. A opcode or operation code can have zero to two operands. 26 with a prefix $ indicates an immediate number 26 in decimal. A register name cx with prefix % indicates the content inside of the register. This instruction tells CPU to move the immediate decimal number 26 into the register cx, which is a 16 bits register.

## Coming secitons

Explain first.s

Print Ascii code on screen

print a diagram on screen

Load FreeDOS or other 16-bit OS in?

Point: ASCII Code, Legacy BIOS, UEFI BIOS

## Appendix A Installing Ubuntu Desktop

You may want to install the Ubuntu on a virtual machine which is running on your current operating system, Windows or macOS. Go and search in your browser on how to install a virtual machine on your current operating system. For these who want to know what is a virtual machine or which virtual machine can be used, you may want to quickly review this page <https://en.wikipedia.org/wiki/Virtual_machine>.

For these who prefer to install the Ubuntu alongside with your current operating system or who have already installed a virtual machine, please move to Ubuntu official website to download the Ubuntu desktop. During the process of downloading, you may need search on how to install Ubuntu desktop on your virtual machine or alongside with your current operating system.

## References

[1] William E. Shotts, Jr., *The Linux Command Line, Fifth Internet Edition*, 2019, <http://linuxcommand.org/tlcl.php>, (accessed 3 April 2019).

[2] <https://en.wikipedia.org/wiki/Assembler>

[3] [https://en.wikipedia.org/wiki/Machine\_code#Instruction\_set](https://en.wikipedia.org/wiki/Machine_code" \l "Instruction_set)

[4] <https://en.wikipedia.org/wiki/Linker_(computing)>

## Resources

* 1. <https://en.wikipedia.org/wiki/Virtual_machine>.
  2. <https://help.ubuntu.com/stable/ubuntu-help/>
  3. <https://en.wikipedia.org/wiki/X86>

as manual https://sourceware.org/binutils/docs-2.32/as/index.html#SEC\_Contents

ld manual https://sourceware.org/binutils/docs/ld/Options.html#Options

qemu manual

Introduction to x86 Assembly: <https://software.intel.com/sites/default/files/m/d/4/1/d/8/Introduction_to_x64_Assembly.pdf>

x86 assembly referenct: <https://www.felixcloutier.com/x86/>

online x86 & x64 assembler and disassembler: <https://defuse.ca/online-x86-assembler.htm>

x86 assembly wikibook: <https://en.wikibooks.org/wiki/X86_Assembly>

x86 assembly with Ubuntu: <http://www.egr.unlv.edu/~ed/assembly64.pdf>

using as, The GNU Assembler: <https://web.eecs.umich.edu/~prabal/teaching/resources/eecs373/Assembler.pdf>

<http://www.phoenix.com/resources/specs-bbs101.pdf>

[https://firmware.intel.com/sites/default/files/resources/A\_Tour\_Beyond\_BIOS\_Memory\_Map\_in%20UEFI\_BIOS.pdf](https://firmware.intel.com/sites/default/files/resources/A_Tour_Beyond_BIOS_Memory_Map_in UEFI_BIOS.pdf)

<https://www.cs.cmu.edu/~410/doc/minimal_boot.pdf>