A Map to OS/CS/Paper

BY JWNHY

COMPASS Lab

2022/7/23

1. **Personal experience only.**
2. **Follow at your own risk.**
3. **Some personal BS included.**

Who am I?

Name: Hongyi Lu (@jwnhy)

Bio: 17' B.Sc @ SUSTech (Math)

22' Ph.D Student @ HKUST (CSE)

Email: luhy2017@mail.sustech.edu.cn

Interests: generally everything in CS/MA

Publications:

- `Raven: A Novel Kernel Debugging Tool on RISC-V [DAC' 22]`
- `A Novel Memory Management for RISC-V Enclaves [HASP' 21]`
- `BadUSB-C: Revisiting BadUSB with Type-C [WOOT' 21]`

Community work:

- Submitted a 'one-letter' patch to Linux kernel

This is?

- *Suggestions* on CS learning/research
- A *map* to OS study
- Some personal BS (私货)

This is not?

- Step-by-step tutorial
- GPA-boost magic
- Silver bullet for everyone

How to use Google?

When you want to learn a new tech?

- "<techname>+tutorial", e.g. rust tutorial, os tutorial

When you want to practice coding?

- "write a <something> from scratch", e.g. write an OS/database/... from scratch

When you want some books?

- "<techname>+book"->some useful book
- libgen/zlibary->pdf copy without copyright

What if something magically breaks?

- See next page.

Use Google to solve problem

General Guide

1. Any Info ? Google; goto 4 : goto 2
2. Google "<techname>+verbose/log/debug/more info"; goto 3
3. Do Experiments; goto 1
4. Exact Solution ? Copy & Paste; goto 5 : goto 4
5. Read Relevant Info; Google; goto 1
6. Problem Solved ? Celebrate : Assess Differences; goto 1

Remark. If the above procedure is repeated 5 to 6 times without luck, go to “<techname>+community” , post your effort and wait for others.

When a solution is not working?

Possible Issues

- Network: proxy, DNS/hosts, client/server firewall, router setting, ISP
- Compilation: missing libaries/tools, env variable, mismatched tool/source (gcc 12 v.s Linux 2.6)
- Installation: disk space, folder/file permission, hash check
- Execution: missing libaries, wrong architecture, executable permission

Last Resort

- If everything fails, grab a docker image and call it a day.
- Exercise:

```
Error response from daemon: Get https://registry-1.docker.io/v2/: dial
tcp 54.152.209.167:443: getsockopt: connection refused
```

Ask nicely

Do this.

- Read Smart Questions (提问的艺术) by Eric Steven Raymond.
- Try your best to search on Web/Manual/FAQ/Maillist/ . . .
- Post detailed info and your efforts when asking, and **be polite and patient**.

  (unless you have paid >$10,000 to them, then you can be angry and rude)
- "Something <ver.> breaks, I have checked A/B/C, and tried D/E/F. Here is what I've got. . . ,The log is as follows. . . , My guess is that. . . , Your help is much appreciated"

Don't do this

- "Something breaks, I dnk what to do, plz help"

Case Study: Learn `makefile`

How to learn `makefile` through Google

1. Search “makefile tutorial” on Google.
2. Check out those tutorials, you will probably meet the following issues.
   - `Makefile:5: *** missing separator. Stop.` -> Google

     -> tab/space -> “makefile tab space” …
3. Go through these tutorial, find one that fits your current knowledge level.
4. Spending next few hours typing command from the tutorial and keep Googling to solve problems.

Note. `hello` or `he1lo` this is a question. (special thanks to Jerry Lu)

Case Study: A Mythical Bug

Description:

1. You compiled an executable called `a` in `/home/<name>/a.out` with proper permission.
2. You tried to run it with `./a.out` it gives you this error.

   ```
   $ bash: ./a.out: No such file or directory
   ```

3. You double checked with `ls` to make sure it's there.

   ```
   -rwxrwxr-x 1 <name> <name> 16K Jul 24 10:43 a.out
   ```

Question:

1. What are the possible causes for this?
2. How to solve them?

Things You'll Need (System)

- Any Linux Distribution

  (Ubuntu/Debian/Fedora/Archlinux/Gentoo)

  Suggestion: Try them all; throw away Windows.
- Knowledge of "shell/gdb/vim/ . . . "

  Tutorial: `https://missing.csail.mit.edu/`
- Courage to step out of Comfort Zone (Clion/Eclipse/PyCharm . . .)

  Using vim+gdb+QEMU to code/debug can be hard at first

  but it can be made easy with proper configurations
- **Patience** and endless Google

Learning Linux

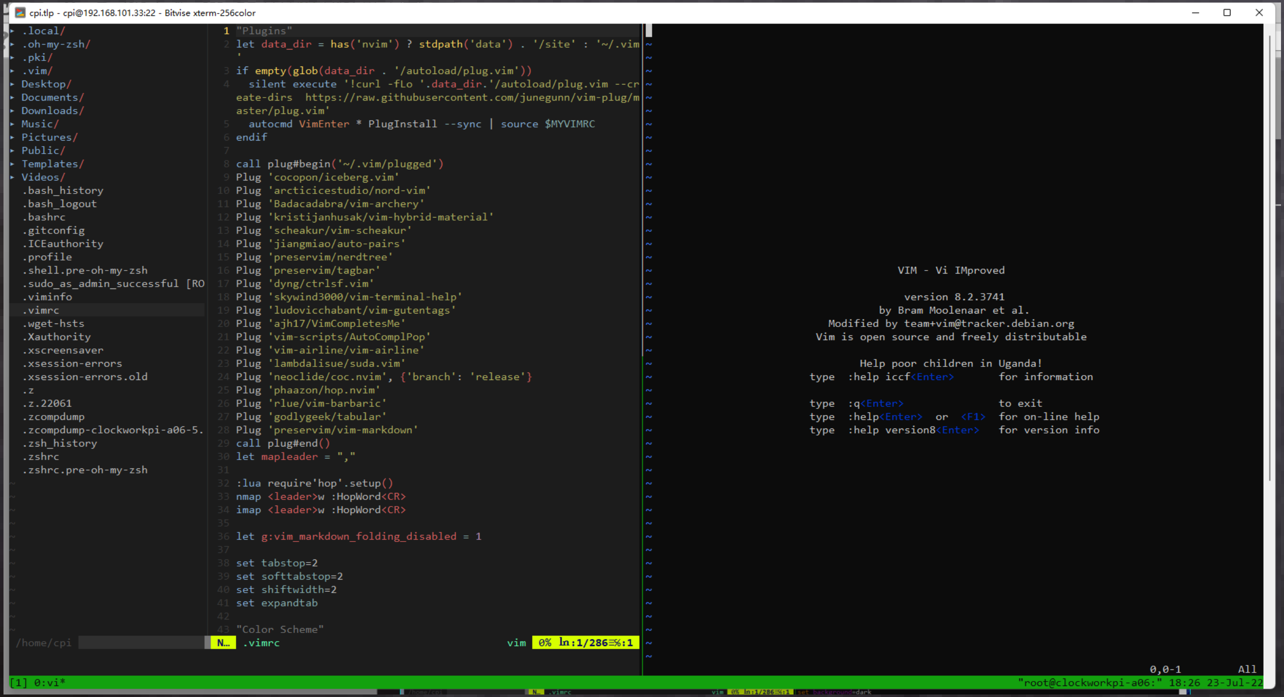
Three Levels of Knowledge through Installation

- Ubuntu: GUI, package management, disk partition
- Archlinux: CLI, bootloader, timezone, network, fstab
- Gentoo: compilation, kernel hacking, drivers

Note. Get used to Ubuntu, go to Archlinux, then go to Gentoo.

Old ≠ Primitive

Both are **vim**



cpi.tlp - cpi@192.168.101.33:22 - Bitvise xterm-256color

```
▸ .local/
▸ .oh-my-zsh/
▸ .pki/
▸ .vim/
▸ Desktop/
▸ Documents/
▸ Downloads/
▸ Music/
▸ Pictures/
▸ Public/
▸ Templates/
▸ Videos/
  .bash_history
  .bash_logout
  .bashrc
  .gitconfig
  .ICEauthority
  .profile
  .shell.pre-oh-my-zsh
  .sudo_as_admin_successful [RO
  .viminfo
  .vimrc
  .wget-hsts
  .Xauthority
  .xscreensaver
  .xsession-errors
  .xsession-errors.old
  .z
  .z.22061
  .zcompdump
  .zcompdump-clockworkpi-a06-5.
  .zsh_history
  .zshrc
  .zshrc.pre-oh-my-zsh
```

```vim
"Plugins"
let data_dir = has('nvim') ? stdpath('data') . '/site' : '~/.vim'
if empty(glob(data_dir . '/autoload/plug.vim'))
  silent execute '!curl -fLo '.data_dir.'/autoload/plug.vim --create-dirs  https://raw.githubusercontent.com/junegunn/vim-plug/master/plug.vim'
  autocmd VimEnter * PlugInstall --sync | source $MYVIMRC
endif

call plug#begin('~/.vim/plugged')
Plug 'cocopon/iceberg.vim'
Plug 'arcticicestudio/nord-vim'
Plug 'Badacadabra/vim-archery'
Plug 'kristijanhusak/vim-hybrid-material'
Plug 'scheakur/vim-scheakur'
Plug 'jiangmiao/auto-pairs'
Plug 'preservim/nerdtree'
Plug 'preservim/tagbar'
Plug 'dyng/ctrlsf.vim'
Plug 'skywind3000/vim-terminal-help'
Plug 'ludovicchabant/vim-gutentags'
Plug 'ajh17/VimCompletesMe'
Plug 'vim-scripts/AutoComplPop'
Plug 'vim-airline/vim-airline'
Plug 'lambdalisue/suda.vim'
Plug 'neoclide/coc.nvim', {'branch': 'release'}
Plug 'phaazon/hop.nvim'
Plug 'rlue/vim-barbaric'
Plug 'godlygeek/tabular'
Plug 'preservim/vim-markdown'
call plug#end()
let mapleader = ","

:lua require'hop'.setup()
nmap <leader>w :HopWord<CR>
imap <leader>w :HopWord<CR>

let g:vim_markdown_folding_disabled = 1

set tabstop=2
set softtabstop=2
set shiftwidth=2
set expandtab

"Color Scheme"
```

```
/home/cpi                N... .vimrc                vim  0% ㏑:1/286≡%:1
```

```
                 VIM - Vi IMproved

                 version 8.2.3741
             by Bram Moolenaar et al.
       Modified by team+vim@tracker.debian.org
     Vim is open source and freely distributable

            Help poor children in Uganda!
   type  :help iccf<Enter>       for information

   type  :q<Enter>               to exit
   type  :help<Enter>  or  <F1>  for on-line help
   type  :help version8<Enter>   for version info
```

```
                                                      0,0-1          All
[1] 0:vi*                                 "root@clockworkpi-a06:" 18:26 23-Jul-22
```

Practice makes perfect

x86

- Writing an OS in Rust by Philipp Oppermann ✓
- PDOS 6.S081 by PDOS Lab

Arm

- Building an Operating System for the Raspberry Pi by Jake Sandler

RISC-V

- rCore Tutorial by THU ✓

Note. ✓ means I have finished this tutorial

How to use?

Tutorial Components

- Code + Documents

Usage

1. Read through code
2. Use Google + Documents to understand each **line**
3. Type again the same code (do not copy, but you can look at the original)
4. Try to run the code and fix any typos

Note. rCore/xv6 uses a so-called *increamental coding*

filling up the blank instead of reinventing the wheel (I don't think it's a good idea)

What’s more?

Yet Another Table of Contents

1. Suggested courses/books.
2. Where to find (research) inspiration?
3. How to generates new idea?
4. How to improve academic writing?
5. General BS.

Suggested Courses

CS315: Computer Security

- Taught by Prof. Zhang Fengwei
- Topics includes buffer overflow, format string, web, SQL injection, …

CS323: Compilers

- Taught by Prof. Liu Yepang
- Suitable for students who are curious in how to build compilers.

CLE063: Writing for Publication

- Taught by Dr. Adrian Rowland
- The structure and philosophy of scientific papers, plus style and grammar principles for scientific writing.

Suggested Book

NO BOOK HERE

I geniunely believe that BOOKS are only good for reference, but not for learning.

Please go to writing code, getting your hands dirty and dealing with bugs.

Where to find inspiration?

Personal Opinions Only

- Papers

  Everybody knows.

- YouTube/HackerNews/V2EX/Github/...

  There are quite a LOT weird (attack) ideas in the wild that are not fully exploited.

  Learn them, expand them, fully evaluate them, and write a paper about them.

- Twitter

  A mixed sources with academic and industry.

  Both academic papers and community weird stuff can be found.

Some Random Source

YouTube

- LiveOverflow: Hacking, CTF.
- PwnFunction: CTF.
- Computerphile: General CS.
- NDCC: Gerneral CS.

Conference & Journal

- BlackHat {USA, Asia, Euro}, CCC (Chaos Communication Congress)
- DEFCON, Phrack…

How to generate new idea?

- Ask your supervisor

  Most simple and efficient way, but sometimes you may not like their ideas

- Keep watch on new tools

  New tools + Old problem = Paper

- Keep watch on trending spot

  Old tools + New problem = Paper

- Borrow other's tool

  You may have $A \rightarrow B$ and $C \rightarrow D$, then you could probably read more papers and find other's $B \rightarrow C$ (**with proper reference**)

Academic Writing

How important?

If writing is rubbish, most reviewers just assume your work is the same.

Even if it is not the case and your paper is “Turing-award winning”.

How to improve it?

- Treat EAP CLE030 *seriously*; it is way more than a GPA-boost course.
- Be bold and interact more with your teachers (native speakers).
- Choose native speakers as your teacher whenever possible.
- Apart from EAP, there is another course called WfP CLE063 available.
- Seek help from CLEs on EHall.

General BS

- Keep toxic people away, even (especially) if they're your teammate or supervisor.
- Don't be crushed by other's achievement, deconstruct them and be confident.
- Don't care GPA too much unless you need 保研/联培.
- Don't be afriad to seek help from your supervisor/teacher/...
- Don't doubt yourself when something goes wrong, most likely it's just unlucky
- Focus on what's important

  for research, it's paper

  for job-hunter, it's intern experience.
- Make sure you **REALLY** want a Ph.D and your supervisor is **NICE** before pursuing one.

Thanks

Acknowledgement:

- Jerry Lu, Ziqin Wang, Zhao Li, Fengwei Zhang, Adrian Rowland, Yuki, Kaixin.