

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 libraries/tools, env variable, mismatched tool/source (gcc 12 v.s Linux 2.6)
- Installation: disk space, folder/file permission, hash check
- Execution: missing libraries, 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
```

Exercise: 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> 8.9K Jul 24 10:43 a.out
```

Question:

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

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 Git

How to learn Git through Google

1. Search “git tutorial” on Google.
2. Check out those tutorials, you will probably meet the following issues.
 - On Windows, git isn't installed by default ->  -> Search “git installation” (that's why I throw away Windows)
 - In Mainland China, Github is blocked -> “git connection closed” -> “git proxy”
-> “git proxy ssh” -> “git proxy https”...
3. Go through these tutorial, find one that fits your current knowledge level.
(Installation? Setup repo? Local commit? Remote origin? Merge?)
4. Spending next few hours typing command from the tutorial and keep Googling to solve problems.

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” ...
 - . `make: No rule to make target 'xxx'. Stop.` -> Google
-> dependency filename -> “makefile dependency”...
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.

Case Study: Learn LKM

How to learn LKM through Google

1. Search “linux kernel module tutorial” on Google.
2. Check out those tutorials, you will probably meet the following issues.
 - . Lack of tools -> “xxx is missing/not found” -> “xxx installation on Debian/Ubuntu”
 - . Ancient guide from Linux 2.4.x -> some magical error -> Check latest tutorials
 - . WTF are `make`, `kernel` and ...? -> Fill the gap before you proceed
3. Go through these tutorial, find one that fits your current knowledge level.
(if not sure, ask a senior friend/supervisor for their advice)
4. Spending next few hours typing command from the tutorial and keep Googling to solve problems.

Things You'll Need

- 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 \neq Primitive

Both are vim

```
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

1 "Plugins"
2 let data_dir = has('nvim') ? stdpath('data') : '~/vim'
3
4 if empty(glob(data_dir . '/autoload/plug.vim'))
5   silent execute '!curl -fLo "' . data_dir . '/autoload/plug.vim --cr
6   eate_dirs https://raw.githubusercontent.com/junegunn/vim-plug/m
7   aster/plug.vim"'
8   autocmd VimEnter * PlugInstall --sync | source $MYVIMRC
9 endif
10
11 call plug#begin('~/.vim/plugged')
12 Plug 'cocopon/iceberg.vim'
13 Plug 'arcticicestudio/nord-vim'
14 Plug 'Badacabara/vim-archery'
15 Plug 'kristijanhusak/vim-hybrid-material'
16 Plug 'scheakur/vim-scheakur'
17 Plug 'jiangmiao/auto-pairs'
18 Plug 'preservim/nerdtree'
19 Plug 'preservim/tagbar'
20 Plug 'dyng/ctrlsf.vim'
21 Plug 'skywind3000/vim-terminal-help'
22 Plug 'ludovichabant/vim-gutentags'
23 Plug 'ajhi17/vimCompletesMe'
24 Plug 'vim-scripts/AutoComplPop'
25 Plug 'vim-airline/vim-airline'
26 Plug 'lamdalisue/suda.vim'
27 Plug 'neoclide/coc.nvim', {'branch': 'release'}
28 Plug 'phaazon/hop.nvim'
29 Plug 'r1ue/vim-barbaric'
30 Plug 'godlygeek/tabular'
31 Plug 'preservim/vim-markdown'
32 call plug#end()
33 let mapleader = ","
34
35
36 :lua require'hop'.setup()
37 nmap <leader>w :HopWord<CR>
38 imap <leader>w :HopWord<CR>
39
40 let g:vim_markdown_folding_disabled = 1
41
42 set tabstop=2
43 set softtabstop=2
44 set shiftwidth=2
45 set expandtab
46
47 "Color Scheme"
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

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 genuinely 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.

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 afraid 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