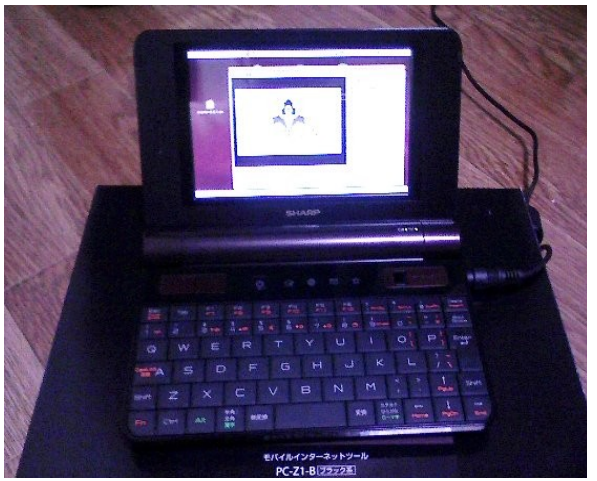
Hacking with ARM devices (Netwalker and also) on Linux

1、Self introduction
2、Introduction with ARM devices
3、Customized of Linux Mobile & Board PC ARM devices
- ・x86 Emulation
- ・Bootloader & External Card Boot
- ・Crouton & ChrUbuntu (Chromebook)
- ・Customized of Android devices(Nexus7)

4、Customized「End of Life」ARM Devices
- ・Chroot
- ・PKGSRC
- ・Mainline Linux Kernel Compile
- ・NetBSD

5、Japan (only) favorite OSS project

About Netwalker



This Presentation:
Slideshare & PDF files
publication of my HP

HKOSC 2015/6/26 17:15~
Place：Charles K Kao Auditorium,
Hong Kong Science Park, Shatin

Speaker：
Kenji Shimono

Self Introduction

- My name: Kenji Shimono
- Pseudonym(Pen name)：Kapper
- Twitter account：@kapper1224
- HP：http://kapper1224.sakura.ne.jp
- Slideshare: Kenji Shimono
- My Hobby：Linux、*BSD、and Mobile ARM Devices
- My favorite words：Record than experiment important
- Test Model：Netwalker(PC-Z1,T1)、Nokia N900、DynabookAZ、RaspberryPi
  Nexus7(2012、2013)、Hercules eCAFE EX HD、Jetson TK-1、
  OpenPandora、ARM Chromebook、ZTE OPEN C（FirefoxOS）
  Taiwan Android Electronic Dictionary 無敵CD-920、CD-928

- Recent Activity：
  Netwalker on the Linux from Scratch.

  Hacking of Android Nexus7.

  I have recently often use the ARM Chromebook.

My Activity of ARM Devices

- Linux Zaurus～RaspberryPi and Chromebook

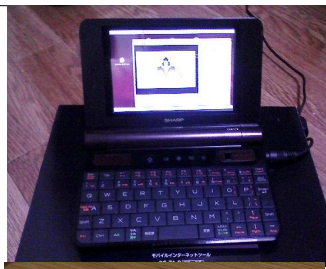
2002 2009 2010 2012 2014

Linux
Zaurus(Xscale)

Armel(EABI)
Debian 6
Ubuntu 9.04

Armhf
Ubuntu
12.04

Netwalker
CortexA8

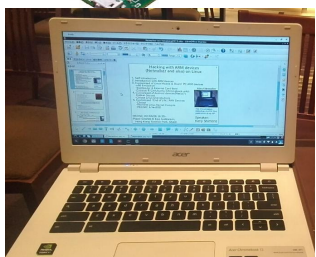


Dynabook
AZ(AC100)
Tegra2

Nexus7
Tegra3

Raspberry
Pi ARM11

ARM
Chromebook
Exynos5250,
Tegra K-1



OpenSourceConference in Japan
Once it is held in one month

KOF 2015 Nov6~7

My point of view about ARM Linux

1,Custmized ARM Linux OS,Applications

⇒ARM Linux had limited software and CPU ago.

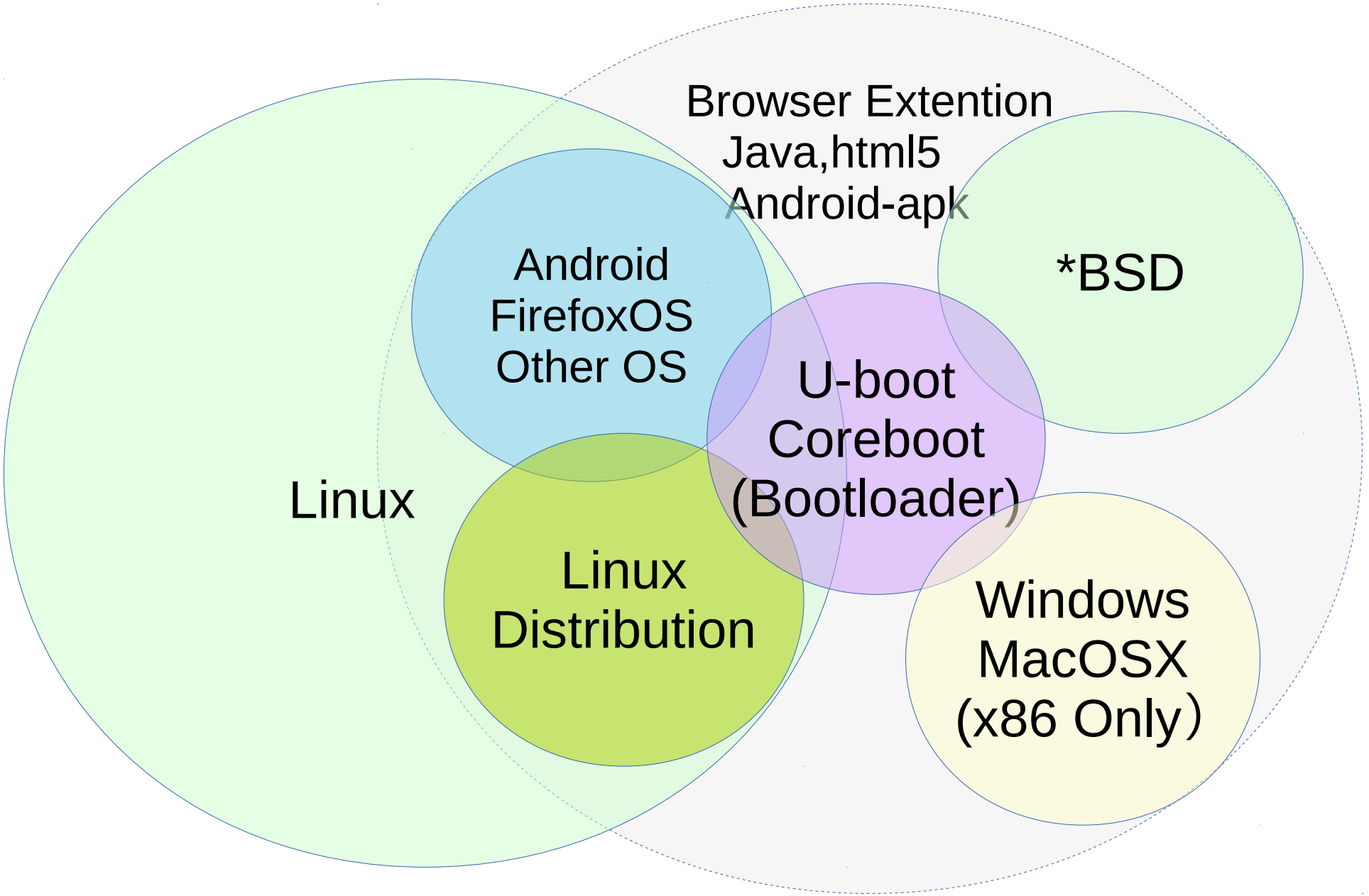
2,Customized ARM Android and Chromebook devices

⇒Many ARM devices used on Android in 2010.
SmartPhone, Tablet.
I want to use Linux Distributions on Android.

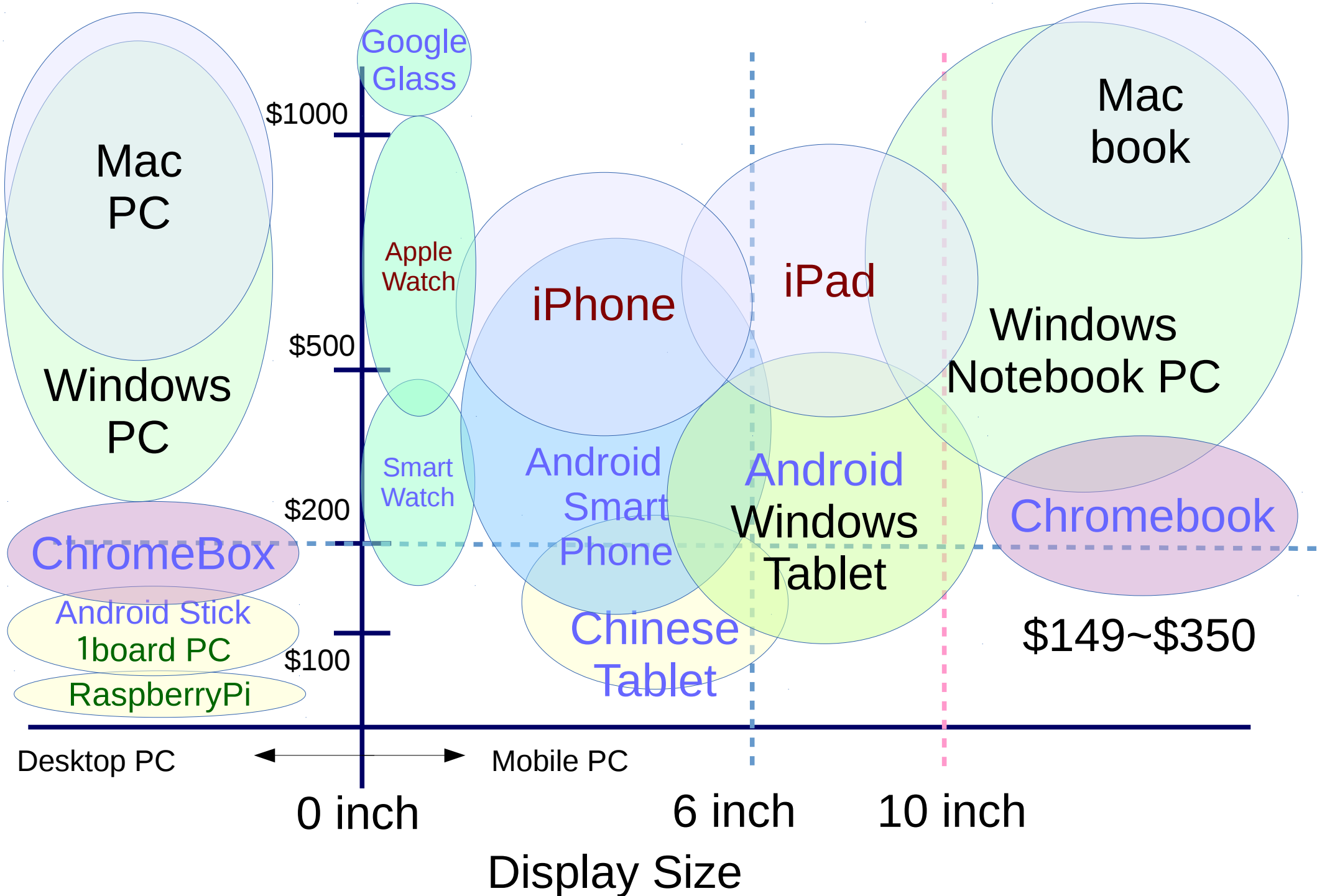
3,Customized「End of Life」ARM devices

⇒Not supporsed ARM devices are increasing.
But ARM devices「End of Life」is too shorts.
About mainly Linux Kernel and Distributions.

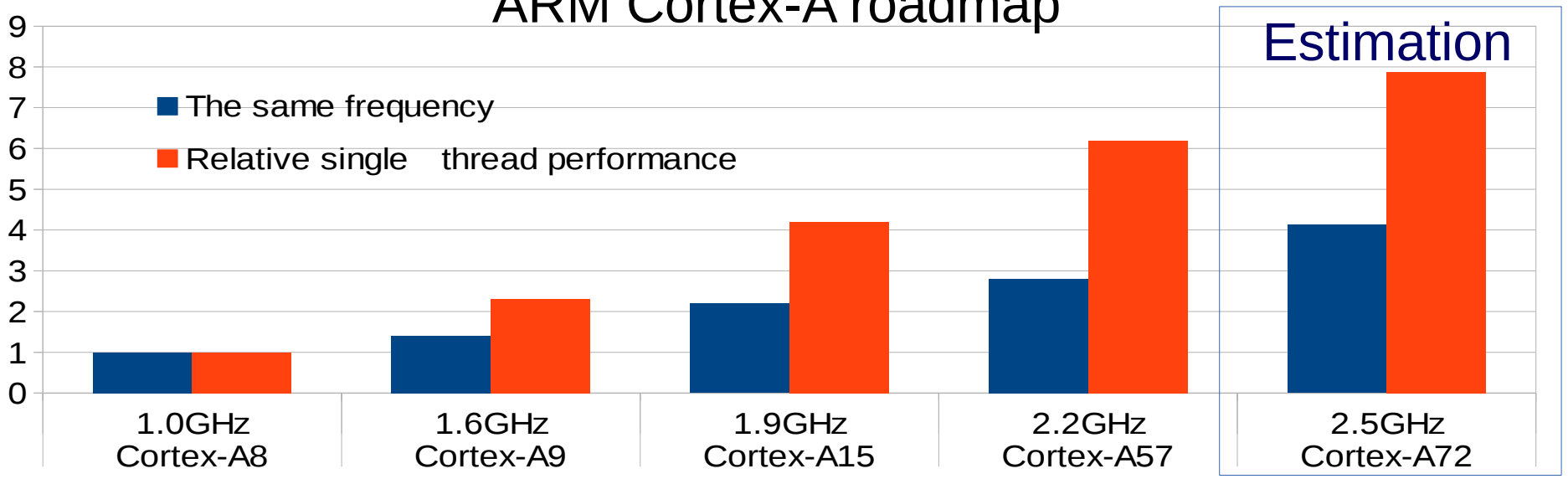
About ARM devices on Linux



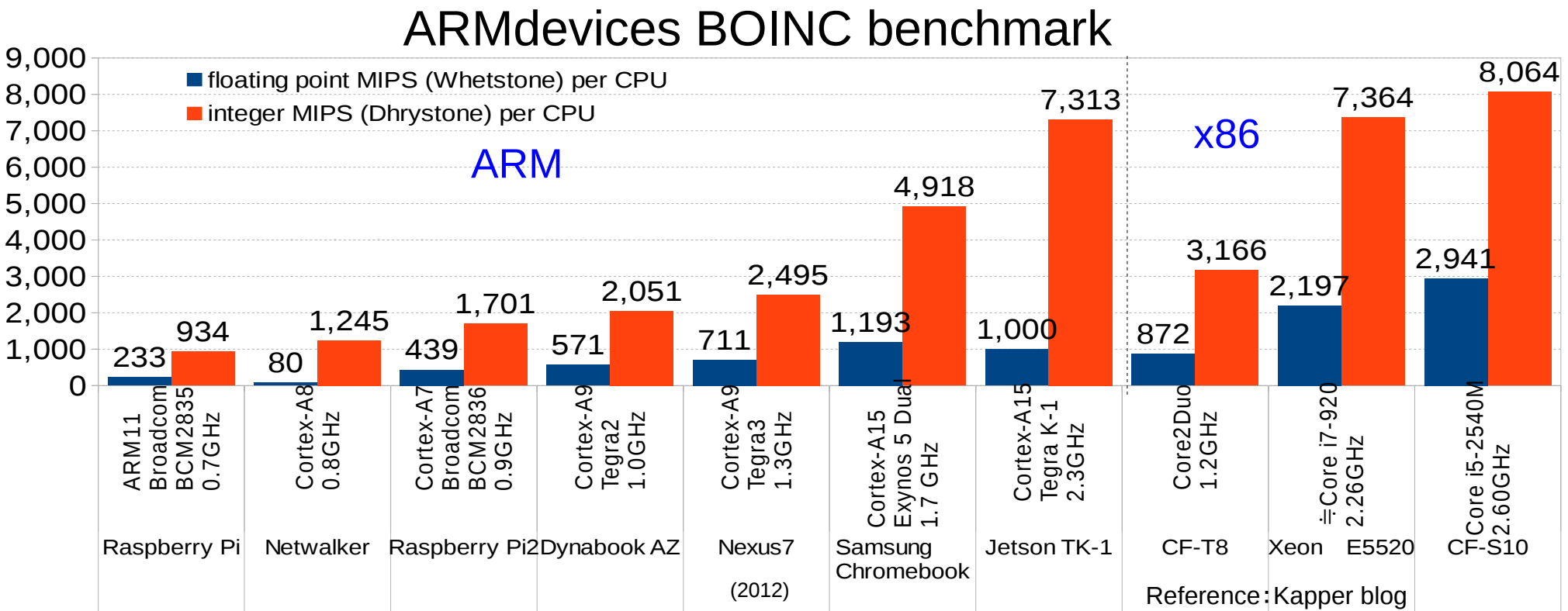
ARM devices on PC Market



ARM devices Benchmark score



Reference：A Walk Through the Cortex-A Mobile Roadmap
http://community.arm.com/groups/processors/blog/2013/11/19/a-walk-through-the-cortex-a-mobile-roadmap



ARM devices Linux & *BSD distro

Recently ARM Based on Linux & *BSD Distrobutions

Distribution	Ubuntu	Debian	Fedora	Open Suse	Gentoo	Arch	Open Cocon	Android	Free BSD	Net BSD
version	9.04～	2.2～	20～	12.2～			v8～	1.5～		1.6～
LinuxZaurus	△	◎	?		△			△		◎
Nokia N900	◎	◎	○	?	○	△		○	?	◎
Netwalker	◎	○	△		△			△		◎
DynabookAZ	◎	○	○	◎	◎	◎		◎		
Nexus7 (excpt chroot)	◎	?				○		◎		
RaspberryPi		◎	◎	◎	◎	◎	◎	◎	◎	◎
MK802 USBAndroid	◎	○	○	○	△	○		◎	△	?
Samsung Chromebook	◎	◎	◎	◎	◎	◎		△	◎	△
comment	Refer ence model	A lot of Device	RasPi Support	RasPi Support	A lot of Device	RasPi Supp ort	Thin client	Smart Phone Tablet	board PC main	Over40 Device support

Kapper's survey results on the Internet（If I will be modified once this is wrong）
◎：Official Support、○：Official Install report、△：User install report only

Impressions of NokiaN900、Dynabook AZ、RaspberryPi Famous ARM Linux devices

・Nokia N900
First generation of Linux Smart phone in 2009.
It is based on Maemo(Debian based Distribution), it was hacked all over the world.
ARM Flashplayer,PCSXreArmed, Video encoder,skype,Opera, Overclocked kernel,and Qemu+ Wine.
Main ARM machine until Raspberry Pi exits.Kubuntu had supported.

・Dynabook AZ(AC100）
Dynabook AZ is a Tegra2 Android notebook in Sep 2010.
It is possible to rewrite the boot loader in Nvflash, and to start the Ubuntu using U-boot,It became a development model of ARMhf Ubuntu. Ported Fedora,OpenSuse,Gentoo,Arch , and Android original build.
This CPU is 2 times / 1processor the specs RaspberryPi and Netwalker.

・RaspberryPi
The Raspberry Pi is credit card-sized single-board ARM11 computers that is most developed in the world.
The spec is the same as the N900 and Netwalker,it can be the same hacking.
Ideal for people who want to develop in the ARM debices since the information source is abundant.

Customized ARM Linux Distro

It is difficult and you can do with ARM Linux

Blue：A result of my tested
Purple: I want to try

- Basic

  Internet、OpenOffice : Work without Problems
  ARM Server :Work without Problems
  Youtube and Stream Movie: Work without Problems
  Games and Emulator : You can use Linux software.
  WindowsXP under spec : You can use if customize even on older models.
  Remote Desktop and Thinclient : Work without Problems

- Intermediate

  Windows app⇒qemu+Wine, but for advanced users only.
  ⇒ExaGear-Desktop is easy install x86 Ubuntu 12.04LTS emulation and wine.
  Change the default operating system⇒about Android,Ubuntu, and NetBSD
  Degital TV⇒One segment TV driver build on ARM
  FlashPlayer⇒ Installing Flash Player Plugin on ARM version
  The operation of the latest version of the app ⇒How to build from the source code
  Graphics Accelerated video codec Driver⇒It is difficult if there is no official support
  Port the game and x86 emulation⇒ use converter and build from the source code
  DRM and film⇒ use Flash Player Plugin on GooglePlay or Amazon Instant video streaming.

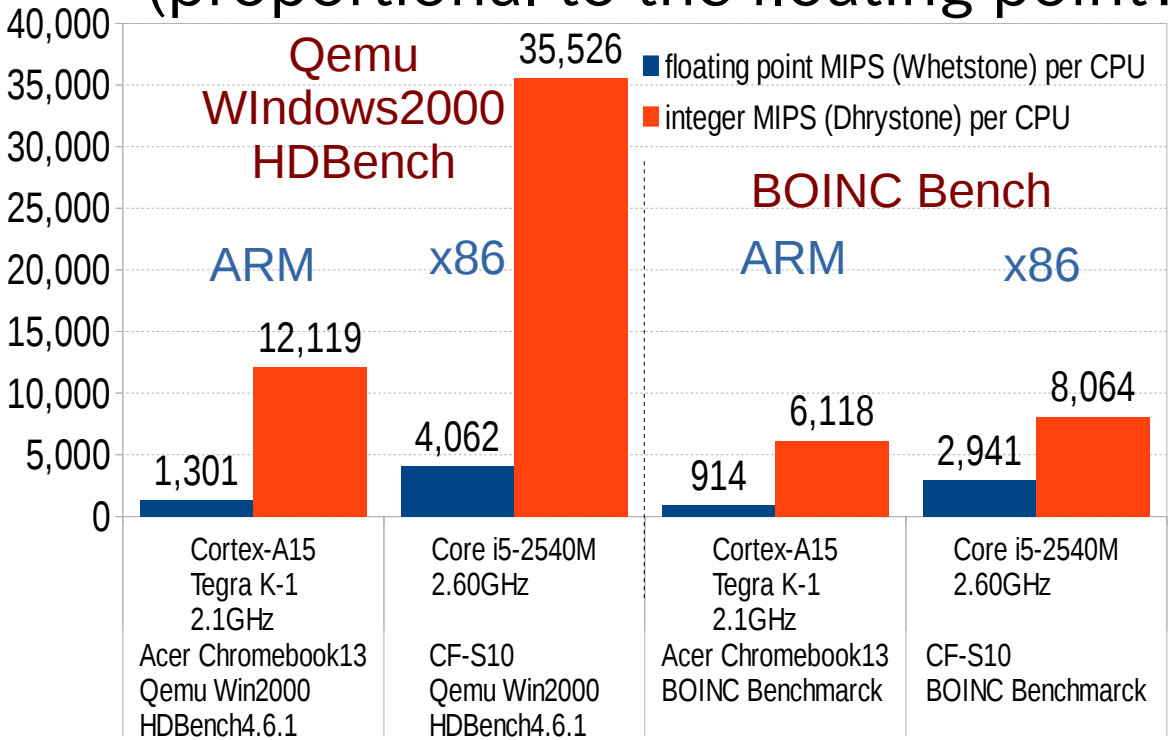
- Advanced (Easy if Android)

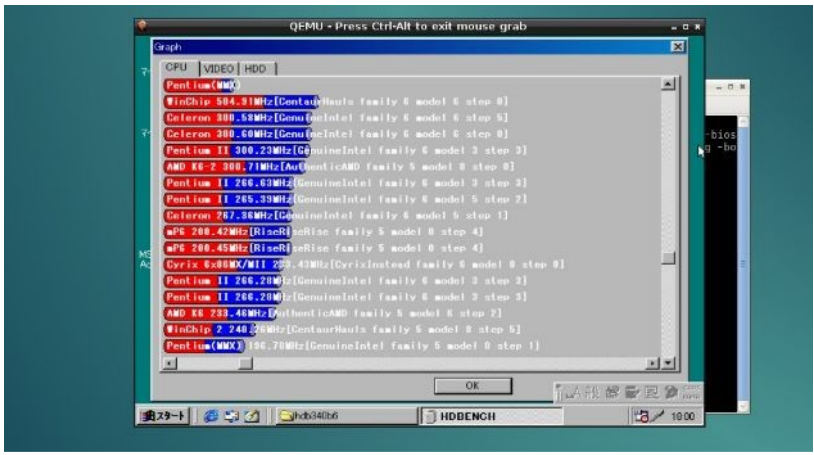
  Skype is not use ARM Ubuntu ⇒ExaGear-Desktop can use Skype for Linux(x86)
  ⇒Android apk Skype and Skype for Web
  Line is only Android⇒Pidgin can use Line protocol

x86 Emulation on ARM Linux Devices

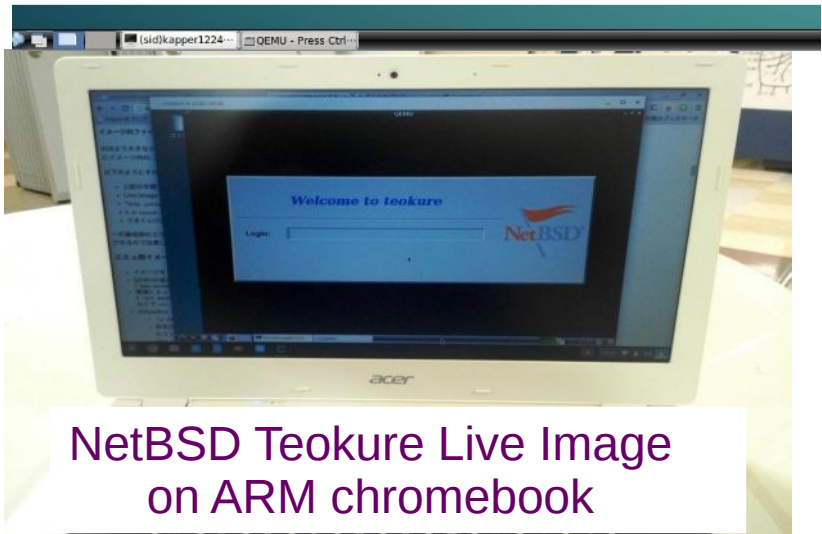
x86 Qemu Emulation on ARM devices

- You can use the x86 emulator will be like can be moved and Wine Windows apps and Steam and Skype.
- The x86 emulator also works such as Windows and NetBSD. TegraK-1 in Using Qemu Pentium2 266MHz equivalent Win98 is in HDBench, it was to use and Pentium4 1.8GHz equivalent to ExaGear-Desktop.
- In ARM Devices,Qemu is x86:ARM=3:1 (proportional to the floating point?)





Windows98、2000 on ARM chromebook

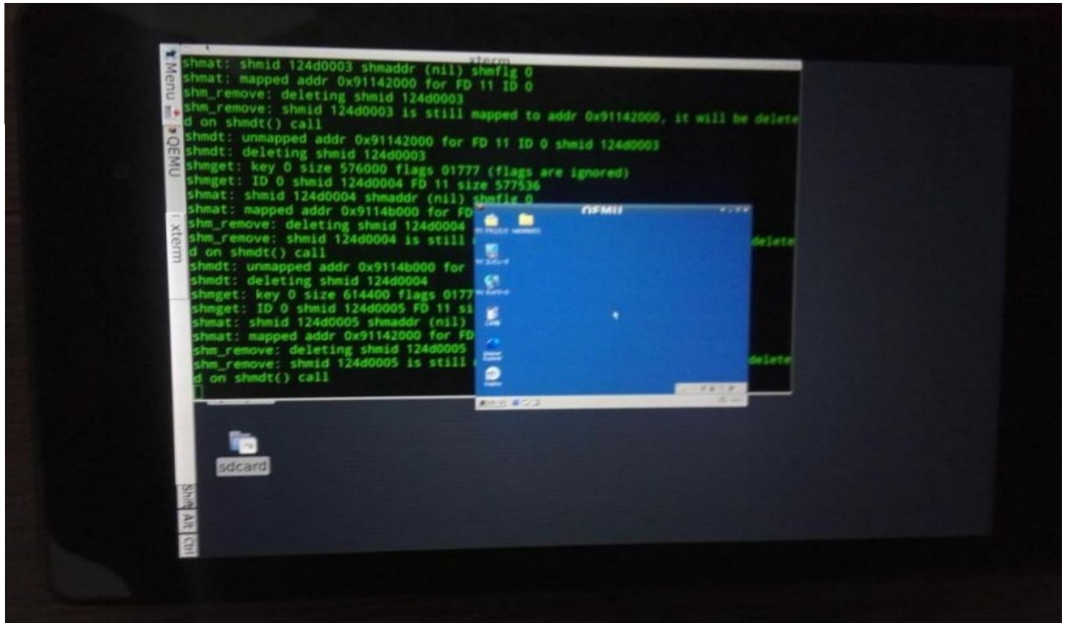


NetBSD Teokure Live Image on ARM chromebook

x86 Emulation on Android

- You can operate the Windows or NetBSD by the use of Android even x86 emulation
- PC: Bochs,Qemu,DOSBox,Limbo PC emulation MAC:vMacMini
- In the case of Qemu、Windows and NetBSD, and the others operation.

Windows9x、2000(Qemu) on Nexus7

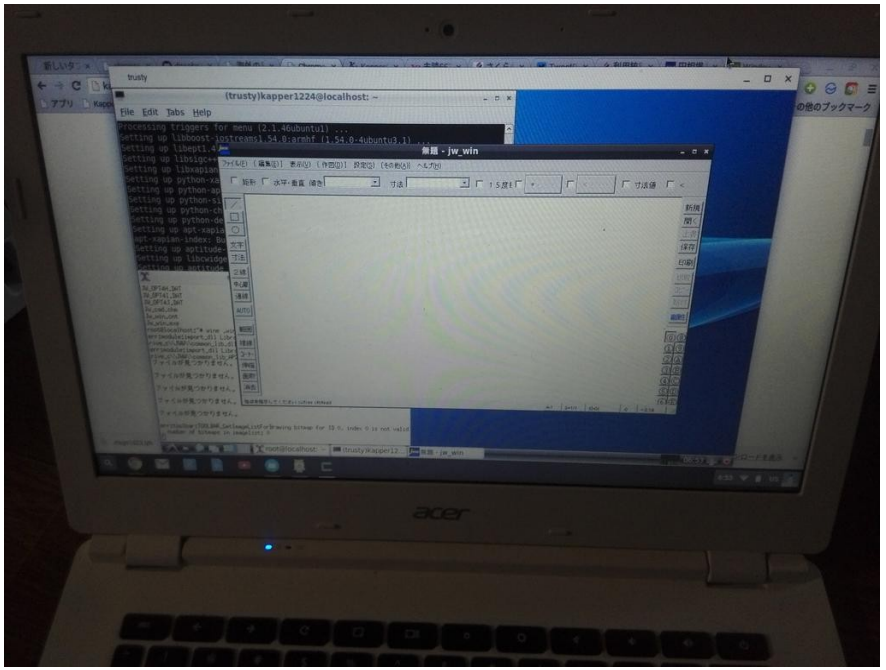


NetBSD Teokure Live Image(Qemu) on Nexus7

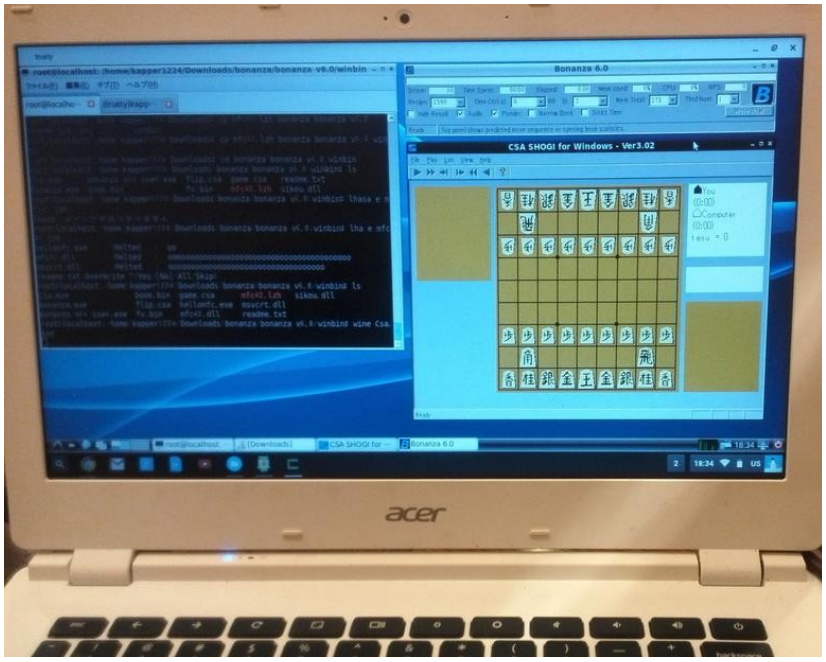
x86 Emulation on ExaGear-Desktop 1 board PC, and ARM Chromebook

- ExaGear-Desktop is 4.5 times faster than qemu.
- i686 Ubuntu12.04LTS on ARMhf Ubuntu 14.04,12.04
- Boinc Benchmarchs:@ ARM Chromebook CB5-311 TegraK-1
  Integer points (ARMhf Base) : 6118 ⇒ (i686): 1800 29.4%
  Flotings points (ARMhf Base) : 914 ⇒(i686): 200 21.9%
  about Pentium4 1.8GHz on ARM.(Qemu =Pentium2 266MHz)
- Windows applications on Wine, on ARM devices.

jw-cad(Wine) on ARM Chromebook



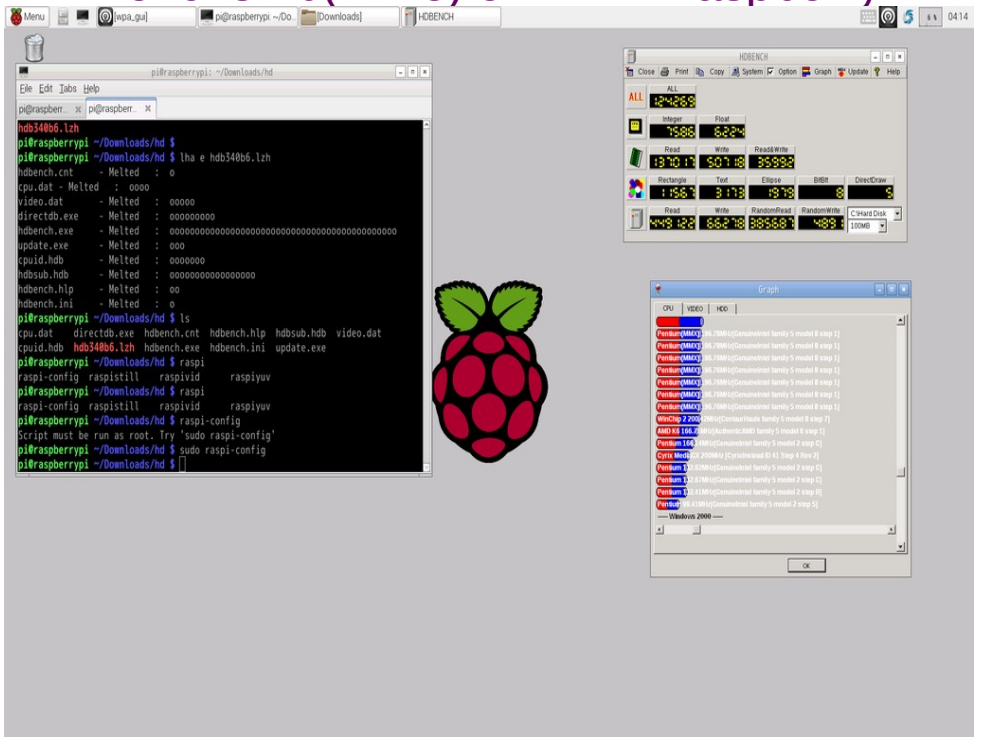
Bonanza(Wine) on ARM Chromebook



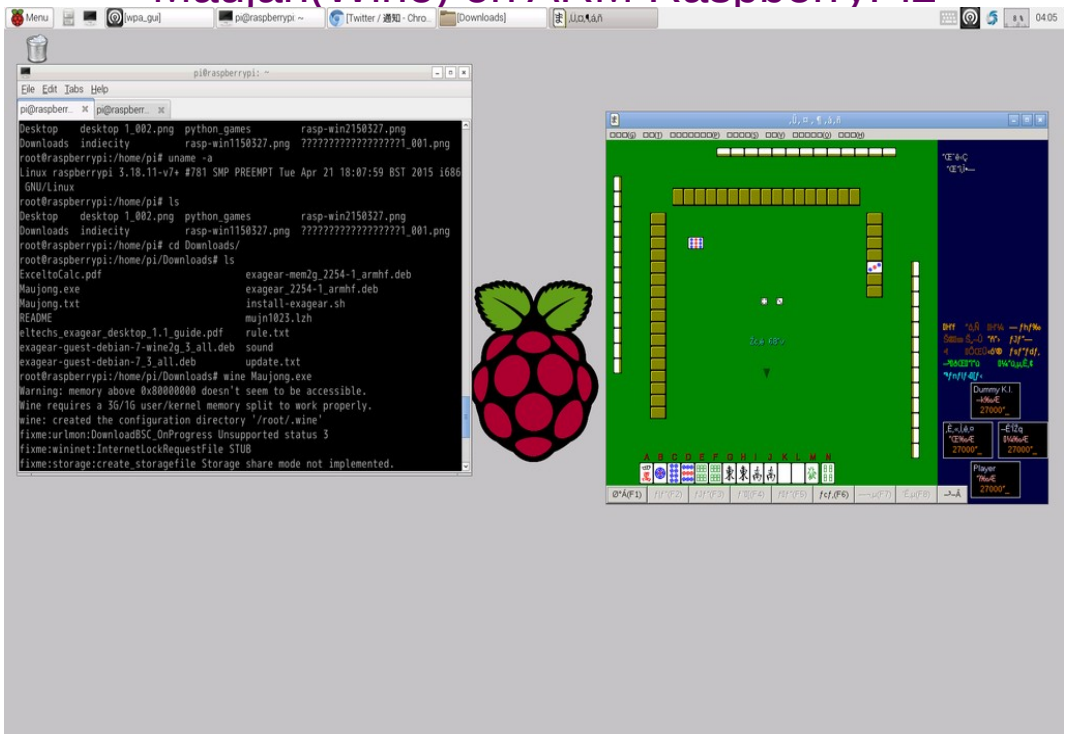
x86 Emulation on ExaGear-Desktop ARM RaspberryPi, RaspberryPi2

- ExaGear-Desktop RaspberryPi is 5 times faster than Qemu.
- i386 Debian7Wheezy on ARMhf Raspbian,Ubuntu14.04,Debian7
- HDBench Benchmarchs:@ ARM Raspberry Pi2
  Integer points (ExaGear i686) : 7586 (Qemu i386: 1999 26.4%)
  Flotings points (ExaGear i686) :6224 (Qemu i386: 384 6.2%)
  about MMX Pentium 200MHz on ARM. (Qemu =Pentium 40MHz?)
- Windows applications on Wine, on ARM devices.

HDBench3.40(Wine) on ARM RaspberryPi2



Maujan(Wine) on ARM RaspberryPi2



Custmized ARM Chromebook

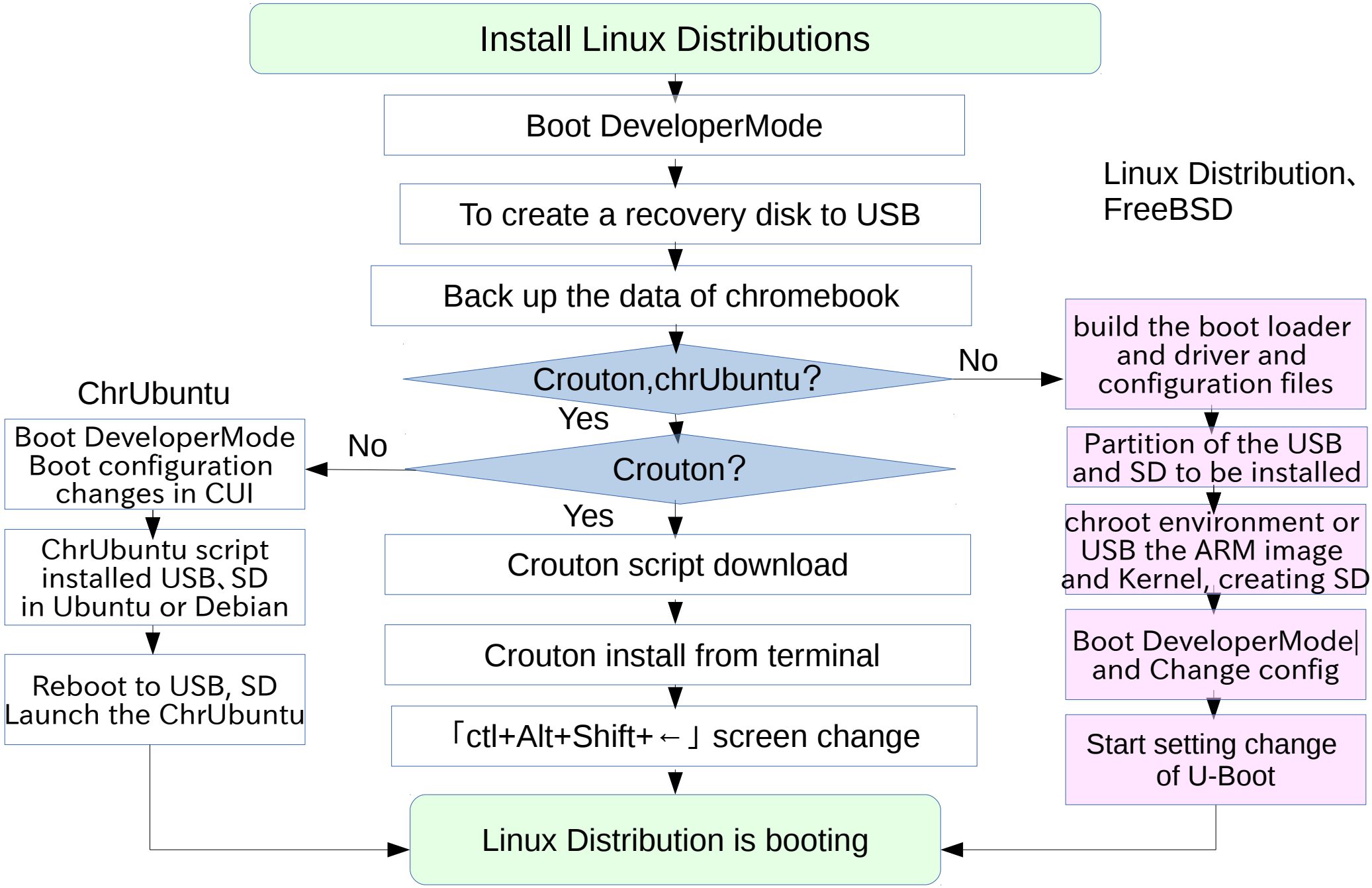
Linux Distribution on Chromebook

- How to install the following three main

  1、Crouton with chroot
  2、ChrUbuntu with dualboot
  3、To install the boot loader every various OS
  by rewriting the firmware

  4、USB boot using the Dev channel
  (1/2015)～

Flowchart of Linux installation on Chromebook



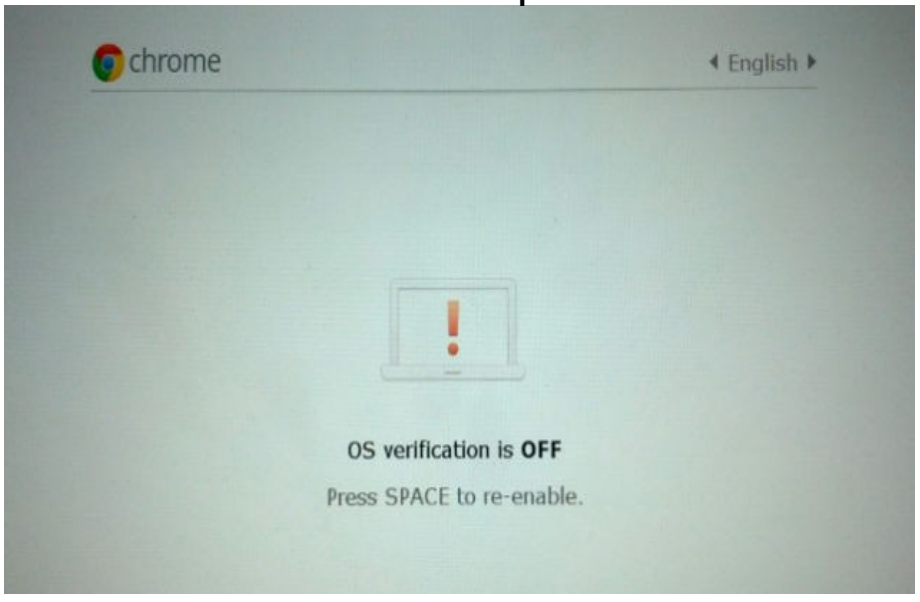
Developer Mode on Chromebook

- DeveloperMode of ChromeOS is the ability to internal access to unlock the security function.Various play for the switching is required to DeveloperMode the ChromeOS.
- DeveloperMode press the "Esc" + "refresh (F4)" + "Power button" to turn off the power.This is the so called the so-called forced reset referred to in the Chromebook.Since it goes into recovery mode, "Ctrl" + "D" → When enough to press the "Enter" 10 seconds beep sound is then later to developer mode.
- When you start in DeveloperMode, you need a recovery disk creation and data backup since the internal data is reset.
- The creation of recovery discs from the address bar of Chrome-browser
  chrome://imageburner
  Installing USB or to SD by typing

Reference：The Chromium Projects　Developer Mode

Create recovery disk on Chrome

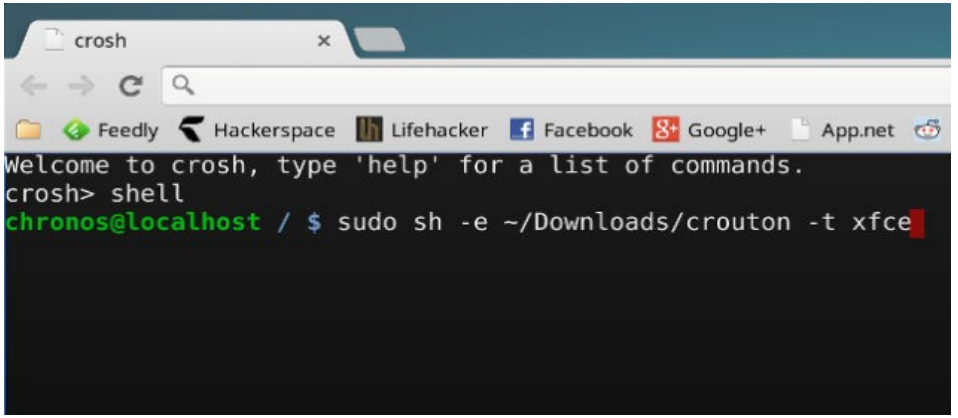
Boot DeveloperMode



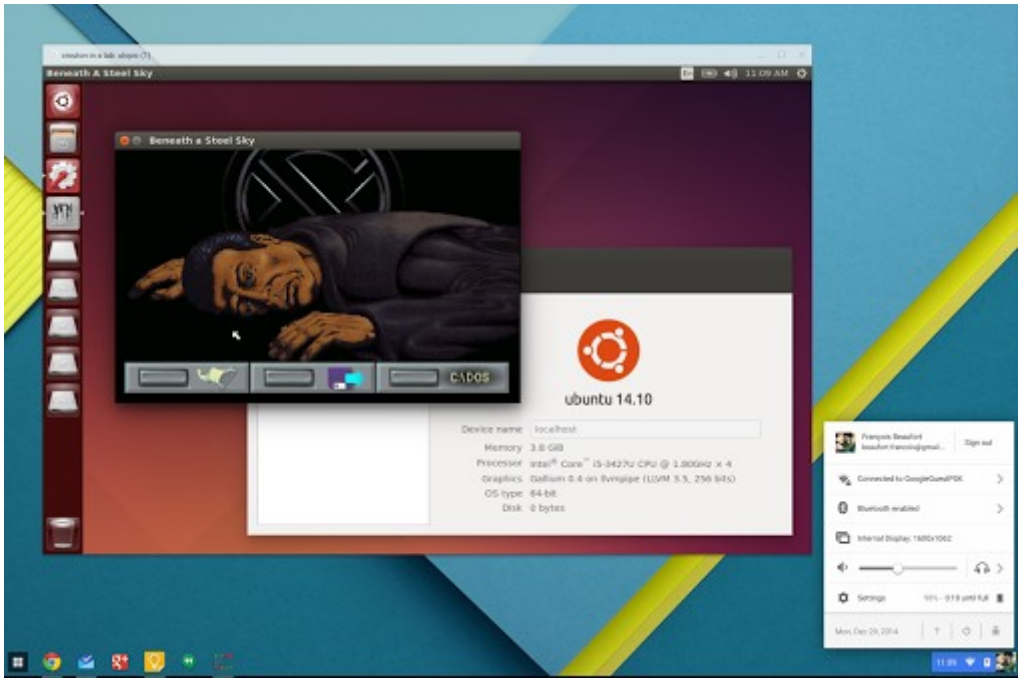
Crouton on Chromebook

- ChRomium Os Universal chrooT envirONment
  The author Google developers, Mr. David Schneider.
- Chroot automation tool for Ubuntu and Debian https://goo.gl/fd3zc
- To display the terminal in the "ctl + alt + t", used from the terminal to activate the "shell"
  sudo sh ~/Downloads/crouton -t xfce
- How to download the chroot environment by dropping the main script from github
  /mnt/stateful_partition/crouton/(Distribution name)

Terminal on Chrome-browser



Crouton Window Extention



Recognized debian releases:
potato* woody* sarge* etch* lenny* squeeze* wheezy jessie sid

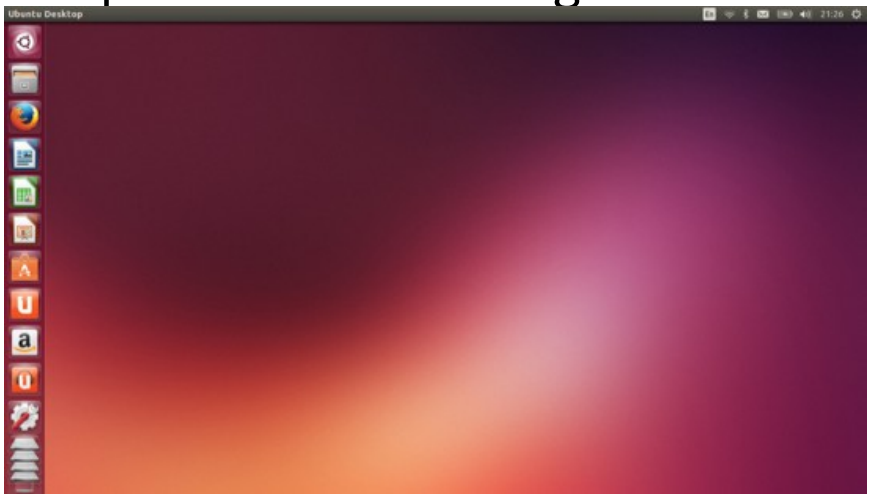
Recognized kali releases: kali

Recognized ubuntu releases:
warty* hoary* breezy* dapper* edgy* feisty* gutsy* hardy* intrepid* jaunty* karmic* lucid* maverick* natty* oneiric* precise quantal* raring* saucy* trusty utopic*

Releases marked with * are unsupported, but may work with some effort.

ChrUbuntu on Chromebook

- Dual-boot & SD USB automated installation tool for Ubuntu.
  The author Google developers, Mr. Jay Lee
  Method to accept the Linux Kernel and driver module of ChromeOS.
  x86 does not officially support the ARM in the corresponding. It notes that there is also not operate models.
- When you press the "ctrl + alt + → key", a mechanism to install the Ubuntu switched to CUI of the screen called Developer Console.
  curl -L -O http://goo.gl/9sgchs; sudo bash 9sgchs（34v87 /dev/mmcblk1）
  change Partition
  curl -L -O http://goo.gl/9sgchs; sudo bash 9sgchs
- Use switch in the "ctl + L" the ChromeOS and Ubuntu the OS when you boot
  How to download the chroot environment by dropping the main script from github
- Although Ubuntu is started normally, a method is somewhat time-consuming in the start-up manual switching.



Reference：Chromebooks and Chrome OS

Linux distribution and FreeBSD install in Chromebook

●FreeBSD

- build the source code with Kernel
- USB to be installed, partitioning of SD
- Partitioning of U-Boot and the Kernel, setting of Root partition
- To start the Chromebook in DeveloperMode. Move to the previous login to CUI.
- USB, SD boot can be set changed as.
  localhost ~ # crossystem dev_boot_usb=1
- USB and SD partition table setting of cpgt
- Restart and set of U-Boot. Activate the OS

●OpenSuse

- It will install ChrUbuntu way.
- To start the Chromebook in DeveloperMode. Move to the previous login to CUI.
  USB, SD boot can be set changed as.
  localhost ~ # crossystem dev_boot_usb=1

⇒Crouton and ChrUbuntu
both installation possible

Reference：FreeBSD on Samsung Chromebook "SNOW" model XE303C12
HCL:ARMChromebook

Customized Android

Debian Noroot on Android

- Debian Noroot can be installed in a chroot without taking root privileges Android apps Debian
- You can use a Bluetooth keyboard, a simple notebook PC
- Contents to build a chroot environment in the normal user privileges use the fakechroot, are viewing the Xorg in Xserver-SDL
- There are challenges to capacity because storage is based on the premise visceral / sdcard
- The ease popular anyone can be introduced
- Recent Ver corresponding with Android4.0 later
- Difficulties in compatibility that does not move Xserver-SDL with the old OS

Taiwan Electronic Dictionary
無敵CD-920

Debian Kit and Complete Linux

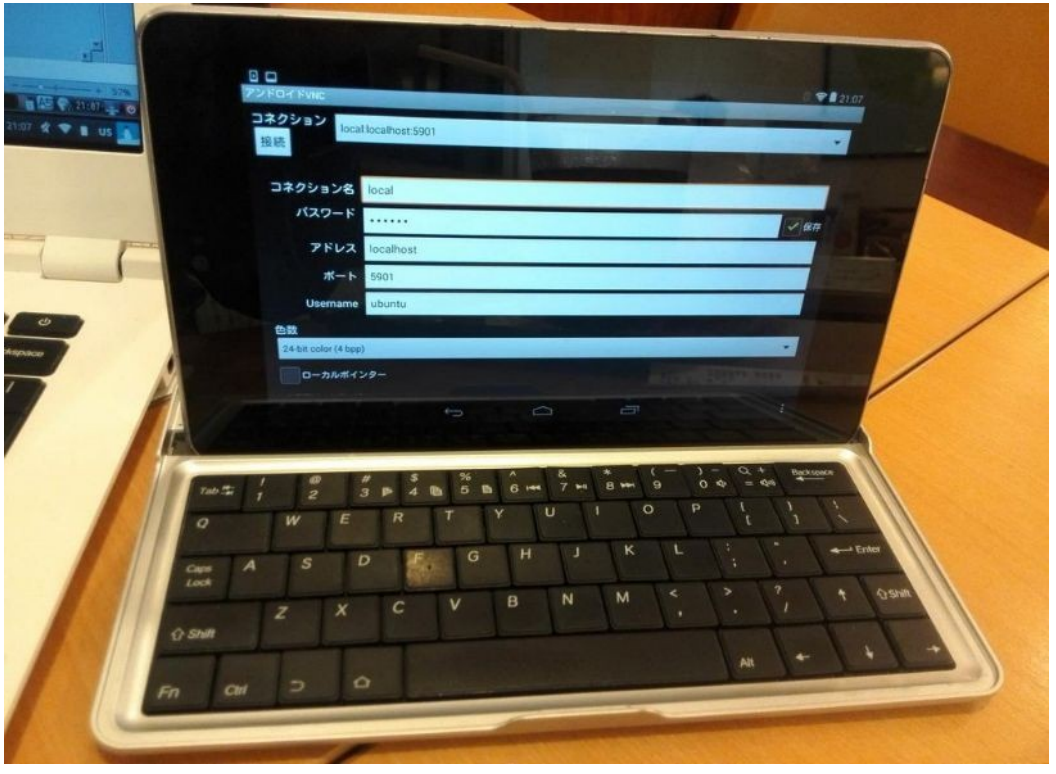
- App to put the package to build a chroot environment on Android with apt-get. Debian reduction can be.
- I can server of the Android simple. and those that do not need as there are root of.
- Debian Kit because it is a mechanism that can be used is apt-get at the root environment of the parent process of Android, has a high degree of freedom (high risk?)
- Also old environment for the Debian Noroot can not be put

Complete Linux

TightVNCserver and VNCviewer

- Alternate of the easiest X server VNCserver
- If you invoke the TightVNCserver in a chroot environment and easily launched the X environment on Android. Localhost:8080 (127.0.0.1)
- Of course, it is also possible to use by remote control.

VNC Viewer

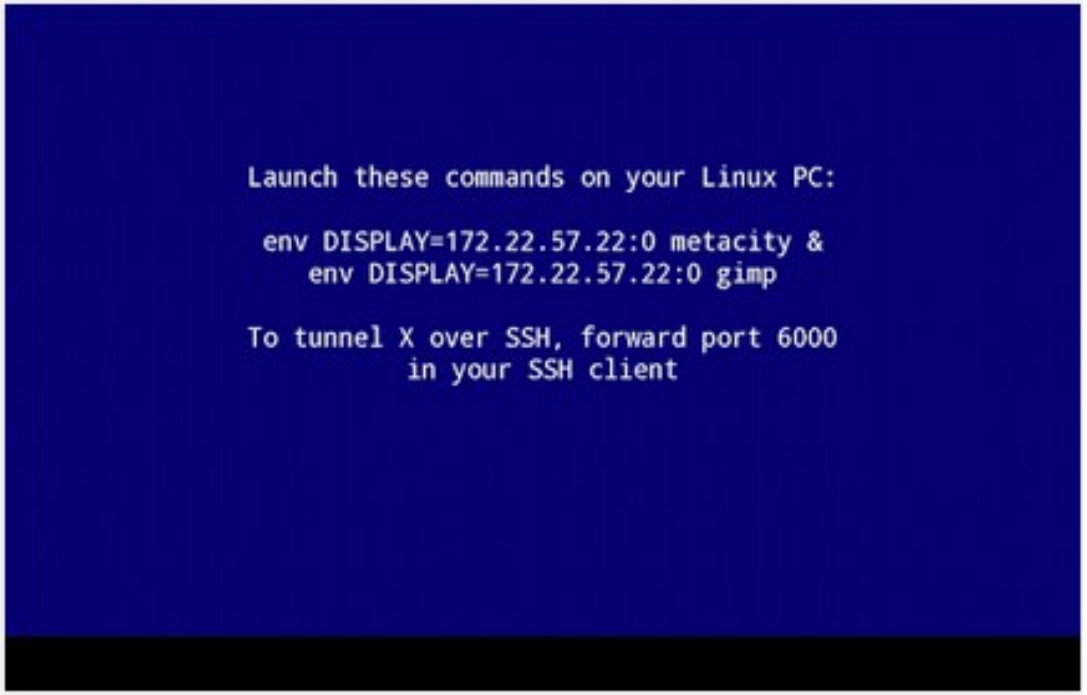


Complete Linux

Use Xserver-SDL alone on Android

- It can also be used alone Xserver-SDL, which is also used Debian noroot as an alternative to the Xserver.
- From how to use activates the Xserver-SDL, from the terminal in Chroot environment,
  env DISPLAY=xxx.xxx.xxx.xxx:0 lxsession &
  The activated Show Xserver-SDL again on Android

Xserver-SDL



Complete Linux

Customized Bootloader

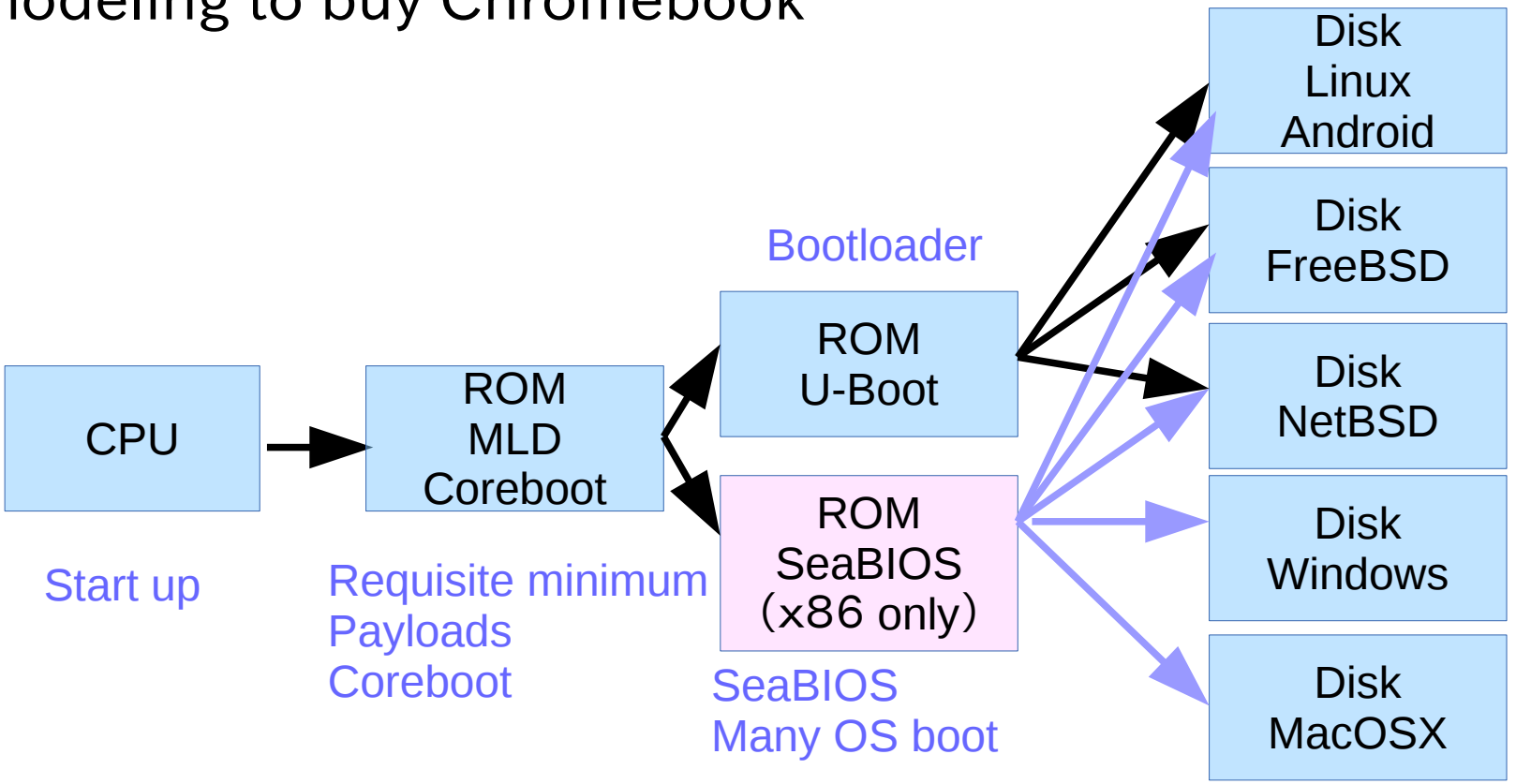
Mechanism of the bootloader on ARM devices and compare x86 devices.

In the case of ARM, it transfers the bootloader from FlashROM in RAM, and is configured to read the Kernel and rootfs.Bootloader that is being written to ROM is so called "firmware". In the case of Android, it is required Unlock “firmware”.

Devices	ROM	RAM	MBR (Disk)	Kernel	init	Login	Features
x86~ Linux	BIOS Device Bootdisk		GRUB LILO	Kernel Driver	Daemon and also	CUI Xorg	BIOS & DISK bootloader
ARM Android	Initialization driver RAMtransfer	Kernel transfer	Kernel rootfs loading	Kernel driver rootfs	Devices Daemon Context manager Zygote	Dalvik VM Android GUI	Bootloader unlock is important
	MLO	Android Bootloader（ROM）					
x86- Chrome book	Initialization driver RAMtrasfer	Kernel transfer	Kernel Rootfs loading	Kernel Driver	Daemon And also	CUI Xorg	After the bootloader in common
	MLO	Bootloader（U-boot）					
ARMLinux Distribution Chrome book	Initialization driver RAMtransfer	Kernel transfer	Kernel rootfs loading	Kernel Driver	Daemon and also	CUI Xorg	After the bootloader in common with x86
	MLO	Bootloader（U-boot）					

ARM and x86 bootloader

- Start When you power ON from Firmware written to the ROM. Starting from next boot loader with a payload from Coreboot.
- The SeaBIOS you can start the various OS if the corresponding model.The need is to move the Windows and MacOSX in the Chromebook.Challenge the corresponding hard less SeaBIOS.
- SeaBIOS correspondence Haswell generation 9 models. Bay-Trail generation is not supported.Careful in the selection models when remodeling to buy Chromebook



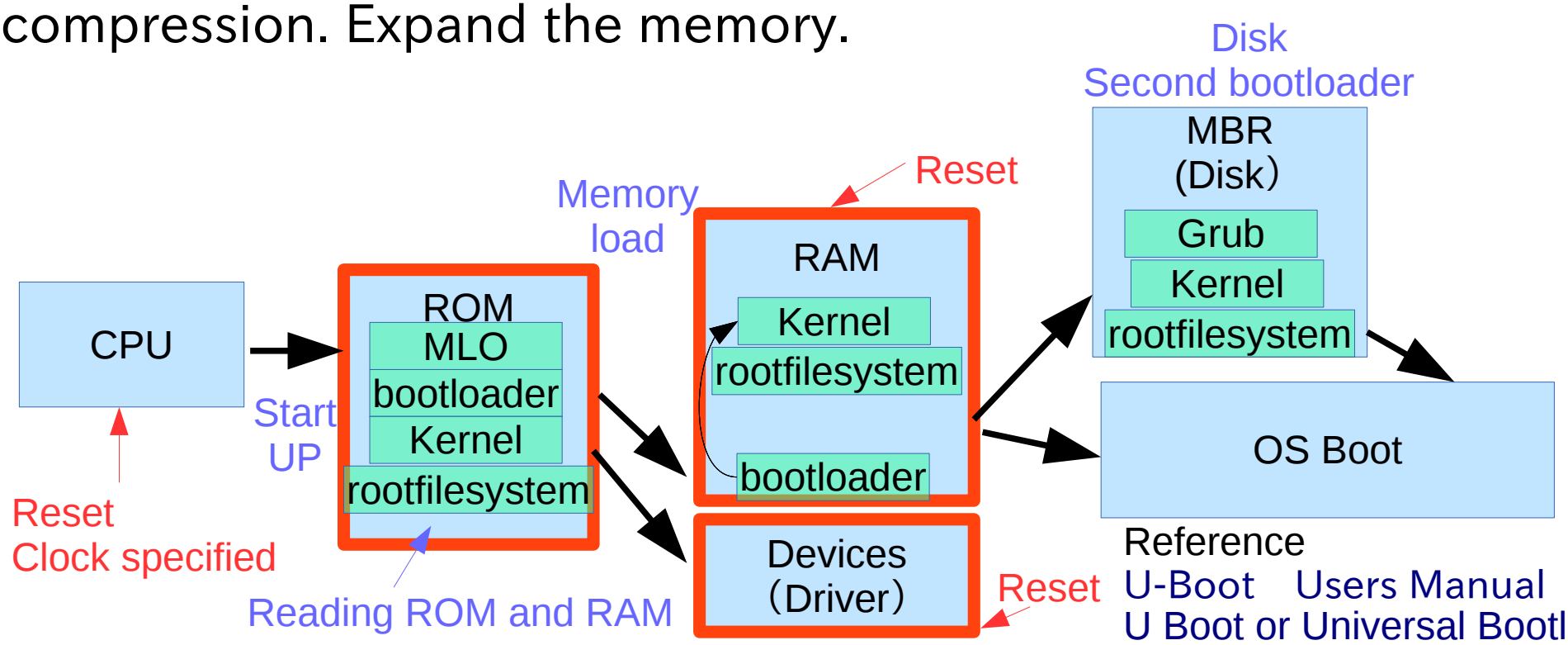
ARM devices Bootloader

Bootloader are classified into ROM and Disk Bootloader.

Boot loader	MPU	OS	Storage	Format	Boot Modules	License
GNU GRUB	x86	Linux *BSD MacOSX MSDOS	HDD,floppy USB,LAN TFTP,Serial	All	DISK	GPLv3
LILO	x86	Linux *BSD MSDOS	HDD,floppy USB,LAN TFTP,Serial	All	DISK	BSD Licence
eCos Redboot	ARM,x86,68k, MIPS,Altera,PowerPC,SuperH, others	Linux *BSD MacOSX MSDOS	HDD,floppy USB,LAN TFTP,Serial	JFFS2、EXT2、EXT3、EXT4、FAT, others	ROM、RAM	Mod GPLv2+
Das U-boot	ARM,x86,68k, MIPS,Altera,PowerPC,SuperH, others	Linux *BSD Android	HDD,floppy USB,LAN,Zip TFTP,Serial NFS	Cramfs、EXT2、EXT3、EXT4、FAT、FDOS、JFFS2、ReiserFS、UBIFS、YAFFS2	ROM、RAM	GPLv2
SeaBIOS	x86	Win,MAC *BSD	SecondaryROM Disk	EXTx、FAT32、NTFS	ROM、RAM Coreboot	LGPLv3
Multirom	ARM	Android Linux	Android SecondaryROM USB	EXTx、FAT32、NTFS	ROM、RAM	GPLv3

Das U-Boot

- High-performance ROM boot loader, which is the ARM other a well used.
- It became a major from around 2010 as an alternative to the Redboot.
- Das U-Boot written in C. Specify the CPU and memory map directly, it requires an understanding.
- In the case of Linux, it converts the Kernel or the like to uImage in mkimage command.Boot from ROM with flash ROM baked by compression. Expand the memory.



Customized「End of Life」ARM Devices

- What do you think of that「End of Life」with ARM devices?

1, First End of Life: Official Support Out
with Linux Distribution and Android

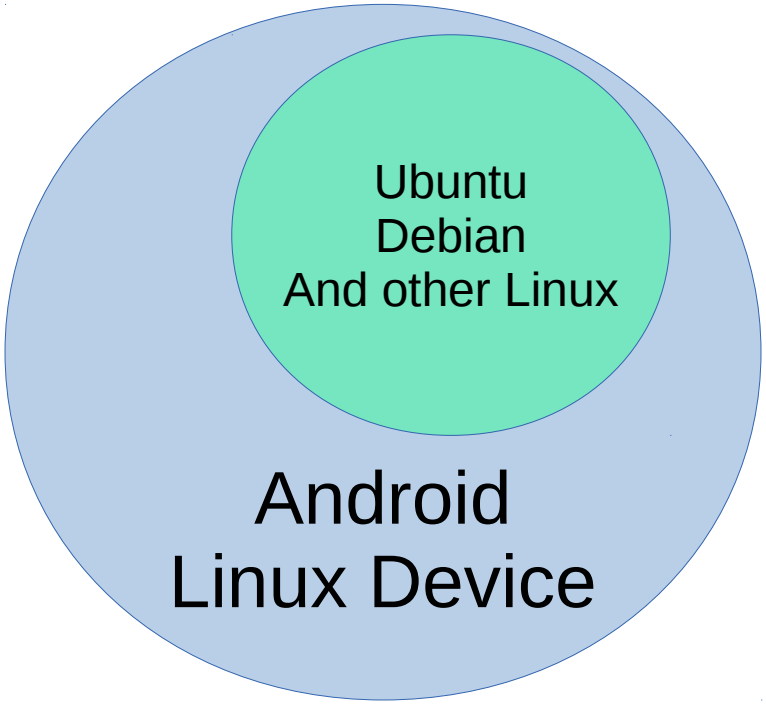
2, Second End of Life: Linux Kernel and libc

libc is demand of linux kernel version.
If it is not supported with Mainline Kernel.
This devices will not supported libc and others.
This distributions will be not able to upgrade.

3, Third End of Life: pkgsrc and NetBSD
Pkgsrc and NetBSD is not restraint Linux Kernel.

Chroot on Old ARM Linux

- Chroot to operate in the Create a new root directory under Linux environment
- Start independently different versions of OS
- It is no longer possible to access the outside of the OS from the Chroot Environment
- Chroot the Root authority only. In general user privileges Fakechroot need
- Since Kernel is a common one, driver or module class is affected by the original Kernel
  → Kernel unsupported features, OS can not be used



PKGSRC on「End of life」ARM Devices

- Try to use the NetBSD of packager pkgsrc even Ubuntu chromebook⇒Why?
  ⇒1, I want to use the latest version of the package.
  I want to use Mikutter at any time the latest version
  2, There is almost no ARM binary latest package in Ubuntu of PPA.
  One by one manually compile required from the source package.
  Very troublesome.
  3,OS and Unix pkgsrc is independent from architecture,
  highly portable enough to use even Unix,Linux,Mac and Win very useful to the ARM environment
  4, I do not want to mixed whether the LTS the Debian Sid Deb development version. I want to be independent latest packages.
  5, If ARM Ubuntu side, I want to use the latest version to continue be Kernel support out. Strongest packager can also be used from the end manufacturers official support.

Mikutter (Ruby based Twitter client)

ARM Chromebook Mainline Kernel

1、U-boot build and install
・make partition
  1st partition: kernel partition with nv u-boot.
  2nd partition: boot partition (must be formatted as FAT32 or Ext2).
  3rd partition: root partition.
・U-boot build
  wget -O - http://commondatastorage.googleapis.com/chromeos-localmirror/distfiles/nv_uboot-snow.kpart.bz2 | bunzip2 > nv_uboot.kpart
/Kernel
  dd if=nv_uboot.kpart of=/dev/mmcblk1p1
  cgpt add -i 1 -S 1 -T 5 -P 10 /dev/mmcblk1

2、Mainline Kernel build and install
/git clone --depth 1 https://github.com/linux-exynos/linux.git -b dts-config linux

cd linux
make exynos_defconfig
make menuconfig

mount /dev/mmcblk1p2 /mnt/externcp arch/arm/boot/{uImage,dts/exynos5250-snow.dtb} /mnt/extern
umount /mnt/extern

mount /dev/mmcblk1p3 /mnt/extern
INSTALL_MOD_PATH=/mnt/extern make modules_install
umount /mnt/extern

NetBSD on New and old(End of Life) ARM and others devices

LUNAII@68040 and Twitter

Many New ARM single board PCs

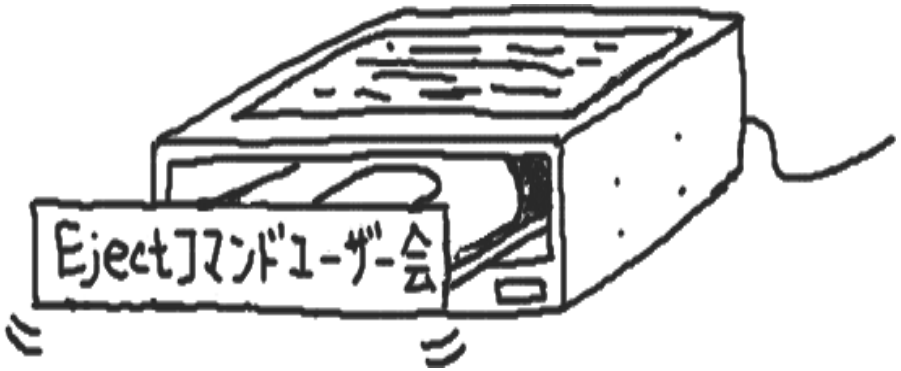
NetBSD on Sega Dreamcast

Zaurs and Netwalker and others

https://www.facebook.com/NetBSD.jp

Japan only favorite OSS project

Eject-command Japanese Users Group



http://eject.kokuda.org/

mikutter User Group

http://mikutter.hachune.net/

Opencocon
Thinclient distribution

SHIMADA Hirofumi,
@shimadah

http://opencocon.org/

Next My Presentation OSC Kyoto、Tokyo

- OSCKyoto、Tokyo、and my exhibition schedule
- Content:OSC Kyoto:Hacking of Android Nexus7
- OSC Kyoto　8/8
  OSC Tokyo　10/24-25
  KOF(Kansai Open Forum) 11/?
- The following content will be determined by your opinion.I look forward to your comments.

  My twitter : @kapper1224
- Let's me talk even there because tomorrow will my booth.

- That's all for now. Thank you very much!
  Do you have any questions?