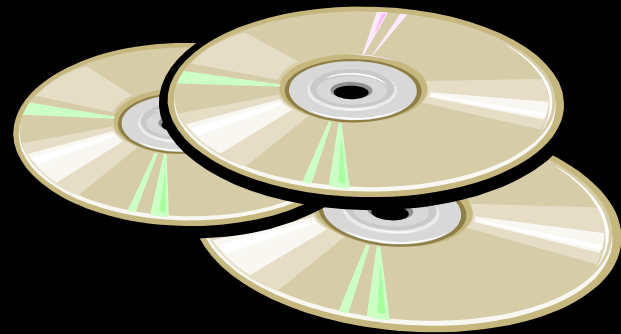


BOOT DEVICES: OR IN CANADIAN, WHAT IS THIS ALL ABOUT

Adrian Crenshaw



About Adrian

- ▣ I run Irongeek.com
- ▣ I have an interest in InfoSec education
- ▣ I don't know everything - I'm just a geek with time on my hands
- ▣ (ir)Regular on the ISDPodcast <http://www.isd-podcast.com/>
- ▣ Prepare yourselves for a disorganized boot CD/DVD/UFD braindump, but as notes they may help you to avoid my mistakes



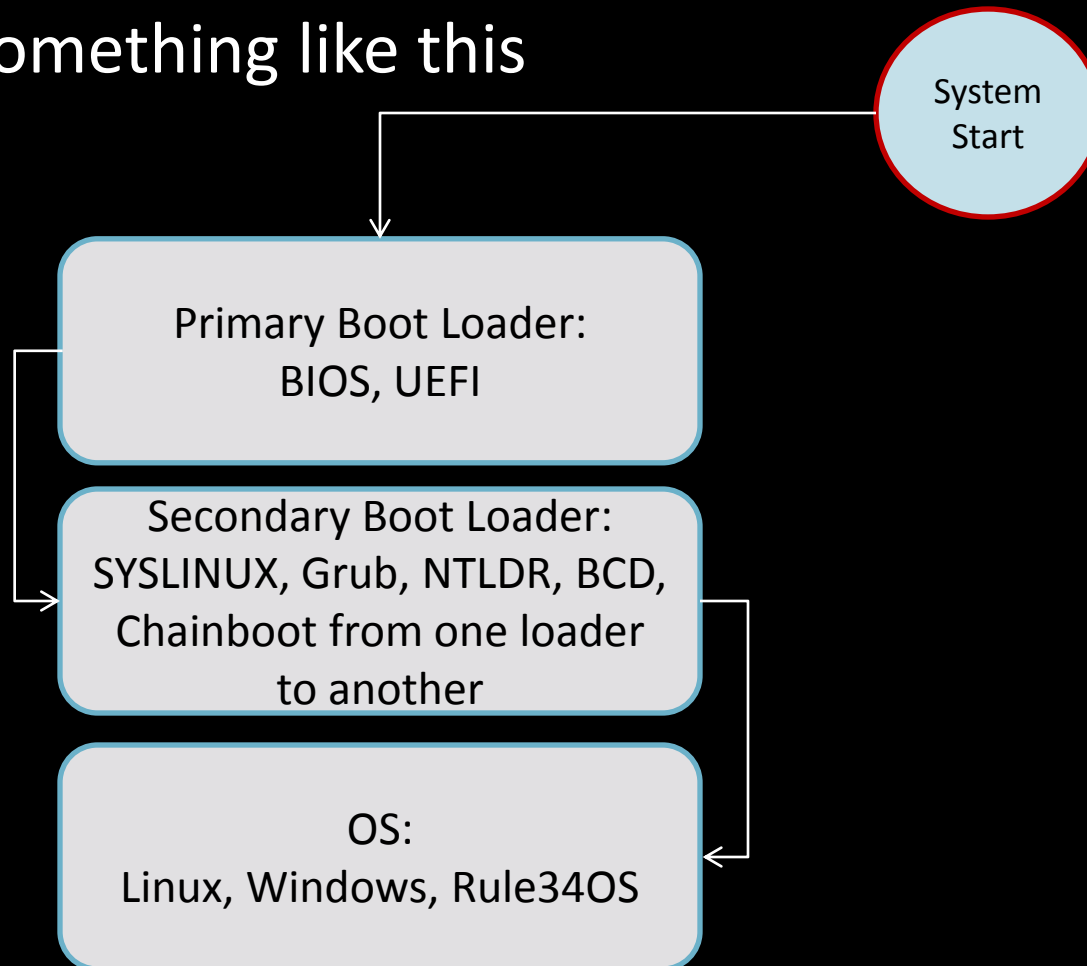
Why care?

- ▣ Malware removal
- ▣ Forensics
- ▣ Privacy
- ▣ Access to restricted tools
- ▣ Imaging
- ▣ Physical access = pwnage
- ▣ These guys may come to visit



Dumbed down boot process

- ▣ Something like this



RAM Disks

Why use memory?

- ▣ For optical media, it's read only (mostly)
- ▣ For USB, it only has so many write cycles
- ▣ For both: Speed
- ▣ For some hardware, RAM disk just works better than UFD

Not quite the same thing

- ▣ UnionFS, AuFS or EWF, which redirect writes to what would otherwise be a read only file system



Distros/Boot environments

Just a few:

- ▣ BackTrack Linux
<http://www.backtrack-linux.org>
- ▣ Tails (The Amnesic Incognito Live System)
<http://tails.boum.org/>
- ▣ Bart's PE/UBCD4Win
<http://www.nu2.nu/pebuilder/>
<http://www.ubcd4win.com/>
- ▣ Winbuilder/Win7PE SE
<http://winbuilder.net/> & <http://reboot.pro/12427/>
- ▣ Konboot
<http://www.piotrbania.com/all/kon-boot/>



BackTrack Linux

- ▣ Tons of security tools
- ▣ Awesome hardware support for odd wireless needs
- ▣ Well maintained
- ▣ Can do a hard drive install if you wish

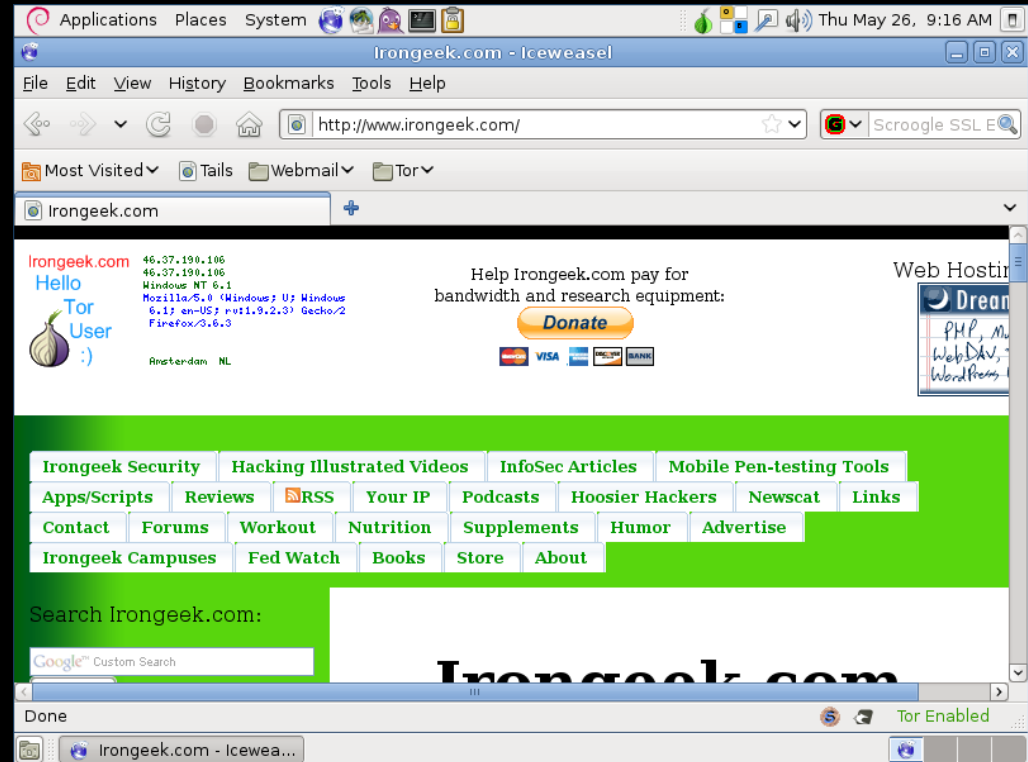


Image from <http://www.backtrack-linux.org/screenshots/>



Tails

- ▣ Boot from CD/DVD to leave less of a trail
- ▣ Use Tor to anonymize traffic



Bart's PE/UBCD4Win

- ▣ Bart's PE can be build from the files on a Windows XP CD
- ▣ UBCD4Win is Bart's Pe with a bunch of extras + Multi-boot (DBAN)
- ▣ Plugins can be made to add functionality

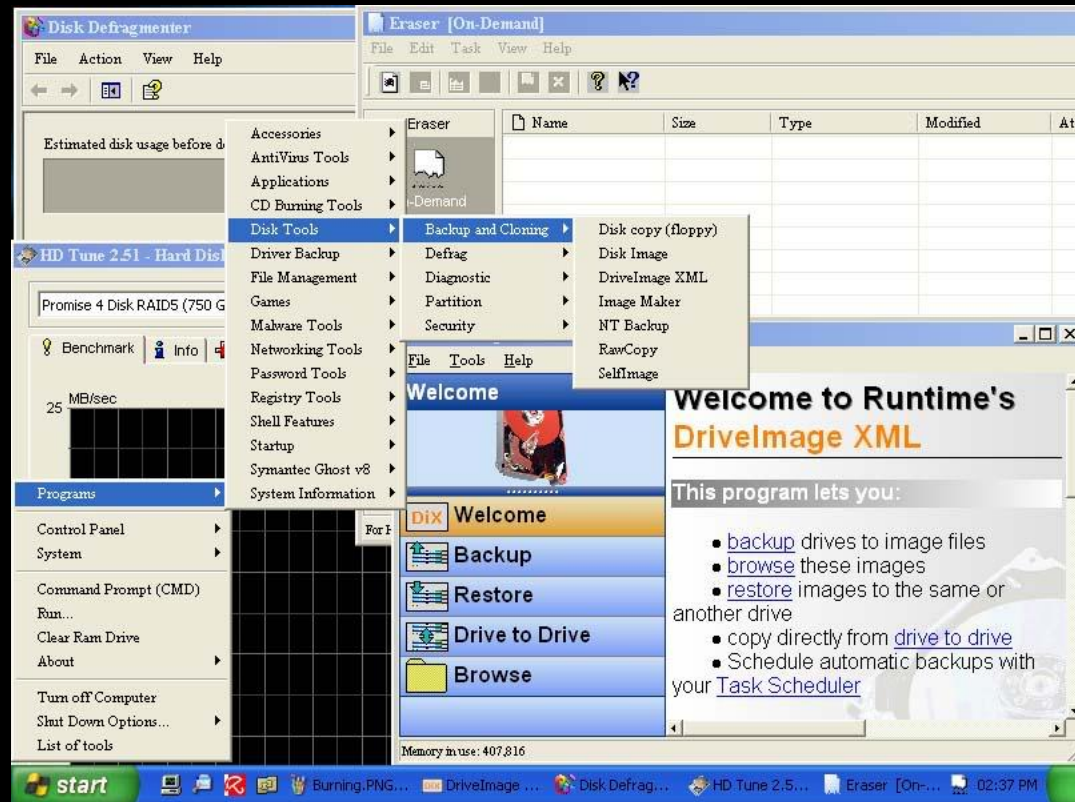


Image from <http://www.ubcd4win.com/screen.htm>



Winbuilder/Win7PE SE

- ▣ Make a Windows based boot USB/CD/DVD
- ▣ Starting OS needed depends on build
- ▣ Plugins can be made to add functionality
- ▣ Build even up to Win7 SP1 32/64bit
- ▣ Hardcore roll your own

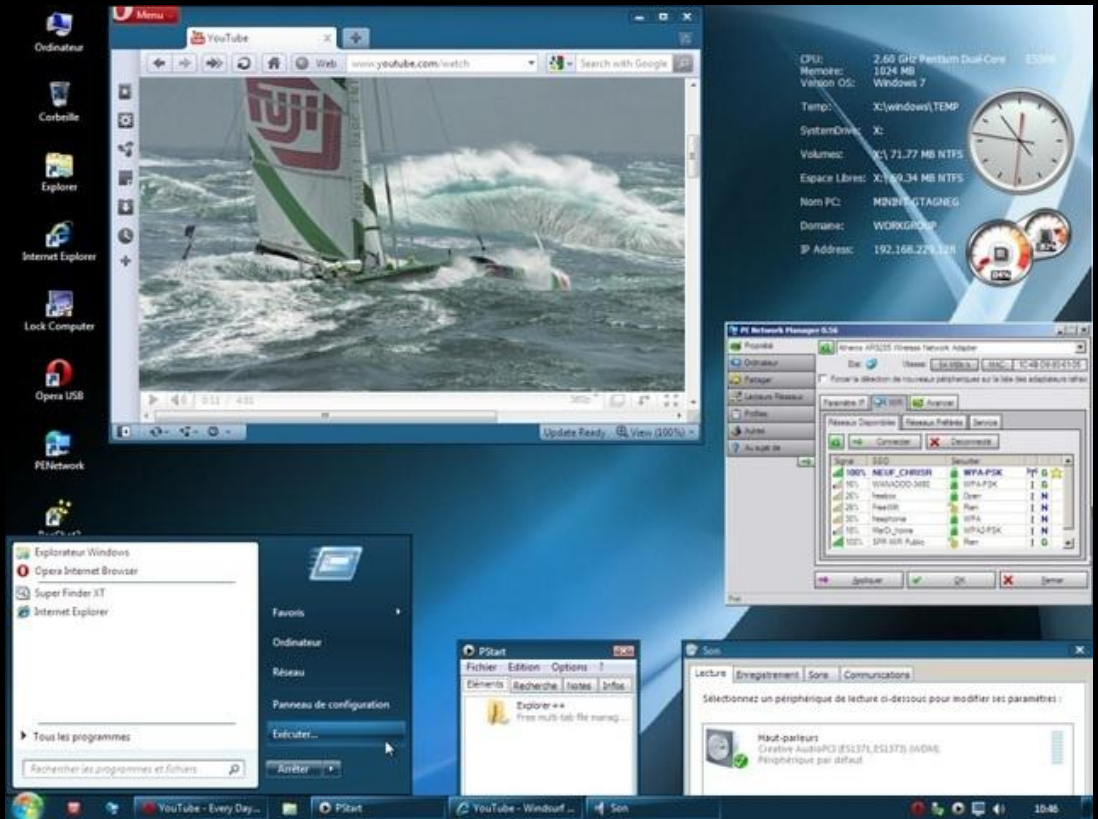


Image from <http://reboot.pro/12427/>



Konboot

- ▣ Bypass password on some versions of Windows and Linux
- ▣ Changes kernel on boot
- ▣ Login to Linux with “konusr” as username.
- ▣ Use a blank password in Windows
- ▣ Meant to run from a CD/Floppy, sometimes works from a UFD using instructions found here: <http://www.irongeek.com/i.php?page=security/kon-boot-from-usb>



Image from <http://www.piotrbania.com/all/kon-boot/>



Burn an ISO



Windows

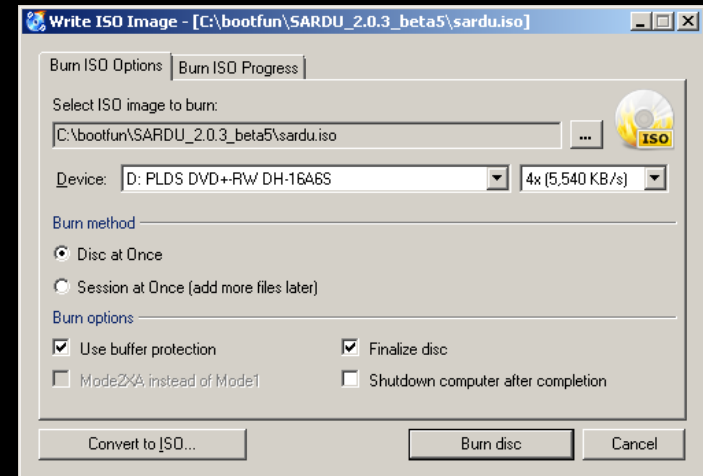
- ▣ CD Burner XP
<http://cdburnerxp.se/>

- ▣ ImgBurn
<http://www.imgburn.com/>

Linux

- ▣ Brasero
<http://projects.gnome.org/brasero/>
<https://help.ubuntu.com/community/Brasero>

Don't forget to close an finalize!!!



Make that Linux ISO a bootable USB

- ▣ UNetBootin (multiplatform)
<http://unetbootin.sourceforge.net/>
- ▣ Universal USB Installer
<http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/>
- ▣ Persistence

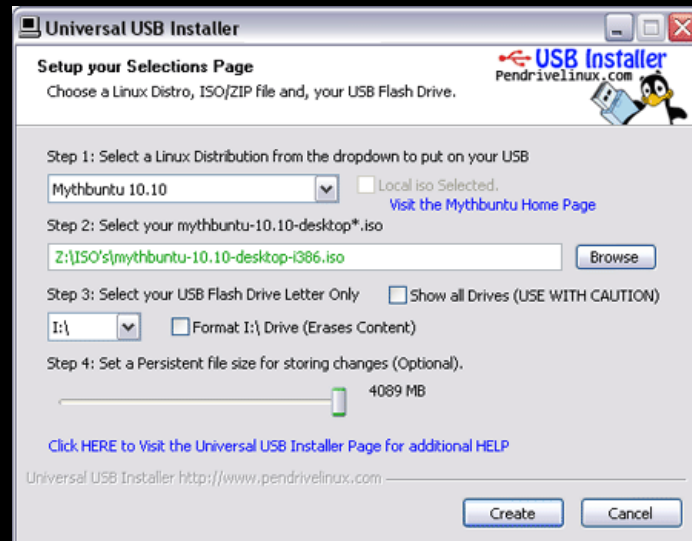
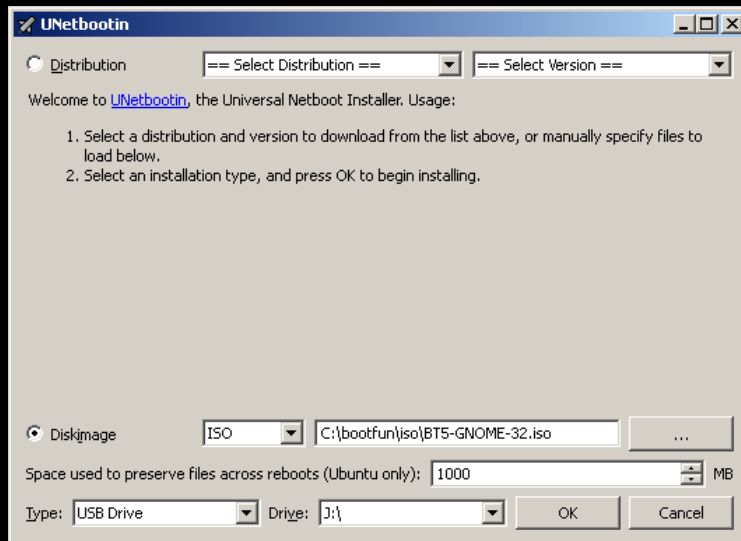
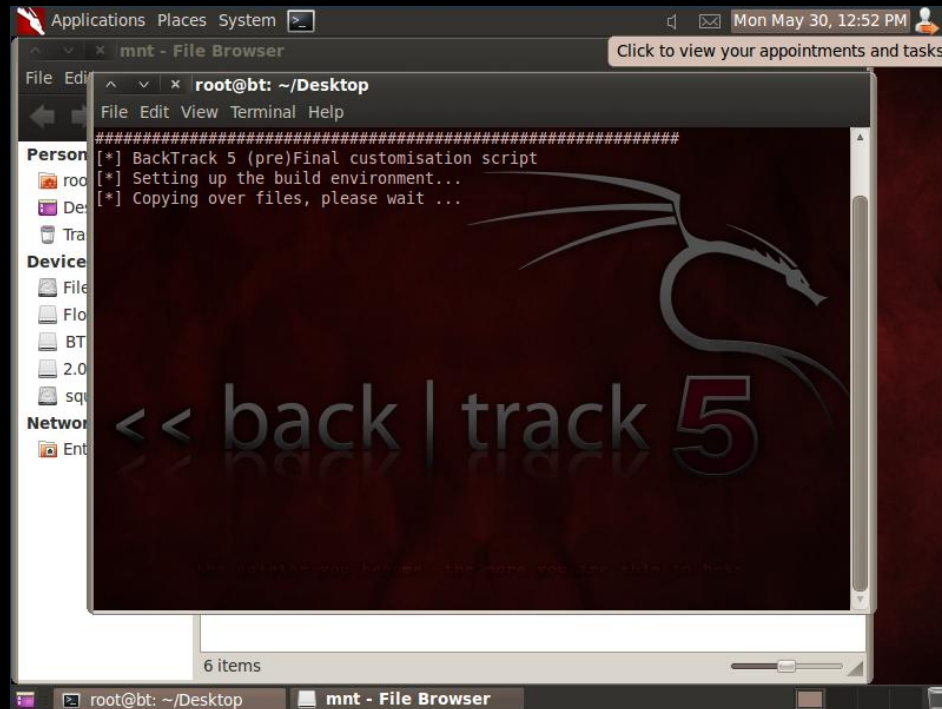


Image from <http://www.pendrivelinux.com>



Linux Remastering

- ▣ Mount the ISO , Chroot, Edit, make a new ISO
- ▣ Made a script base on morning_wood's post here:
<http://www.backtrack-linux.org/forums/backtrack-5-beginners-section/40515-customise-script-bt5.html>



Windows based bootables

- ▣ What is Windows PE?
 - Windows Preinstallation Environment
 - Part of Microsoft's Windows Automated Installation Kit (WAIK)
 - Cut down version of Windows for installs/repairs/diagnostics
 - Not all Windows features are available
- ▣ Other PE based tools give us extra capabilities



A few notes on the Windows based tools and AV

- ▣ May want to turn off anti-virus while building
- ▣ Speed reasons
- ▣ Some tools trip it, like Nir's password tools



UBCD4Win/Bart's PE

UBCD4Win PE Builder v3.1.10a

Builder Source Help

Builder

Source: (path to Windows installation files)

E:\bootfun\winxp-w-sp3\

Custom: (include files and folders from this directory)

E:\bootfun\UBCD4Win\extra

Output: (E:\bootfun\UBCD4Win\BartPE)

BartPE

Media output

None

Create ISO image: (enter filename)

E:\bootfun\UBCD4Win\UBCD4WinBuilder.iso

Burn to CD/DVD AutoErase RW

Burn using: StarBurn

Device:

Plugins Build

UBCD4Win PE Builder v3.1.10a - Plugins

Plugin list:

Enabl...	Name	File
Yes	!!! (Do Not Disable) FixOEM	!Critical\FixOEM\FixOEM.inf
Yes	!Critical: DComLaunch Service [Building with XP SP1-DISABLE]	!Critical\DcomLaunch\dcomlaunch.inf
Yes	!Critical: Joshuas-WinPE-PreLogon Config	!Critical\Config-PreLogon\ConfigPreLogon.inf
No	!Critical: LargeIDE Fix (KB331958) [Building with XP SP1-ENABLE]	!Critical\Large IDE-Fix\Large IDE-Fix.inf
Yes	!Critical: ubcd4winToUSB V-1.00 <Press CONFIG to install ubcd4win to usb-drive>	ubcd4wintousb\ubcd4winToUSB\ubcd4winToUSB.inf
Yes	!Critical: User Settings (Required)	!Critical\UserSettings\User-Settings.inf
Yes	!Multiboot: !USB Boot Menu Support	Multiboot-003\USB-Boot\USB-Boot.inf
Yes	!Multiboot: BCDW (Required for MultiBoot)	Multiboot-003\bcdw\bcdw.inf
Yes	!Multiboot: BCDW <CONFIG to Test menu from last build>	Multiboot-003\bcdw\bcdw_TestMenu.inf
No	!Multiboot: BCDW: Enable "Press any key to boot from CD"	Multiboot-003\bcdw\bcdw_bootfix.inf
Yes	!Multiboot: BCDW: Enable Boot Logo	Multiboot-003\bcdw\bcdw_logo.inf
No	!Multiboot: BCDW: Enable Boot password <CONFIG- to change password>	Multiboot-003\bcdw\bcdw_password.inf
No	!Multiboot: BCDW: Use menu style #1 (multicolor combination)	Multiboot-003\bcdw\bcdw_template1.inf
No	!Multiboot: BCDW: Use menu style #2 (grey/white shadowbox style)	Multiboot-003\bcdw\bcdw_template2.inf
No	!Multiboot: BCDW: Use menu style #3 (blue/white)*default*	Multiboot-003\bcdw\bcdw_template3.inf
No	!Multiboot: BCDW: Use menu style #4 (USER Defined) <EDIT ME>	Multiboot-003\bcdw\bcdw_template4.inf
Yes	!Multiboot: DBAN (Darik's Boot And Nuke) v2.0	Multiboot-003\dban\dban.inf
No	!Multiboot: Easeus Partition Manager <Press CONFIG>	Multiboot-003\Easeus\easeus.inf
Yes	!Multiboot: FreeDOS	Multiboot-003\FreeDos\freedos.inf
Yes	!Multiboot: GOBACK Removal Tool	Multiboot-003\goback\goback.inf
No	!Multiboot: Gujin Boot manager for Linux	Multiboot-003\gujin\gujin.inf
No	!Multiboot: Memtest86 v3.5	Multiboot-003\memtest-3.5\memtest.inf
Yes	!Multiboot: Memtest86+ v4.10	Multiboot-003\Memtest86+\memtest.inf
Yes	!Multiboot: NTFS for DOS	Multiboot-003\NTFS4DOS\ntfs4dos.inf
Yes	!Multiboot: Office XP Recovery & Registry Editor	Multiboot-003\Office\office.inf

Close Enable/Disable Config Refresh

Edit Add Remove Help

UBCD4Win/Bart's PE

Demo/Overview



Common issues with UBCD4Win

- ▣ Problems may be caused by building from Vista/Win 7
- ▣ PreLogon File Not Found
- ▣ Copy C:\Windows\Registration\R0000000000001.clb to USB at \MININT\Registration\R0000000000001.clb
- ▣ Blue Screen of Death 0x0000007B error may require a hacked ntdetect.com



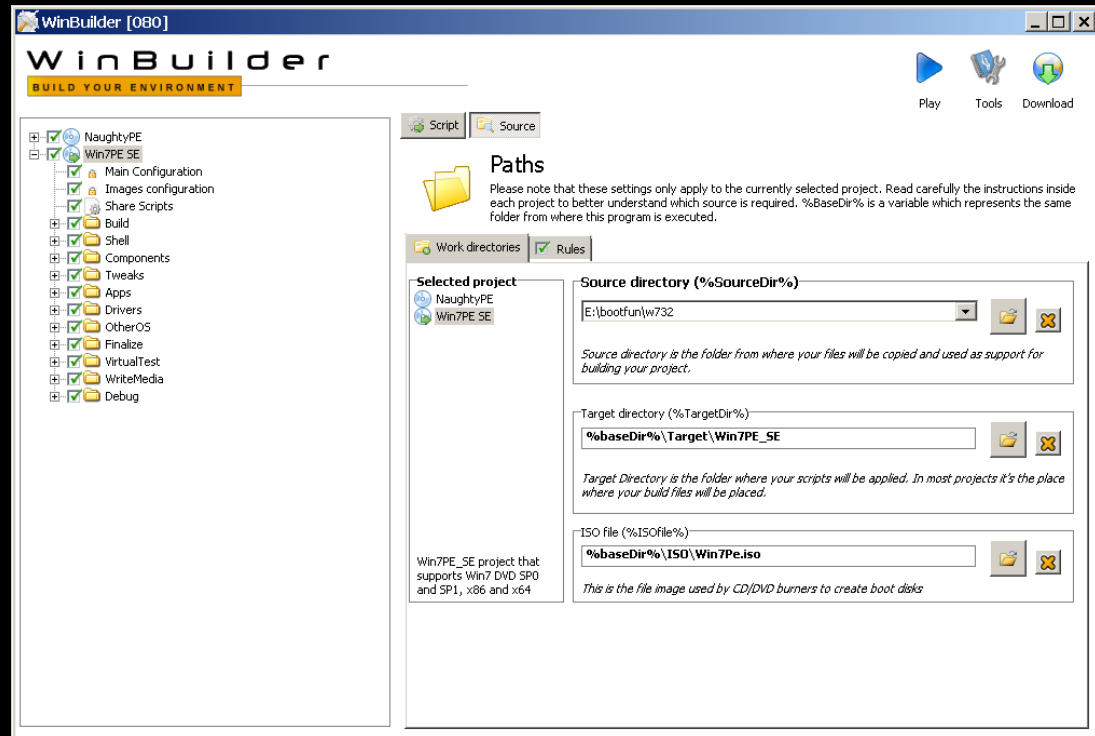
Putting UBCD4Win to a USB

- ▣ UBUSB Utility (act's like it's locked up, just give it time)
<http://www.ezpcfix.net/ubcd4win/UBUSB.exe>
 - ▣ UBUSB Instructions
<http://ubcd4win.com/forum/index.php?showtopic=11375>
 - ▣ Other options:
 - ▣ RMPrepUSB (Nice details on problems)
<http://sites.google.com/site/rmprepush/tutorials/ubcd4win>
 - ▣ Bootable USB-Drive Utility
<http://www.911cd.net/forums//index.php?showtopic=2170>
- 2



WinBuilder/Win7PE SE

- ▣ Tons of scripts to roll your own
- ▣ Demo is the best way to show you
- ▣ Download from <http://winbuilder.net/>



Needed files to build

- ❑ Download and install KB3AIK_EN.iso from <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=696dd665-9f76-4177-a811-39c26d3b3b34&displaylang=en>
- ❑ After install copy the following files from C:\Program Files\Windows AIK\Tools\amd64\
 - bcdedit.exe
 - imagex.exe
 - wimgapi.dll
 - wimmount.inf
 - wimmount.sys
 - wimserv.exe
- ❑ to C:\bootfun\winbuilder\Projects\Tools\Win7PE_SE\x64
- ❑ Path will vary depending on build platform
- ❑ WinFE may already have the needed tools



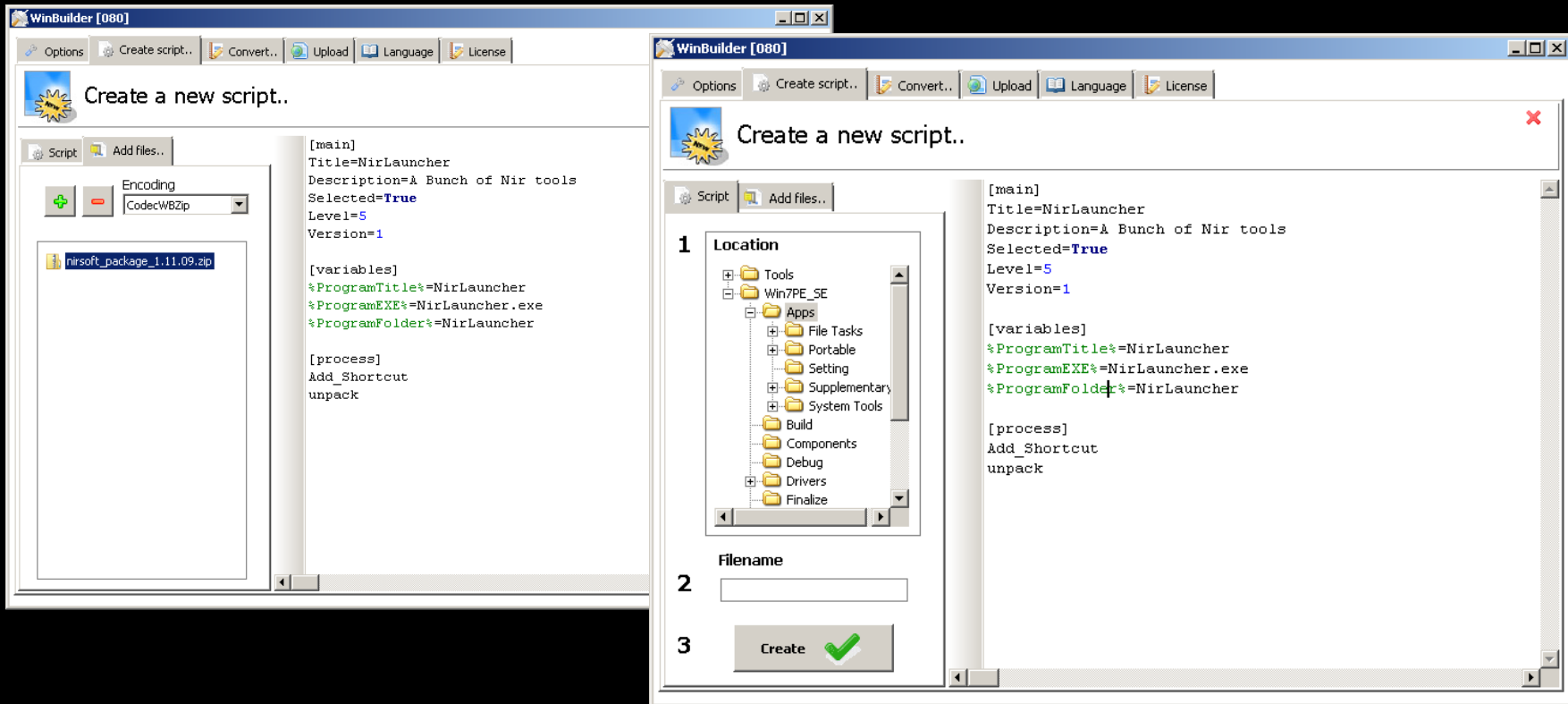
If you get this error, reboot and try again

- ▣ Some of the WIM tools may be mismatched



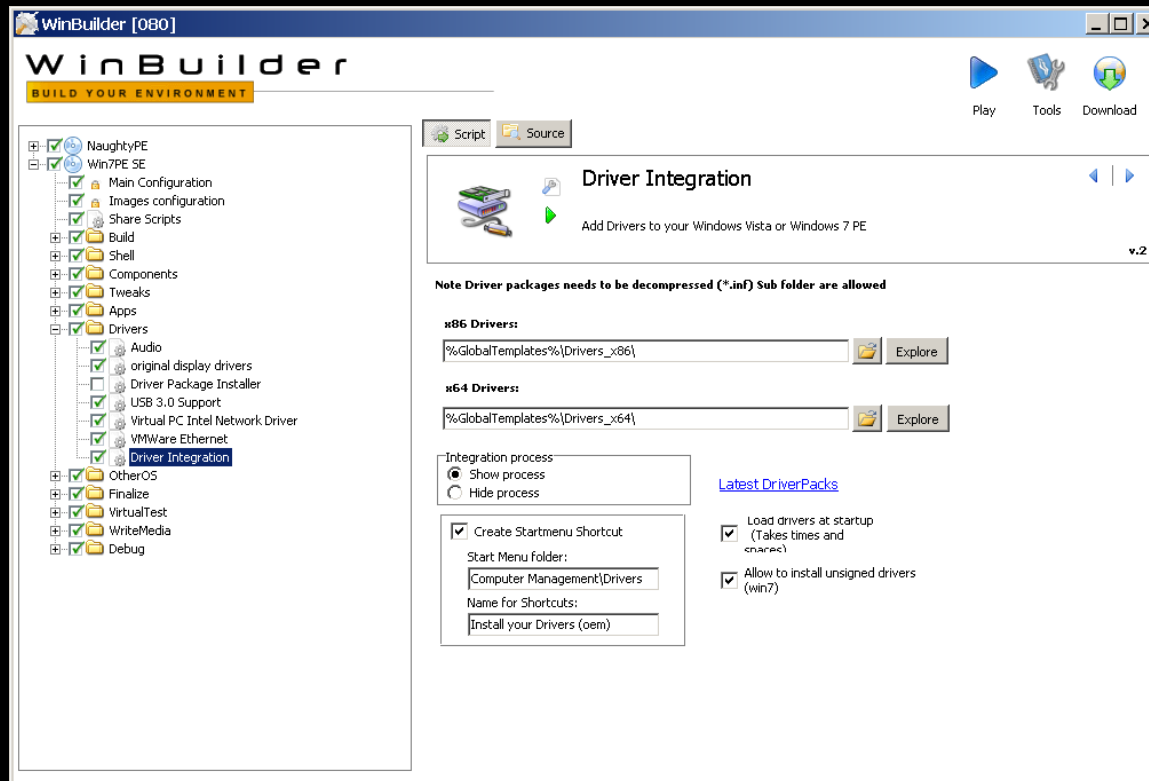
WinBuilder Scripts

▣ Best of luck



Driverpacks

- ▣ Grab some drivers
<http://driverpacks.net>

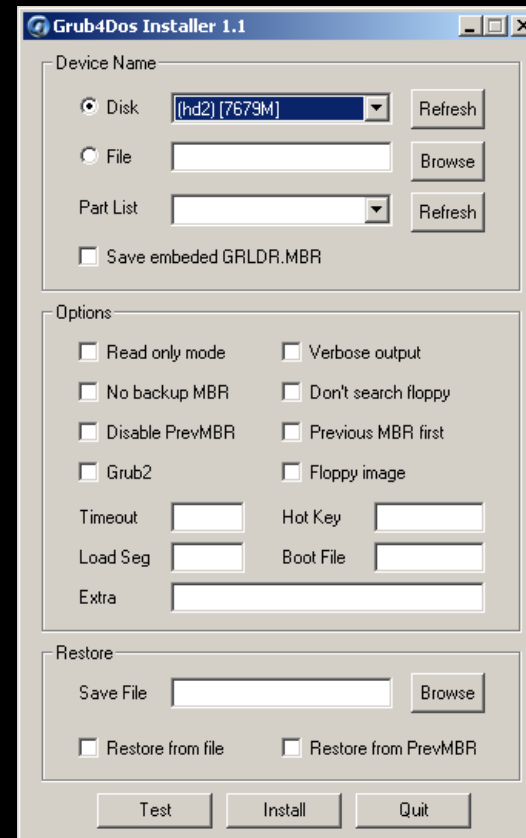
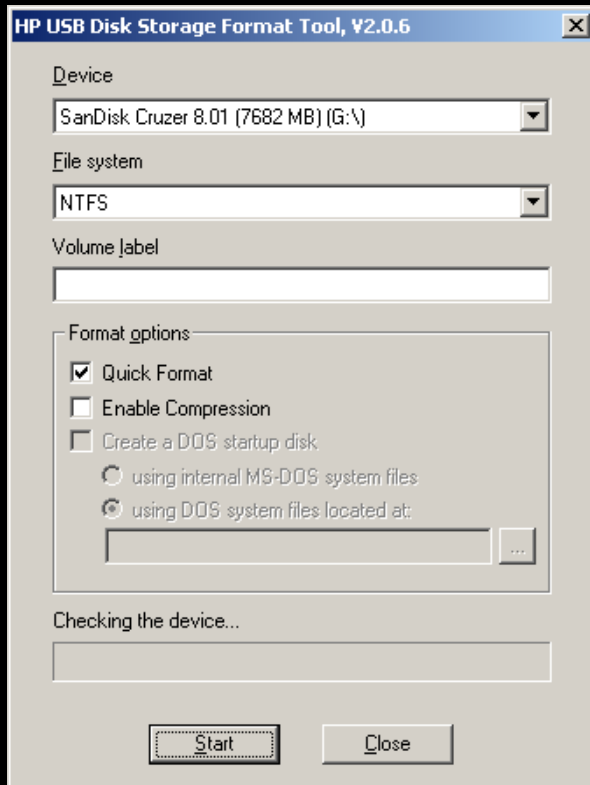


The screenshot shows the WinBuilder [080] application window. The title bar includes standard window controls and icons for Play, Tools, and Download. The main interface is divided into a left sidebar and a main content area. The sidebar contains a tree view of the build process, with 'Driver Integration' selected. The main content area is titled 'Driver Integration' and features a sub-header 'Add Drivers to your Windows Vista or Windows 7 PE'. Below this, there is a note: 'Note Driver packages needs to be decompressed (*.inf) Sub folder are allowed'. Two input fields are provided for driver paths: 'x86 Drivers' with the value '%GlobalTemplates%\Drivers_x86' and 'x64 Drivers' with the value '%GlobalTemplates%\Drivers_x64'. Each field has an 'Explore' button. There are also checkboxes for 'Integration process' (Show process selected), 'Create Startmenu Shortcut' (checked), 'Load drivers at startup' (checked), and 'Allow to install unsigned drivers' (checked). A link for 'Latest DriverPacks' is also visible.



Putting WinBuilder to a USB

▣ Using Built-in USB creator



WinBuilder/Win7PE SE

Demo/Overview



A few key tools

- ▣ Runscanner for registry redirection

<http://www.paraglidernc.com/winbuilder/Scripts/scripts.htm>

- ▣ Portable Apps

<http://portableapps.com/>

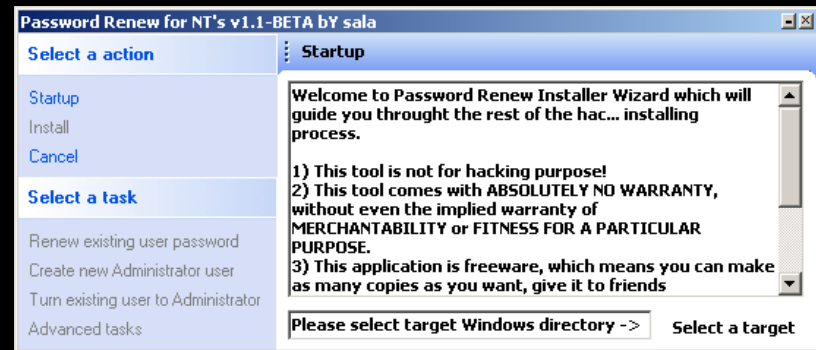
- ▣ Sala's Password Renew

<http://www.kood.org/windows-password-renew/>

<http://thuun.boot-land.net/WinBldr/XP-2K3/Projects/>

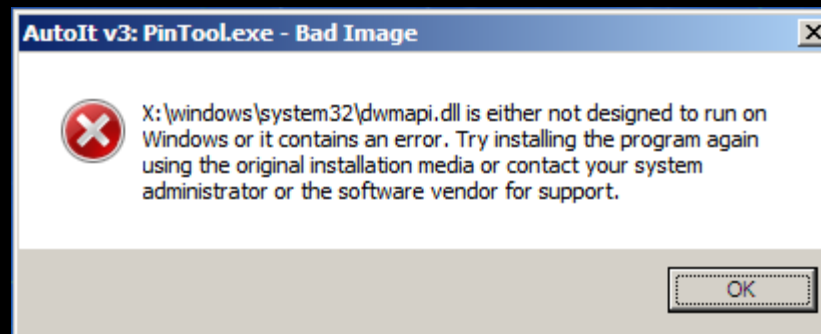
- ▣ Tons more scripts for Winbuilder can be found at

<http://reboot.pro/forum/65/>



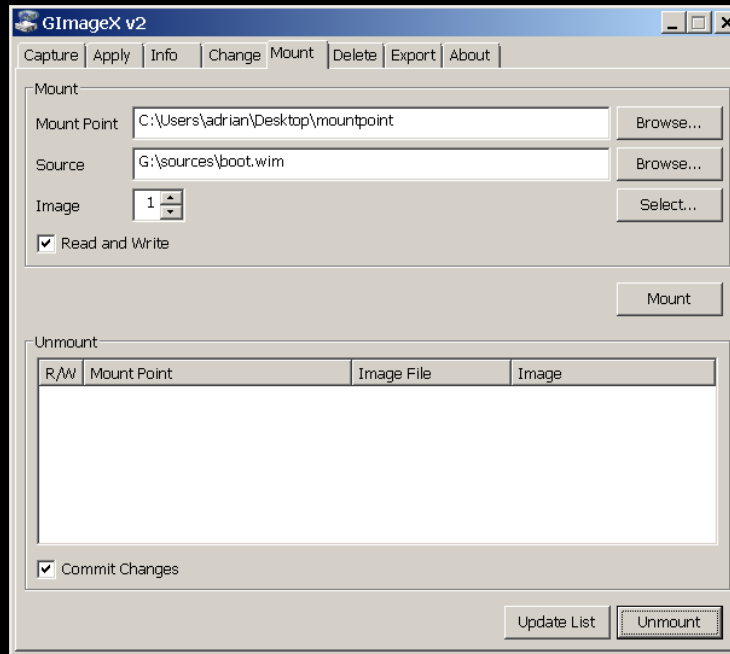
Other Winbuilder Projects

- ▣ NaughtyPE
<http://reboot.pro/3866/>
- ▣ WinFE
<http://winfe.wordpress.com/>
- ▣ Note on building FE with the wrong sources...



Edit a WMI file

- ▣ Might be easier to do than writing a script



- ▣ May have to use “subst y: f:\” or the like to get paths to match for shortcuts



Saving your WinBuilder project for later USB creation

Saving:

- ▣ Zip up all the files

Re-deploying to a new USB:

- ▣ Unzip to a new USB
- ▣ Reinstall GRUB4DOS boot loader with
<http://download.gna.org/grubutil/grubinst-1.1-bin-w32-2008-01-01.zip>

You could also make an image, but that might be
space restrictive



Multibooting

- ▣ Katana

<http://www.hackfromacave.com/katana.html>

- ▣ YUMI

<http://www.pendrivelinux.com/yumi-multiboot-usb-creator/>

- ▣ Xboot

<http://sites.google.com/site/shamurxboot/>

- ▣ SARDU

<http://www.sarducd.it/>



Katana Notes

- ▣ Bear to download, but has a bunch of ISOs already there
- ▣ May have to update yourself



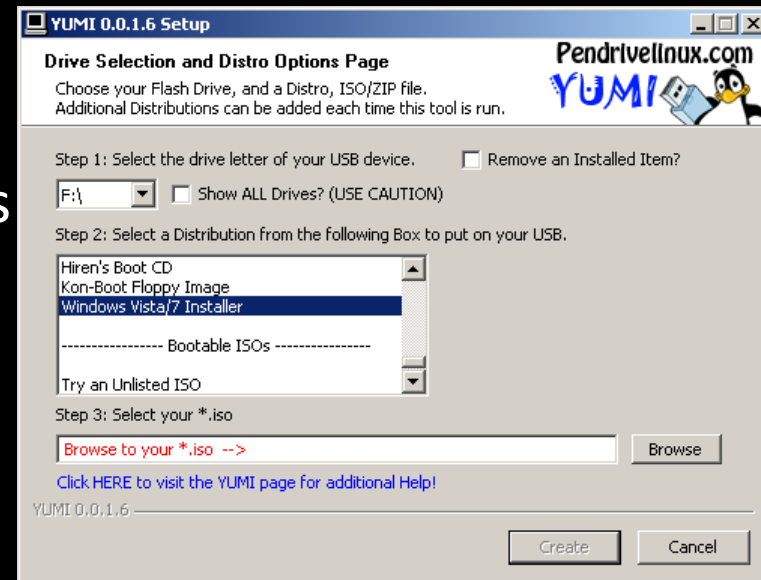
Image from <http://www.hackfromacave.com>



YUMI Notes

ver. 0.0.1.6

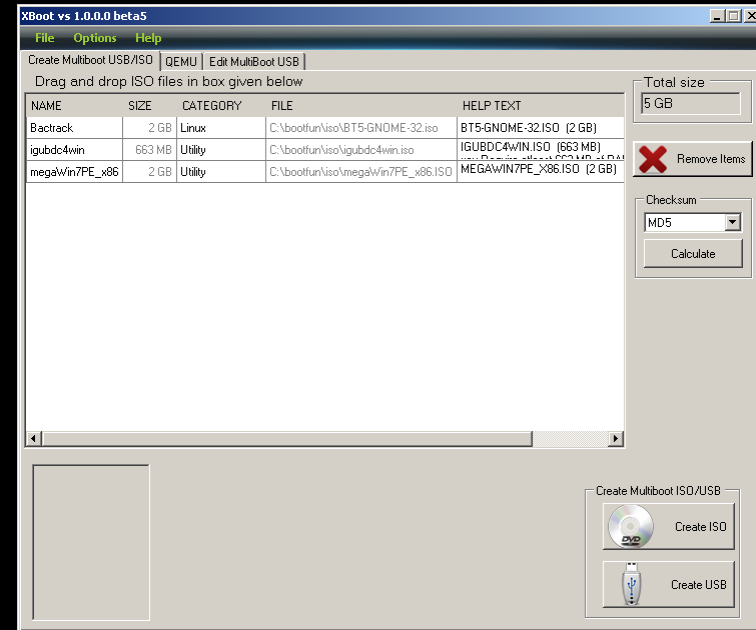
- ▣ WinBuilder from ISO with “Windows 7/Vista Installer” works fine
- ▣ UBCD4Win from ISO fails/Bluescreens/locks up/reboots
 - Windows 7/Vista Installer
 - Try an Unlisted ISO
 - Try an Unlisted ISO (from memory)
- ▣ Backtrack sometimes works, sometime fails



XBOOT Notes

ver. 1.0.0.0 beta 6

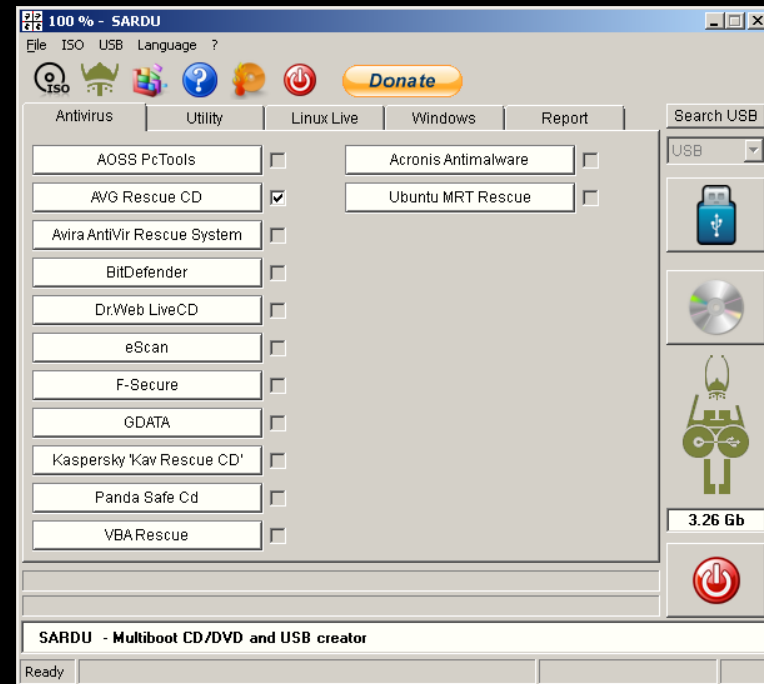
- ❑ Create ISO or UFD
- ❑ Look at ErrorLog(CreateISO).txt
- ❑ Edit category
- ❑ Rename Bactrack to Backtrack
- ❑ From USB:
 - WinBuilder from ISO with “Windows 7/Vista Installer” works fine
 - UBCD4Win with (PE, MSDART, ERD (Windows XP Only)) copies to memory but seems to work
 - Backtrack fails to pass 2nd boot menu
- ❑ From ISO:
 - Had to use VMWare to emulate the DVD from the ISO, Burned both a DVD-R and a DVD+RW and neither worked
 - Same results as USB above in VM



SARDU Notes

ver. 2.0.3 beta 5

- ❑ Create ISO or UFD
- ❑ Auto-download, like some others
- ❑ Having to give the ISOs a certain name suck
- ❑ Seems to update regularly
- ❑ UFD defrag option
- ❑ From USB:
 - Had problems getting BT5 to fully load
 - UBCD4Win rebooted
 - Even Win7PE SE dies
- ❑ From ISO:
 - UBCD4Win Bluescreens 0x0000007B
 - BT5 works
 - Win7FE SE works (slowly)



Best way to dual boot Backtrack and Win7PE SE

- ▣ Install Backtrack 5 to the UFD with Unetbootin
- ▣ Copy over the Win7PE files
- ▣ Get chain.c32 from <http://www.kernel.org/pub/linux/utils/boot/syslinux/syslinux-4.04.zip> in \com32\modules
- ▣ Add something like the following to your

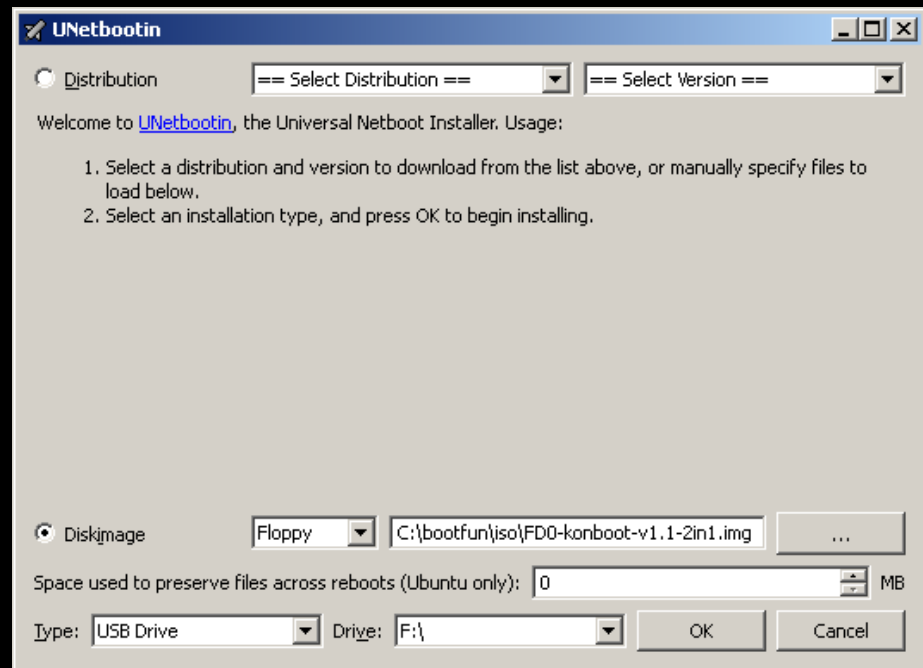
syslinux.cfg:

```
LABEL WinPE via Grub  
COM32 /chain.c32  
APPEND ntldr=/grldr
```



Putting Konboot on a USB

- ▣ Details at <http://www.irongeek.com/i.php?page=security/kon-boot-from-usb>
- ▣ Use Unetbootin to write the floppy image to the drive
- ▣ Chain booting to HD
- ▣ Best to show you the `syslinux.cfg`



Other distros of interest

- ▣ GParted
<http://gparted.sourceforge.net/>
- ▣ WinFE (Windows Forensic Environment)
<http://winfe.wordpress.com/>
- ▣ Hiren's Boot CD
Seems to be partly pirated, Google if you care
- ▣ Ultimate Boot CD
<http://www.ultimatebootcd.com/>
- ▣ Symantec Ghost Boot Wizard



U3 Notes

- ▣ Yet to ever get an ISO on a U3 to boot
- ▣ Still useful for “read only” feature
- ▣ Grab the following tools:

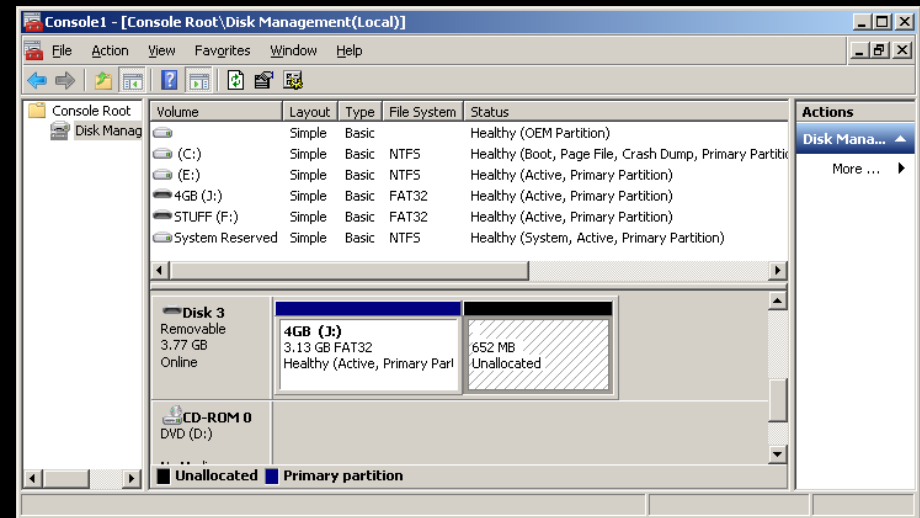
<http://u3-tool.sourceforge.net/>

<http://code.google.com/p/create-iso-file/>



Making/Loading your own U3

1. Make an ISO from a directory (ImgBurn is also an option):
`CDIMAGE.EXE -IU3 -nt -h nirsoft_package_1.11.09 myU3.iso`
2. See u3-tool options by running it without parameters.
3. See information about thumb drive K: (or whatever)
`u3-tool.exe -i k`
4. Find the size of your ISO:
`dir myU3.iso`
5. Repartition:
`u3-tool.exe -p 14655488 k`
6. Load ISO:
`u3-tool.exe -l myU3.iso k`
7. If you have issues getting rid of partitions, use Linux instead of Windows drive tools



More resources

- ▣ My guide and files for Konboot from a USB:
<http://www.irongeek.com/i.php?page=security/kon-boot-from-usb>
- ▣ Pen Drive Linux
<http://www.pendrivelinux.com>
- ▣ Reboot Pro (change the default skin)
<http://reboot.pro>
- ▣ My dated Pebuilder tutorial
<http://www.irongeek.com/i.php?page=security/pebuildertutorial>
- ▣ Live CD List
http://www.livecdlist.com/?order=field_lastrelease_value&sort=desc
- ▣ Linux Live scripts
<http://www.linux-live.org>
- ▣ USB Flash Drive Speed Tests
<http://usbspeed.nirsoft.net/>



Booting Demos

- ▣ Not sure if there will be time...



Thanks

- ▣ ISSA Kentuckiana for having me
- ▣ By buddies from Derbycon and the ISDPodcast



Events

- ▣ DerbyCon 2011, Louisville Ky
Sept 30 - Oct 2
<http://derbycon.com/>
- ▣ Louisville Infosec
<http://www.louisvilleinfosec.com/>
- ▣ Other Cons:
<http://www.skydogcon.com/>
<http://www.dojocon.org/>
<http://www.hack3rcon.org/>
<http://phreaknic.info>
<http://notacon.org/>
<http://www.outerz0ne.org/>



QUESTIONS?

42

