# Welcome to Anubis-Linux (v.2)

**– a programming/networking/security -oriented remastered version of SimplyMEPIS –**

A gentle introduction to Linux for (ex-)Windows® users.

# DISCLAIMER/LICENSE

Anubis-Linux is a distribution based on SimplyMEPIS. Being a remaster means that MEPIS LLC doesn't support it and its development in any way. The original MEPIS License and documentation are preserved in docs.MEPIS.zip and info.MEPIS.zip for informational purposes.

Anubis-Linux contains cryptographic software that is forbidden under U.S. law to be exported to and used in certain countries. Please inform yourself on the matters particular to the region where you live in.

Anubis-Linux is provided AS-IS. No guarantees, and no warranties whatsoever (expressed or implied) are given regarding Anubis-Linux's correct functioning or fitness for a particular purpose. The authors of Anubis-Linux shall not be held liable in case of any kind of damage whatsoever (i.e. data loss) induced or caused by the use of Anubis-Linux. This is experimental software. You use Anubis-Linux at your own risk.

By installing, running or otherwise using Anubis-Linux, you must understand, agree to and comply with the above terms. Otherwise do not use Anubis-Linux.

The documentation and software in Anubis-Linux are freely redistributable but licensed varyingly. Please check their individual licenses for more information.



Anubis-Linux technical help discussions are supported by volunteers over at:

MEPISLovers.org Forums and

AnLin-Jackal Forums.

**END OF DISCLAIMER/LICENSE.**

## 01. New Style

I hope you'll get accustomed to the extra buttons on the app's titlebars, feel free to experiment.

A neat thing beside "shade" and "keep on top" is that you can modify the style yourself by right-clicking on the titlebar and selecting Configure Window Behavior or the Control Center in the K Start Menu.

Also, you don't have to always move the window from the titlebar, keep *Alt* depressed and you can click and drag a given app window from anywhere. Fast and comfortable, but it'll take getting used to – so try it. You also have multiple desktops, see the 4-part thing in the taskbar? You can even set to have more than 4 desktops, if you wish.

## 02. Important Keyboard Shortcuts

| key stroke | function / effect |
|---|---|
| Ctrl + Esc | Process Table (like Win's Task Manager) |
| Ctrl + Alt + Esc | mouse pointer of death |
| Ctrl + Alt + Del<br>Ctrl + Alt + Shift + Del | almost the same as Ctrl + Alt + Del in Win |
| Ctrl + F1 … F12 | fast switch to desktop 1 … 12 |
| Alt + F1 | K Start Menu |
| Alt + F2 | run command (I use this a lot) |
| Alt + F3 | app context menu |
| Alt + F4 | close app |
| Ctrl + C | send "kill" to console app |
| Ctrl + D | send "end input" to console app |

## 03. BASH (Bourne Again SHell)

Knowing how to use BASH will raise your Linux experience to a whole new level.

I also wrote a fast tutorial on it, it's a text file in Linux docs section. Or, you could read the big book on BASH, also there.

Bottom line, BASH will also teach you the basic inner workings of your Linux, so if you want to work in more advanced areas, such as LiveCD remastering, you can't do it without knowing how to use the shell. Not to mention, some commands don't have immediate "click-button" correspondent. It is easy to back up your original MBR from the shell, by using the dd command (raw copy utility). Read more about it in the Linux documentation section and the built-in BASH introduction.

## 04. Fast Facts about Linux/MEPIS/AL

- in Linux, case matters. "ABC", "Abc" and "aBc" are all different files/directories/commands. the filesystem also allows you to use some symbols in the filename that you can't use under Win. and then there's something called hardlinking which again you can't do under Windows becau..... whoops got carried away. see above *03.* if you want to know more.
- another nice thing about Linux: if a file doesn't have an extension, it will try to automatically detect its type. you can try this by *clearing* the extension for an image file, or PDF.
- Linux doesn't use drives. everything is "seen" as a file. so how do you access the contents of a "drive"? – you mount it. see Kwikdisk app (lower right taskbar), or KDE Help Center, or my BASH tutorial. after mounting with Kwikdisk, use Konqueror or Krusader to move around.
- in Linux, you will install software through packages (or by compiling it). you will normally use Synaptic for downloading & installing packages. for local packages you will use KPackage (unless you become fond of BASH, and then you'll use apt-get and dpkg).
- the Clipboard function in KDE is slightly smarter than the one in Win. a short history of the contents is saved, see app Klipper (lower right taskbar again). also, you only need to select the text, and it'll automatically be copied.
- what sets *MEPIS* apart from other distros are its MEPIS Assistants (see K Menu → System). for instance, repairing a damaged bootloader, or installing nVIDIA/ATi video card drivers is a fairly easy task, using the Assistants.

  **NOTE: for this version of AL, the Mepis tools may not work correctly, sorry.**
- KDE can install and use Windows fonts. this has a dramatic impact on your surfing experience. see: K Menu → Control Center → System Administration → Font Installer
- Windows® will never be able to run Linux apps natively. fortunately, Linux can run most Win apps. *Anubis-Linux* comes with Wine, which will allow you to install and use your favorite softwares (IrfanView, Winamp, 7-Zip FM, WinRAR, etc.), most games will work too (I tested Counter-Strike 1.6, worked fine).
- *AL* comes with the famed Tor/Privoxy combo which can enhance your anonymity on the Internet. a fast explanation: Tor is a SOCKS proxy and can't be used directly. Privoxy is set to use Tor, and finally your browser is set to use Privoxy. In Firefox, go to: Edit → Preferences → Advanced → Network → Settings, choose Manual Proxy Configuration and fill in the fields with IP **127.0.0.1**, port **8118**. be advised, loading times will be lengthened. but the better anonymity is well worth it. you should also try out Konqueror, which is in some respects superior to Firefox. for instance, it can be set to not send a User ID string; and can split up the window, etc. It can also make use of Tor/Privoxy of course. please use Vidalia to start/stop Tor.
- the Guarddog firewall is by default configured very aggressively. it will allow DNS, HTTP, HTTPS, FTP and that's about it. no miscellaneous network protocols, no instant messaging, etc. to change this, start Guarddog and set it up to your liking.
- the SELinux and Snort systems are activated by default. they *may* affect your online experience to some degree. if you have any questions or problems, visit our forums and post.

## 05. CD-added content

I wanted to make *Anubis-Linux* a base distribution for those interested to study programming and networking, amongst other things. Feel free to explore around the documentation, and don't forget about the Experts Guide. The apps added were in my opinion important and left out in the plain-vanilla *MEPIS*:(some of these will need to be run in a shell with wine – marked with *)

| category/application | description |
|---|---|
| Programming | tools to help you code your own programs |
| GNU C++ Compiler (g++) | GCC's brother |
| Code::Blocks (codeblocks) | an elegant IDE for C/C++ programmers |
| Dev-C++ | same as above, but compiles Win32 executables |
| Sphinx C-- Compiler* | Russian-made C-- compiler (C-- is a hybrid between C and ASM, its name parodies C++) |
| Netwide Assembler (nasm) | a great assembler |
| Flat Assembler (fasm) | same as above |
| High Level Assembler (hla) | assembler for HLA (High Level Assembly, a newer language, improving on ASM) |
| Yasm Modular Assembler (yasm, tasm, …) | a great NASM rewrite |
| BCC, AS86 and LD86 | C compiler, assembler and linker for the venerable Intel 80x86 CPU series |
| flawfinder | helps find security problems in C/C++ source |
| Experts Guide | both as Win32 with GUI and Linux console app, this utility can help you (learn) a lot. |
| POSIX Manuals | invaluable collection of MANuals for any system programmer |
| Anti-programming (joke) | tools to help you analyze executables |
| KHexEdit | KDE's own hexeditor |
| KDebugger (kdbg and gdb) | KDE's own debugger, based on GDB |
| OllyDbg | the famed shareware Win32 debugger |
| hte | "professional file viewer/editor/analyzator" |
| NTCore Explorer Suite | valuable tools for Win32 executable analysis |
| Networking | various tools |
| Wireshark, tshark, tcpdump | network traffic analysis tools (sniffers) |
| Wicd | replacement for KNetworkManager, some report it works better |
| PuTTY | Telnet/SSH/Rlogin connections program |
| Tor/Privoxy | better anonymity protection on the Internet |

| Networking *(continued)* | various tools |
|---|---|
| rkhunter/chkrootkit/unhide/lynis/ Navale/KSystemLog | security auditing tools |
| Vidalia/TorK | Tor configuration utilities |
| harden-nids (snort) | Network Intrusion Detection System (remember to run *dpkg-reconfigure snort*) |
| hunt/packit/PackEth | penetration testing tools |
| KNmap | KDE's own Nmap GUI program |
| OS work | manage your own operating systems |
| SYSLINUX | package for bootable media creation |
| qemu + qemulator | package for OS testing in a virtual machine (i.e. from inside another OS) and its GUI frontend |
| chntpw/Ophcrack | WinNT SAM database editors |
| Miscellaneous | various useful utils |
| Midnight Commander (mc) | Norton Commander® clone for Linux |
| Krusader | Total Commander® clone for Linux |
| KCHMViewer | KDE's own CHM Help file viewer |
| UHARC* (included for fun) | Uwe Herklotz's famed high compression archiver (and deserves) |
| 7-Zip Archiver (7zFM.exe) | Win32 version of 7-Zip, included because everyone loves a GUI |
| SMXI-family scripts | powerful scripts for system configuration, see http://www.smxi.org |
| CSFP Anubis-Linux Edition | my very own "secure password" (re)generators |
| OpenGL/SDL/Fmod/Allegro libraries | for game programmers |

With all these tools and docs, you could now do interesting things; such as make Linux FASM recompile itself for AMD64 (if AMD64 is what you're running on now, otherwise it'd be pointless). Or maybe write bootloaders, or even BIOS firmware. Or spy on people using the same networks as you. Heh, heh.

Some things had to be uninstalled; if you need them, nobody stops you from remastering AL. It's quite easy, all you need to do is read the BASH and Remastering docs. Then you can add OpenOffice to your own LiveDVD edition of AL.

Also, for some apps such as *FASMW* and *EG*, you should change the display font. Courier is my personal choice.

## 06. Several Notes On Security

Please bare in mind that *Anubis-Linux* incorporates a large amount of **unstable** and **insecure** software. In other words – software that has not yet been thoroughly tested against security flaws. Malicious individuals could discover flaws in the software and use it to gain control over your computer.

You could ask: why not just stick to the **stable**, tested and secure versions instead? Answer is: progress. Newer, better, and with more features. Newer kernel, newer filesystems, newer base apps. After all, *AL* is not designed as a home operating system, it's mainly about teaching you to code and use Linux more efficiently, so that you will eventually be able to do those "advanced" geeky things by *yourself*. A bit like the *Linux From Scratch* project but less Spartan, in my opinion. And then – a lot of effort has been put into making *AL* as secure as possible even *with* its inherently insecure software packages.

Since we got that sorted, I'd now like to speak about Internet usage and how can *AL* provide good online security. Some of these programs can only be run as root user. Use either kdesu as precedent in the Run Command address bar, or start the Konsole and login with su.

- Snort is an IDS (Intrusion Detection System) – you must reconfigure it with

  *dpkg-reconfigure snort*

  and then document yourself on how it's used best (see Section 4 of the AL Docs)

- Guarddog is a firewall which uses iptables in the background. once you become familiar with iptables (read the ***Iptables Tutorial*** in Section 3) you may want to start using it directly. or maybe not heh, heh

- Guidedog is a tool used to masquerade IP addresses through the router. I have personally never used it to this time, but it should come in handy for those using a router

- macchanger will change the MAC address of your network interface to the desired value.

- Privoxy is **more** than just a way to connect to the Tor network. it is a very efficient web-filtering program, which can block ads and known malicious sites, modify the referrer header, hostname, and so on.

  if you want Privoxy to function simply as a content filter, feel free to edit the file:

  */etc/privoxy/config*

  removing or commenting the line (this will make Privoxy to stop "asking" Tor for data):

  *forward-socks4a / 127.0.0.1:9050 .*

  you will still have to connect to Privoxy by local IP **127.0.0.1**, port **8118** – after restarting it:

  *# /etc/init.d/privoxy restart*

- The Onion Router network... aka Tor. what is it and how does it work? it's a worldwide network of computers, of which you are a client for as long as you have Internet connection and the Tor daemon is running (start, stop or restart via */etc/init.d/tor*). *relay nodes* route the traffic along. the special "exit nodes" are the ones which finally contact the outside Internet, i.e. your destination website. you can configure the Tor daemon to run from your PC as an *exit node* if you wish – but you might want to inform yourself on the possible legal issues beforehand.

anyway, *relay nodes* exchange encrypted HTTPS traffic (port **443**). that means other *relay nodes* won't know what you're transmitting towards the *exit node*. but the *exit node* does! so if you're using Tor to log into a forum, for example (and they usually don't encrypt the login such as let's say Email providers) the *exit node* will possibly know your login details, and where they fit. but it won't know your IP. you can read more about Tor in the AL Docs, Section 4.

in the end – using Tor is much like using a highly anonymous proxy server (as far as the Internet is concerned) which doesn't have any information on you (except that what it's carrying out to the Internet on your behalf) – and that server's world location changes all the time (unless you force otherwise). a list of the *exit nodes* is maintained though – so it's possible for someone to figure out you're behind Tor – but less likely that they find out exactly who you are.

finally, some sites can bypass proxies and even Tor; that's because they use active content (for example flash media) which when run, can establish connections themselves and won't care about what proxy you've set in your browser, which leads us to the next point:

- never disable NoScript in Firefox, and remember to use the Scroogle SSL search engine. those intercepting your network traffic (including your ISP) will or *should* have a hard time figuring out what you search for, and Google™ will or *should* have a hard time profiling you. it's said that they will log your search *and* IP for 1.5 years!
- iptstate and netstat are small but efficient utilities to keep track of the current network connections. netstat will also list ports open by daemons – even though these may be blocked by the Guarddog/iptables firewall anyway. NetActView AL Edition (Navale) is a powerful GUI version of netstat, its author says.
- tshark, tcpdump and Wireshark are *sniffers* and go a step further – they capture and dissect the traffic to offer great detail of what's happening. alas they require advanced networking knowledge in order to be truly useful. (see part 07 for suggested books.)
- you can run dmesg, last, lastb to display kernel, logins and bad logins respectively.
- KSystemLog and fwlogwatch (console app) are more specialised than the above.
- csfp1 and csfp2 can be used as password re-generators. feel free to edit the source code and recompile it to better suit your needs. they can currently create strong passwords which have a length of up to 128 characters (or even 2048 in version 2). as re-generators, they can take the "password crafting data" from standard input (max 128 bytes) or a file (unlimited length). with most secure password generators, you end up having to store the password – breaking that tradition is the goal of CSFP!
- Darik's Boot And Nuke aka DBAN is available on the LiveCD. it allows for secure erasure of your hard disk's data. otherwise, skilled individuals using the right software can recover your supposedly erased data – which is sometimes undesirable.
- beware of Flash (tracking) cookies, they will be stored as SOL files in your ~/.macromedia folder. as the browsers do not automatically clean this folder, it is advised that you do it yourself. these cookies can potentially render any IP spoofing technique ineffective.
- Vidalia should be used to start, stop and configure Tor. TorK disabled the firewall during tests!

Feel free to check out the designated documentation in Section 4 – books such as ***CINSS*** and ***Advanced IDS T. with Snort*** are of great importance. ***Buffer Overflow***, ***Smashing the Stack*** and ***Secure Progs*** (Section 3) are good if you want to become a *respectable* systems programmer.

## 07. Check These Out!

All the documentation hereby provided is freely redistributable.

But there are some major books, that you should really check out. Who knows, maybe by the time you read this, they were already re-released under the GNU Free Documentation License, or, I mean and made available to freely download. All these books are for after you've already learned the basics – well with the exception of the first two.

| book | author |
|---|---|
| How Linux Works | Brian Ward |
| Computer Networks | Andrew Tanenbaum |
| Maximum Security | Mark Taber |
| Hardening Linux | James Turnbull |
| Applied Cryptography | Bruce Schneier |
| Hacknotes: LUPSR | Nitesh Dhanjani |

Thinking in C++ (1) and Advanced Linux Programming (2) would've been in the list too, but apparently they're free at this time. And, don't forget about the MEPIS User's Manual, it's a must-read.

(1) Mr. Eckel was kind enough to give me permission to redistribute the TIC volumes and the source code within *Anubis-Linux*, unmodified and solely for educational purposes.

(2) The included PDF has the wrong copyright information. Please see

http://www.advancedlinuxprogramming.com/errata.html

for detailed information.

Have fun using *Anubis-Linux*, I hope you'll find it useful!

## Addendum: Common Problems

- take care to edit out Standby and Suspend to … settings from KPowersave, as some computers stop responding trying to suspend. (this was already done by default but left in as a warning.)
- Wine will not start Win32 executables marked as executable. unmark them by accessing the file properties sheet, or right-click and select *Run with Wine* or, even better, fix the bug then send me the fix!
- be careful when using Wine on the LiveCD especially as root; it will fill up the ramdisk with temporary files in the ~/.wine/ directory and choke your system. this can be fixed by deleting that directory, or it can be prevented by creating a symlink named .wine which points someplace where there are no space constraints, maybe a directory you make in /var/?
- FASMW cannot assemble its examples in the /ANUBIS/ folder – this happens because the filesystem is read-only, you must move the examples to a writable directory, such as your home directory