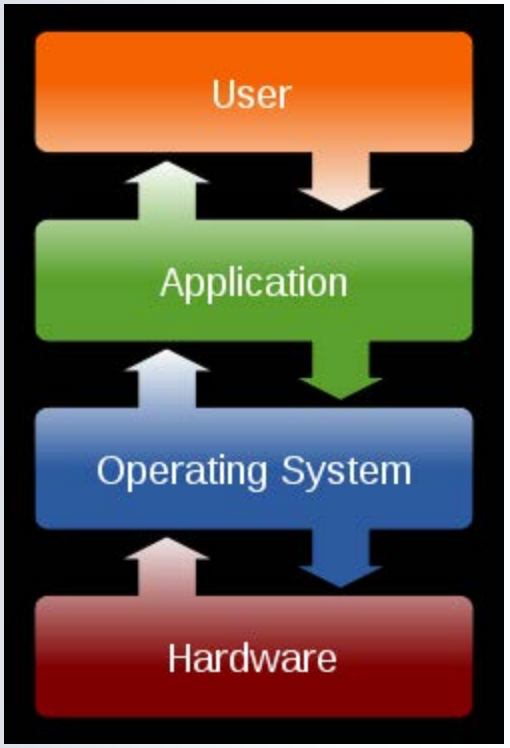
COMP 175

System Administration and Security



OPERATING SYSTEM OVERVIEW

Operating System

- An Operating System controls (manages) hardware and software.
  - It provides support for peripherals such as keyboard, mouse, display, disk drives, ...
  - Software applications use the OS to communicate with peripherals.
  - The OS typically manages (starts, stops, pauses, etc) applications.
  - In simple terms, an operating system is a manager.

Single vs. Multitasking

- Some operating systems can only do one thing at a time (CP/M, DOS).
- Most modern systems can support multiple applications (tasks)
- Some support multiple users (at the same time).
- Supporting multiple tasks/users means the OS must manage memory, CPU time, network interfaces, ...the available resources
- And share them, open files, connections, etc.

  with out getting confused
  - Or bad things happen

User Interface

- The User Interface is the software that supports interactions with a user (typically human).
- Some operating systems directly provide a user interface and some don't.
- Windows is an example of an Operating System that includes a user interface.
- Unix (the OS) does not directly provide a user interface. (termcap, curses libraries)
- Unix systems were typically connected to 'dumb' terminals via serial links.
  - Hence /dev/tty1 (teletype)

Dumb Terminals

Bell System Model 28 Teletype
Mechanical, All caps, 50 Baud, half duplex
Mid-1950's to late 1960's

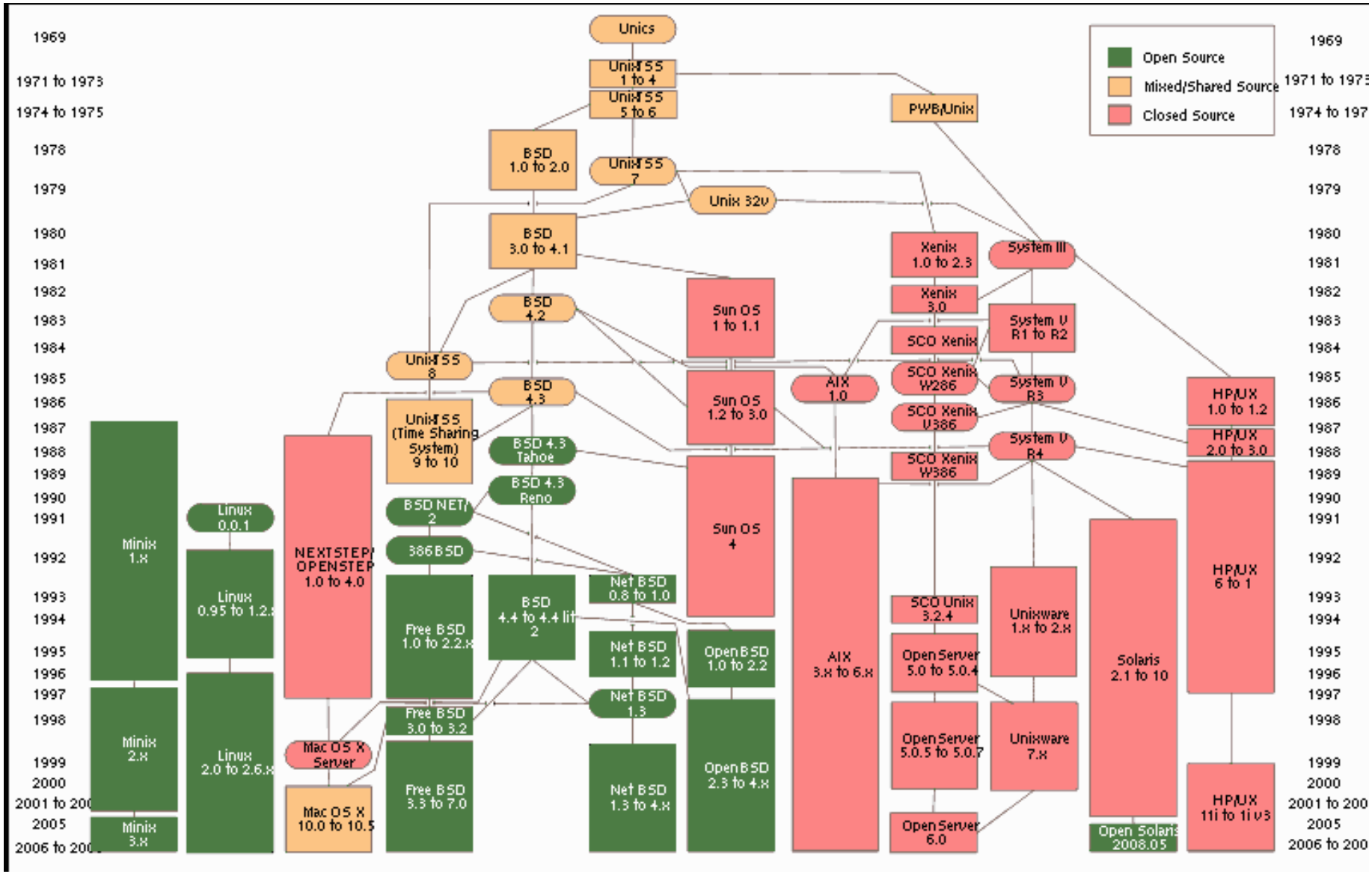
Lear Siegler ADM-3A $1195
1975 24 rows x 80 characters
Common terminal at UCB, key layout influenced key sequences still in use

DEC VT52 & VT100
1975 1978
24 rows x 80 characters
Common terminals still emulated today (Putty)

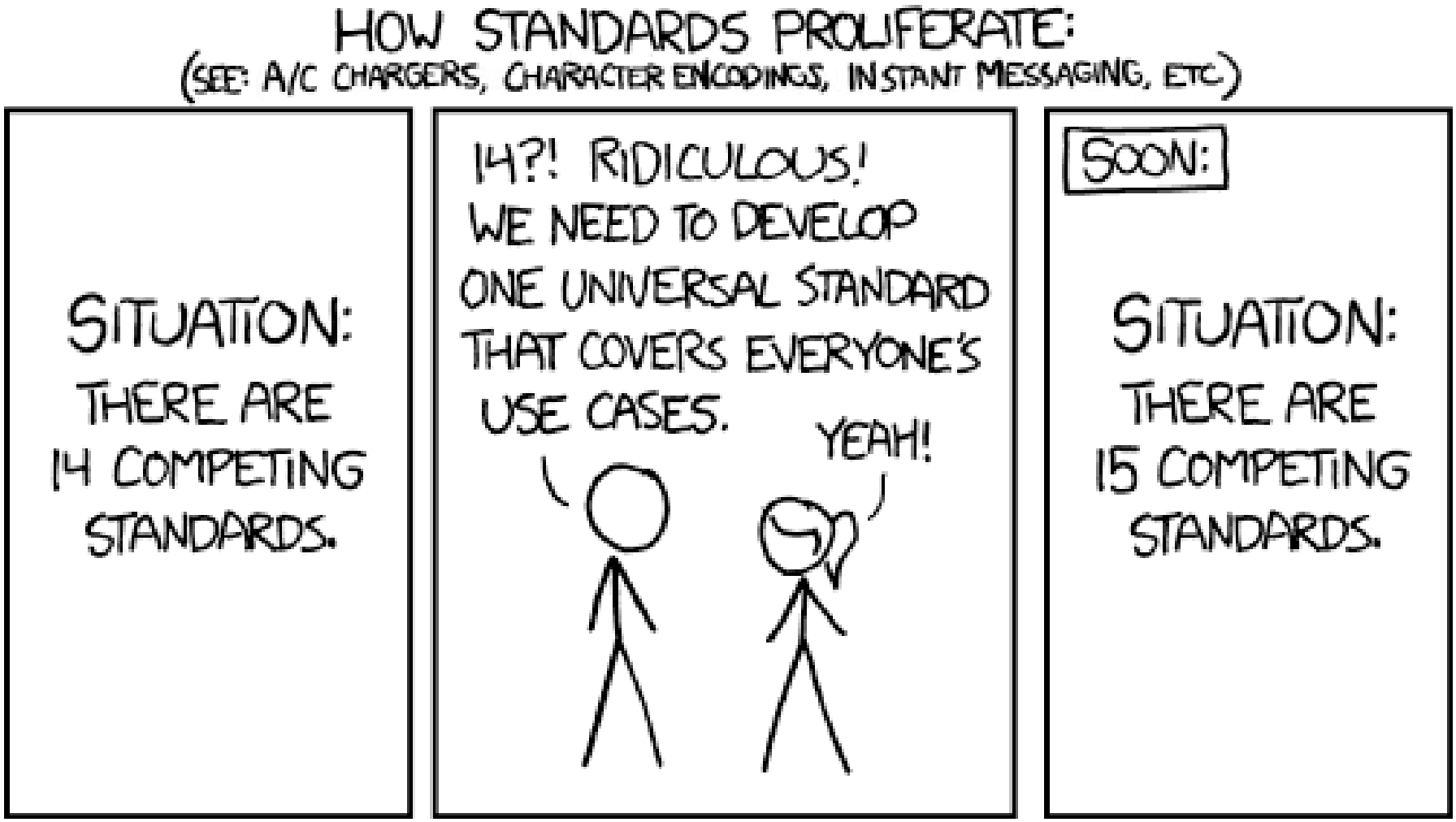
UNIX and Users

- Most flavors of UNIX provide the same set of applications to support users (commands and shells)
- Although these user interface programs are not part of the OS directly, they are standardized enough that learning your way around one flavor of Unix is enough
- SysV (from AT&T)
- BSD (from Berkeley)
- Solaris (Sun)
- IRIX (SGI)
- AIX (IBM)
- HP/UX (HP)
- LINUX (many distros)

UNIX Family Tree



Distros

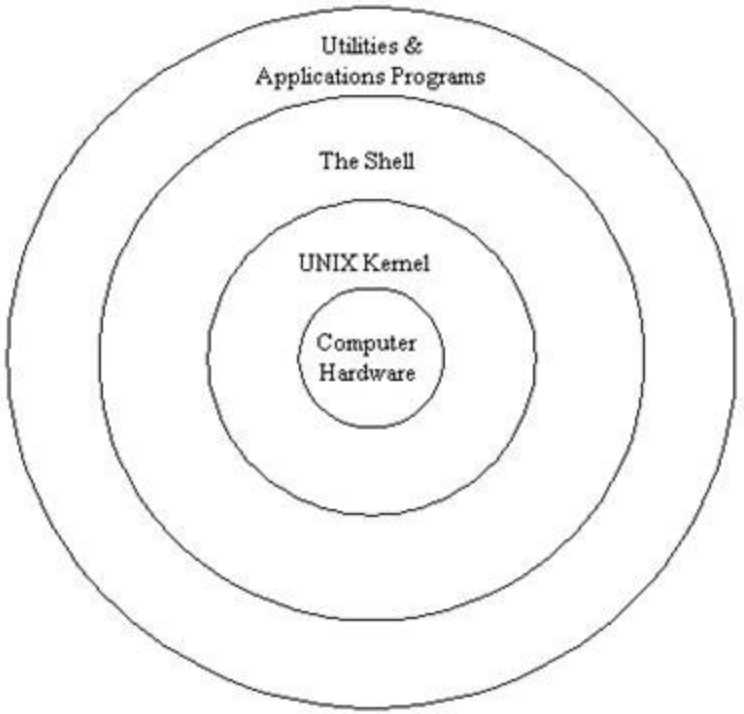

HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

UNIX Features

- Large number of applications available for UNIX operating systems, ranging from commercial applications such as CAD, Maya, WordPerfect, to many free apps, compilers and interpreters.
- Less Resource Intensive - in general, most UNIX installations tend to be much less demanding on system resources.
- **Internet Development - Much of the Internet backbone is run on UNIX servers.**
  - **BIND – DNS**
  - **Apache web server**

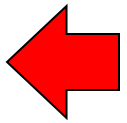
Parts of the UNIX OS

- The Kernel
- The Shell and Graphical User Interface(s) GUI
- Built-in System Utilities
- Application Software and Utilities



Operating System Concepts

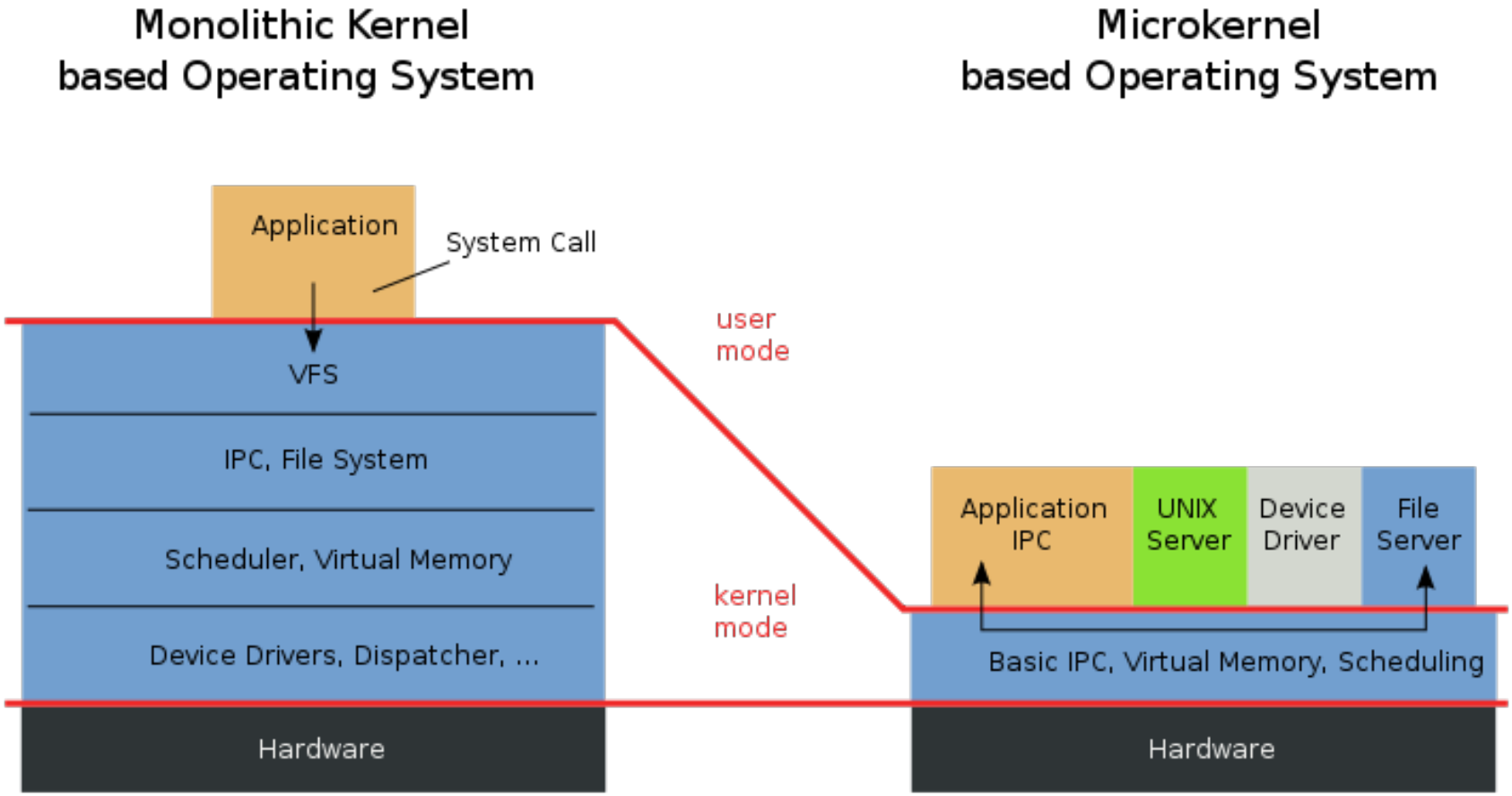
- UNIX systems refer to the Operating System's core component as the kernel.
  - A UNIX kernel handles the interaction with the system hardware.
  - The UNIX kernel is specific to a particular computer or group of computers that share a common hardware design.
  - UNIX kernels are built around one of two designs:
    - single, monolithic kernel or
    - micro-kernel



Operating System Concepts

- The monolithic design is older and uses a single binary image to provide the resource management and hardware interface functions of the core layer. Some examples of the monolithic design are Linux and Solaris.
- A micro-kernel design uses a very small task management component and a suite of modules for all other resource management functions. Windows NT, Windows XP, 8, etc. and Mac OS X are examples of micro-kernel designs.

Monolithic vs Microkernel

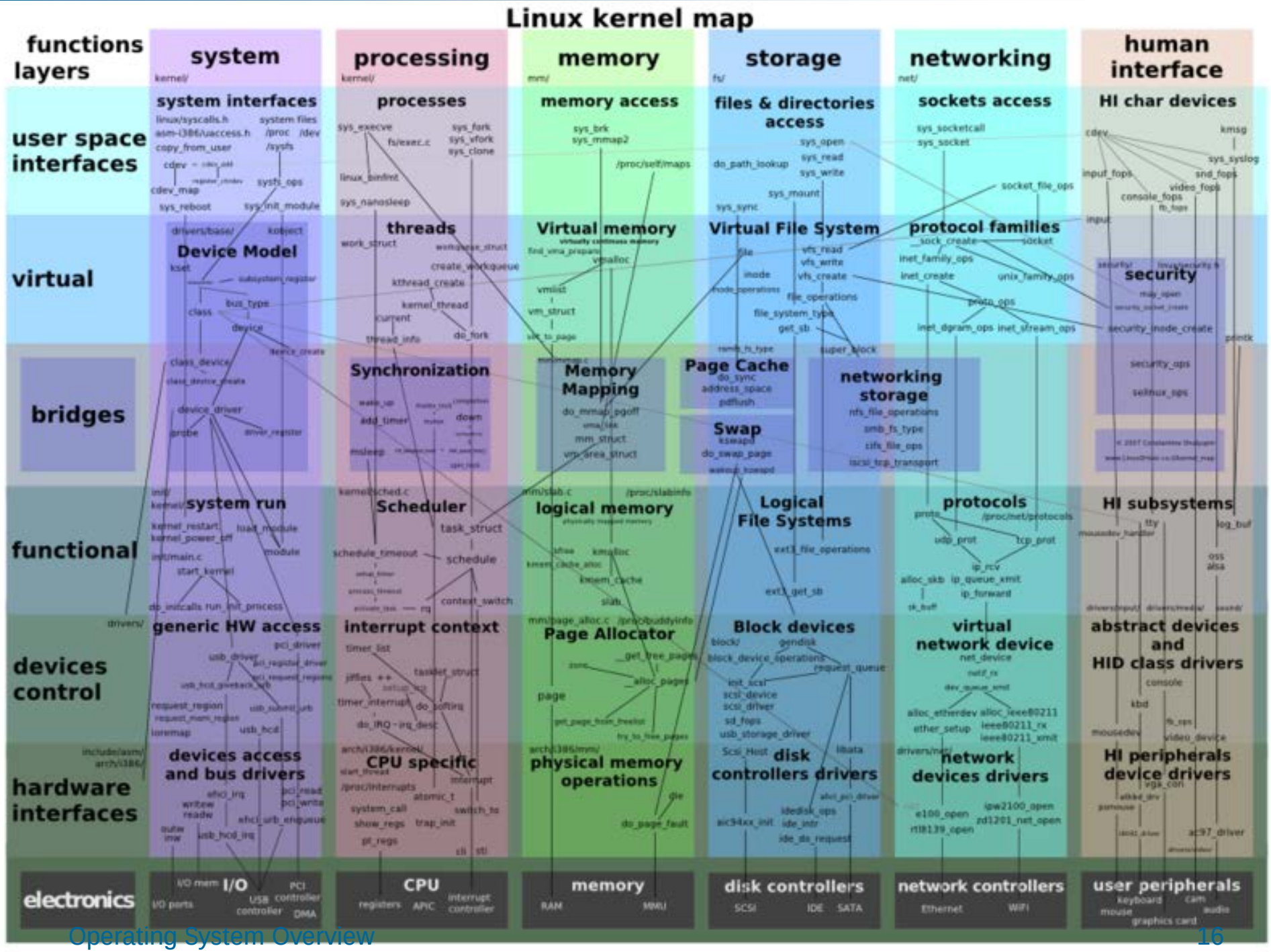


Loadable Modules

- Today's monolithic kernels use loadable modules to extend the running kernel – such as by supporting a device
- Alternative would be to recompile the kernel
- Changes to the kernel are a security issue
- Linux and Solaris have monolithic kernel designs that include loadable modules

Kernel

- The Kernel - handles memory management, input and output requests for data/file access, and program scheduling. It provides the basic software connection to the hardware, and enforces security.
- Technically speaking, the kernel is the OS.
- Device drivers and kernel extensions run in kernel space (ring 0 in many CPU architectures), with full access to the hardware, although some exceptions run in user space.


Linux kernel map
functions layers
system
processing
memory
storage
networking
human interface
user space interfaces
virtual
bridges
functional
devices control
hardware interfaces
electronics
system interfaces
processes
memory access
files & directories access
sockets access
HI char devices
Device Model
threads
Virtual memory
Virtual File System
protocol families
security
Synchronization
Memory Mapping
Page Cache
networking storage
Swap
system run
Scheduler
logical memory
Logical File Systems
protocols
HI subsystems
generic HW access
interrupt context
Page Allocator
Block devices
virtual network device
abstract devices and HID class drivers
devices access and bus drivers
CPU specific
physical memory operations
disk controllers drivers
network devices drivers
HI peripherals device drivers
I/O
CPU
memory
disk controllers
network controllers
user peripherals

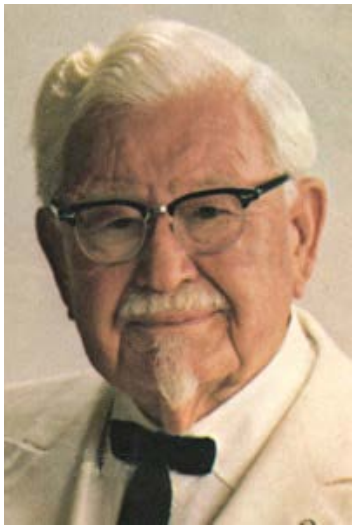
Other Popular Kernels

- Popcorn kernels

- Kernel of a matrix
  - also called the null space

$$\mathrm{Ker}(\mathbf{A}) = \{\mathbf{x} \in \mathbf{R}^n : \mathbf{Ax} = \mathbf{0}\},$$

- Colonel Saunders



Kernel Security

- Security breach at kernel.org - discovered Aug. 28 2011
- Intruders gained root via compromised user credential
  - Multiple servers compromised
  - ssh files modified and running live
  - Trojan startup file added to startup scripts
- Recovery Process
  - Take servers offline - still down 9.12.2011
  - Complete reinstalls from known clean - test
  - Complete reinstall – all systems - test
  - Review code repository
  - Notify authorities and community of the breech

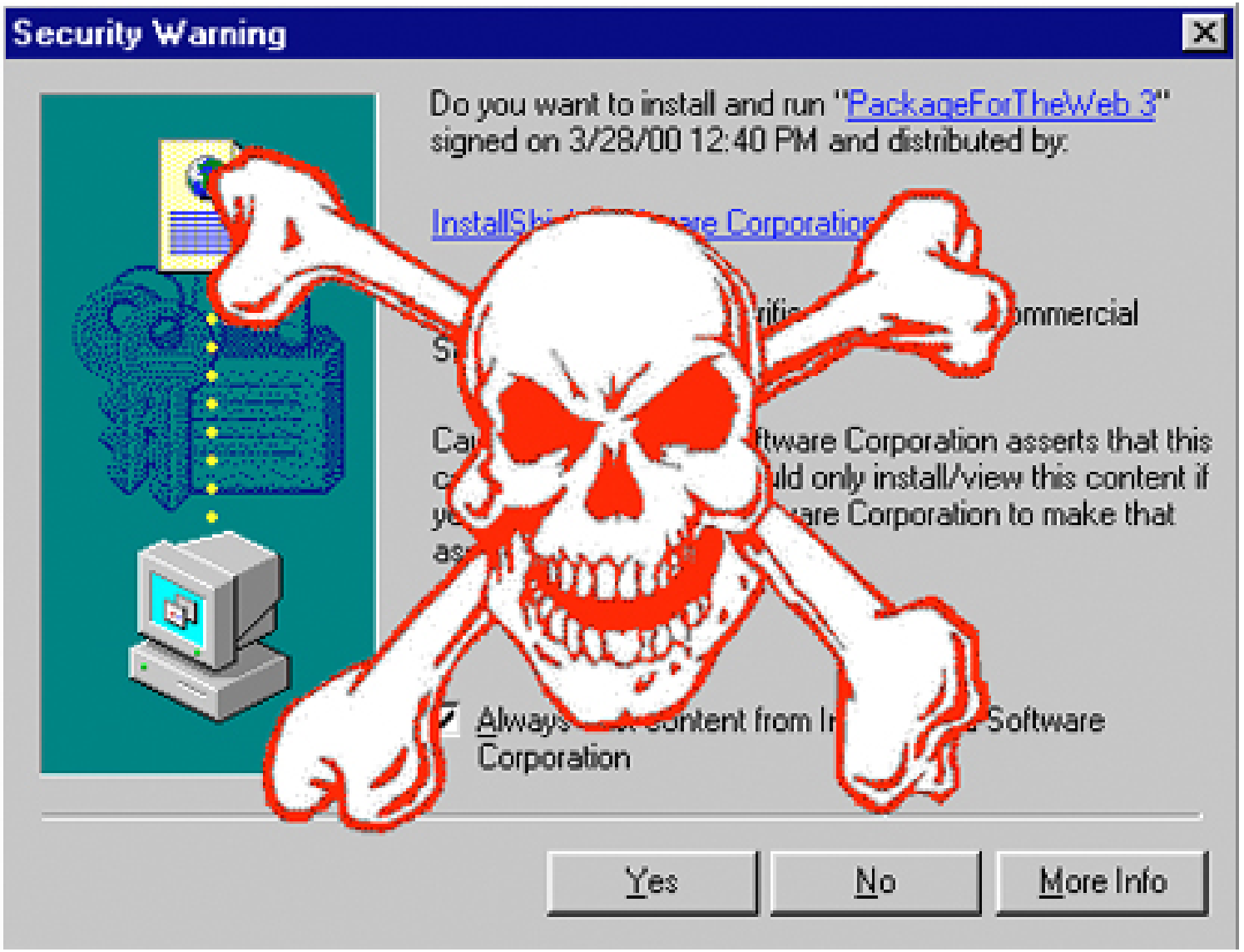
And it only gets worse

Linux Security

- All Linux Foundation sites down
  - Linux.com
  - LinuxFoundation.org
- Security breach discovered 9.8.2011
- Believed connected to kernel.org breach
- May have compromised username, password, email address, SSH keys, etc.

- Down for a month

Chain of Trust

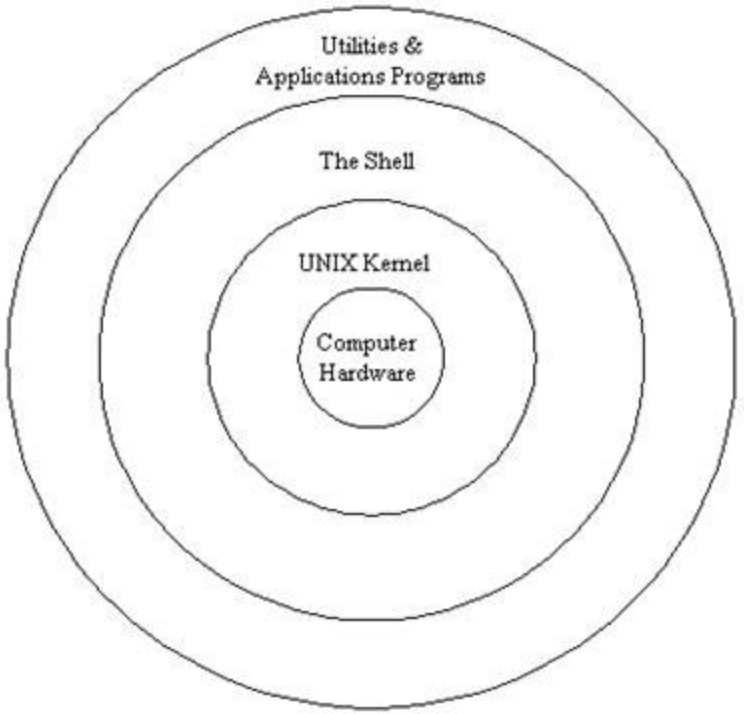


Certificate Authority

- GlobalSign server hacked – no signs of CA breach
- DigiNotar CA taken over by Dutch gov. 9.3.2011
- Issued fake certificate for Google
  - Used for MITM attack on Gmail
  - Google has blacklisted 247 certificates
- Issued fake certificates for Yahoo!, Mozilla, WordPress, Tor Project
- F-Secure found DigiNotar site defaced since 2009
- Iranian hackers allegedly responsible
- Security updates used to revoke certs

Parts of the UNIX OS

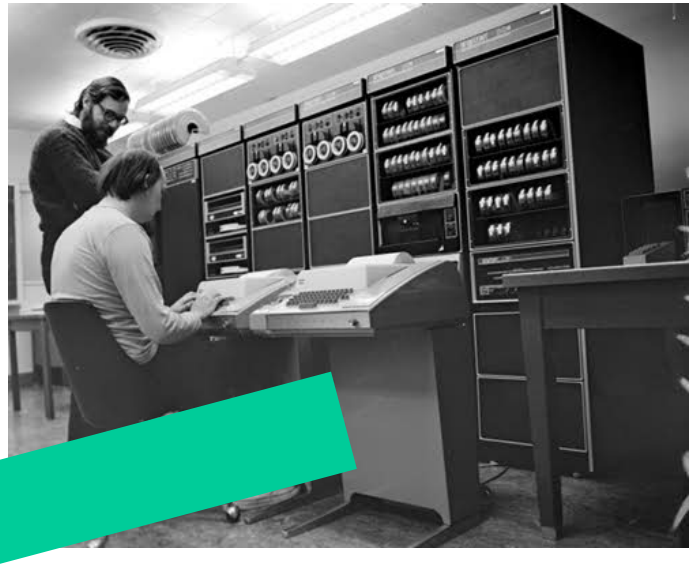
- The Kernel
- The Shell and Graphical User Interface(s) GUI
- Built-in System Utilities
- Application Software and Utilities



Shell and GUI

- Shells provides a “command line” interface which allows the user to type in commands. These commands are translated by the shell into something the kernel can comprehend, and then executed by the kernel.
- Bourne shell /etc/profile
- Bourne-Again shell - bash /etc/profile
- C shell /etc/.login
- Korn shell /etc/profile
- Z shell /etc/zprofile

CLI vs GUI



In the beginning – there were CLI's. Period.

GUI's

- Most UNIX systems can be installed without the GUI using only a CLI.
- The GUI is just another application that runs on top of the operating system.
- There are many implementations of all three of these components.
- It is possible to mix and match implementation and versions of these. They need not be alike and need not be all by the same organization.
- *This is quite a paradigm shift from Microsoft and Apple.*

Pair of dimes

X Window System

- X window: program that draws windows on the screen under most GUI-based versions of UNIX.
- X windows consists of 2 distinct parts
  - the X server and
  - 1 or more X clients
- The X window server runs on the machine to which the monitor is connected.
- The server controls the display directly, and is responsible for all input/output via the keyboard, mouse or display.

X Window System

- The clients do not access the screen directly - they communicate with the server, which handles all input and output
- It is the clients which do the "real" computing work - running applications
- The clients communicate with the server, causing the server to open one or more windows to handle input and output for that client
  - Bass ackwards
- From MIT > Open Group > x.Org

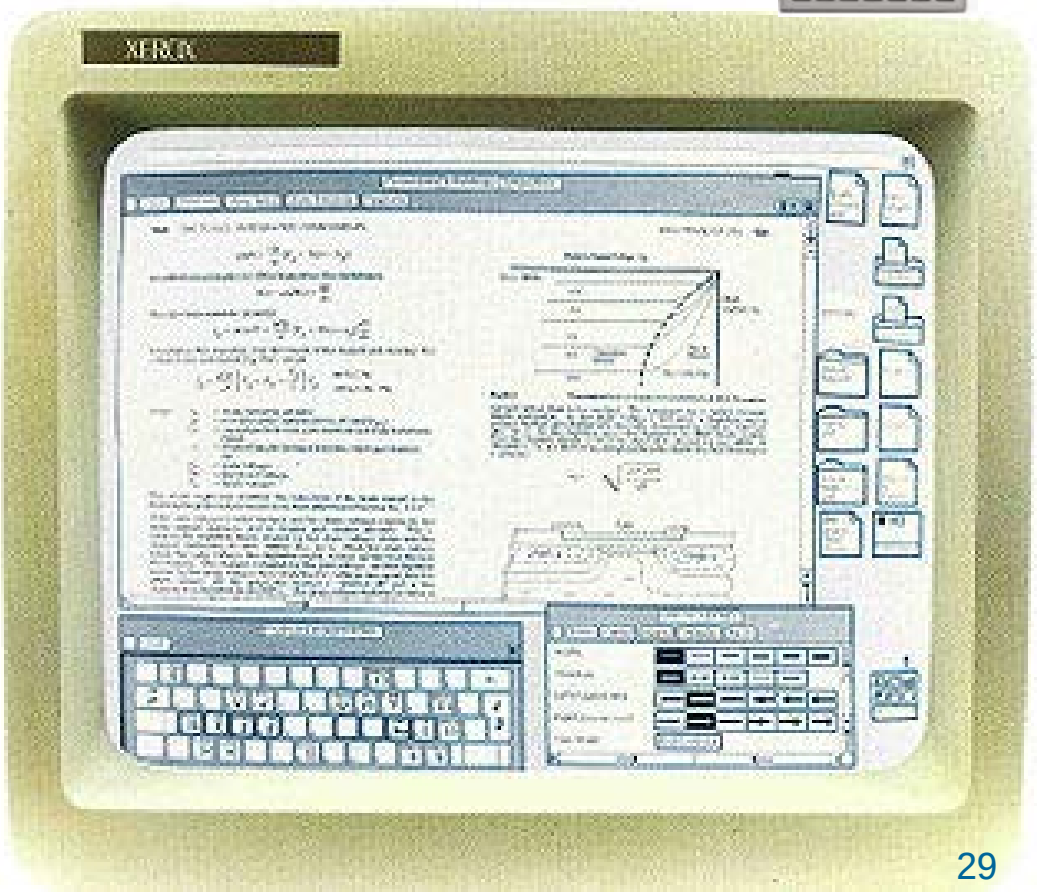
X Window System

- The clients may run on the server, communicating directly with the server. On most workstations, this is the normal situation
- X is a networked window system, and the client may run on a remote machine, communicating with the server over the network
- 1920x1200 video = 1.65 Gbit/s per client display
- Aka: X11, X
- X11R7.6 (2010) XFree86 4.8.0 (2008)
- There are X window server programs for Microsoft Windows – Xming, WierdX (Java), Cygwin/X

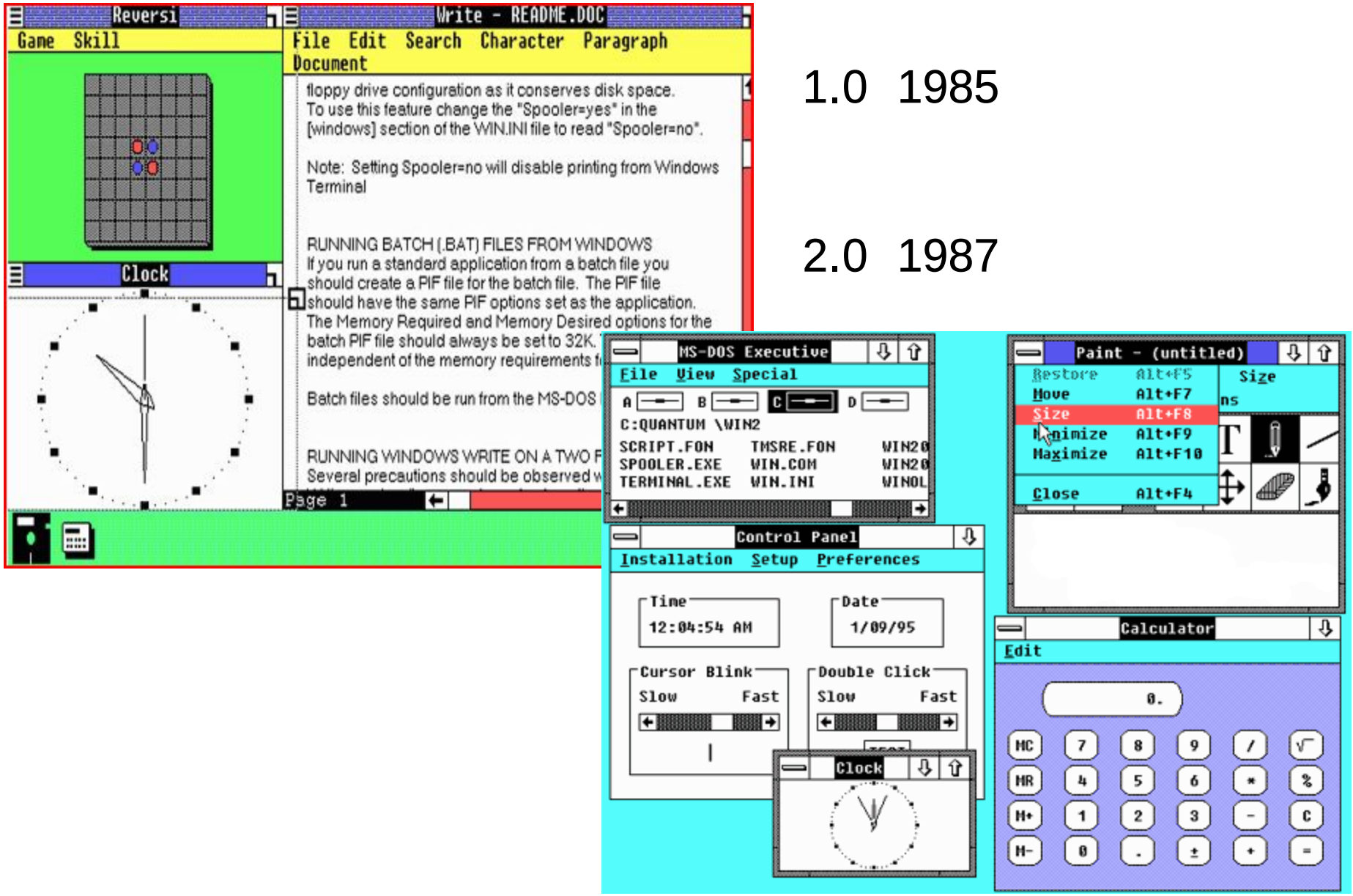
Bitmap Display Systems

Pre-X

- Xerox Alto 1973
- Xerox Star 1981
- Apollo Display Manager 1981
- Apple Lisa 1983
- Macintosh 1984
- Andrew Project 1982



On a side note…MS Windows



1.0 1985

2.0 1987

2014

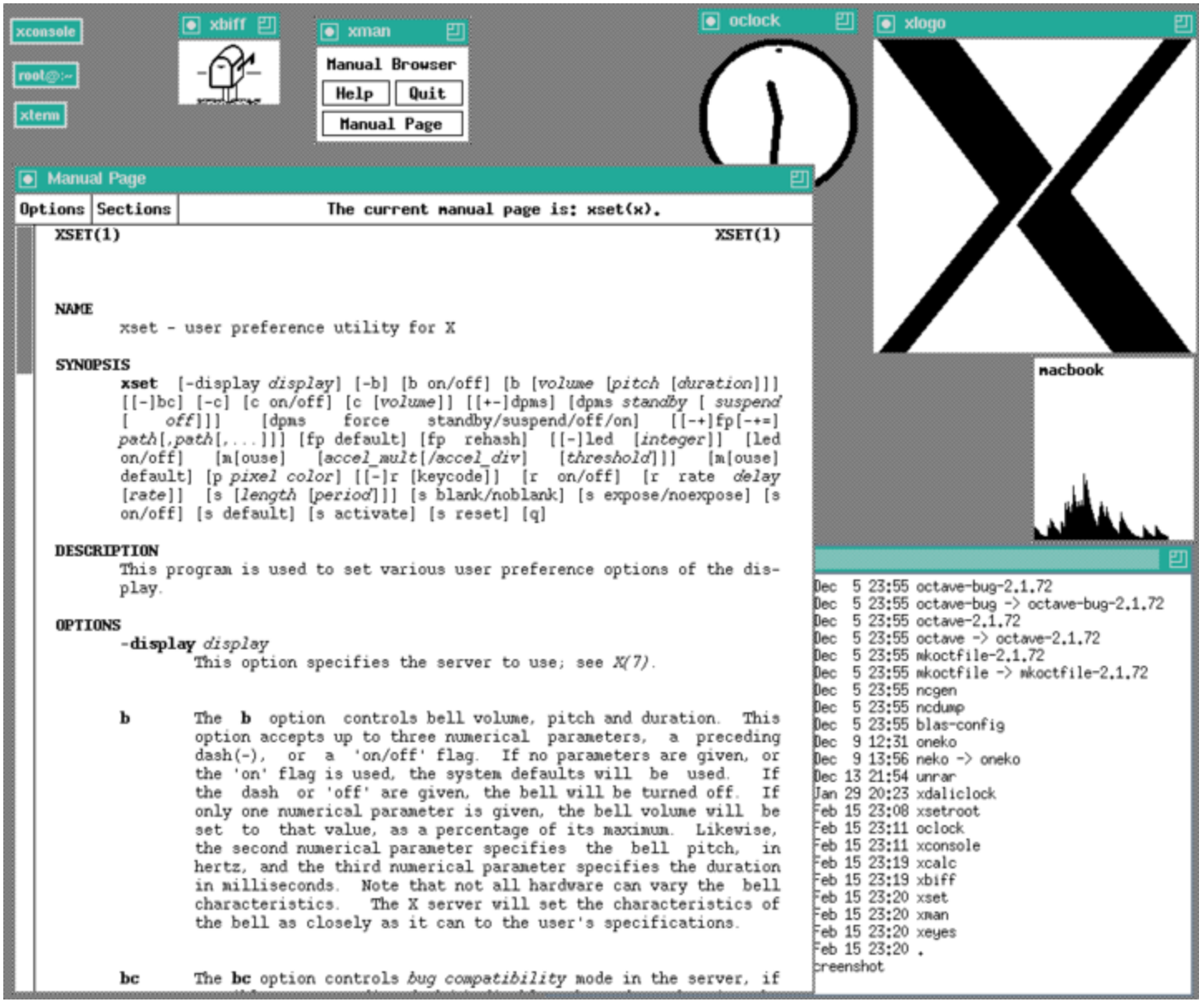

kobo


Welcome to Windows 8
Windows 8 includes a new way to manage your desktop.
e have focused on making it easy and accessable for everyone,
if you find the new system a bother, you can revert to a older one
Just click the Manager you want and you can return to work!
ndow Manager 8
Windows Superbar
Classic Taskbar
All Programs
Search...

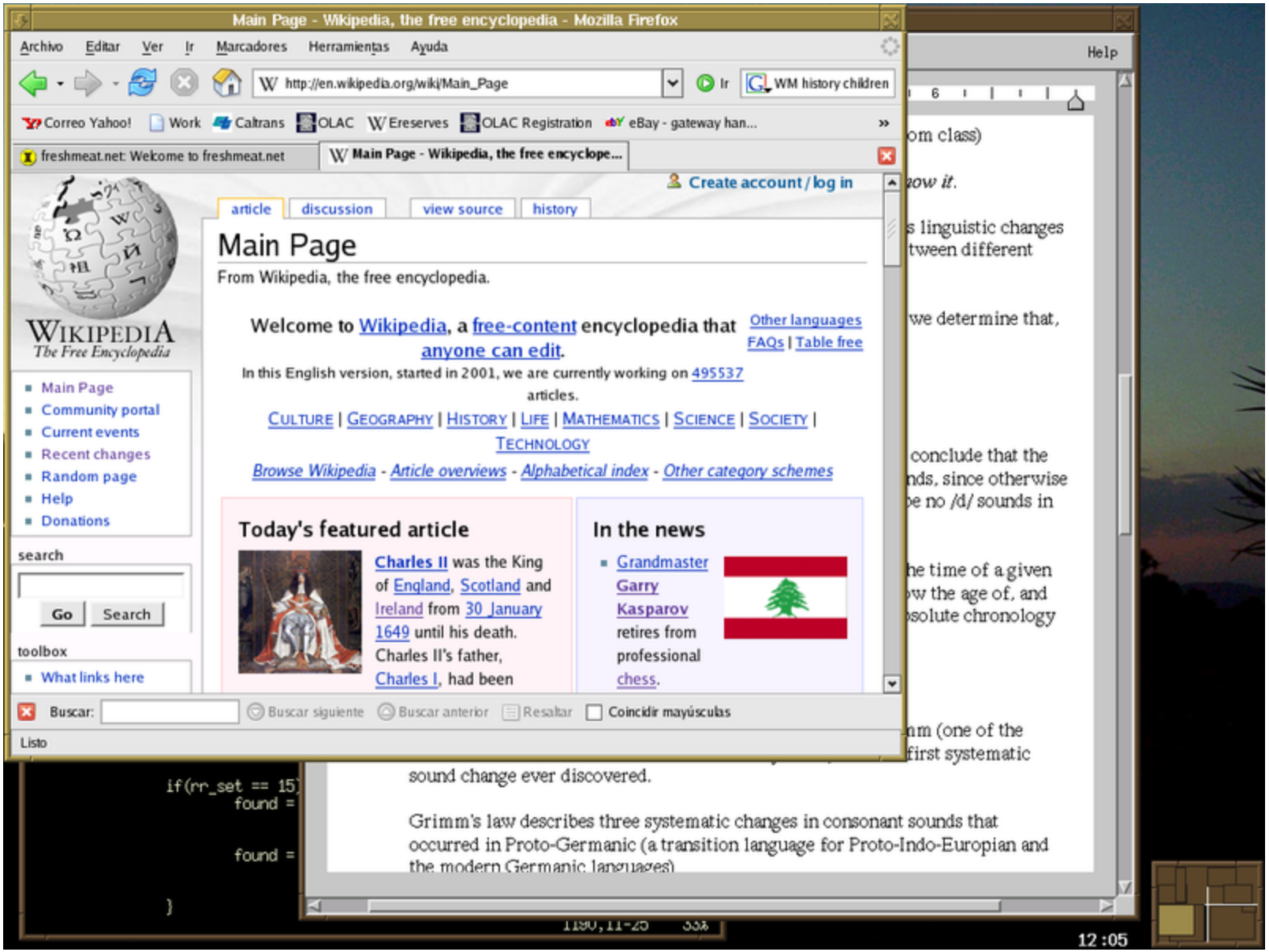
Window Managers

- Window Manager manages the placement of Windows on your system, making it possible to move, resize, and minimize the various programs. running on your computer
- KDE handles this functionality. Gnome does not directly, uses an independent window manager.
- Think of the Window Manager as the framing around the windows as well as all of the associated functionality that they provide.
- Window managers add decoration and customization, shading, sticky/nonsticky, history, and desktop and workspace manipulations.

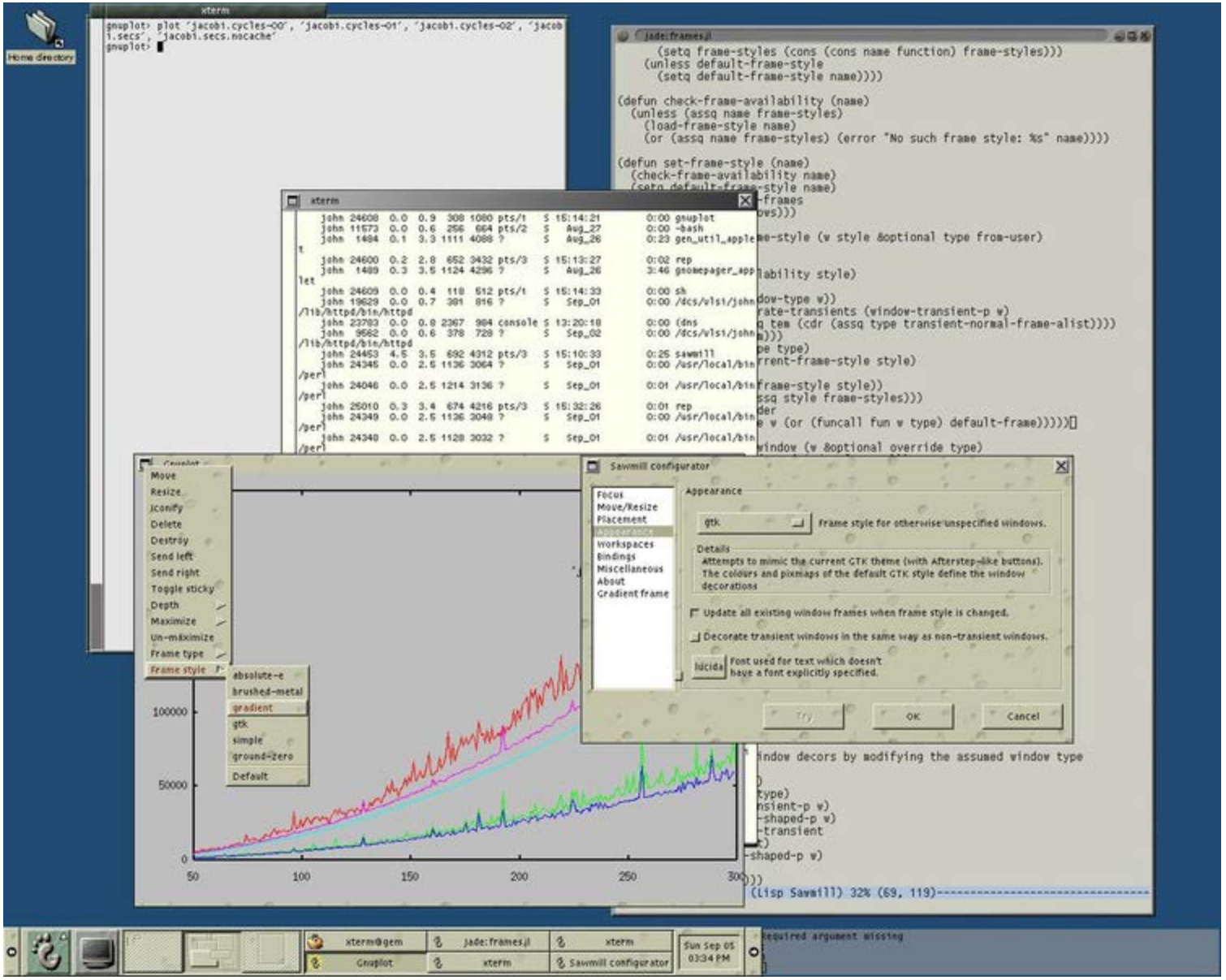
Tom's Window Manager - twm



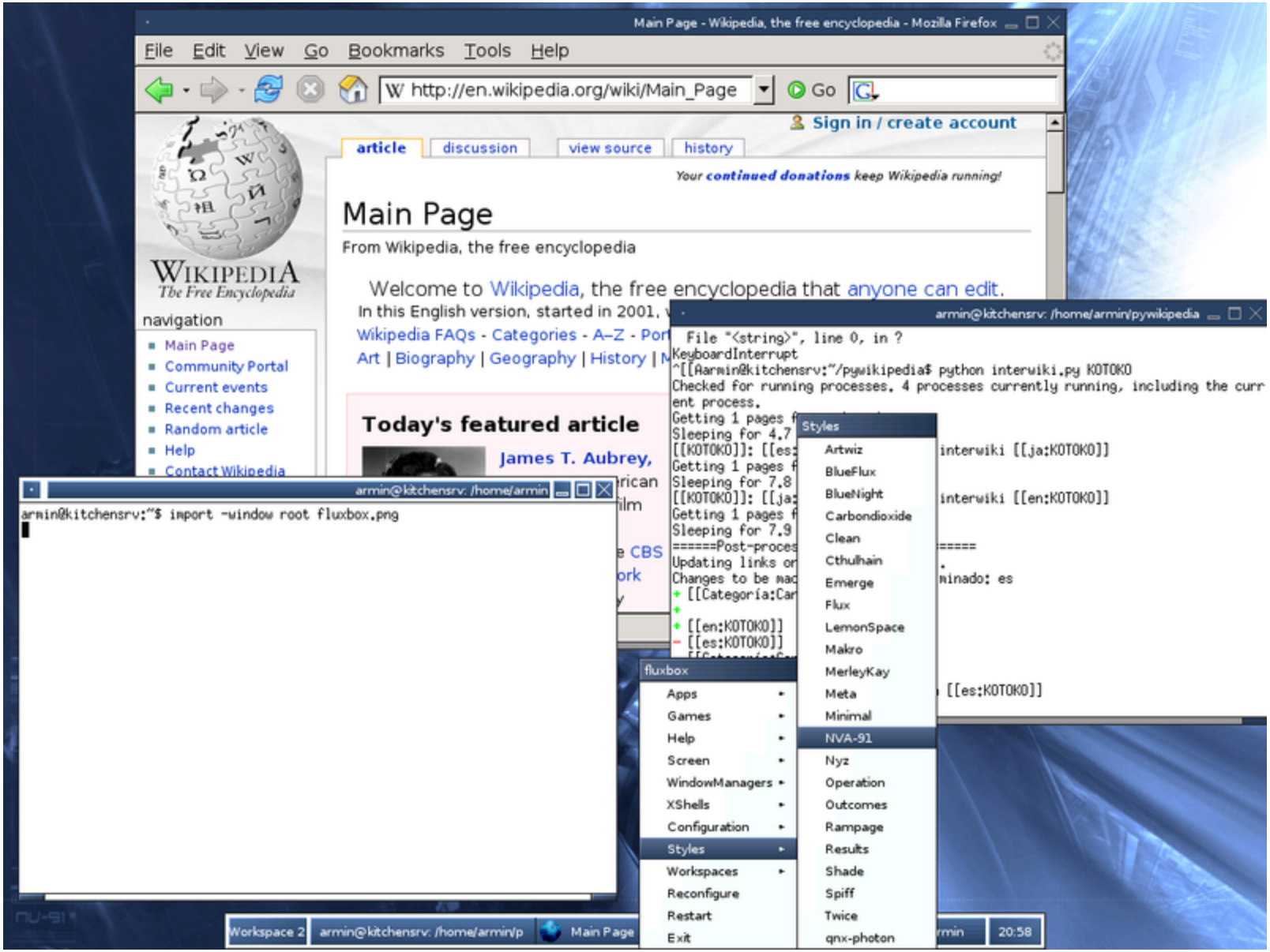
FVWM Feeble Virtual Window Manager



Sawfish


Home directory
xterm
gnuplot> plot 'jacobi.cycles-00', 'jacobi.cycles-01', 'jacobi.cycles-02', 'jacobi.secs', 'jacobi.secs.nocache'
gnuplot>
Move
Resize
Iconify
Delete
Destroy
Send left
Send right
Toggle sticky
Depth
Maximize
Un-maximize
Frame type
Frame style
absolute-e
brushed-metal
gradient
gtk
simple
ground-zero
Default
100000
50000
0
50
100
150
200
250
300
Sawmill configurator
Focus
Move/Resize
Placement
Appearance
Workspaces
Bindings
Miscellaneous
About
Gradient frame
gtk
Frame style for otherwise unspecified windows.
Details
Attempts to mimic the current GTK theme (with Afterstep-like buttons). The colours and pixmaps of the default GTK style define the window decorations
Update all existing window frames when frame style is changed.
Decorate transient windows in the same way as non-transient windows.
lucida
Font used for text which doesn't have a font explicitly specified.
Try
OK
Cancel
(Lisp Sawmill) 32% (69, 119)
xterm@gem
jade:frames.jl
xterm
Gnuplot
xterm
Sawmill configurator
Sun Sep 05
03:34 PM

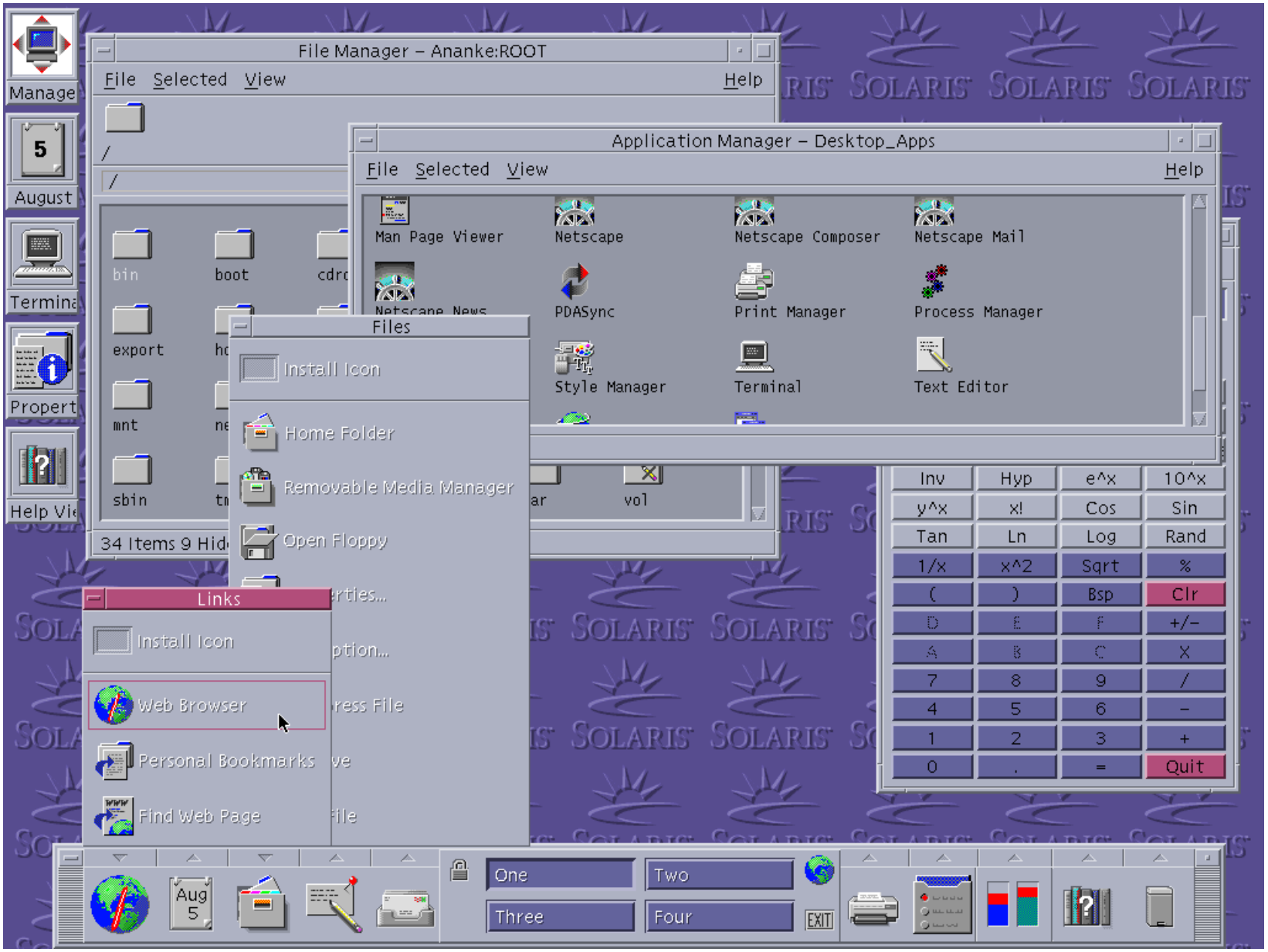
Fluxbox


Main Page - Wikipedia, the free encyclopedia - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://en.wikipedia.org/wiki/Main_Page
Go
Sign in / create account
article discussion view source history
Your continued donations keep Wikipedia running!
Main Page
From Wikipedia, the free encyclopedia
Welcome to Wikipedia, the free encyclopedia that anyone can edit.
WIKIPEDIA
The Free Encyclopedia
navigation
Main Page
Community Portal
Current events
Recent changes
Random article
Help
Contact Wikipedia
Today's featured article
James T. Aubrey,
armin@kitchensrv: /home/armin
armin@kitchensrv:~$ import -window root fluxbox.png
armin@kitchensrv: /home/armin/pywikipedia
File "<string>", line 0, in ?
KeyboardInterrupt
^[[Aarmin@kitchensrv:~/pywikipedia$ python interwiki.py KOTOKO
Checked for running processes. 4 processes currently running, including the curr
ent process.
Styles
Artwiz
BlueFlux
BlueNight
Carbondioxide
Clean
Cthulhain
Emerge
Flux
LemonSpace
Makro
MerleyKay
Meta
Minimal
NVA-91
Nyz
Operation
Outcomes
Rampage
Results
Shade
Spiff
Twice
qnx-photon
fluxbox
Apps
Games
Help
Screen
WindowManagers
XShells
Configuration
Styles
Workspaces
Reconfigure
Restart
Exit
Workspace 2
armin@kitchensrv: /home/armin/p
Main Page
20:58

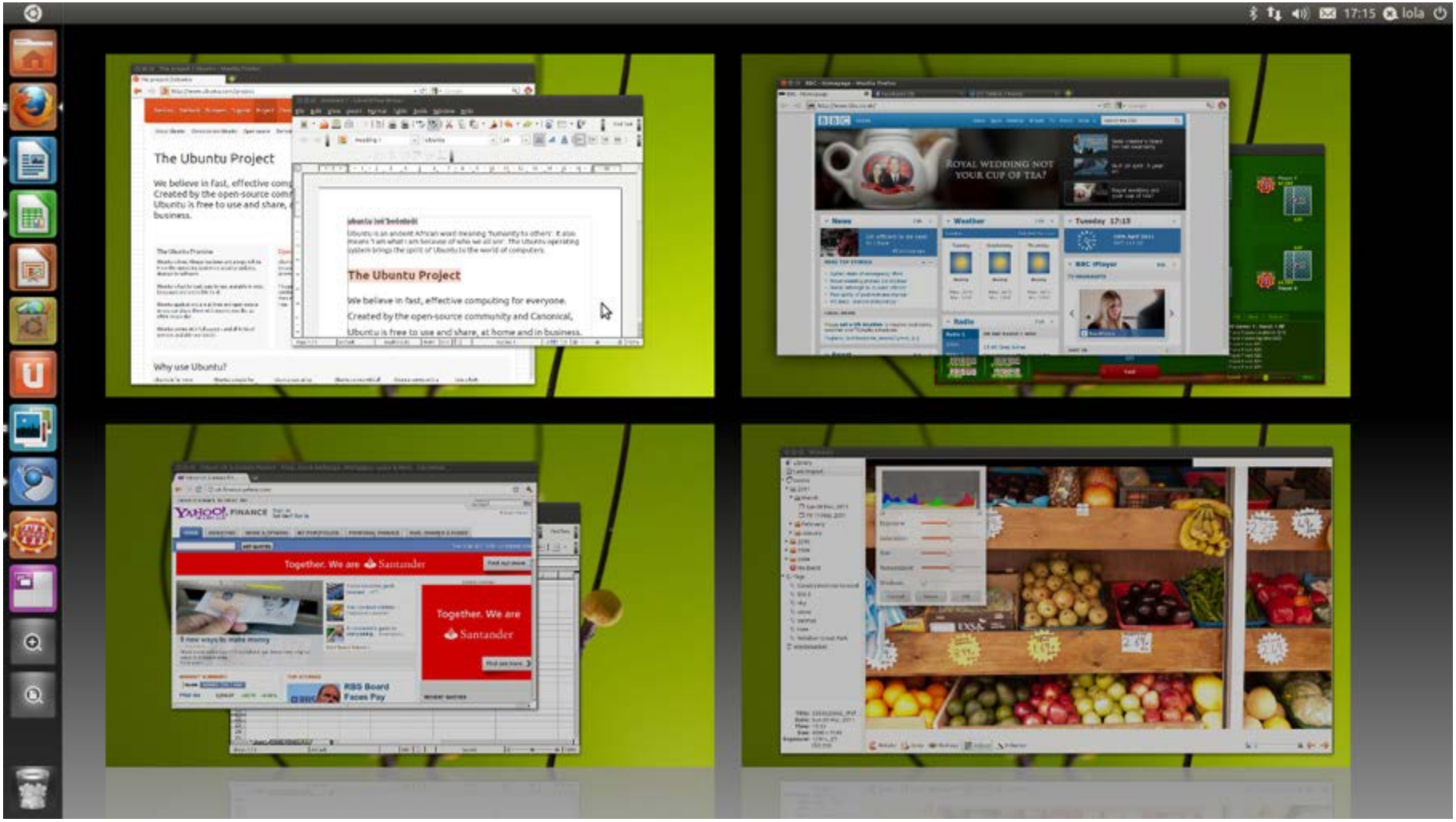
Desktop Managers

- Gnome and KDE are desktop managers. Both of these look a lot like Microsoft Windows.
- They have the equivalent of a Start Menu, have an equivalent of Windows Explorer, and have some sort of control panel.
- Desktop Manager role is to provide ability to manage all the system details that would otherwise require many commands in a CLI.
- These details include managing your files, launching programs, configuring system, etc.
- The desktop manager is optional.

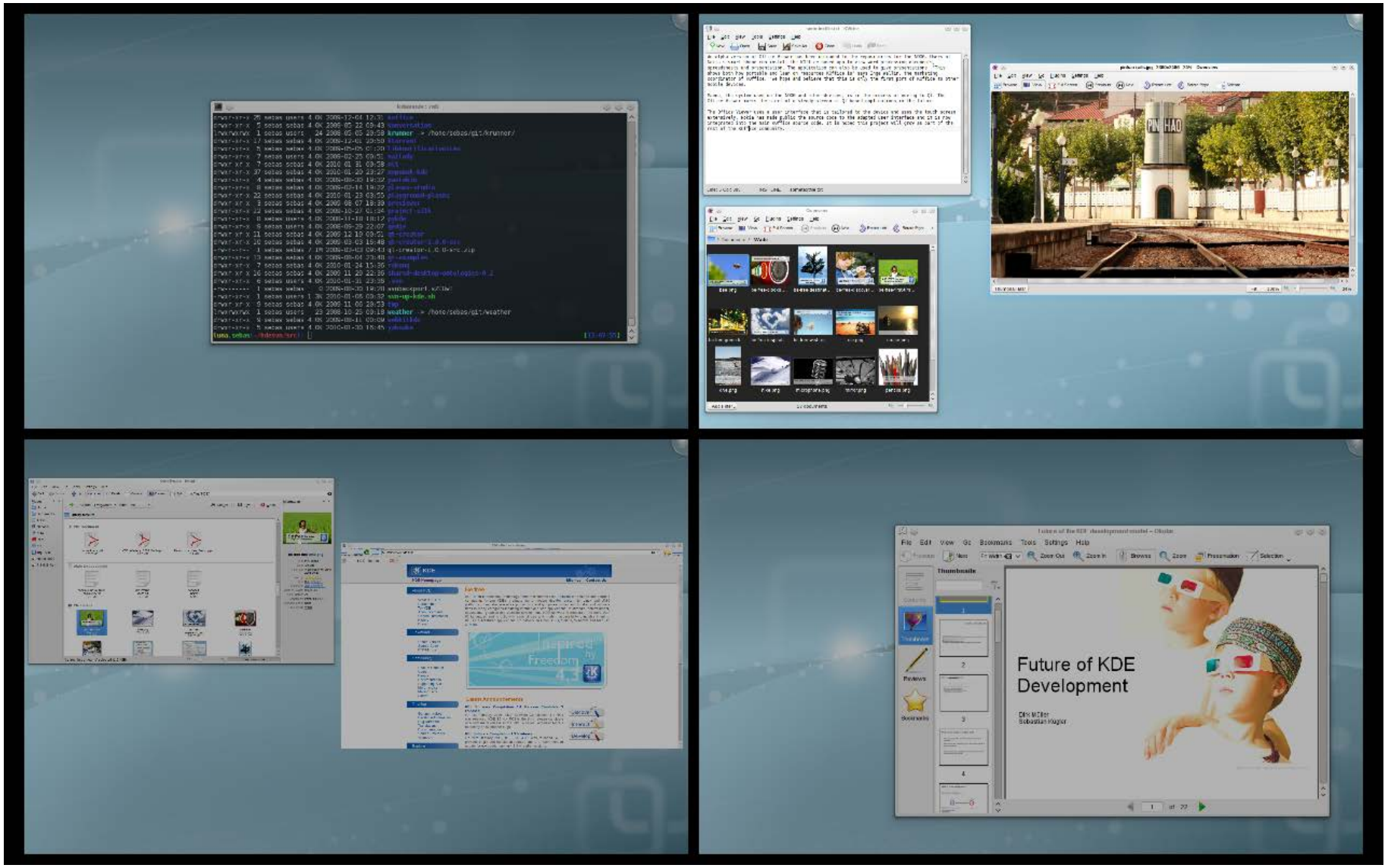
CommonDesktopEnvironment



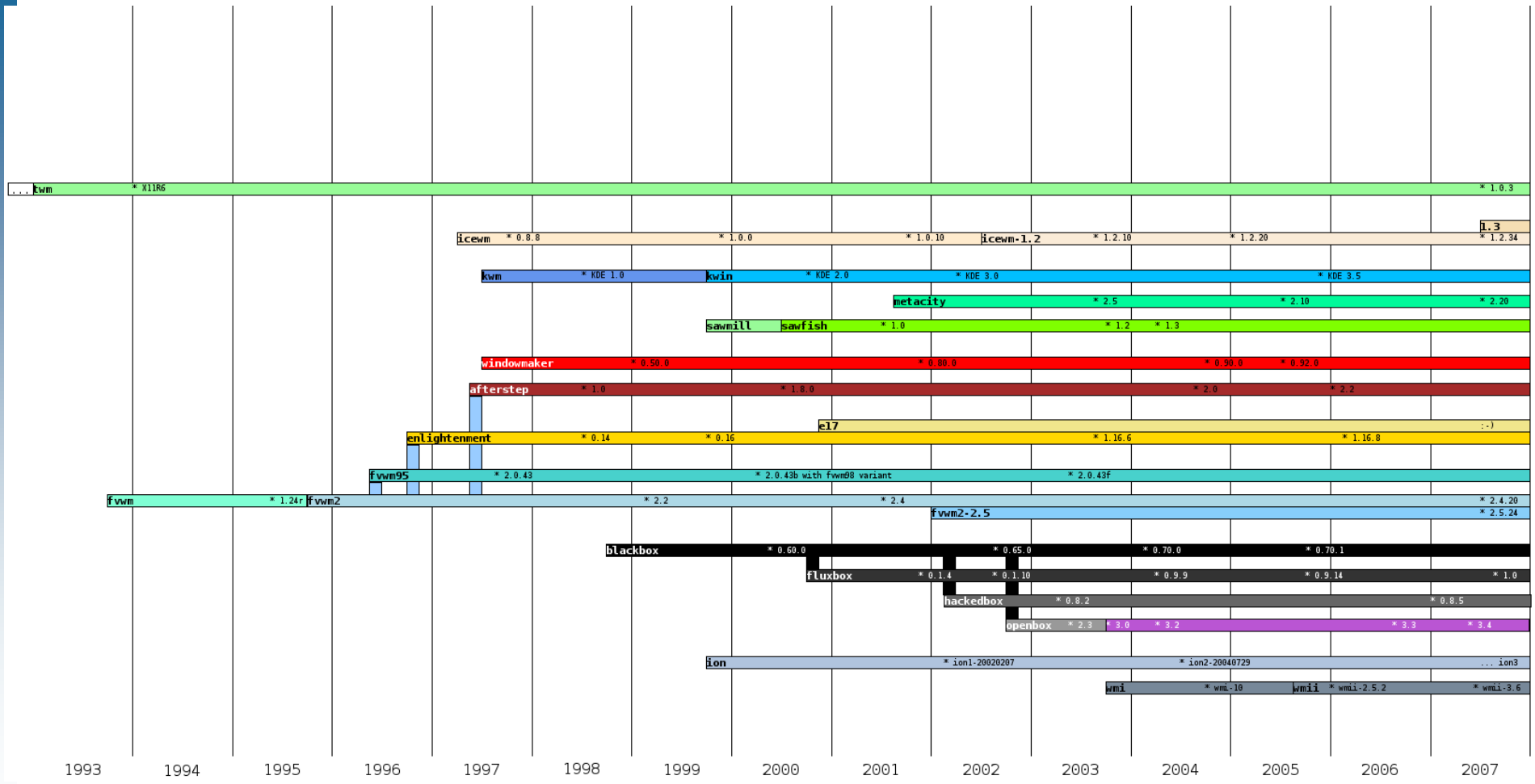
Gnome on Ubuntu



KDE (Plasma)



Window Manager Timeline

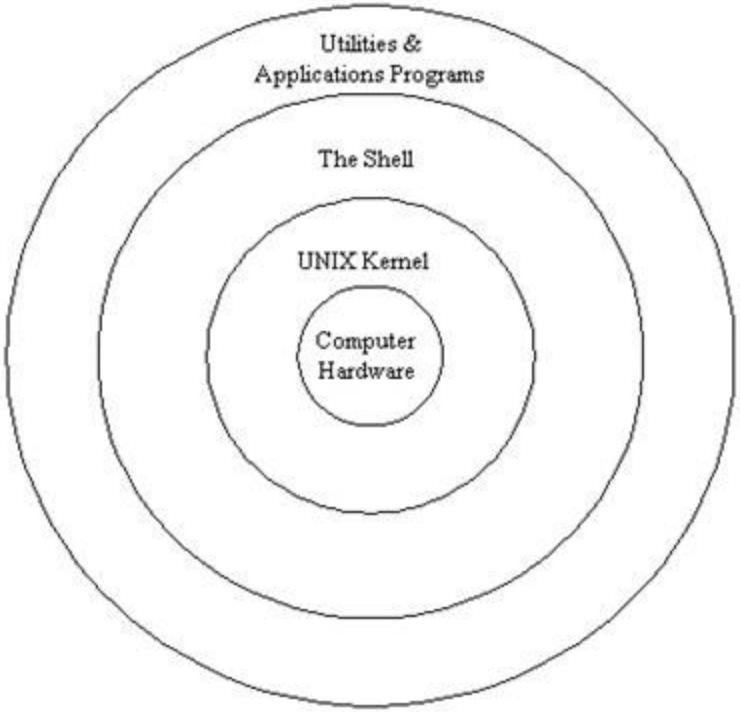


Built-In System Utilities

- Programs that provide user interface functions that are basic to an operating system, but which are too complex to be built into the shell. Examples of utilities are programs that let us see the contents of a directory, move & copy files, remove files, etc…
- du
- rm
- ls ls –al
- chown
- cp
- chgrp

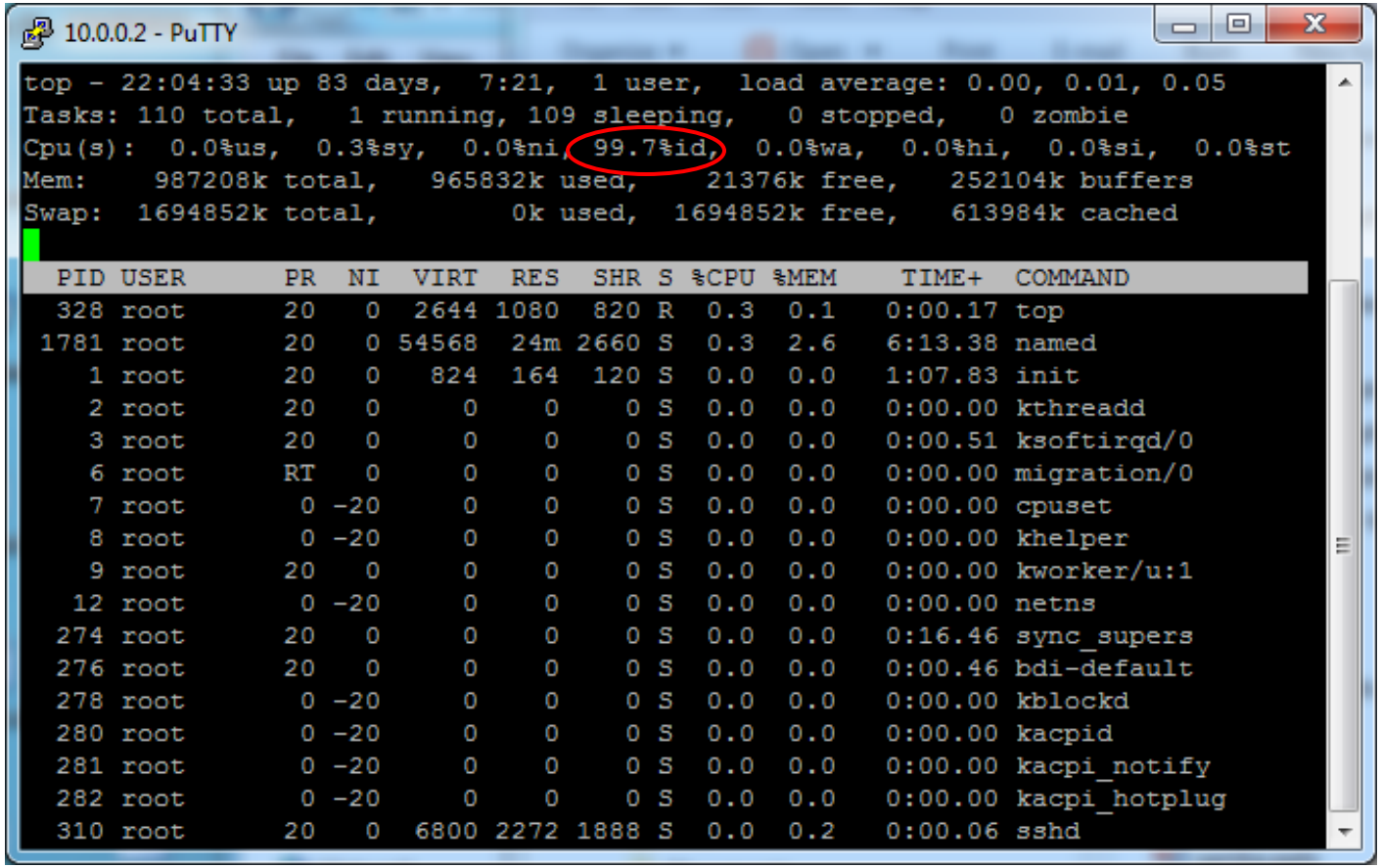
Application Software & Utilities

- Additional programs bundled with the OS distribution, or available separately. These can range from additional or different versions of basic utilities, to full scale commercial applications



Trade Offs

- GUI imposes a performance overhead
- Typically the largest resource load
- With CLI – this server is idle



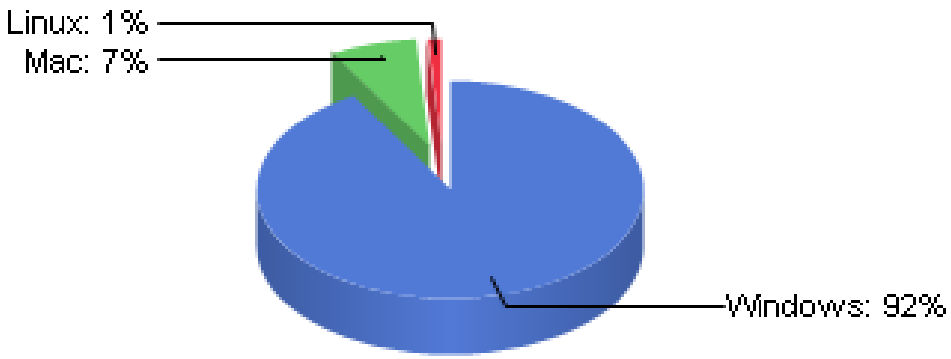
OS Market Share

Source: W3Techs

Servers		
UNIX/Linux	64%	
Windows	36%	28%

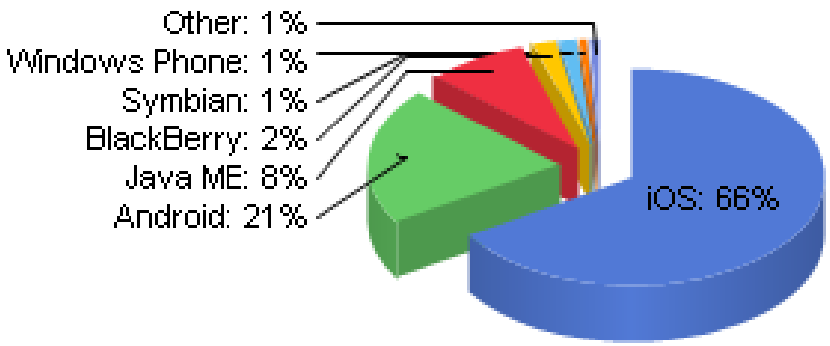
Desktop

Total Market Share



Mobile/Tablet

Total Market Share



Source: www.netmarketshare.com

Remember

- Single, monolithic kernel
  - Loadable modules
- Micro-kernel

- Hardware
- Kernel
- Shell {Bourne, C, Bash, Korn, Ash, Z}
- Applications/Utilities

- CLI vs. GUI
- Window and Desktop Managers (eat resources)