UNIX/Linux Overview

For Law Enforcement Personnel

Presented By CJ Fearnley

http://www.cjfearnley.com/UNIX-Linux-Basics.2005.01.pdf

Modified from a presentation by SSA William W. Blevins

Original presentation produced by SSA Edward Arias

Objectives

- What is Unix?
- Why do I need to know Unix?
- Unix history.
- Architecture of Unix/Linux.
- Important files and commands.
- How is Unix/Linux booted?

What is Unix?

What is an operating system?

- The low-level (first layer loaded) software which handles the interface to system hardware (input/output devices, memory, file system, etc), schedules tasks, and provides common core services such as a basic user interface.
- Colloquially, all of the software that comes with a system before applications are installed.

What Is Unix?

Examples of Operating Systems:

- Unix and Unix-like: A/UX, AIX, *BSD (Free, Micro, Net, Open, etc), Darwin (Mac OS X), HP-UX, Hurd, IRIX, Linux, LynxOS, Minix, QNX, SE-Linux, Solaris, System V, Triance, TRUSIX, Tru64, UnixWare, VSTa, z/OS, etc.
- Embedded: BeOS, Chorus OS, eCos, FreeRTOS, IOS, JUNOS, LynxOS, QNX, VRTX, VxWorks, Windows CE, RTLinux, RTAI, Symbian, etc.
- Others: AOS, JavaOS, MorphOS, Primos, Windows 3.1/95/98/NT/XP/2000/2003, etc.

What is Unix?

A portable, multi-tasking and multi-user operating system

- Portable: runs on many different hardware architectures (Intel x86 and IA-64, Alpha, MIPS, HP PA-RISC, PowerPC, IBM S/390, SPARC, Motorola 680x0, etc.).
- Preemptive multi-tasking: several programs can run at the same time (time slices, interrupts, and task switching).
- Multi-user: many users can share the computer system at the same time.

What is Unix?
Other Features

- Uses a simple, uniform file model which includes devices and access to other services in a flexible, hierarchical file system.
- Written in a high-level language (“C”) making it easy to read, understand, change and port.
- The command prompt is a simple user process, the Unix shell, which is also a convenient job programming language.
- Includes support for regular expressions which are convenient for complex searching.

What is Unix?

The Unix Philosophy

- Write programs that do one thing and do it well.
- Write programs to work together.
- Write programs to handle text streams because that is a universal interface.

Do one thing, do it well.

-- Doug McIlroy

Why Do I Need to Know This?

- Ubiquitous: Most big computers and much of the Internet infrastructure runs on some variant of Unix (SUN, SGI, HP, etc.).
- Linux is the fastest growing operating system in the market.
- Source code availability provides the ability to "get under the hood" of operating system design and function (and TCP/IP).
- By understanding the Unix/Linux community and its culture, you will be able to collect critical information.

Why Do I Need to Know This?
Crackers Love Unix.

- Linux and *BSD are freely distributed. Anyone can download them from the Internet for free and install.
- Many tools are native to Unix and the source code is available for anyone (crackers, too) to modify.
- Used on computers at universities.
- Some crackers use Unix to develop, test and run their illegal activities.

Why do I need to know this?

- Unix is what some crackers use.

Picture from Def Con. “Hackers Pose”

Why do I need to know this?

- **Hacking:** Before the term hacking became associated with computers, MIT undergraduates used it to describe any activity that took their minds off studying, suggested an unusual solution to a technical problem, or generally fostered nondestructive mischief.
- **Cracking:** The act of breaking into a computer system; what a cracker does. Contrary to widespread myth, this does not usually involve some mysterious leap of hackerly brilliance, but rather persistence and the dogged repetition of a handful of fairly well-known tricks that exploit common weaknesses in the security of target systems. Accordingly, most crackers are only mediocre hackers.

Unix History

- 1964 joint project between AT&T Bell Labs, GE, and MIT to develop a new OS.
- Goal : develop an OS that could provide computational power, data storage and the ability to share data among multiple users.
- Result: **Mult**iplexed **I**nformation & **C**omputer **S**ervice - **MULTICS.**

Unix History

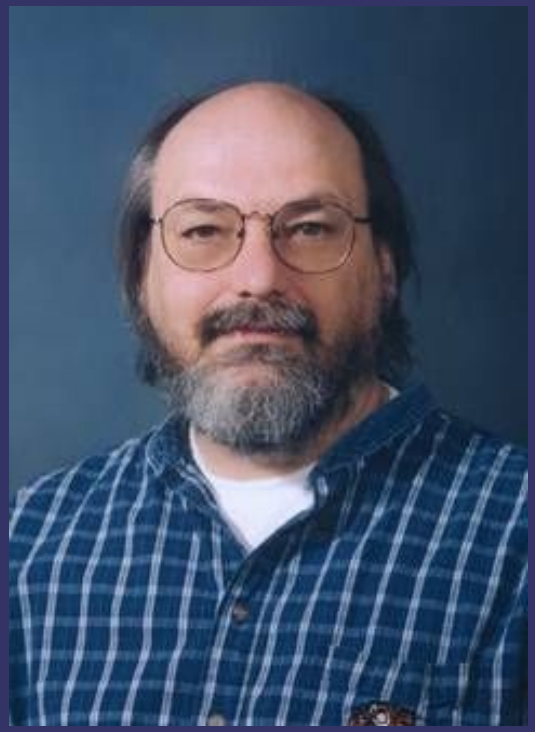
- 1969 Bell Labs withdraws from group.

- Two Bell Lab scientists, Ken Thompson and Dennis Ritchie, continue research. They were still left without a “Convenient interactive computing service”*.

* Ritchie, D.M. “The Evolution of the Unix Time-sharing System”, AT&T Bell Laboratories Technical Journal, Oct. 1984, Vol 63, No.8, Part 2, pp. 1577-1594.

Unix History

- At the same time Ken Thompson wrote a game “space travel” in Fortran to run on GECOS OS (Honeywell 635).



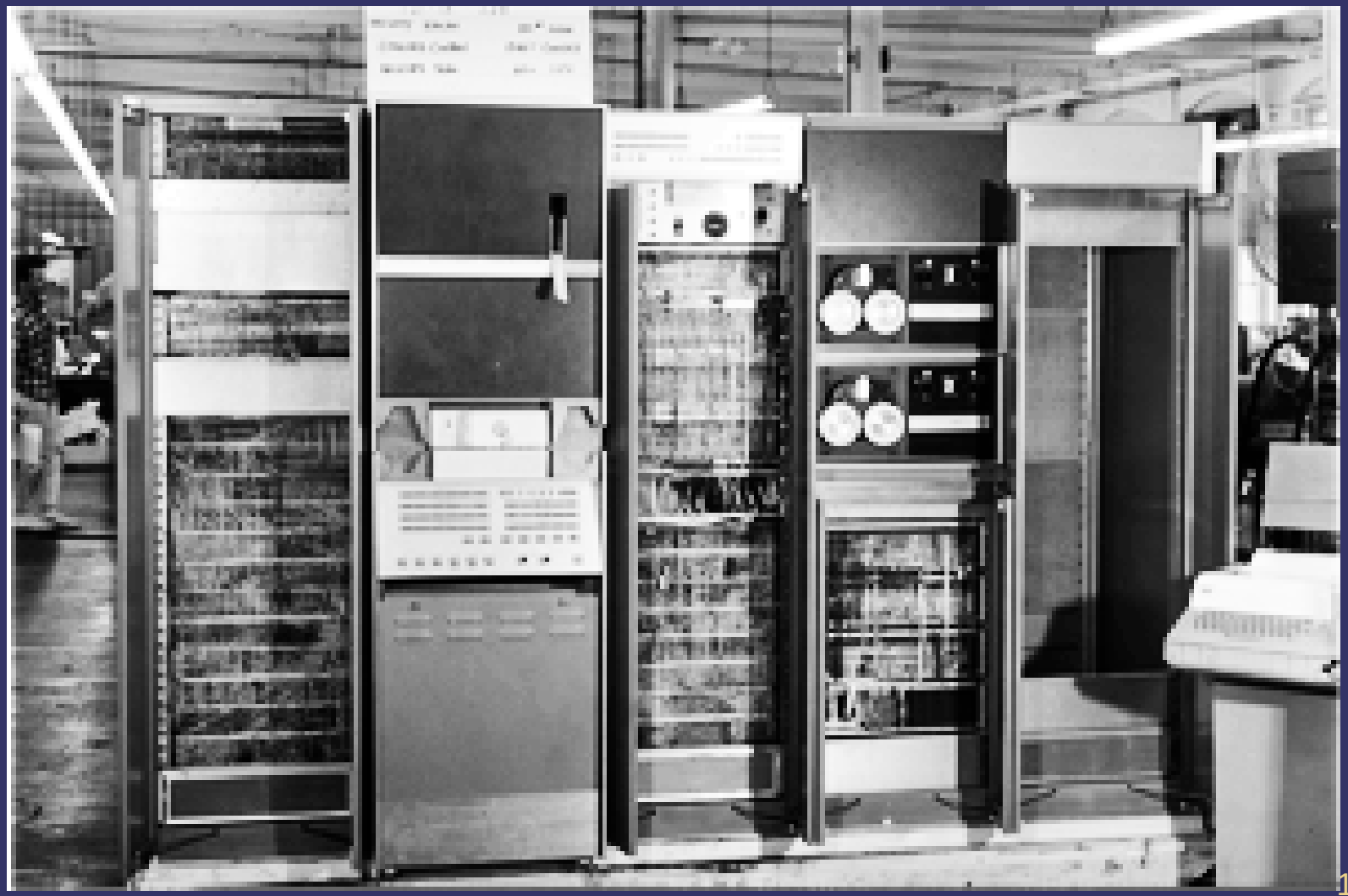
- The spaceship was hard to control and it was expensive to run. He was told to get the game off his work computer.

Unix History

- Thompson ported the game to a little used PDP-7 computer.
- Unics (later Unix) was born as a pun on Multics.

Unix History

PDP-7



Unix History

- Dennis Ritchie developed “B” . Then wrote “C” a compiled language.
- In 1973 entire OS ported to “C”.

Unix History

- Because of a 1956 Consent Decree AT&T could not market Unix so it provided it to academia.
- Late 70s : Thompson took a sabbatical to teach Unix at UC Berkley –

  Birth of BSD Unix. Introduced many new features.
- AT&T Bell Labs realized the commercial potential and began distributing System V.
- Commercialization of Unix (70s / 80s)

  AT&T, Sun, SGI, HP, DEC, NCR, IBM.

Linus Torvalds

- 1991 Linux 0.02 is first released to the public.
- 1994 Linux 1.0 is released.

Three Definitions of Linux

- Linux Kernel: The very low-level software that manages your computer hardware and provides a library (POSIX) interface for user-level software. The Linux kernel runs on many platforms (Intel x86 and IA-64, Alpha, MIPS, HP PA-RISC, PowerPC, IBM S/390, SPARC, Motorola 680x0, etc.).

- GNU/Linux OS: The Linux kernel plus utility software to provide a useful working environment.

- Linux Distributions: The packaging of the Linux Kernel, the GNU/Linux OS and lots of other software to make Linux easy to install, configure, and use (at least for the target audience).

Tux, the Linux Mascot

The "Free" Software Movement

The GNU Project: www.gnu.org

The Four Freedoms

- The freedom to run the program, for any purpose.
- The freedom to study how the program works, and adapt it to your needs.
- The freedom to redistribute copies so you can help your neighbor.
- The freedom to improve the program, and release your improvements to the public, so that the whole community benefits.

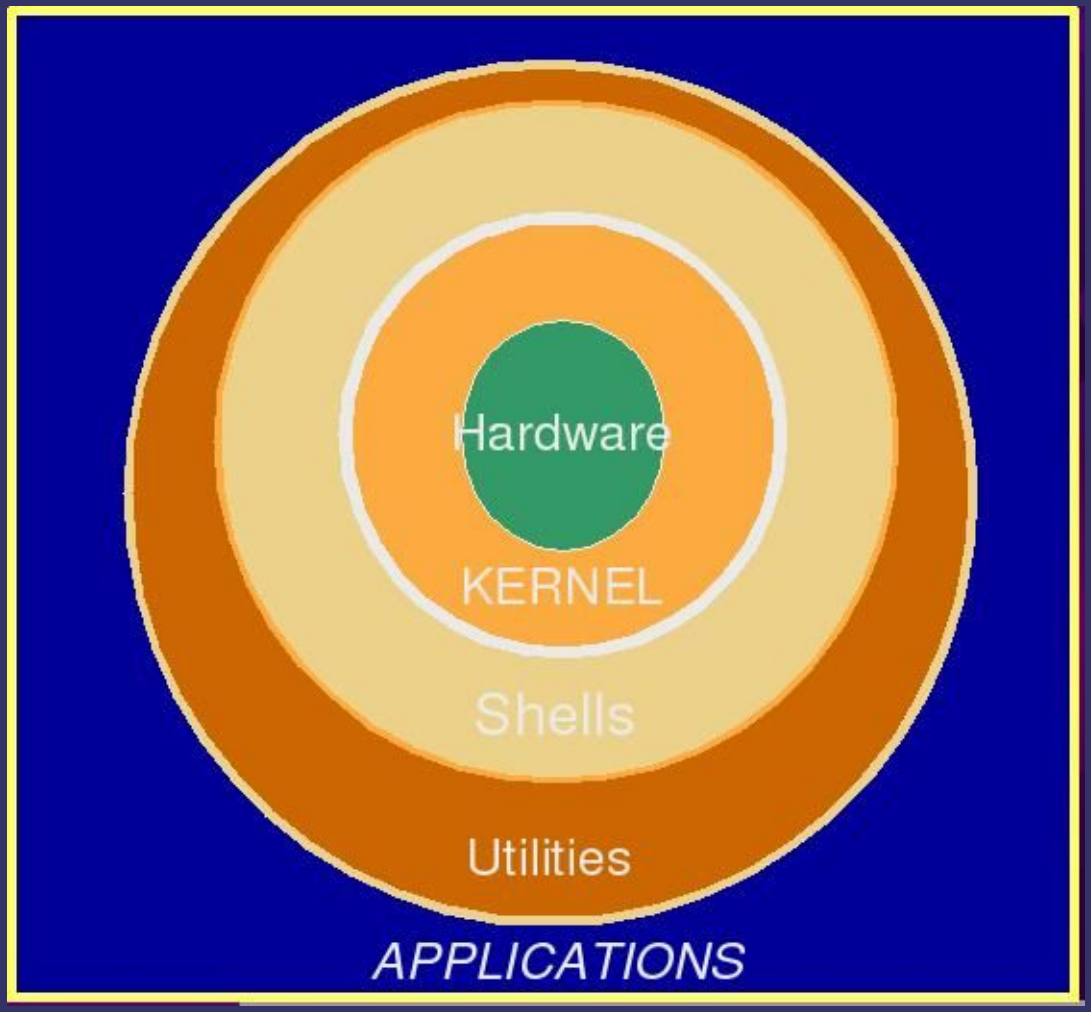
Architecture of Unix

- Kernel: Schedules programs,
  Manages data/file access and storage,
  Enforces security,
  Performs all hardware access.

- Init: First program run by kernel on booting.

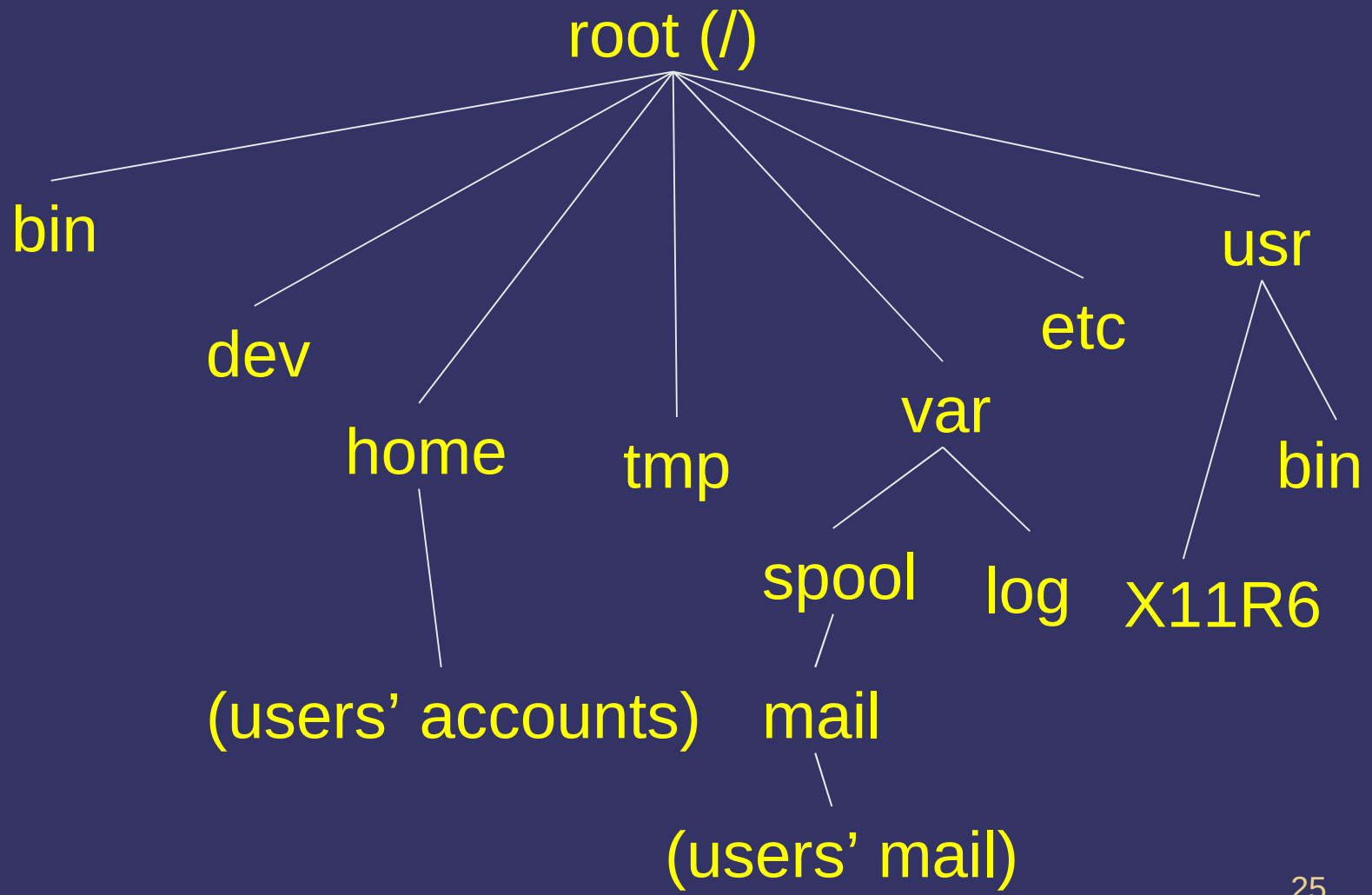
- Shell: Presents each user a prompt,
  Interprets commands typed by user,
  Executes users commands,
  Provides user/programming environment.

Architecture of Unix



Architecture of Unix

Unix file system



Typical Directories

- **/ :** Root of the tree. Where it starts.
- **bin, sbin, usr/bin:** software for the shells and most common Unix commands.
- **dev:** short for devices, holds the files necessary to operate peripherals such as printers and terminals.
- **home:** contains the home directories of users (/export/home on sun computers).

Typical Directories

- **tmp:** holds temporary files.
- **var:** contains files that vary in size; (Mail directories, printer spool files, logs, etc.)
- **etc:** administrative files such as lists of user names and passwords.

Typical Directories

- **usr:** Contains application programs
- **lib**: Contains libraries for programs
- **proc**: a pseudo-filesystem used as an interface to kernel data structures.

File and Directory Name Rules

- Valid names can be made up of:
  - Uppercase letters (A to Z).
  - Lower case letters (a to z). Case sensitive!!!
  - Numbers (0 to 9).
  - Period (.), underscore (_), commas (,).
- Should not contain spaces or the following:
  - & * \ | [ ] { } $ < > ( ) # ? ‘ “ ; ^ ! ~ %. Never /.
  - You should avoid naming files or directories with Unix commands.

File System Structure

- Unix stores a file's administrative information (its physical location on disk, permissions including ownership and modification times) in an inode (i-node or Index Node).

- The file name (link) is stored in the contents of a directory entry. Deleting a file consists of removing a link to the inode (the inode itself is not deleted).

File System Structure

Data Recovery:

- When a file is deleted the number of links to the inode is reduced by one.
- Note: an inode may have more than one link (or name) --- see ln(1).
- If the number of links becomes zero, the kernel may reuse the disk space making recovery difficult. Magnetic Force Microscopy (MFM) can recover most data unless wipe(1) is used.

Important Files

- passwd, shadow: Password files
- group: Sets up group permissions
- services: Defines names for services
- hosts: Defines names for IP addrs
- inetd: Defines net services to run

Passwd File

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
ftp:x:14:50:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:
```

Shadow File

root:1lLZaaozy$fxRqBZE54ldQHJzHwKPWj/:11749:0:99999:7:::

bin:*:11749:0:99999:7:::

daemon:*:11749:0:99999:7:::

adm:*:11749:0:99999:7:::

lp:*:11749:0:99999:7:::

sync:*:11749:0:99999:7:::

shutdown:*:11749:0:99999:7:::

halt:*:11749:0:99999:7:::

mail:*:11749:0:99999:7:::

news:*:11749:0:99999:7:::

operator:*:11749:0:99999:7:::

games:*:11749:0:99999:7:::

ftp:*:11749:0:99999:7:::

nobody:*:11749:0:99999:7:::

earias:1aRGG/G8W$naSp6L7hskKDFPV0tddRg/:11749:0:99999:7:::

Services File

```
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, most entries here have two entries
# even if the protocol doesn't support UDP operations.
# Updated from RFC 1700, ``Assigned Numbers'' (October 1994).  Not all ports
# are included, only the more common ones.
#
# service-name  port/protocol  [aliases ...]   [# comment]

ftp-data 20/tcp
ftp-data 20/udp
ftp      21/tcp
ftp      21/udp
ssh      22/tcp                          # SSH Remote Login Protocol
ssh      22/udp                          # SSH Remote Login Protocol
telnet   23/tcp
telnet   23/udp
smtp     25/tcp    mail
smtp     25/udp    mail
time     37/tcp    timserver
time     37/udp    timserver
finger   79/udp
http     80/tcp    www www-http          # WorldWideWeb HTTP
http     80/udp    www www-http          # HyperText Transfer Protocol
```

Port Numbers

- For the latest list of assigned port numbers go to :

http://www.iana.org/assignments/port-numbers

Hosts File

```
#Do not remove the following line, or various
#programs that require network functionality will
#fail.
127.0.0.1   localhost.localdomain localhost
10.3.23.2   intranet.mycompany.com  intranet
10.3.23.3   mail.mycompany.com mail
```

Inetd File

```
# /etc/inetd.conf:  see inetd(8) for further informations.
#
# Internet server configuration database
# Lines starting with "#:LABEL:" or "#<off>#" should not
# be changed unless you know what you are doing!
#
# If you want to disable an entry so it isn't touched during
# package updates just comment it out with a single '#' character.
#
# Packages should modify this file by using update-inetd(8)
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
#:INTERNAL: Internal services
#echo       stream   tcp  nowait   root internal
#echo       dgram    udp  wait root internal
#chargen    stream   tcp  nowait   root internal
#chargen    dgram    udp  wait root internal
#discard        stream   tcp  nowait   root internal
#discard        dgram    udp  wait root internal
#daytime        stream   tcp  nowait   root internal
#daytime        dgram    udp  wait root internal
#time       stream   tcp  nowait   root internal
#time       dgram    udp  wait root internal
```

Architecture of Unix

- Basic Utilities
  - Directory/File management: cd, ls, pwd, mkdir, rmdir, cp, mv, rm, find, du, file
  - File viewing/editing: touch, more, less, ed, vi, emacs
  - User management: passwd, chmod, chown, su, who
  - Process management: kill, killall, ps
  - Documentation: man, info, /usr/share/doc
- Applications: X11, KDE, Gnome, OpenOffice, Apache, Sendmail, Gimp, Mozilla, Firefox
- Security Software: gpg, ssh, iptables, ACID, snort, prelude, tcpdump, ethereal, nmap, nessus, tcpspy, tiger, ClamAV, spamassassin

Important Network Commands

- telnet: Remote login
- ping: Echo request
- su: Switch User
- ftp: File Transfer
- finger: Information

telnet

- Connect to a host machine over the network.

Syntax: telnet [options] {IP or Computer Name} [port number]

Example:

telnet 127.0.0.1

telnet 127.0.0.1 25 SMTP may not be running.

Alternative: **nc** (from the netcat package)

Telnet does not encrypt connections and so is NOT secure.
Use **ssh** for encrypted secure connections.

telnet example

```
$ telnet 127.0.0.1 -l eaa
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Floppix Server floppixeaa
Unauthorized Access Prohibited

floppixeaa login: eaa
Password:

Welcome to Floppix 2.1r6 - Linux on a floppy - developed by L.M.MacEwan
This floppy version of Linux is based on Debian GNU/Linux 2.1.  The programs
in floppix were developed by many and are copyright (C) 1993-1999 Software in
the Public Interest, and others.
Floppix  and  Debian GNU/Linux come with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.  It works for our purposes; your mileage may vary.
For information about Debian, visit the Debian web site at http://www.debian.org
For information about GNU (GNU's not Unix), and the GPL copyleft visit their web
site at http://www.gnu.org.

Have FUN.

$
```

ping

- Send ICMP ECHO-REQUEST packets to a network host.

Syntax: ping [option] {IP or host name}

Options: -f ping flood: send as many as you can.
Must be superuser (root).

Example:

ping 127.0.0.1

ping example

```
PING 127.0.0.1 (127.0.0.1) from 127.0.0.1 : 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=392 usec
64 bytes from 127.0.0.1: icmp_seq=1 ttl=255 time=93 usec
64 bytes from 127.0.0.1: icmp_seq=2 ttl=255 time=35 usec
64 bytes from 127.0.0.1: icmp_seq=3 ttl=255 time=92 usec
64 bytes from 127.0.0.1: icmp_seq=4 ttl=255 time=58 usec
64 bytes from 127.0.0.1: icmp_seq=5 ttl=255 time=92 usec
64 bytes from 127.0.0.1: icmp_seq=6 ttl=255 time=31 usec
64 bytes from 127.0.0.1: icmp_seq=7 ttl=255 time=89 usec
64 bytes from 127.0.0.1: icmp_seq=8 ttl=255 time=33 usec
--- 127.0.0.1 ping statistics ---
9 packets transmitted,
9 packets received,
0% packet loss
round-trip min/avg/max/mdev = 0.031/0.101/0.392/0.106 ms
```

su

- Switch user.

Syntax: su [options] {username or blank}

Example:

```
$ su
Password:
# ping –f 127.0.0.1
# exit
$
```

ftp

- File Transfer Protocol.

Syntax: ftp [options] {IP or Hostname}

Example:

ftp 127.0.0.1

ftp example

```
$ ftp 127.0.0.1
Connected to 127.0.0.1.
220 floppixeaa FTP server (Version 6.2/OpenBSD/Linux-0.10)
    ready.
Name (127.0.0.1:eaa): eaa
331 Password required for eaa.
Password:

*******   Message of the Day

230 User eaa logged in.
Remote system is UNIX
Using binary mode to transfer files
ftp>
```

finger

- User information lookup.

Syntax: finger [option] {user@computer}

Example:

finger root

finger (username)

finger example

```
$ finger earias
Login: earias                   Name: Edward Arias
Directory: /home/earias                Shell: /bin/bash
Last login Thu Jun 27 08:22 (EDT) on :0
No mail.
No Plan.
```

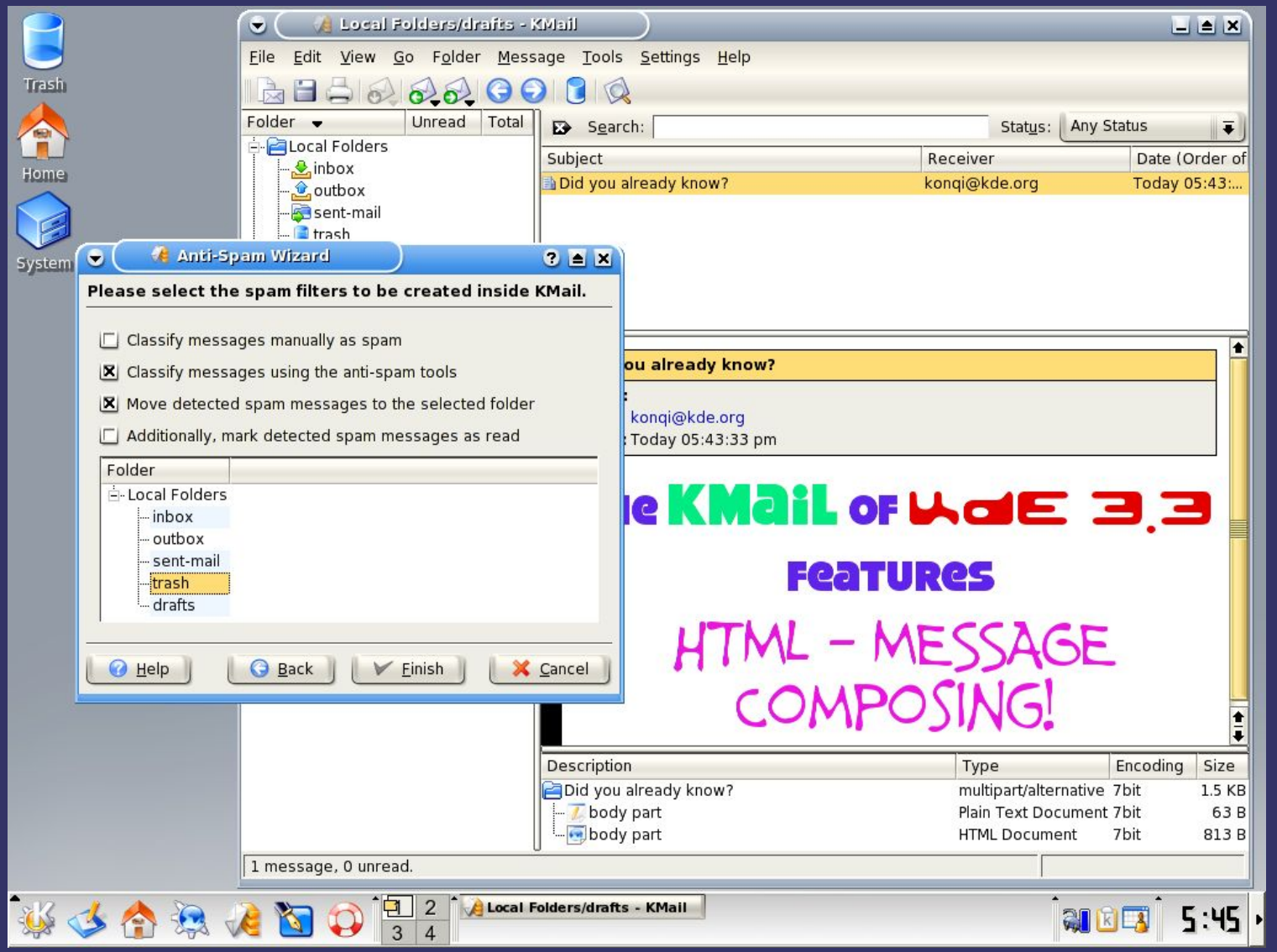
CLI vs. GUI

- CLI: Command Line Interface: type declarative commands to tell the computer exactly what you want it to do. Advantage: greater flexibility.
- GUI: Graphical User Interface: use a pointer to select from menus and other graphical widgets to tell the computer what to do. Advantage: easier to use (for some things).

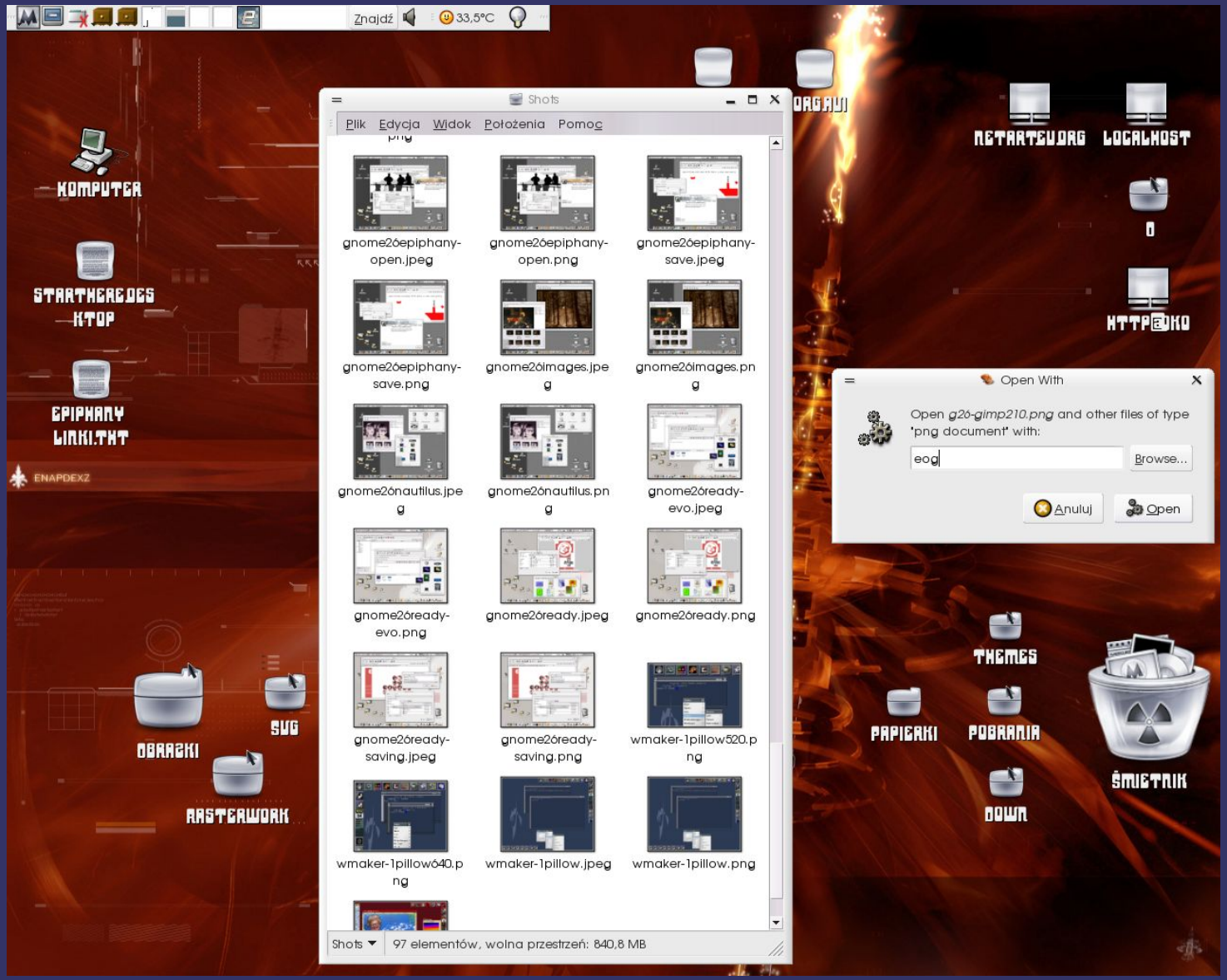
The X Window System (X11)

- Created at MIT (1984 project Athena)
- Primary software for running a GUI on Unix.
- Handles the communication between the terminal and the server (main computer).
- You need a “windows manager” to handle how the windows will look on your computer.

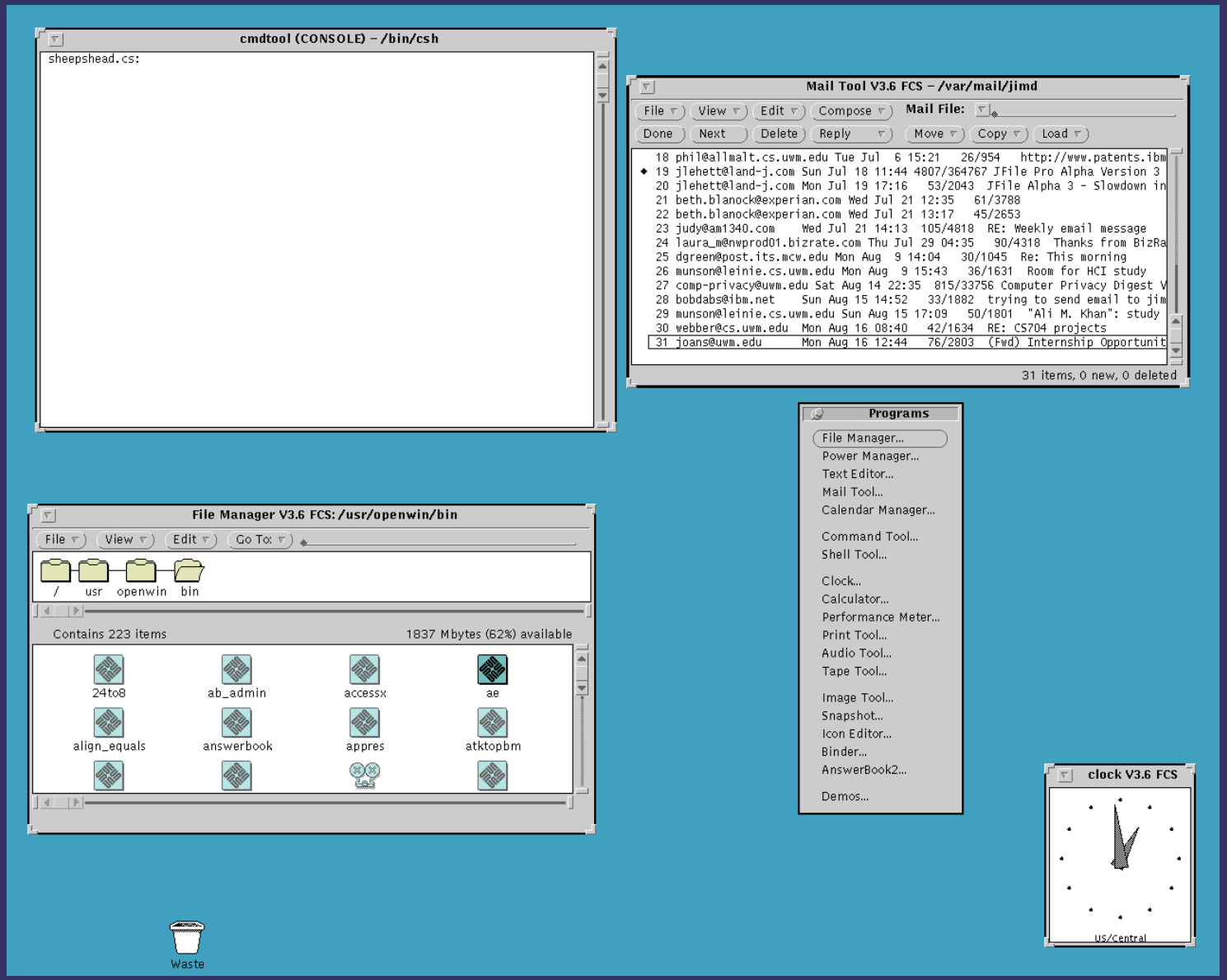
The K Desktop Environment (KDE)



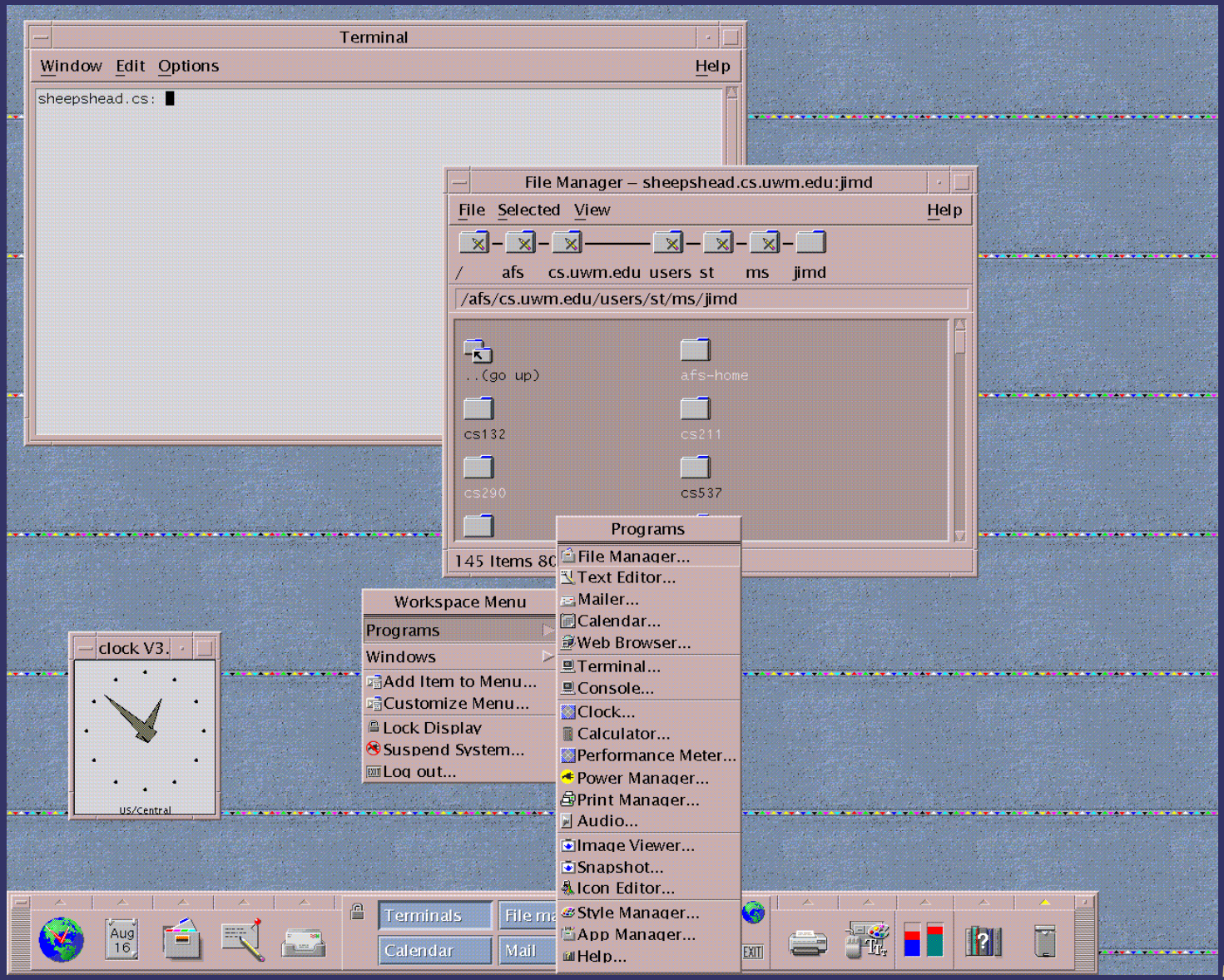
GNOME


Znajdź
33,5°C
Shots
Plik Edycja Widok Położenia Pomoc
gnome2ópiphany-open.jpeg
gnome2ópiphany-open.png
gnome2ópiphany-save.jpeg
gnome2ópiphany-save.png
gnome2óimages.jpeg
gnome2óimages.png
gnome2ónautilus.jpeg
gnome2ónautilus.png
gnome2óready-evo.jpeg
gnome2óready-evo.png
gnome2óready.jpeg
gnome2óready.png
gnome2óready-saving.jpeg
gnome2óready-saving.png
wmaker-1pillow520.png
wmaker-1pillow640.png
wmaker-1pillow.jpeg
wmaker-1pillow.png
Shots
97 elementów, wolna przestrzeń: 840,8 MB
Open With
Open g2ó-gimp210.png and other files of type "png document" with:
eog
Browse...
Anuluj
Open
KOMPUTER
STARTHERE.DES KTOP
EPIPHANY LINKI.TXT
ENAPDEXZ
OBRAZKI
SVG
ARSTERWORK
ORGAVI
NETARTSV.ORG
LOCALHOST
0
HTTP@KO
THEMES
PAPIERKI
POBRANIA
DOWN
ŚMIETNIK

OpenLook Windows Manager (olwm)



Common Desktop Environment (CDE)



How Do You Boot Unix?
Multi-boot Programs

- Windows NT OS loader- select the OS of choice
- Linux LILO (Linux loader)- the tab key will show
  Selections. Type the name of the OS to load
- Grub – Newer versions of Linux (i.e., 9.0) use this loader to choose the OS
- Other methods to boot- Norton system commander, boot disc, Boot Magic…

Additional Reading

- Bach, Maurice J. The design of the Unix operating system. Englewood cliffs: prentice-hall software series, 1986.
- Kernighan, Brian W., Ritchie, Dennis M. The C programming language. Englewood cliffs: prentice-hall software series, 1988.
- Jerry peek, grace Todino, john Strang learning the Unix operating system, 5th edition , A concise guide for the new user. 5th edition, O'Reilly press, October 2001.
- A great website containing on-line books on hacking Unix systems: http://hal.csd.Auth.gr/unix-books/.
- The Linux Documentation Project: http://www.tldp.org.

Questions?

CJ Fearnley

http://www.cjfearnley.com/UNIX-Linux-Basics.2005.01.pdf