




Computo forense en ambientes Unix

Roberto Gómez Cárdenas
 ITESM-CEM
 rogomez@itesm.mx

Lámina 1

Dr. Roberto Gómez Cárdenas

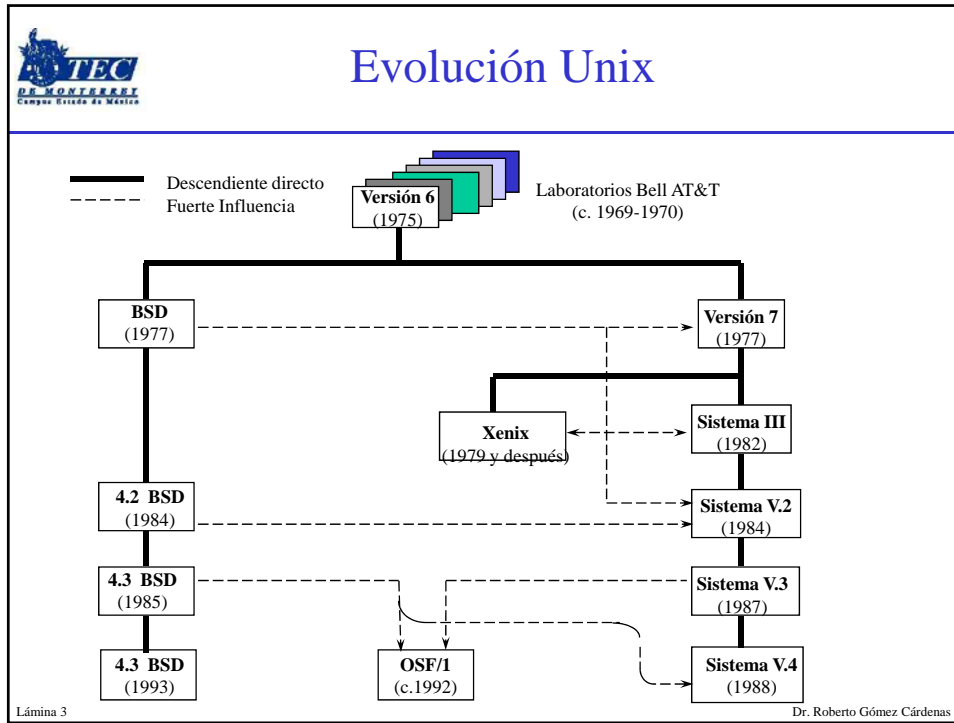


Sistemas Unix y Linux

- Sabores de Unix
 - System V variants, Sun Solaris, IBM AIX, and HP-UX
 - BSD, FreeBSD, OpenBSD, and NetBSD
- Distribuciones Linux
 - Red Hat, Fedora, Ubuntu, and Debian
 - Most consistent UNIX-like OSs
- El núcleo de Linux es regulado bajo la licencia GPL
- Licencia BSD es similar a la de GPL



Lámina 2

Dr. Roberto Gómez Cárdenas

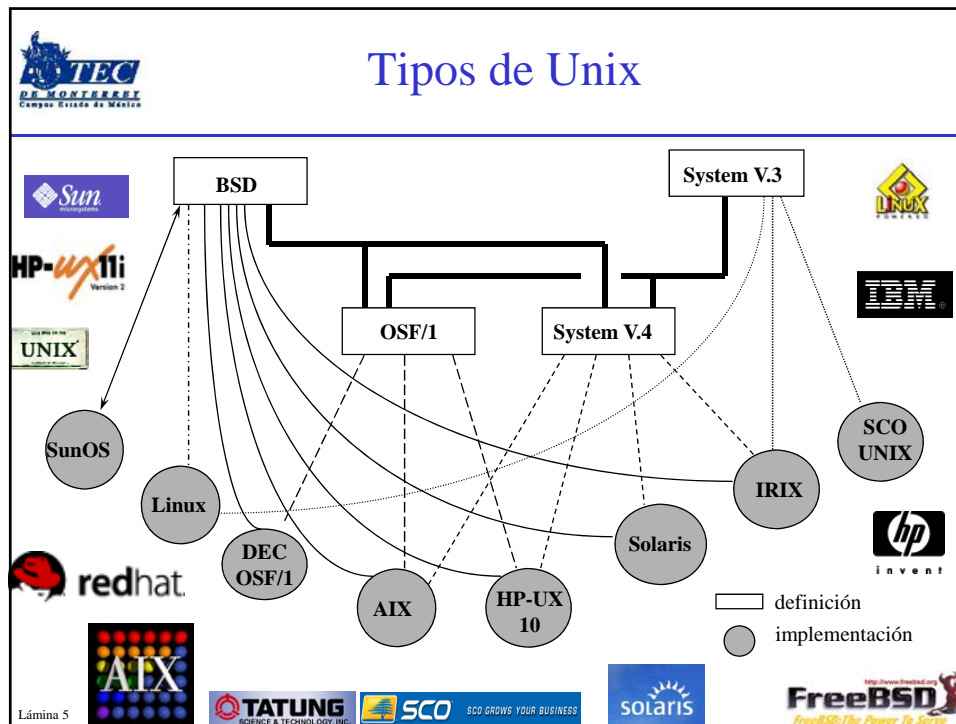


Unix y Bill Gates

- Microsoft Corporation y Santa Cruz Operation (SCO) colaboran para llevar Unix a Intel 8086
- Resultado: XENIX
- Última variante comercial de Unix
- Su primera versión, 2.3, fue liberada en 1980 y vendida para IBMs PC y compatibles
- Última versión 5.0 fue liberada en 1985

Tom Carlson



¿Y Linux ???

- Sistema orientado Unix para diferentes plataformas
- Creado por Linus Torvalds
- Inspirado del sistema operativo Minix desarrollado por A. Tanenbaum para fines académicos
- Bajo licencia GPL (GNU Public Licence)
- Algunas compañías y asociaciones han desarrollado su propia distribución de Linux
- Las distribuciones se diferencian por:
 - la versión del núcleo del sistema operativo (kernel)
 - la combinación de utilerías que la acompaña




Lámina 6 Dr. Roberto Gómez Cárdenas



El origen de Linux

From: torvalds@klavaa.Helsinki.FI (Linus Benedict Torvalds)
Newsgroup: comp.os.minix
Subject: Free minix-like kernel sources for 386-AT
Message-ID: <1991Oct5.054106.4647@ klavaa.Helsinki.FI>
Date: 5 Oct 91 05:41:06 GMT
Organization: University of Helsinki

Do you pine for the nice days of minix-1.1, when men were men and wrote their own device drivers? Are you without a nice project and just dying to cut your teeth on a OS you can try to modify for your needs? Are you finding it frustrating when everything works on minix? No more all-nighters to get a nifty program working? then this post might be just for you :-)

As I mentioned a month(?) ago, I'm working on a free version of a minix-lookalike for AT-386 computers. It has finally reached the stage where it's even usable (though may depending on what you want), and I am willing to put out the sources for wider distribution. It is just version 0.02 (+1 very small) patch already), but I've successfully run bash/gcc/gnu-make/gnu-sed/compress etc. under it

Lámina 7

Dr. Roberto Gómez Cárdenas



Opinión Tanenbaum sobre Linux


What do you think of Linux?

I have never used it. People tell me that if you like lots of bells and whistles, it is a nice system. I would like to take this opportunity to thank Linus for producing it. Before there was Linux there was MINIX, which had a 40,000-person newsgroup, most of whom were sending me email every day. I was going crazy with the endless stream of new features people were sending me. I kept refusing them all because I wanted to keep MINIX small enough for my students to understand in one semester. My consistent refusal to add all these new features is what inspired Linus to write Linux.

Fuente: http://www.cs.vu.nl/~ast/ast_home_page/faq.html

Lámina 8

Dr. Roberto Gómez Cárdenas



Otros núcleos linux libres

- Free BSD (<http://www.freebsd.org>)
 - Derivado de Unix BSD
 - Desarrollo por voluntarios
 - Disponible por ftp o CD's
 - Última versión: 4.5
 - Plataformas: Intel ia32 compatible, DEC Alpha, y PC-98 architectures
- Open BSD (<http://www.openbsd.org>)
 - disponible gratis via ftp o a bajo precio en 3 CD's
 - versión actual: 3.0 (diciembre 2001)
 - desarrollado por voluntarios
 - esfuerzos dirigidos a portabilidad, estandarización, correctness, seguridad proactiva y criptografía integrada
 - Plataformas: i386 - CD bootable, sparc - CD bootable, hp300, amiga, mac68k, macppc - CD bootable, sun3, mvme68k, alpha, vax



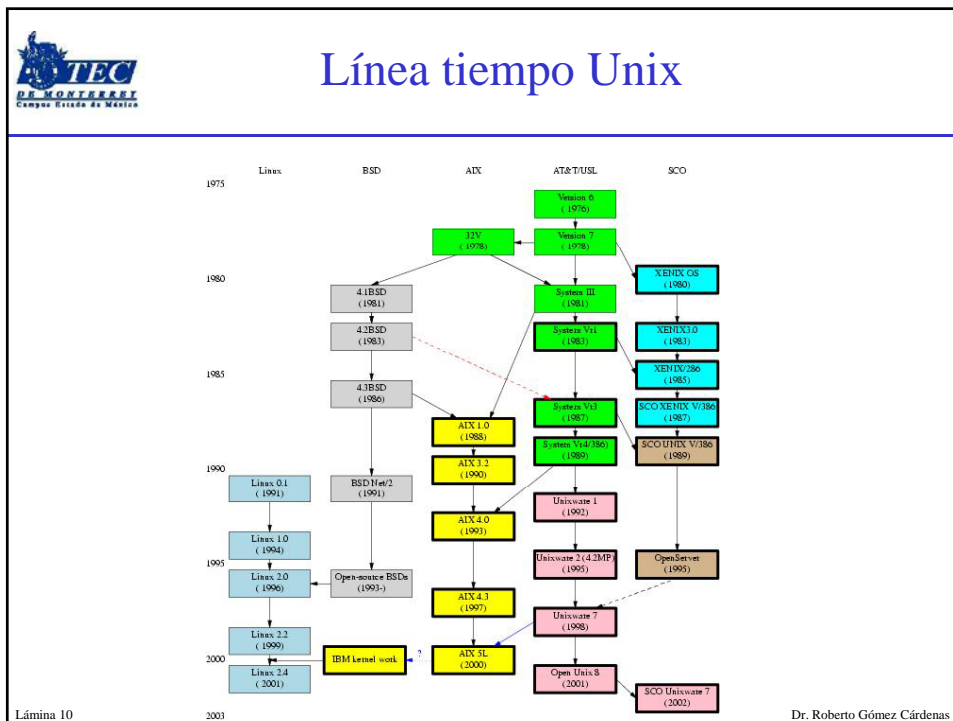
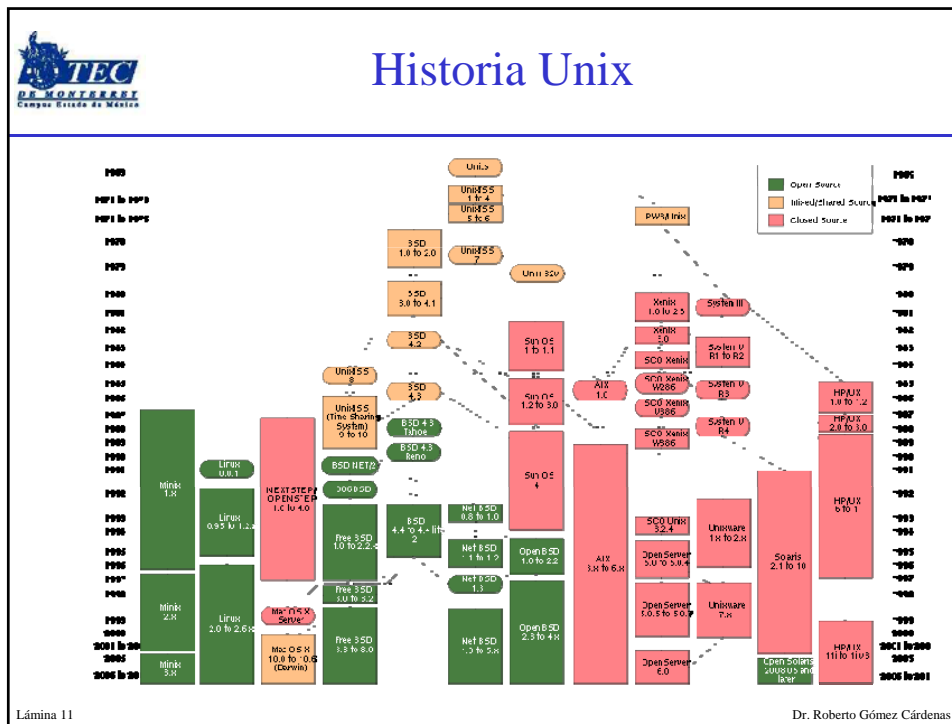



Lámina 9

Dr. Roberto Gómez Cárdenas






El ambiente Unix

- Cuando uno entra al sistema UNIX, el sistema proporciona un **ambiente** propio.
- El **ambiente** del usuario contiene toda la información necesaria, así como ciertas variables.
- Ambiente definido por variables locales y externas.
- Las variables locales sólo son conocidas por el shell que las creó o modificó.
- Las variables exportadas pueden ser vistas por todos los sub-shells.
- Usuario puede definir las variables locales y externas


Lámina 12 Dr. Roberto Gómez Cárdenas



Las variables de entorno/ambiente

- Valor dinámico cargado en la memoria, que puede ser utilizado por varios procesos que funcionan simultáneamente.
- En la mayoría de los sistemas operativos, la ubicación de algunas bibliotecas o de los archivos ejecutables del sistema más importantes puede variar según la instalación.
- Las aplicaciones utilizan estas variables para encontrar configuraciones que ayudan a su ejecución.
- En sistemas UNIX, las variables del entorno están precedidas por el carácter "\$".
 - Se puede usar el comando echo para conocer su contenido.

Lámina 13
Dr. Roberto Gómez Cárdenas




Ejemplos variables

- Ejemplos variables

| Variable | Descripción |
|-----------|--|
| \$ARCH | Contiene la descripción de la arquitectura del equipo. |
| \$DISPLAY | Contiene la identificación de la terminal de visualización que se utilizará en el administrador de ventanas (x11). |
| \$HOME | Muestra la ruta de acceso al directorio actual del usuario. |
| \$HOST | Muestra el nombre del equipo. |
| \$LANG | Muestra el código del idioma predeterminado. |
| \$PATH | Muestra una lista de rutas de acceso a los directorios que contienen archivos ejecutables, separadas por punto y coma. |
| \$SHELL | Indica la ruta del intérprete de comandos utilizado. |
| \$USER | Muestra la identificación del usuario actual. |
- Se puede usar los comandos set, env, printenv para desplegar todas las variables y su valor.

Lámina 14
Dr. Roberto Gómez Cárdenas




Ejemplo salida comando printenv

```

emata@francia:17>printenv
MANPATH=/usr/dt/man:/usr/man:/usr/openwin/share/man
LANG=en_US
OPENWINHOME=/usr/openwin
EDITOR=asedit
LOGNAME=rogomez
MAIL=/var/mail/emata
PS1=$PWD $
USER=rogomez
LC_MESSAGES=C
LC_CTYPE=en_US
DISPLAY=:0.0
SHELL=/bin/ksh
TERM=sun-cmd
PWD=/home/emata
HOME=/home/emata
:
:
LC_COLLATE=en_US
LC_NUMERIC=en_US
TZ=US/Central
HOST=francia.ccm.itesm.mx
HOSTTYPE=sun4
ENV=/home/emata/.kshrc
VENDOR=sun
OSTYPE=solaris
MACHTYPE=sparc
SHLVL=1
GROUP=unknown
emata@francia:18>

```


Lámina 15 Dr. Roberto Gómez Cárdenas



Principales comandos y utilerías

- pwd • rmdir • time • chsh • uniq • lprm • ypserv
- cd • chmod • jobs • chage • tr • df • ypcat
- ls • cp • kill • groupadd • comm • fdisk • ypmatch
- touch • mv • pkill • groupdel • cmp • mkfs • man
- file • which • id • groupmod • diff • fsck • history
- more • whereis • passwd • groups • telnet • dump • alias
- cat • chown • who • date • ftp • restore • tee
- strings • chgrp • whoami • cal • rlogin • mount • tty
- od • find • ulimit • grep • rsh • umount • uname
- tar • umask • su • sort • rcp • showmount • echo
- gzip • ps • sudo • wc • ssh • quota • clear
- gunzip • pgrep • useradd • tail • scp • edquota • catman
- ln • top • userdel • head • lpr • quotacheck • xterm
- mkdir • nice • usermod • cut • a2ps • makedbm • awk
- rm • nohup • chfh • paste • lpq • ypbind • sed


Lámina 16 Dr. Roberto Gómez Cárdenas



Clasificando comandos Unix

- Comandos manejo archivos
- Comandos manejo procesos
- Comandos administración usuarios
- Comandos relacionados con el tiempo
- Comandos tipo filtro
- Comandos comparación archivos
- Comandos de red
- Comandos impresora
- Comandos disco
- Comandos varios


Lámina 17
Dr. Roberto Gómez Cárdenas



Comandos manejo de archivos

| Comando | Descripción |
|---------|---|
| pwd | despliega el directorio de trabajo (¿ontoy?) |
| cd | cambiar de directorio |
| ls | listado de archivos |
| touch | crear archivo (vacío) y actualiza fecha modificación |
| file | tipo de archivo |
| more | desplegar contenido archivo texto por pantalla |
| cat | concatenar archivos |
| strings | desplegar secuencias caracteres imprimibles dentro archivos |
| od | desplegar representacion octal del contenido de un archivo no texto |
| tar | almacenar y extraer archivos de un solo archivo |
| gzip | comprimir archivos a formato .gz |
| gunzip | descomprimir archivos .gz |
| ln | ligas simbolicas y duras |
| mkdir | crear directorio |
| rm | borrar archivo |
| rmdir | borrar directorio (solo directorios vacios) |
| chmod | cambiar permisos archivos |

Lámina 18
Dr. Roberto Gómez Cárdenas



Comandos manejo de archivos

| Comando | Descripción |
|---------|--|
| cp | copiar archivo |
| mv | mover un archivo, renombrar un archivo |
| which | despliega la ruta completa de un comando |
| whereis | localiza el archivo binario, fuente y los archivos de los manuales de un comando |
| chown | cambia el propietario de un archivo |
| chgrp | cambia el grupo propietario de un archivo |
| find | permite encontrar archivos de acuerdo a varios criterios |
| umask | asignación de permisos por default |
| getfacl | desplegar la ACL de un archivo |
| setfacl | asignar campos ACL a un archivo |


Lámina 19
Dr. Roberto Gómez Cárdenas



Comandos manejo procesos

| Comando | Descripción |
|---------|---|
| ps | proporciona una lista de los procesos ejecutandose |
| pgrep | busca entre los procesos ejecutandose |
| top | proporciona una vista de la actividad del procesador a tiempo real |
| nice | ejecuta un comando con una determinada prioridad de calendarización |
| nohup | permite que el programa continúe ejecutandose aun cuando el usuario haya terminado su sesión. |
| time | proporcionando estadísticas sobre el tiempo de ejecución de un programa |
| jobs | imprime una lista de los trabajos ejecutandose y su status |
| kill | envía una señal a un proceso |
| pkill | envía la señal especificada a cada proceso que coincida con el criterio de busqueda |


Lámina 20
Dr. Roberto Gómez Cárdenas



Comando administración usuarios

| Comando | Descripción |
|----------|---|
| id | datos usuario usa el sistema |
| passwd | cambiar el password del usuario |
| who | quien esta usando el sistema |
| whoami | usuario que esta usando el sistema |
| ulimit | control sobre recursos disponibles al shell y los procesos inicializados por él |
| su | cambio de usuario |
| sudo | ejecución de comandos con privilegios root |
| useradd | Añadir un usuario |
| userdel | Eliminar un usuario |
| usermod | Modificar los atributos de un usuario |
| chfn | cambiar información de contacto |
| chsh | cambiar shell especificado |
| chage | cambiar datos del aging de la contraseña |
| groupadd | Añadir un grupo |
| groupdel | Eliminar un grupo |
| groupmod | Modificar los atributos de un grupo |
| groups | lista grupos a los que pertenece |

Lámina 21 Dr. Roberto Gómez Cárdenas



Comandos relacionados con tiempo

| Comando | Descripción |
|---------|--------------------------------|
| date | desplegar y/o definir la fecha |
| cal | calendario |


Lámina 22 Dr. Roberto Gómez Cárdenas



Comandos tipo filtro

| Comando | Descripción |
|---------|--|
| grep | despliega líneas dentro de un archivo que coinciden con una expresión regular |
| sort | ordenar las líneas de un archivo texto |
| wc | contar el número de líneas, palabras y caracteres de un archivo |
| tail | imprime la parte final de un archivo en la salida estándar |
| head | imprime el principio de un archivo en la salida estándar |
| cut | elimina secciones de cada línea de archivos, y el resultado se envía a salida estándar |
| paste | mezcla líneas de archivos |
| uniq | elimina líneas duplicadas de un archivo que se encuentra ordenado |
| tr | traduce o borra caracteres |


Lámina 23 Dr. Roberto Gómez Cárdenas



Comandos comparación archivos

| Comando | Descripción |
|---------|---|
| comm | despliega diferencias de archivos en tres columnas |
| cmp | compara dos archivos e indica, si la hay, el lugar donde se produce la primera diferencia |
| diff | compara el archivo original y el nuevo línea a línea e imprime el resultado en la salida estándar en un formato específico. |

Lámina 24 Dr. Roberto Gómez Cárdenas



Comandos de red

| Comando | Descripción |
|---------|---|
| telnet | permite conectarse a otro sistema (no necesariamente Unix) |
| ftp | permite conectarse a otro sistema distante, con el fin de transferir archivos |
| rlogin | permite conectarse a otro sistema Unix, de la misma forma que telnet |
| rsh | permite ejecutar un comando sobre otra máquina Unix |
| rcp | permite copiar archivos de una máquina a otra. |
| ssh | permite una conexión de forma segura (cifrada) |
| scp | permite copia de archivos de forma segura (cifrada) |

Lámina 25
Dr. Roberto Gómez Cárdenas



Comandos impresora

| Comando | Descripción |
|---------|--|
| lpr | crea un trabajo de impresora en un área de spooling para una impresión subsecuente |
| a2ps | imprime un archivo ASCII en formato postscript |
| lpq | permite ver el estado de las colas de espera de impresión |
| lprm | permite suprimir los archivos en espera de ser impresos |


Lámina 26
Dr. Roberto Gómez Cárdenas



Comandos disco

| Comando | Descripción |
|------------|---|
| df | información sobre el uso de un disco/partición |
| fdisk | comando de manipulación y/o creación de particiones |
| mkfs | formateo de particiones |
| fsck | verificación y reparación de disco |
| dump | copia (vaciado) de información "en bruto" de una partición a un archivo |
| restore | restablecimiento de la información "vacuada" en un archivo |
| mount | montaje de una partición |
| umount | desmontaje de un partición |
| showmount | historial de montajes de un servidor |
| quota | verificación cuotas de usuarios |
| edquota | configuración cuotas usuarios |
| quotacheck | examina sistemas de archivos con cuotas activadas |
| makedbm | construcción de mapas NIS |
| ypbind | asocia un cliente NIS con su servidor |
| ypserv | lanzar el demonio servidor NIS |
| ypcat | interrogación de mapas |
| ypmatch | interrogación de campos de los mapas |
| ypinit | inicialización servidores NIS |


Lámina 27 Dr. Roberto Gómez Cárdenas



Comandos varios

| Comando | Descripción |
|----------|--|
| man | manual, permite conocer todo lo referente a un comando, llamada de sistema o dispositivo |
| history | despliega un historial de lo tecleado por el usuario |
| alias | permite asignar un equivalente, o alias, de un comando |
| tee | lee de la entrada estándar y escribe a la salida estándar y archivos |
| tty | regresa nombre archivo que controla la terminal del usuario |
| uname | identificación del sistema |
| echo | desplegar mensajes o contenido variable |
| clear | limpiar la pantalla |
| catman | activar indexación en manuales para uso opción -k de comando man |
| xterm | se lanza una terminal virtual en modo gráfico |
| awk | utilería de edición de flujo de datos |
| sed | utilería de edición de flujo de datos |
| runlevel | desplegar nivel de ejecución anterior y actual |
| init | cambiar el nivel de ejecución |
| shutdown | apagado y reinicialización del sistema |
| crontab | edición archivo crontab usuarios |
| rpcinfo | información servicios ofrecidos a través protocolo RPC |
| logger | generación de bitácoras |

Lámina 28 Dr. Roberto Gómez Cárdenas




Metacaracteres del shell

- Carácter tilde: ~
 - directorio hogar
 - usando ~ username
 - usando ~+ y ~-
- Carácter dash: -
 - cambio entre directorios específicos
- Carácter asteristico: *
- Carácter signo interrogación: ?
- Los corchetes: []

```

$ pwd
/export/home/user1
$ cd /tmp
$ pwd
/tmp
$ cd -
/export/home/user1
$ cd -
/tmp
$
            
```


Lámina 29
Dr. Roberto Gómez Cárdenas



Los scripts

- Archivos que contienen comandos a ser ejecutados por el shell.
- Puede ser cualquier comando que pueda teclearse a partir del prompt:
 - comando que invoque una utilidad Unix, (vi, netscape, etc)
 - un programa compilado
 - otro script
- Aparte de estos comandos existe un grupo de comandos, (los *comandos de control de flujo*), que fueron diseñados para ser usados en scripts.

Lámina 30
Dr. Roberto Gómez Cárdenas



Principales comandos de control de flujo

- echo
- exit
- read
- let
- break

```
if [ expression ];
then
    statements
else
    statements
fi
```


```
case $var in
val1)
    statements;;
val2)
    statements;;
*)
    statements;;
esac
```

```
for var in list
do
    statements
done
```

```
while [ expression ]
do
    statements
done
```

```
until [ expression ]
do
    statements
done
```

Lámina 31 Dr. Roberto Gómez Cárdenas




Ejemplo scripts

```
toto@cachafas:1>cat quienesta
date
echo Usuarios actualmente conectados
who
toto@cachafas:2> quienesta
quienesta: execute permission denied
toto@cachafas:3> ls -lg quienesta
-rw-r--r-- 1 toto pubs 42 Jun 17 10:55 quienesta
toto@cachafas:4> chmod +x quienesta
-rwxr--r-- 1 toto pubs 42 Jun 17 10:55 quienesta
toto@cachafas:5> quienesta
Fri Jun 17 10:59:40 PDT 1994
Usuarios actualmente conectados
toto console Jun 17 08:26
cachafas tty02 Jun 17 10:04
dongato tty06 Jun 17 08:51
toto@cachafas:6>
```

```
toto@cachafas:6> cat prueba
echo " palabra 1 : \c"
read word1
echo " palabra 2 : \c"
read word2
if test "$word1" = "$word2"
then
    echo Concuerdan
fi
echo Fin del programa
toto@cachafas:7>
```

Lámina 32 Dr. Roberto Gómez Cárdenas




Los sistemas de archivos de Linux

| Nombre | Creador | Año introducción | Log. Máxima nombre archivo | Caracteres permitidos en entradas directorio | Long. máxima pathname | Long. máxima archivo | Long. máxima volumen |
|-----------|--------------------|------------------|----------------------------|--|-----------------------|----------------------|----------------------|
| ext2 | Remy Card | 1993 | 255 bytes | cualquiera excepto NUL | No limite definido | 16 Gb a 2 Tb | 2 Tb a 32 Tb |
| ext3 | Stephen Tweedie | 1999 | 255 bytes | cualquiera excepto NUL | No limite definido | 16 Gb a 2 Tb | 2 Tb a 32 Tb |
| ext4 | Andrew Morton | 2006 | 255 bytes | cualquiera excepto NUL | No limite definido | 16 Gb a 2 Tb | 1024 Pb |
| reiser FS | Namesys | 2001 | 4032 bytes/255 c | cualquiera excepto NUL | No limite definido | 4Gb a 8Tb | 16 Tb |
| reiser4 | Namesys | 2004 | 3976 bytes | cualquiera excepto NUL | No limite definido | 8Tb en x86 | ? |
| GFS | Sistina (Red Hat) | 2000 | 255 bytes | cualquiera excepto NUL | No limite definido | 2Tb a 8Eb | 2Tb a 8Eb |
| OCFS | Oracle Corporation | 2002 | 255 bytes | cualquiera excepto NUL | No limite definido | 8Tb | 8Tb |
| OCFS2 | Oracle Corporation | 2005 | 255 bytes | cualquiera excepto NUL | No limite definido | 4Pb | 4Pb |
| GFS* | Google | 2003 | | | | | |
| NILFS | NTT | 2005 | | | | | |

GFS* = Google File System c= caracteres


Lámina 33
Dr. Roberto Gómez Cárdenas



El nodo-i

- El inodo, nodo-i o nodo índice es una estructura de datos propia de los sistemas de archivos de Unix.
- Cada inodo esta identificado por un número entero, único dentro del sistema de archivoss.
- Los directorios recogen una lista de parejas formadas por un número de inodo y nombre identificativo que permite acceder al archivo en cuestión.
- Cada archivo tiene un único inodo, pero puede tener más de un nombre en distintos o incluso en el mismo directorio para facilitar su localización.
 - Opción -i del comando ls, despliega el nodo-i de un archivo.


Lámina 34
Dr. Roberto Gómez Cárdenas



Propiedades de un archivo

- Identificador de dispositivo del dispositivo que alberga al sistema de archivos.
- Número de inodo que identifica al archivo dentro del sistema de archivos
- Longitud del archivo en bytes.
- Identificador de usuario del creador o un propietario del archivo con derechos diferenciados
- Identificador de grupo de un grupo de usuarios con derechos diferenciados


Lámina 35 Dr. Roberto Gómez Cárdenas



Propiedades de un archivo

- Modo de acceso: capacidad de leer, escribir, y ejecutar el archivo por parte del propietario, del grupo y de otros usuarios.
- Estampillas de tiempo con las fechas de última modificación (mtime), acceso (atime) y de alteración del propio inodo (ctime).
- Número de enlaces, esto es, el número de nombres (entradas de directorio) asociados con este inodo.


Lámina 36 Dr. Roberto Gómez Cárdenas



Sistema archivos ext2

- Sistema de archivos estándar en Linux por varios años y continúa siendo ampliamente utilizado.
 - diseñado originalmente por Rémy Card.
- La principal desventaja de EXT2 es que no posee una bitácora
 - muchos usuarios emigran a ReiserFS y su sucesor EXT3.
- Aunque no es leído por Windows, hay varias utilidades para acceder al EXT2 desde Windows
 - Ext2 IFS For Windows NT4.0 a XP (<http://www.fs-driver.org/>)
 - Explore2fs (<http://uranus.it.swin.edu.au/~jn/linux/explore2fs.htm>)


Lámina 37 Dr. Roberto Gómez Cárdenas



Sistema archivos ext2

- El ext2 tiene un tamaño de i-nodo fijo entre 1 y 4K, independientemente del tamaño de la partición.
- El tamaño del i-nodo se selecciona al crear el sistema de archivos y es seleccionable por el usuario.
- El ext2 tiene una unidad similar al cluster, llamada bloque, y que es, por lo general de 1K, especificable por el usuario e independiente del tamaño de la partición,
 - asegura un buen aprovechamiento del espacio libre con archivos pequeños.


Lámina 38 Dr. Roberto Gómez Cárdenas



Sistema archivos ext2

- El ext2 no usa una FAT, sino una tabla de i-nodos distribuidos en un número determinable de grupos a través de la superficie,
 - permite balancear la distribución de los bloques de archivos en la superficie a través de dichos grupos para asegurar la mínima fragmentación.
- El ext2 tiene un límite máximo de 4GB de archivo, pero no limita el tamaño


Lámina 39
Dr. Roberto Gómez Cárdenas



Los superbloques

- Sistema divide la partición lógica que ocupa en grupos de bloques
- Cada bloque contiene una copia de la información crítica para la integridad del sistema archivos
 - copia del superbloque, y el descriptor del sistema de archivos

Lámina 40
Dr. Roberto Gómez Cárdenas



El superbloque ext2

- Contiene una descripción del tamaño básico y alcance del sistema de archivos
- Información contenida permite al sistema de archivos para usar y mantener el sistema de archivos.
- Usualmente el superbloque en el grupo de bloques 0, se lee cuando el sistema de archivos se monta
 - pero cada grupo de bloques contiene una copia de duplicado en el caso de una corrupción del archivo

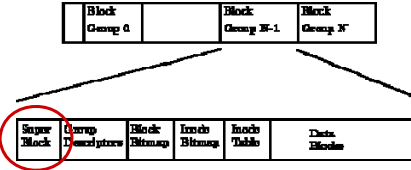



Lámina 41

Dr. Roberto Gómez Cárdenas




Campos superbloque

- **Numero mágico**
 - permite al software de montaje verificar que el superbloque es un sistema archivos EXT2
 - para EXT2 actual este es 0xEF53
- **Nivel revisión**
 - permite verificar si sistema archivos soporta características que solo se encuentran disponibles en revisiones del sistema archivos
- **Mount Count y Maximum Mount Count**
 - permiten determinar si el sistema de archivos debe ser verificado por completo
 - mount count es incrementado cada vez que el sistema es montado y cuando iguala a maximum cont:

maximal mount count reached, running e2fsck is recommended

Lámina 42


Dr. Roberto Gómez Cárdenas



Campos superbloque (cont.)

- **Block Group Number**
 - El numero de grupo de bloque que almacena la copia de este superbloque
- **Block size**
 - tamaño del bloque en este sistema archivos
- **Bloques por grupo**
 - número de bloques en un grupo, al igual que el tamaño del bloque se asigna cuando el sistema de archivos se crea
- **Free blocks**
 - numero de bloques libres en el sistema de archivos
- **Free Inodes**
 - numero de inodes libres en el sistema de archivos
- **First inode**
 - número de inode en el primer inode en el sistema de archivos
 - el primer inode en un sistema archivos raíz EXT2 es la entrada del directorio raíz (/)

Lámina 43
Dr. Roberto Gómez Cárdenas



El descriptor de Grupo de EXT2

- Estructura de datos que describe al grupo
- Se encuentra duplicado en cada grupo de bloques
- Cada descriptor contiene la información siguiente
 - **Blocks Bitmap**
 - numero de bloque que contiene el bitmap para este grupo de bloques
 - usado durante la asignación y desasignación de bloques
 - **Inode Bitmap**
 - bitmap de los inodes
 - usado durante asignación y desasignación de inodes
 - **Inode Table**
 - numero de bloque, del bloque donde inicia la tabla de inodes para el grupo de bloques

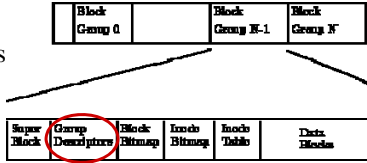



Lámina 44
Dr. Roberto Gómez Cárdenas



El inode el ext2

- mode
 - tipo archivo y permisos
- owner information
 - identificadores usuario y grupo
- size
 - tamaño archivo en bytes
- timestamps
 - tiempo creación y ultima modificación
- datablocks
 - apuntadores a bloques que contienen los datos que el inode esta describiendo
 - último tres son más niveles de inderección

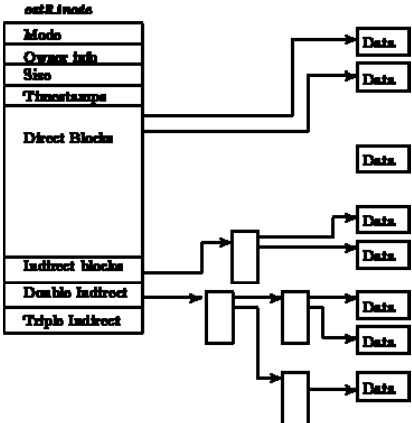



Lámina 45

Dr. Roberto Gómez Cárdenas



Directorios EXT2

- Archivos especiales usados para crear y contener paths de acceso a los archivos del sistema
- Información
 - inode
 - inode para el directorio
 - name length
 - longitud del directorio en bytes
 - name
 - nombre del directorio
- Dos primeras entradas de cada directorio son: “.” y “..”

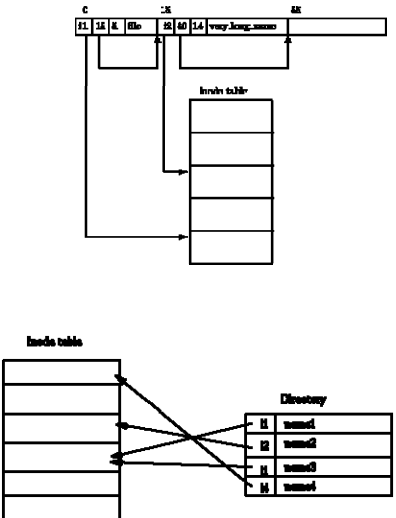



Lámina 46

Dr. Roberto Gómez Cárdenas



Ejemplo entrada directorio

- Formato de la entrada del directorio

número inode

longitud entrada

longitud nombre


nombre archivo

- Ejemplo de un directorio que cuenta con tres archivos: file1, long_file_name y f2

| | | | |
|----|----|----|----------------|
| i1 | 16 | 05 | file1 |
| i2 | 40 | 14 | long_file_name |
| i3 | 12 | 02 | f2 |

Lámina 47

Dr. Roberto Gómez Cárdenas



Descripción física en UNIX (i-nodo)

Bloque de i-nodos

| |
|---------------------------------------|
| Tipo y Protección |
| Número de enlaces |
| Propietario / Grupo |
| Tamaño |
| Fecha: Creación /Modificación/ Acceso |
| Puntero a datos 1 |
| Puntero a datos 2 |
| ⋮ |
| Puntero a datos n |
| Puntero indirecto simple |
| Puntero indirecto doble |
| Puntero indirecto triple |

i-nodo

Bloques de disco


Bloque con dir. de bloques

Puntero indirecto simple

Puntero indirecto doble

Lámina 48

Dr. Roberto Gómez Cárdenas



Interpretación de nombres en Linux

Nombre Nodo-i: Puntero a descripción física del archivo

| | |
|-------|-----|
| • | 2 |
| •• | 2 |
| tmp | 43 |
| users | 342 |
| | |
| usr | 318 |

Directorio con nodo-i 2

| | |
|--------|-----|
| • | 342 |
| •• | 2 |
| marivi | 430 |
| miguel | 256 |
| ... | |
| elvira | 78 |


Directorio con nodo-i 342

| | |
|--------|------|
| • | 256 |
| •• | 342 |
| claves | 758 |
| textos | 3265 |

Directorio con nodo-i 256

Lámina 49

Dr. Roberto Gómez Cárdenas

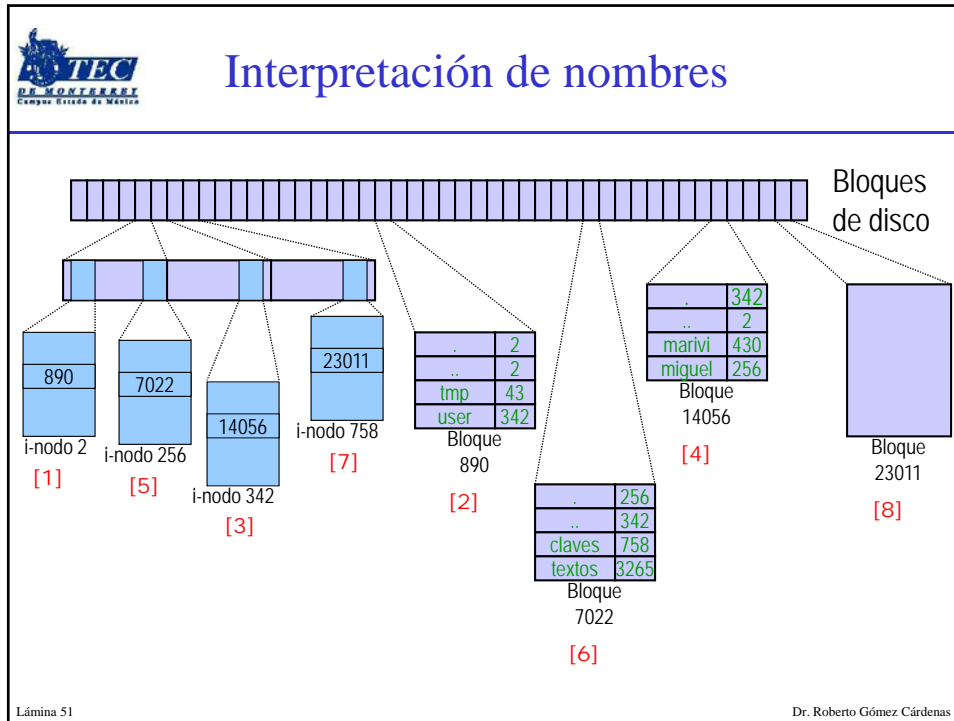


Ejemplo búsqueda archivo

- Considerando: /home/toto/.cshrc
 - Primer inode: el de la raíz del sistema archivos
 - Se encuentra en el superbloque del sistema archivos
 - Para encontrar el inode se debe leer en la tabla de inodes del grupo de bloques apropiado
 - p.e. número inode es 41, es necesario el 42avo. inode de la tabla de inodes del Grupo de Bloques 0
 - El inode raíz es un directorio que contiene entradas de directorio
 - Dentro de las entradas se encuentra home
 - Se lee las entradas de home para encontrar toto
 - Se lee las entradas de toto para encontrar .cshrc
 - De esta última se obtiene los bloques que contienen la información del archivo

Lámina 50

Dr. Roberto Gómez Cárdenas



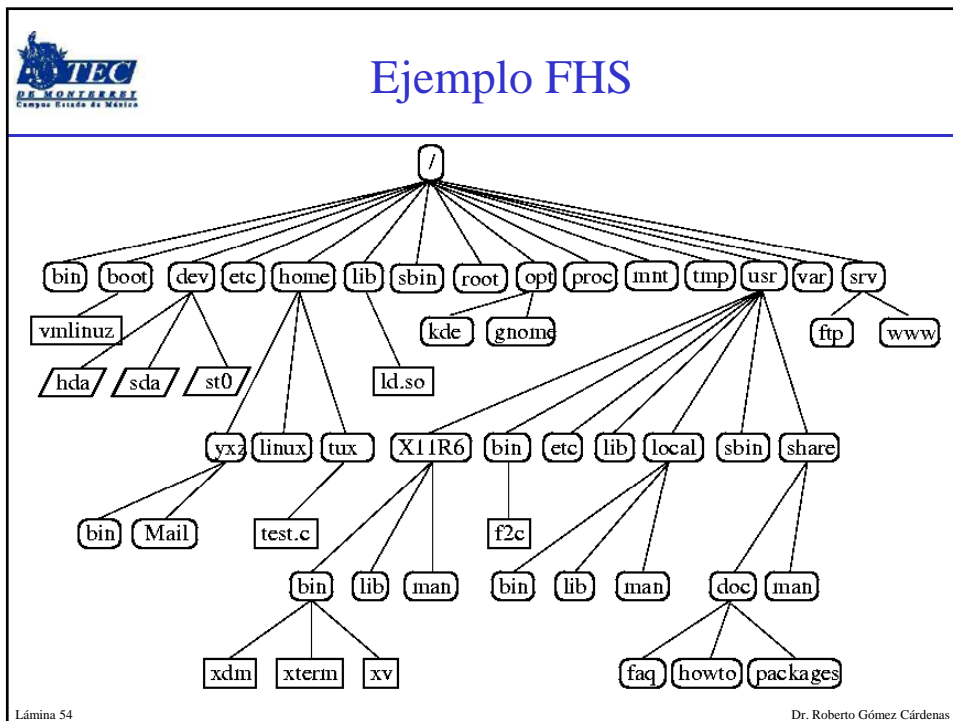
-
- Organización sistema archivos**
- Abstracción que usa el núcleo de Unix para representar y organizar la información contenida en distintos dispositivos de almacenamiento.
 - Toda la información es integrada por el núcleo jerárquicamente bajo un único directorio llamado directorio raíz.
 - FHS The Filesystem Hierarchy Standard
 - forma oficial de organizar los archivos en directorios Linux
 - directorios organizan archivos usuarios, núcleos, logs, programas, utilerías y demás información dentro de diferentes categorías.
- Lámina 52 Dr. Roberto Gómez Cárdenas




Directorios básicos del FHS

| Directorio | Descripción |
|------------|--|
| / | directorio raíz |
| /bin | utilerías esenciales a nivel comando |
| /boot | archivos de arranque |
| /dev | drivers de dispositivos |
| /etc | la mayoría de los archivos de configuración |
| /home | directorios hogar para la mayor parte de los usuarios |
| /lib | librerías/bibliotecas del núcleo y varios comandos de línea |
| /mnt | punto de montaje para dispositivos almacenamiento removibles |
| /opt | aplicaciones como WordPerfect, OpenOffice |
| /proc | información sobre status máquina y procesos ejecutandose |
| /root | directorio hogar para root |
| /sbin | comandos del administrador de sistemas |
| /tmp | archivos temporales |
| /usr | programas pequeños accesibles a todos los usuarios |
| /var | spools de la impresora y bitácoras |

Lámina 53
Dr. Roberto Gómez Cárdenas






Sistemas Archivos AIX

| Archivo | Propósito |
|---------------------------|---|
| /etc/exports | Archivo de configuración |
| /etc/filesystems | Tabla sistema archivo de dispositivos y puntos de montaje |
| /etc/utmp | Información de inicio de sesión del usuario actual |
| /var/adm/wtmp | Información del historial de inicio y cierre de sesión. |
| /etc/security/lastlog | Información del último inicio de sesión del usuario. |
| /var/adm/sulog | Información de cambio intentos de cambio de usuario. |
| /etc/group | Membrecías del grupo para el sistema local. |
| /var/log/syslog | Bitácoras del sistema. |
| /etc/security/passwd | Archivo de contraseña maestra para el sistema local. |
| /etc/security/failedlogin | Información de intento de inicio de sesión fracasada. |


Lámina 55 Dr. Roberto Gómez Cárdenas



Sistema Archivos HP-UX

| Archivo | Propósito |
|--------------------------------|--|
| /etc/utmp y /etc/utmpx | Información del logon del usuario en el sistema. |
| /var/adm/wtmp y /var/adm/wtmpx | Información del historial de logon y logoff. |
| /var/adm/btmp | Información de intento de inicio de sesión fracasada. |
| /etc/fstab | Tabla de sistema archivo de dispositivos y puntos de montaje |
| /etc/checklist | Información de la tabla de sistema de archivo (versión 9.x) |
| /etc/exports | Archivos de configuración |
| /etc/passwd | Archivo de contraseña maestra para el sistema local. |
| /etc/group | Membrecías del grupo para el sistema local. |
| /var/adm/syslog.log | Mensajes de registro del sistema. |
| Syslog | Archivos del sistema de bitácoras. |
| /var/adm/sulog | Información de usuario sustituto tentativo. |


Lámina 56 Dr. Roberto Gómez Cárdenas



Sistema archivos IRIX

| Archivo | Propósito |
|--------------------------------------|---|
| /var/adm/syslog | Archivos del sistema de bitácoras. |
| /etc/exports | Archivos de configuración. |
| /etc/fstab | Tabla de sistema archivo de dispositivos y puntos de montaje. |
| /var/adm/btmp | Información de intento de inicio de sesión fracasada. |
| /var/adm/wtmp and /var/adm/wtmpx | Información del historial de inicio y cierre de sesión. |
| /var/adm/sulog | Información de usuario sustituto tentativo. |
| /etc/shadow | Archivo de contraseña maestra para el sistema local. |
| /etc/group | Membrecías del grupo para el sistema local. |
| /var/adm/utmp/ and /var/adm/utmpx | Información de inicio de sesión del usuario actual |


Lámina 57
Dr. Roberto Gómez Cárdenas



Sistema Archivos Linux

| Archivo | Propósito |
|-------------------|---|
| /etc/exports | Archivos de configuración. |
| /etc/fstab | Tabla de sistema archivos de dispositivos y puntos de montaje |
| /var/log/lastlog | Último inicio de sesión del usuario. |
| /var/log/wtmp | Información del historial de inicio y cierre de sesión. |
| /var/run/utmp | Información de inicio de sesión del usuario actual. |
| /var/log/messages | Mensajes de registro del sistema. |
| /etc/shadow | Archivo de contraseña maestra para el sistema local. |
| /etc/group | Membrecías del grupo para el sistema local. |


Lámina 58
Dr. Roberto Gómez Cárdenas



Sistema Archivos Solaris

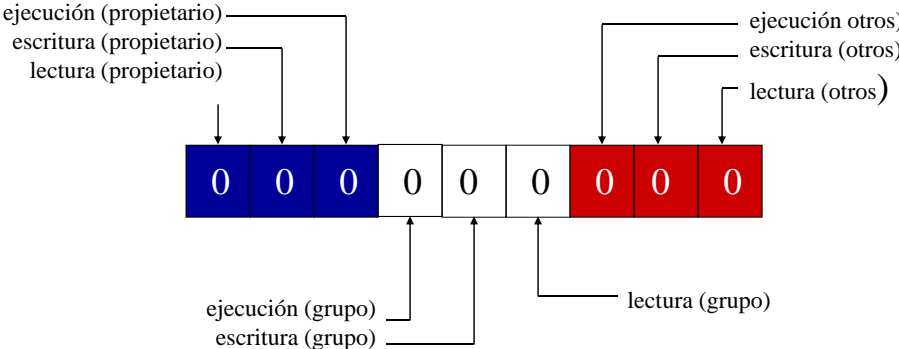
| Archivo | Propósito |
|---|--|
| /etc/passwd | Información de cuentas del sistema. |
| /etc/group | Información de grupos del sistema. |
| /var/adm/sulog | Cambio de información de registro del usuario. |
| /var/adm/utmp | Información de inicio de sesión. |
| /var/adm/wtmp, /var/adm/wtmpx, y /var/adm/lastlog | Información del historial de inicio de sesión. |
| /var/adm/loginlog | Información de inicio de sesión fracasado. |
| /var/adm/messages | Archivos del sistema de bitácoras. |
| /etc/vfstab | Información de archivo de sistema estático. |
| /etc/dfs/dfstab y /etc/vfstab | Archivos de configuración. |

Lámina 59
Dr. Roberto Gómez Cárdenas



Los permisos de los archivos


- Archivos cuentan con permisos, el significado varia un poco entre archivos y directorios



The diagram shows a sequence of nine boxes representing permission bits: three blue boxes (000), three white boxes (000), and three red boxes (000). Arrows point from labels to specific bits:

- Blue boxes: ejecución (propietario) to the first bit, escritura (propietario) to the second, and lectura (propietario) to the third.
- White boxes: ejecución (grupo) to the first bit, escritura (grupo) to the second, and lectura (grupo) to the third.
- Red boxes: ejecución otros to the first bit, escritura (otros) to the second, and lectura (otros) to the third.


Lámina 60
Dr. Roberto Gómez Cárdenas



Significado permisos en directorios

- **r:**
 - autorización de leer el directorio (comando **ls**)
- **w:**
 - autorización de escribir en el directorio
 - (creación, modificación o supresión de archivos)
- **x:**
 - autorización para posesionarse en el directorio (comando **cd**)

Lámina 61
Dr. Roberto Gómez Cárdenas



Comandos útiles para manejo permisos archivos


- Comando **ls -l**
 - despliega los bits de permisos asociado con un archivo o directorio

```

emata@francia:34> ls -l
total 4
drwxr-xr-x 1 cachafas 512 Oct 12 10:13 Sundraw
drwxr-xr-x 1 cachafas 512 Dec 11 20:13 Sunpaint
-rwxr-xr-x 1 cachafas 512 Sep 15 18:13 toto
-rw-r-x--x 1 cachafas 512 Jan 12 1999 curso.html
emata@francia:35>

```


Lámina 62
Dr. Roberto Gómez Cárdenas



El sticky bit

- Aplicable en archivos ejecutables
- Le indica a Unix que deje el ejecutable en memoria después de que esta haya terminado su ejecución
- Dejando el programa en memoria, reduce el tiempo para otros usuarios (en teoría)
- Fue una interesante idea hace tiempo, pero es obsoleta hoy en día
 - técnicas memoria virtual la hacen innecesaria
 - paginación hace que ya no se use


Lámina 63 Dr. Roberto Gómez Cárdenas



Sticky bit y los directorios

- Si un usuario tiene permiso escritura en un directorio puede renombrar o borrar archivos en él (aunque no le pertenezcan)
- Varias nuevas versiones de Unix tiene una forma de impedir lo anterior
- El propietario del directorio puede activar el sticky bit
- Los usuarios que pueden renombrar o borrar archivos en dicho subdirectorio son:
 - el propietario del archivo
 - el propietario del directorio
 - el superusuario

Lámina 64 Dr. Roberto Gómez Cárdenas



Ejemplo uso sticky bit en directorios


```

egarcia>mkdir proyecto
egarcia>chmod 777 proyecto
egarcia>ls -ld
drwxrwxrwx  2 egarcia profes      32 Sep 23 19:30 proyecto

/* usuario jvazquez borra un archivo que no le pertenece */

jvazquez> cd /home/usr/egarcia/proyecto
jvazquez>ls -lg
total 3
-rw-r--r--  1 rogomez  profes  120 Sep 23 19:23 data.rogomez
-rw-r--r--  1 jvazquez  profes 3421 Sep 24 20:03 data.jvazquez
-rw-r--r--  1 egarcia   profes  728 Sep 25 01:34 data.egarcia
-rw-r--r--  1 aortiz    profes  716 Sep 27 12:52 data.aortiz
jvazquez>rm data.aortiz
    
```

Lámina 65 Dr. Roberto Gómez Cárdenas




```

jvazquez>ls -lg
total 2
-rw-r--r--  1 rogomez  profes  120 Sep 23 19:23 data.rogomez
-rw-r--r--  1 jvazquez  profes  3421 Sep 24 20:03 data.jvazquez
-rw-r--r--  1 egarcia   profes  728 Sep 25 01:34 data.egarcia

egarcia>chmod 1777 proyecto
egarcia>ls -ld
drwxrwxrwxt  2 egarcia profes      32 Sep 23 19:30 proyecto

jvazquez>rm data.rogomez
data.rogomez: 644 mode ? y
rm: data.rogomez not removed
Permission denied
jvazquez>
    
```


Lámina 66 Dr. Roberto Gómez Cárdenas



Modificando el sticky bit

- Es posible modificar el sticky bit de un archivo a partir de `chmod`
- Sintaxis: `chmod Innn archivo`
- Donde *nnn* son los permisos del directorio para el propietario, grupo y resto del mundo


Lámina 67 Dr. Roberto Gómez Cárdenas



Los usuarios y los procesos


- Procesos pertenecen a un solo y único usuario
- El propietario es el que lanzó el proceso
 - puede enviarle señales y, en consecuencia, matarlo
- Para lanzarlo debe poseer los permisos de ejecución del archivo que contiene el código binario

Lámina 68 Dr. Roberto Gómez Cárdenas



- La “propiedad” del archivo del código no influye en la del proceso
 - usuario toto ejecuta código de un archivo que pertenece a cachafas
 - el proceso pertenece a usuario toto
- Esto es limitativo
 - se desea permitir a un usuario modificar el contenido de un archivo sin darle derecho de escritura en él
 - ejemplo archivo /etc/passwd, un usuario debe poder cambiar su password sin poder modificar el archivo que lo contiene


Lámina 69 Dr. Roberto Gómez Cárdenas



El bit Set UID (SUID)

- Derecho complementario de un proceso que condiciona la propiedad del proceso que ejecuta su código
- Retomando el ejemplo anterior:
 - si usuario cachafas activa el bit SUID del archivo
 - el usuario toto es el propietario del archivo, pero el propietario efectivo es cachafas
 - toto adquiere los derechos de cachafas durante el tiempo que dure la ejecución del proceso


Lámina 70 Dr. Roberto Gómez Cárdenas



Cuidados del bit SUID

- El bit SUID puede representar un hoyo en la seguridad del sistema
- Es necesario minimizar el número de archivos que pertenezcan al super-usuario y que tengan activado el bit SUID
- Algunas versiones de Unix ignoran el bit SUID y SGID en scripts, solo programas compilados pueden tenerlo activo


Lámina 71 Dr. Roberto Gómez Cárdenas



El bit Set Group ID (SGID)

- Mismo principio que SUID pero para grupos
- Ejecutar un archivo con bit SGID activo asigna el ID de grupo del usuario al mismo que el del archivo ejecutado, durante el tiempo que dura la ejecución de este
- Archivos con SGID o SUID activo pierden sus propiedades especiales cuando son copiados


Lámina 72 Dr. Roberto Gómez Cárdenas



Ejemplo bits SUID y SGID


```
rogomez@armagnac:3>ls -l /usr/bin/passwd /usr/bin/login
                        /usr/bin/mailx /etc/passwd
-rw-r--r--  1 root      752 Oct 22 1998 /etc/passwd
-r-sr-xr-x  1 root      29192 Jul 15 1997 /usr/bin/login*
-r-x--s--x  1 bin       127540 Jul 15 1997 /usr/bin/mailx*
-r-sr-sr-x  3 root      96796 Jul 15 1997 /usr/bin/passwd*
rogomez@armagnac:4>
```

Lámina 73
Dr. Roberto Gómez Cárdenas



El comando chmod y los bits SGID, SUID y sticky

chmod n777 a1



| Valor n | Efecto | Ejemplo | Resultado ls -l a1 |
|---------|------------------------------------|---------------|--------------------|
| 1 | Activar sticky bit | chmod 1777 a1 | -rwxrwxrwt |
| 2 | Activar SGID | chmod 2777 a1 | -rwxrwsrwx |
| 4 | Activar SUID | chmod 4777 a1 | -rwsrwxrwx |
| 6 | Activar SUID y SGID | chmod 6777 a1 | -rwsrwsrwx |
| 0 | Desactivar sticky bit, SUID y SGID | chmod 0777 a1 | -rwxrwxrwx |


Lámina 74
Dr. Roberto Gómez Cárdenas



Ejemplo valores permisos

| Codes values | Descripción |
|--------------|------------------------------------|
| 4000 | UID on execution-set |
| 2000 | GID on execution-set |
| 1000 | Sticky bit-set |
| 0400 | Read by owner-allowed |
| 0200 | Write by owner-allowed |
| 0100 | Excetuion/search by owner-allowed |
| 040 | Read by group-allowed |
| 020 | Write by group-allowed |
| 010 | Excetuion/search by group-allowed |
| 004 | Read by others-allowed |
| 002 | Write by others-allowed |
| 001 | Excetuion/search by others-allowed |

Lámina 75
Dr. Roberto Gómez Cárdenas




Dispositivos

- Núcleo presenta interfaz E/S al sistema y procesos usuario como archivos.
 - programador puede usar operaciones archivos regulares para trabajar con los dispositivos
 - algunos dispositivos son accesibles a comandos como cat
- Archivos dispositivos se encuentran en el directorio /dev
- Ejemplo:


```
$ echo hola mundo > /dev/null
```

Lámina 76
Dr. Roberto Gómez Cárdenas




Identificando dispositivos

- Usar el comando ls -l

| | | | | |
|------------|-------------|-------|--------------|---------|
| brw-rw---- | 1 root disk | 3, 65 | Jul 20 1998 | hdb1 |
| crw-rw-rw- | 1 root root | 1, 3 | Jul 20 1998 | null |
| prw-r--r-- | 1 root root | 0 | Mar 3 19:17 | gpmdata |
| srw-rw-rw- | 1 root root | 0 | Dec 18 07:43 | log |
- Tipos dispositivos
 - Bloque: datos en bloques
 - Caracter: datos en flujo
 - Pipe: parecidos a caracteres, pero existe otro proceso al “otro” lado en lugar de un dispositivo
 - Socket: interfaz de red
- Numeros antes fechas
 - números menores y mayores del dispositivo que ayudan al núcleo a identificar al dispositivo

Lámina 77 Dr. Roberto Gómez Cárdenas




Comando dd y dispositivos

- Nombre dd = convert and copy
- Util cuando se trabaja cuando se trabaja con dispositivos de bloques y caracteres
- Lee desde un archivo de entrada o stream y escribe a un stream o a un archivo de salida, posiblemente llevando a cabo alguna codificación
- Copia datos en bloques de un determinado tamaño
- Ejemplo


```
$ dd if=/dev/zero of=new_file bs=1024 count=1
```

 - copia un bloque de 1024 bytes de /dev/zero al archivo new_file


Lámina 78 Dr. Roberto Gómez Cárdenas



Opciones comando dd

- **if=file**
 - archivo de entrada, default STDIN
- **of=file**
 - archivo de salida, default STDOUT
- **bs=size**
 - tamaño del bloque, posible usar b (512) o k (1024)
- **ibs=size, obs=size**
 - tamaño bloque de entrada y salida
 - si es la mismo tamaño de entrada/salida, usar opción bs
- **count=num**
 - número total de bloques a copiar
 - puede usarse junto con skip para copiar una pequeña parte de información de un dispositivo o archivo grande
- **skip=num**
 - se “salta” los primeros num bloques en el archivo o stream de entrada

Lámina 79
Dr. Roberto Gómez Cárdenas




Convenciones nombres dispositivos Linux

- **Discos ATA (IDE)**
 - /dev/hd*
 - dos ejemplos: /dev/hda1 y /dev/hdb
 - letra después hd identifica el disco y el número representa la partición
 - dispositivo sin número es un dispositivo para todo el disco
- **Discos SCSI**
 - /dev/sd*
 - linux asigna nombres conforme encuentra los discos
 - por ejemplo: para dos controladores SCSI, scsi0 y scsi1, con discos en scsi0 en 0 y 3, y scsi1 en 1, las asignaciones son:

| Controlador | Target | Asignación dispositivo |
|-------------|--------|------------------------|
| scsi0 | 0 | /dev/sda |
| scsi0 | 3 | /dev/sdb |
| scsi1 | 1 | /dev/sdc |


Lámina 80
Dr. Roberto Gómez Cárdenas



Convenciones nombres dispositivos Linux

- Terminales
 - /dev/tty*, /dev/pts/*, /dev/tty
- Puertos seriales
 - /dev/ttyS*
 - no se puede hacer mucho a nivle línea de comandos, demasiadas opciones a configurar (baud rate, flow control, etc)
 - COM1 de Windows = /dev/ttyS0
 - COM2 de Windows = /dev/ttyS1
- Floppy Disks
 - /dev/fd*
- Puertos paralelos
 - /dev/lp0, /dev/lp1
 - corresponden a LPT1 y LPT2 en Windows


Lámina 81 Dr. Roberto Gómez Cárdenas



Convenciones nombres dispositivos Linux

- Dispositivos audio
 - /dev/dsp, /dev/audio, /dev/mixer, /dev/snd/*, etc
 - Linux cuenta con dos diferentes conjuntos de dispositivos de audio
 - dispositivos OSS (Open Sound System)
 - nuevo dispositivo ALSA (Advanced Linux Sound device)


Lámina 82 Dr. Roberto Gómez Cárdenas



Esquemas de particionamiento en Unix y Linux

- Etiquetados como una ruta que empieza en el directorio raíz.
 - Disco maestro primario (/dev/hda)
 - Primera partición es /dev/hda1
 - Segunda partición es /dev/hda2
 - Esclavo primario, maestro secundario, o esclavo (/dev/hdb)
 - Primera partición es /dev/hdb2
 - Controladores SCSI
 - /dev/sda con primera partición /dev/sda1
 - Linux trata dispositivos SATA, USB, y FireWire de la misma forma que dispositivos SCSI.


Lámina 83 Dr. Roberto Gómez Cárdenas



Las bitácoras: el sistema syslog

- Administración de la información generada por el kernel y utilidades del sistema.
- Antes cada programa era libre de elegir su política de logging.
- Comprende
 - un demonio, funciones de biblioteca y un comando
 - permite registrar errores en archivos definidos anteriormente
- Administra mensajes/anuncios en base a niveles y entidades
 - posible enviarlos a otras máquinas para su procesamiento

Lámina 84 Dr. Roberto Gómez Cárdenas



Entidades y su origen

| Entidades | Programa que lo utiliza |
|-----------|--|
| auth | Seguridad y comandos de autorización |
| authpriv | Mensajes de autorización privados (no del sistema) |
| cron | mensajes de los daemons at y cron |
| daemon | mensajes del resto de los daemons |
| kern | mensaje del núcleo |
| lpr | mensajes del subsistema de impresión |
| mail | mensajes del subsistema de correo electrónico |
| news | mensajes del subsistema de noticias |
| security | es igual a auth. Se encuentra en desuso |
| syslog | mensajes del propio subsistema de logs |
| user | mensajes genéricos de los usuarios |
| uucp | mensajes del subsistema UUCP (el cual ya no se usa) |
| local0-7 | reservados para uso local |
| mark | Estampillas de tiempo generadas en tiempos regulares |
| * | Todas las facilidades, excepto "mark" |


Lámina 85
Dr. Roberto Gómez Cárdenas



Los niveles de prioridad (severidad)

| Nivel | Significado aproximado |
|---------|---|
| debug | mensajes de depuración de un programa |
| info | mensajes informativos |
| notice | mensajes de sucesos significativos pero normales |
| warning | mensajes de advertencia |
| warn | es igual a warning. Está en desuso |
| err | mensajes de error |
| error | es igual a err. Está en desuso |
| crit | mensajes que indican condiciones críticas |
| alert | mensajes de alerta. Se debe emprender una acción al momento |
| emerg | el sistema se ha vuelto inoperable |
| panic | es igual a emerg. Está en desuso. |


Lámina 86
Dr. Roberto Gómez Cárdenas



Las acciones

| Acción | Significado |
|--------------------------|--|
| <i>nombre-archivo</i> | Escribir mensaje en un archivo ubicado dentro de la máquina local |
| <i>@hostname</i> | Redireccionar el mensaje al syslogd corriendo en <i>hostname</i> |
| <i>@ipaddress</i> | Redireccionar el mensaje al host en la dirección IP <i>ipaddress</i> |
| <i>user1, user2, ...</i> | Escribir mensaje en la pantalla de los usuarios si están conectados |
| * | Escribir mensaje a todos los usuarios conectados |

Lámina 87 Dr. Roberto Gómez Cárdenas




Ejemplo archivo configuración

```

mail.debug                /usr/spool/mqueue/syslog
auth.info;auth.notice    /usr/adm/auth.info
auth.info;auth.notice    floreal
*.info,mail.none;auth.none /usr/adm/syslog
*.alert                  /usr/adm/noticelog
local0.notice;local0.debug /usr/spool/mqueue/POPlog
local7.notice;local7.info /tmp/essai.syslog
    
```

La mayor parte de los archivos de bitácoras se encuentran en el directorio /var/log


Lámina 88 Dr. Roberto Gómez Cárdenas



Software que usa syslog

| Programa | Entidad | Nivel | Descripción |
|-----------------|--------------|---------------|-----------------------------------|
| cron | cron | info | System task-scheduling daemon |
| ftpd | ftp | debug-crit | FTP daemon (wu-ftpd) |
| imspd | mail | info-alert | IMAP mail server |
| inetd | daemon | err,warning | Internet superdaemon |
| login | authpriv | info-err | Loging programs |
| lpd | lpr | info-err | Line printer deamon |
| named | daemon | info-err | Name server (DNS) |
| passwd | auth | notice,waring | Password-setting program |
| popper | local0 | debug,notice | POP3 mail server |
| sendmail | mail | debug-alert | Mail transport system |
| shutdown | auth | notice | Halts the system |
| su | auth | notice | Switches UIDs |
| sudo | local2 | notice,alert | Limited su program |
| syslog | syslog,mark | info-err | Internal errors,time stamps |
| tcpd | local7 | debug-err | TCP wrapper for inetd |
| vmlinuz | kern | all | The kernel |
| xinetd | configurable | info(default) | Variant of inetd (Red Hat) |


Lámina 89 Dr. Roberto Gómez Cárdenas



Rotación bitácoras

- Una forma de mantener información bitácoras por un periodo fijo se conoce como rotación.
- En rotación se mantiene archivos de respaldo que datan de un día, de dos días ... etc.
- Cada día un programa renombra archivos para empujar datos viejos al final de la cadena.
- Ejemplo: archivo logfile
 - copias respaldo pueden ser llamadas logfile.1, logfile.2 ... etc
 - si se trabaja la semana se llega hasta logfile.7 pero no logfile.8
 - a diario, los datos de logfile.7 se pierden ya que logfile.6 los sobre-escribe


Lámina 90 Dr. Roberto Gómez Cárdenas



Paquete logrotate

- El paquete logrotate contiene una tarea de cron que hace circular automáticamente los archivos de log al archivo de configuración /etc/logrotate.conf y los archivos de configuración en el directorio /etc/logrotate.d.
- Por defecto, se configura para circular cada semana y mantener la validez de los archivos previos de log durante cuatro semanas.

Lámina 91 Dr. Roberto Gómez Cárdenas



Ejemplo archivo configuración logrotate

- Rota /var/log/messages cada semana.
- Mantiene 5 versiones del archivo
- Notifica syslog cada vez que el archivo es re-inicializado.
- Archivos bitácoras Samba son rotados cada semana
 - no son movidos y restablecidos, sino copiados y truncados
 - demonios Samba se les envía señal HUP después de que todos los archivos fueron rotados

```
#Example log rotation policy
error sa-book@admin.com
rotate 5
weekly
/var/log/messages{
    postrotate
        /bin/kill - HUP `cat /var/run/syslogd.pid`
    endscript.
}
/var/log/samba/*.log{
    notifempty
    copytruncate
    sharedscripts
    postrotate
        /bin/kill - HUP `cat /var/lock/samba/*.pid`
    endscript
}
```

Lámina 92 Dr. Roberto Gómez Cárdenas



Archivos bitácoras especiales (i)

- /var/adm/sulog
 - archivo texto, registra las ejecuciones comando su
- faillog
 - guarda el último acceso al sistema lo hace del último intento de acceso de cada usuario
- /var/log/wtmp
 - registra todos los ingresos y salidas al sistema
 - archivo en formato binario, puede verse con comando last
- /var/log/utmp
 - lista los usuarios que están actualmente dentro del sistema
 - archivo binario, contenido visible con comandos who

Lámina 93

Dr. Roberto Gómez Cárdenas




Archivos bitácoras especiales (ii)

- /var/log/lastlog
 - información similar a wtmp pero solo registra el tiempo del último login de cada usuario
 - usado por comandos finger o who y se puede ver con comando lastlog
- /var/log/btmp
 - lista los intentos de ingreso fallidos
 - solo disponible en algunos Unix
- /var/adm/loginlog
 - solo para algunas versiones de Unix
 - registran en él los intentos fallidos de *login*

Lámina 94


Dr. Roberto Gómez Cárdenas



Comandos útiles para forensia en Unix

- **dd**
 - Usando para copiar desde un archivo o dispositivo a un archivo o dispositivo de salida.
- **sfdisk y fdisk**
 - Determinar la estructura del disco.
 - Opción: l del comando fdisk
- **grep**
 - Busca de secuencia caracteres en archivo(s).
 - Opciones: a, b, i, f
- **file**
 - Lee información encabezado archivo, para determinar el tipo y características del archivo.


Lámina 95 Dr. Roberto Gómez Cárdenas



Más comandos

- **xxd**
 - Herramienta de línea de volcado hexadecimal.
 - Opción: s
- **md5sum, sha1sum**
 - Programas para obtener huellas digitales.
 - Opción: c
- **hdparm**
 - Desplegar parámetros específicos a un drive.
 - Opción: I
- **find**
 - Búsqueda de archivos con características particulares.


Lámina 96 Dr. Roberto Gómez Cárdenas



Más comandos

- El dispositivo loop
 - Permite asociar archivos regulares con nodos de dispositivos.
 - Permite montar una imagen de bitstream sin tener que escribirla a un dispositivo y/o disco.
- mount
 - Montar una partición
- umount
 - Desmontar una partición

Lámina 97
Dr. Roberto Gómez Cárdenas




Comando dd

- Sintaxis

`dd if=<origen> of=<destino> [opciones]`

 - Algunas opciones:
 - bs: definir tamaño bloque
 - count: número bloques a copiar
- Otras opciones:
 - Utilería dcfldd
 - Utilería dc3dd.

Lámina 98
Dr. Roberto Gómez Cárdenas



Algunos ejemplos dd


- Creando un archivo imagen (imagen.d1) del dispositivo /dev/fd0 en el


```
dd if=/dev/fd0 of=image.disk1
```
- Escribiendo el contenido del archivo imagen (floppy.dd) en el dispositivo /dev/fd0


```
dd if=floppy.dd of=/dev/fd0
```
- Escribiendo 100 bloques de 512bytes del dispositivo /dev/hda en el archivo imagen.disco.dd


```
dd if=/dev/hda of=imagen.disco.dd bs=512 count=100
```


Lámina 99 Dr. Roberto Gómez Cárdenas



Comando find

- Util para encontrar un archivo que cumpla con determinadas características
- El usuario no necesita de ningún privilegio para poder ejecutar dicho comando
- Sintaxis:
 - find pathname(s) expression(s) action(s)
 - pathname
 - path del directorio donde empezara la busqueda
 - expression
 - criterio de busqueda
 - si la expresión es verdadera, la acción especificada se llevará a cabo


Lámina 100 Dr. Roberto Gómez Cárdenas



Expresiones comando find

| Expresión | Busca archivos que |
|----------------|--|
| -name filename | concurden con el nombre |
| -size [+ -] n | mayores que +n, menores -n o iguales a n |
| -atime [+ -] n | accedidos mas de +n días, menores -n días y exactamente n días |
| -mtime [+ -] n | modificados mas de +n días, menores -n días y exactamente n días |
| -user loginID | tengan propietario a loginID |
| -type | concurden con un tipo archivo (f,d,s) |
| -perm | cuenten con ciertos permisos |


Lámina 101
Dr. Roberto Gómez Cárdenas



Acciones comando find

| Acción | Definición |
|----------------------|---|
| -exec command { } \; | ejecuta command a cada archivo encontrado. Los corchetes {}, delimita donde se pasa el archivo como argumento. Espacio, backslash y punto y coma (\;) delimita el final del comando |
| -ok command { } \; | especifica la forma interactiva de -exec. Requiere entrada antes que find aplique el command al archivo, |
| -print | imprime el path completo en la salida estándar, es el default |
| -ls | imprime el pathname con todas sus características |


Lámina 102
Dr. Roberto Gómez Cárdenas



Ejemplos uso comando find

- Búsqueda archivos desde directorio raíz con SUID activo y pertenientes a root
\$ find / -user root -perm -4000
- Búsqueda archivos llamados core, desde directorio hogar y borrarlos cuando se encuentran
\$ find ~ -name core -exec rm {} \;
- Archivos, desde directorio trabajo, que no han sido modificados en los últimos 90 días
\$ find . -mtime +90
- Archivos mayores que 57 bloques (512-byte blocks) a partir directorio hogar
\$ find ~ -size +57

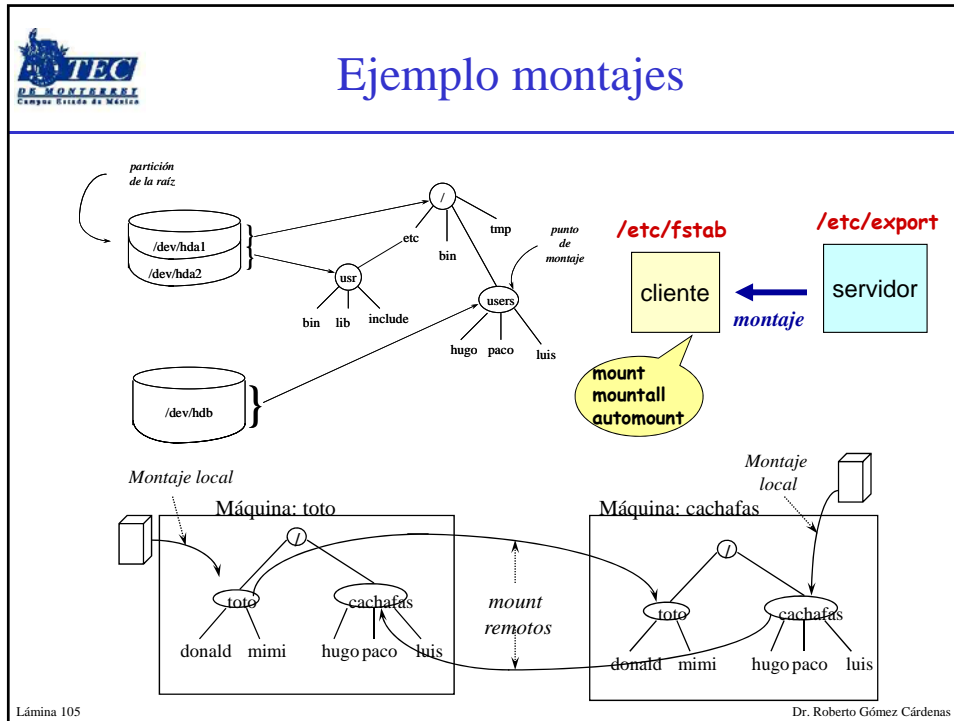
Lámina 103 Dr. Roberto Gómez Cárdenas



Los montajes y el comando mount

- Comando utilizado para montar dispositivos y particiones para su uso por el sistema operativo.
- Montar es hacer que el sistema operativo proyecte el contenido de ese dispositivo o partición en un enlace lógico (un directorio).
- Cuando se desocupa se rompe el enlace y se sigue trabajando con los mismos archivos básicos.

Lámina 104 Dr. Roberto Gómez Cárdenas




El comando mount

- Sintaxis comando mount
mount -t sistema_archivos dispositivo directorio [-o opciones]
- Los argumentos de mount
 - sistemas archivos: cualquiera de los siguientes:

| Tipo | Descripción |
|---------|--|
| ext2 | Sistema de archivos de Linux. |
| msdos | Sistema de archivos de DOS. |
| vfat | Sistema de archivos de Windows 9X (nombres largos) |
| iso9660 | Sistema de archivos de CD-ROM |
| nfs | Sistema de archivos compartido por red ("exportado") |

Lámina 106 Dr. Roberto Gómez Cárdenas




Los argumentos comando mount

mount -t sistema_archivos dispositivo directorio [-o opciones]

- *dispositivo*
 - puede ser cualquier dispositivo del directorio */dev* o, en el caso de nfs, un directorio de otra computadora
- *directorio*
 - directorio donde estará el contenido del dispositivo
- *opciones*
 - pueden ser cualquiera de la tabla
 - en el caso de no poner ninguna opción, mount utilizará las opciones por defecto
 - *rw, suid, dev, exec, auto, nouser, async*

Lámina 107
Dr. Roberto Gómez Cárdenas



Opciones comando mount

| Opción | Descripción |
|--------|---|
| rw | Lectura/escritura. |
| ro | Sólo lectura. |
| exec | Se permite ejecución. |
| user | Los usuarios pueden ``montar''/``desmontar''. |
| suid | Tiene efecto los identificadores de propietario y del grupo |
| auto | Se puede montar automáticamente. |
| async | Modo asíncrono. |
| sync | Modo síncrono. |
| dev | Supone que es un dispositivo de caracteres o bloques. |

- Un ejemplo simple


```
mount /dev/dsk/ls0 /users
```

Lámina 108
Dr. Roberto Gómez Cárdenas



Montando sistemas archivos remotos

- Usar comando mount
- A través de las entradas en la tabla de sistema de archivo: /etc/fstab
 - estas entradas son leídas como respuesta a un comando mount -a o mountall
- Usando el automounter, programa que monta un sistema de archivos por demanda y los desmonta de nuevo si no son accesados durante unos minutos
 - operación controlada usando un conjunto de mapas de automonteo que pueden ser archivos locales o mapas NIS

Lámina 109

Dr. Roberto Gómez Cárdenas



Ejemplo montajes y desmontajes

- Disquete de DOS:


```
# mount -t msdos /dev/fd0 /mnt/floppy -o rw,noexec
# umount /mnt/floppy
```
- Disquete de Windows 9X:


```
# mount -t vfat /dev/fd0 /mnt/floppy -o user,rw
# umount /mnt/floppy
```
- CD-ROM:



```
# mount -t iso9660 /dev/cdrom /mnt/cdrom -o ro
# umount /mnt/cdrom
```
- Directorio exportado de host2:


```
# mount -t nfs host2:/tmp /mnt/host2
# umount /mnt/host2
```
- Montando una imagen en el dispositivo loopback


```
# mount -t vfat -o ro,noexec,loop imagen.dd /mnt/forensia
```

Lámina 110

Dr. Roberto Gómez Cárdenas



Computo forense en ambientes Unix

Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx

Lámina 111

Dr. Roberto Gómez Cárdenas