## IFA. Práctica de laboratorio 02

# Hugo Fonseca Díaz email uo258318@uniovi.es

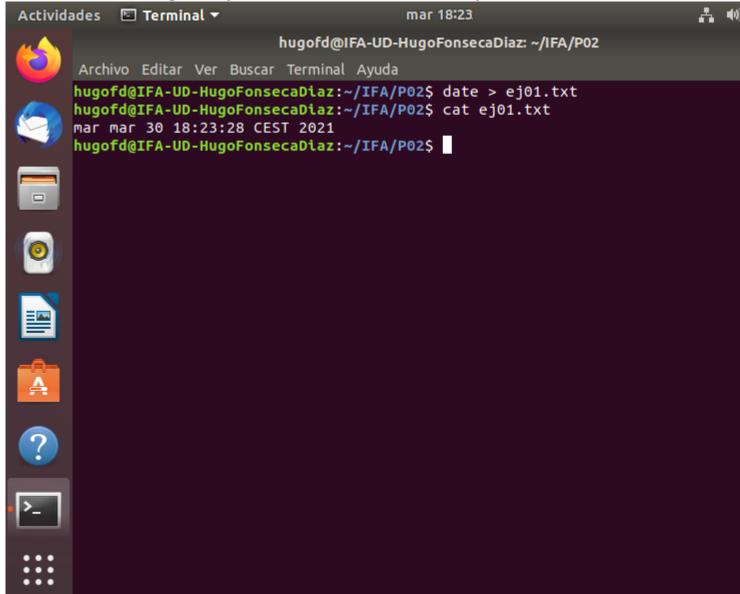
Escuela de Ingeniería Informática. Universidad de Oviedo.

20 de junio de 2021

## 1. Ejercicio 1

Se guarda la fecha y hora del sistema en el archivo ej01.txt con el comando date > ej01.txt. Se muestra ese archivo con el comando cat.

Figura 1: Ejercicio 1: Resultado del comando cat ej01.txt.



Se accede al sitio web https://time.is/es/Spain y se comprueba que la hora es la misma.



Se utiliza el comando uname con las opciones v (lista la versión del kernel) y o (lista el nombre del sistema operativo).

Figura 3: Ejercicio 2: uname -vo. Actividades Terminal ▼ mar 18:52 hugofd@IFA-UD-HugoFonsecaDiaz: ~ Archivo Editar Ver Buscar Terminal Ayuda hugofd@IFA-UD-HugoFonsecaDiaz:~\$ echo "-v lista la versión del kernel, -o l el sistema operativo" -v lista la versión del kernel, -o lista el sistema operativo hugofd@IFA-UD-HugoFonsecaDiaz:~\$ uname -vo #78~18.04.1-Ubuntu SMP Sat Mar 20\_14:10:07 UTC 2021 GNU/Linux hugofd@IFA-UD-HugoFonsecaDiaz:~\$

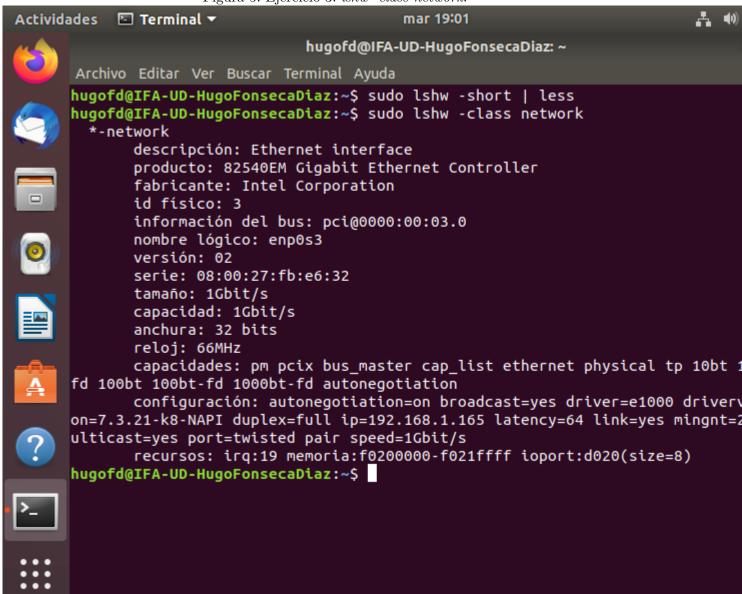
Se utiliza el comando lshw, primero con la flag short para encontrar el nombre de la clase de los dispositivos de red.

Figura 4: Ejercicio 3: lshw -short.

Figura 4: Ejercicio 3: lshw -short.							
Activid	ades 🖆 Terminal	~	mar	19:00	<b>(1)</b>		
4		hu	hugofd@IFA-UD-HugoFonsecaDiaz: ~				
	Archivo Editar Ve	er Buscar Termi	inal Ayuda				
	/0/0		тетогу	128KiB BIOS			
	/0/1		memory	1987MiB Memoria de sistema			
	/0/2		processor	Intel(R) Core(TM) i7-8550U CPU @	1		
	Hz						
	/0/100		bridge	440FX - 82441FX PMC [Natoma]			
	/0/100/1		bridge	82371SB PIIX3 ISA [Natoma/Triton	I		
	/0/100/1.1		storage	82371AB/EB/MB PIIX4 IDE			
	/0/100/2		display	SVGA II Adapter			
	/0/100/3	enp0s3	network	82540EM Gigabit Ethernet Control	le		
	/0/100/4		generic	VirtualBox Guest Service			
	/0/100/5		multimedia	82801AA AC'97 Audio Controller			
	/0/100/6		bus	KeyLargo/Intrepid USB			
	/0/100/6/1	usb1	bus	OHCI PCI host controller			
	/0/100/6/1/1		input	USB Tablet			
	/0/100/7		bridge	82371AB/EB/MB PIIX4 ACPI			
<b>-0-</b>	/0/100/d		storage	82801HM/HEM (ICH8M/ICH8M-E) SATA	C		
A	oller [AHCI mod	_					
	/0/3	scsi1	storage	CD DOW			
	/0/3/0.0.0	/dev/cdrom	disk	CD-ROM			
(?)	/0/4	scsi2	storage	42CD VDOV HADDDIEK			
	/0/4/0.0.0	/dev/sda	disk	42GB VBOX HARDDISK			
	/0/4/0.0.0/1	/dev/sda1	volume	5721MiB partición EXT4			
	/0/4/0.0.0/2	/dev/sda2	volume	4768MiB partición EXT4			
[-]	/0/4/0.0.0/3	/dev/sda3 /dev/sda4	volume volume	23GiB partición EXT4 6626MiB Extended partition			
	/0/4/0.0.0/4		volume	1906MiB partición EXT4			
• • •	/0/4/0.0.0/4/5	/dev/sda5 /dev/sda6	volume	1904MiB partición EXT4			
	/0/4/0.0.0/4/6 :	/dev/Sddo	votune	1904MLB particion EXT4			

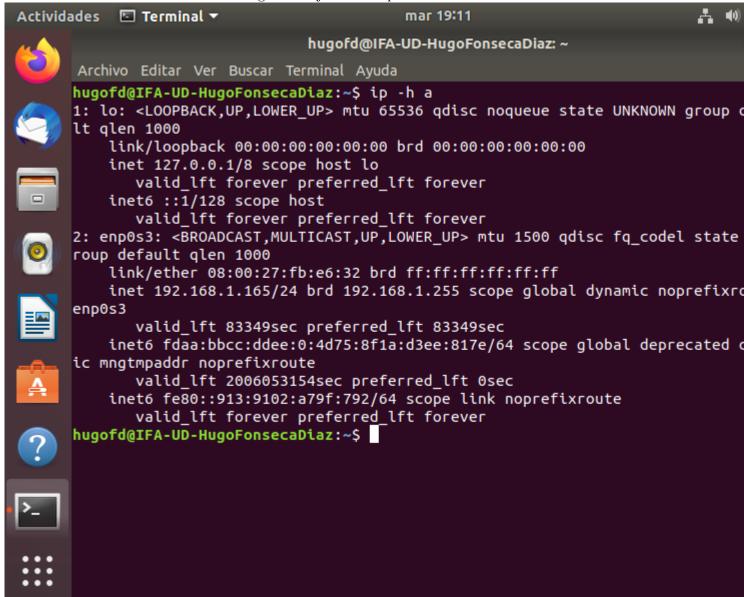
Una vez se sabe que el nombre de la clase de los dispositivos de red es network, se utiliza el comando lshw con la flag -class network.

Figura 5: Ejercicio 3: lshw -class network.



También puede utilizarse el comando ip -h a para mostrar más información sobre el dispositivo de red enp0s3.

Figura 6: Ejercicio 3: ip - h a.



Se utiliza el comando netstat del paquete net-tools. Su flag a permite ver todos los sockets, por lo que sudo netstat -a > ej04.txt guarda la información de los sockets activos y no activos en un fichero de texto. También son interesantes sus flags n (se muestran las direcciones numéricamente), p (se muestran los procesos pertenecientes a los sockets), t (tcp) y u (udp).

Figura 7: Ejercicio 4:  $cat\ ej04.txt\ /\ less.$ 

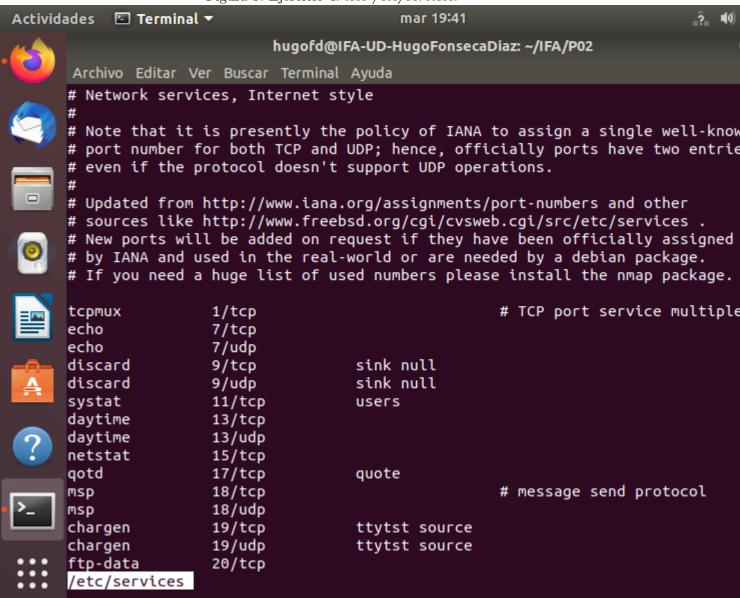
			zjercicio 4. <i>car ej</i>	. ,		
Activid	ades 🖆 Tei	rminal 🔻		mar 19:24		A 🐠
44			hugofd@IFA-U[	)-HugoFonsecaD	iaz: ~/IFA/P0	2
	Archivo Edi	tar Ver Buscar	Terminal Avus	la		
					• *	7
	raw6	0 0 [:: tivos de domi	]:ipv6-icmp	[::]		
	Proto RefC		Type	State	I-Node	Ruta
W. H	unix 2	[ ACC ]	FLUJO	ESCUCHANDO	27759	@/tmp/.ICE-unix/
	unix 2	[ ACC ]	FLUJO	ESCUCHANDO	27310	@/tmp/dbus-q0eqt
	unix 2	[]	DGRAM	25cociii iii bo	27179	/run/user/1000/s
	md/notify					7 - 2 - 7 - 2 - 7 - 2 - 7 - 2 - 7 - 2 - 7 - 7
	unix 2	[ ]	DGRAM		22206	/run/user/121/sy
	d/notify					
	unix 2	[ ACC ]	SEQPACKET	ESCUCHANDO	13206	/run/udev/contro
	unix 2	[ ACC ]	FLUJ0	ESCUCHANDO	27182	/run/user/1000/s
	md/private					
= 🖂	unix 2	[ ACC ]	FLUJ0	ESCUCHANDO	22209	/run/user/121/sy
	d/private					
	unix 2	[ ACC ]	FLUJ0	ESCUCHANDO	27186	/run/user/1000/g
-0-	/S.gpg-age		511176	F.C.C.L.C.L.A.L.D.C.	2227	lava lua desel
A	unix 2	[ ACC ]	FLUJ0	ESCUCHANDO	22377	/run/user/121/gr
	S.gpg-agen		FLUID	ECCUCUANDO	27107	/sup /uses /1000 /s
	unix 2	[ ACC ]	FLUJ0	ESCUCHANDO	27187	/run/user/1000/s
?	unix 2	gent.socket [ ACC ]	FLUJO	ESCUCHANDO	22378	/run/user/121/bu
	unix 2	[ ACC ]	FLUJO	ESCUCHANDO ESCUCHANDO	27188	/run/user/1000/g
		nt.browser	1 2030	ESCOCHANDO	27100	/1 411/ 4361 / 1000/ 9
<u>&gt;</u>	unix 2	[ ACC ]	FLUJO	ESCUCHANDO	27189	/run/user/1000/g
-	/S.gpg-age					,,,, -
	unix 2	[ ACC ]	FLUJO	ESCUCHANDO	22379	/run/user/121/pu
• • •	native					, , , , , , , , , , , , , , , , , , , ,
• • •	:					

Figura 8: Ejercicio 4: sudo netstat -ptun.

	Figura	8: Ejercicio 4: sudo netstat -	-ptun.	
Activid	ades 🖾 Terminal ▼	mar	19:27	? <b>4</b> 0)
44		hugofd@IFA-UD-Hugo	FonsecaDiaz: ~/IFA/P02	
	Archivo Editar Ver Bus	scar Terminal Ayuda		
	hugofd@IFA-UD-HugoFo Conexiones activas o	onsecaDiaz:~/IFA/P02\$ onsecaDiaz:~/IFA/P02\$ de Internet (servidor Dirección local	es w/o)	Estado
	PID/Program name		22. 22.2011 7 2110 23	25 0000
		192.168.1.165:33930	212.230.135.2:53	SYN_SEN
		192.168.1.165:49665	212.230.135.1:53	ESTABLE
0		192.168.1.165:55989	212.230.135.1:53	ESTABLE
		192.168.1.165:60327	212.230.135.1:53	ESTABLE
		192.168.1.165:56493	212.230.135.1:53	ESTABLE
A	udp 0 768 472/systemd-resolve	192.168.1.165:45510		ESTABLE
?	nogor agri A-ob-nagor a			
>_				
:::				

También se puede ver información de los servicios de red en /etc/services.

Figura 9: Ejercicio 4: less /etc/services.



Para resolver este ejercicio se usan tres comandos: who muestra los usuarios conectados y la terminal en la que están, tty muestra la terminal conectada actualmente al standard input y uptime muestra el tiempo que ha pasado desde el arranque del sistema.

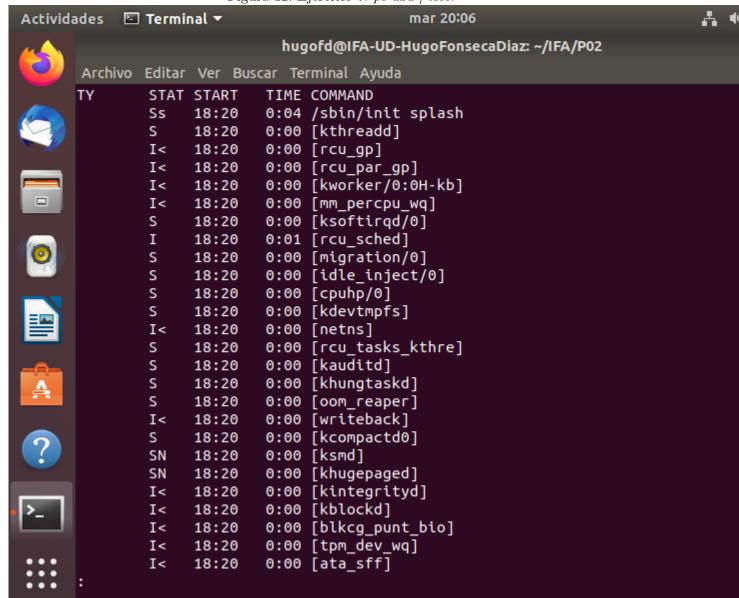
Figura 10: Ejercicio 5: who, tty y uptime. Actividades Terminal ▼ mar 19:47 hugofd@IFA-UD-HugoFonsecaDiaz: ~/IFA/P02 Archivo Editar Ver Buscar Terminal Ayuda hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02\$ who hugofd 2021-03-30 18:21 (:0) hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02\$ tty /dev/pts/0 hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02\$ uptime 19:47:28 up 1:26, 1 user, load average: 0,02, 0,03, 0,00 hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02\$

Existen al menos dos opciones de mostrar la información sobre la tabla de enrutamiento: mediante el comando netstat con su flag r (que muestra la tabla de enrutamiento) o usando el comando route con su flag n (que muestra las direcciones de red de forma numérica).

Figura 11: Ejercicio 6: netstat -r y route -n. Actividades Terminal ▼ mar 19:58 hugofd@IFA-UD-HugoFonsecaDiaz: ~/IFA/P02 Archivo Editar Ver Buscar Terminal Ayuda hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02\$ netstat -r Tabla de rutas IP del núcleo Destino Pasarela Genmask Indic MSS Ventana irtt Ir az default 0.0.0.0 UG 0 0 gateway link-local 0.0.0.0 0 0 255.255.0.0 U 0 er 192.168.1.0 0.0.0.0 255.255.255.0 0 0 0 er hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02\$ route -n Tabla de rutas IP del núcleo Indic Métric Ref Destino Pasarela Genmask Uso Int z 0.0.0.0 192.168.1.1 0.0.0.0 UG 100 0 0 enp 169.254.0.0 0.0.0.0 255.255.0.0 U 1000 0 0 eng 192.168.1.0 0.0.0.0 255.255.255.0 100 0 U 0 enp hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02\$

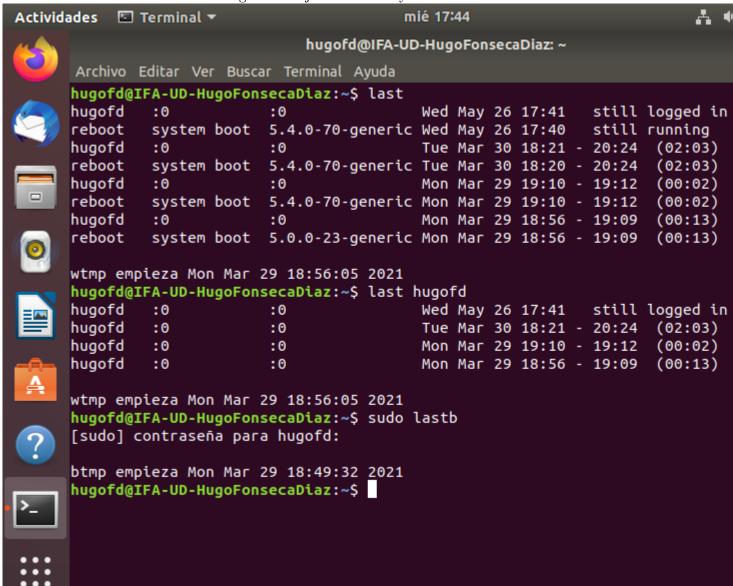
Se usa el comando ps. Dicho comando puede utilizarse siguiendo tres sintaxis: la de UNIX, la de BSD o la de GNU. Para mostrar todos los procesos del sistema con sintaxis de UNIX podría usarse ps -eF. Con sintaxis de BSD se puede usar ps axu. Para que se muestre el nombre del proceso sin cortarse se puede pasar el resultado del comando ps al comando less con una pipe de UNIX.

Figura 12: Ejercicio 7: ps axu / less.



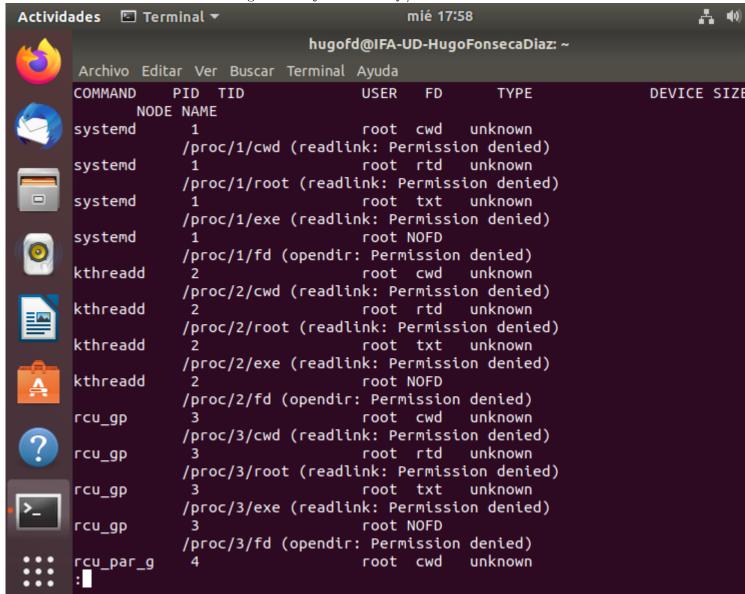
Se usarán los comandos last y lastb. El primero se utiliza para sacar la información de los accesos de todos los usuarios al sistema, incluyendo también un ejemplo de uso para un usuario concreto. El segundo es un comando similar pero buscando en /var/log/btmp, lo que muestra intentos fallidos de acceso al sistema.

Figura 13: Ejercicio 8: last y lastb.



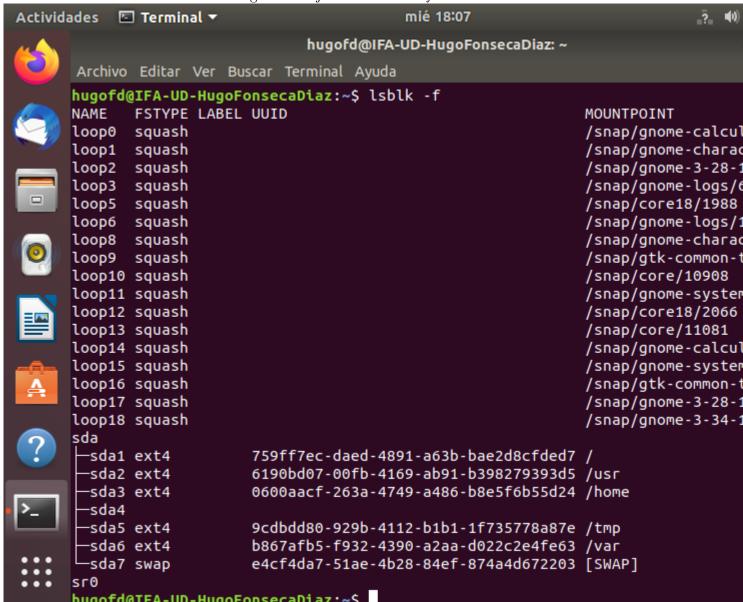
Se utiliza el comando lsof, cuya salida está pensada para ser la entrada de otro programa que la parsee. Se hace una pipe de Unix con el comando less para poder visualizar la salida del comando.

Figura 14: Ejercicio 9: lsof / less.



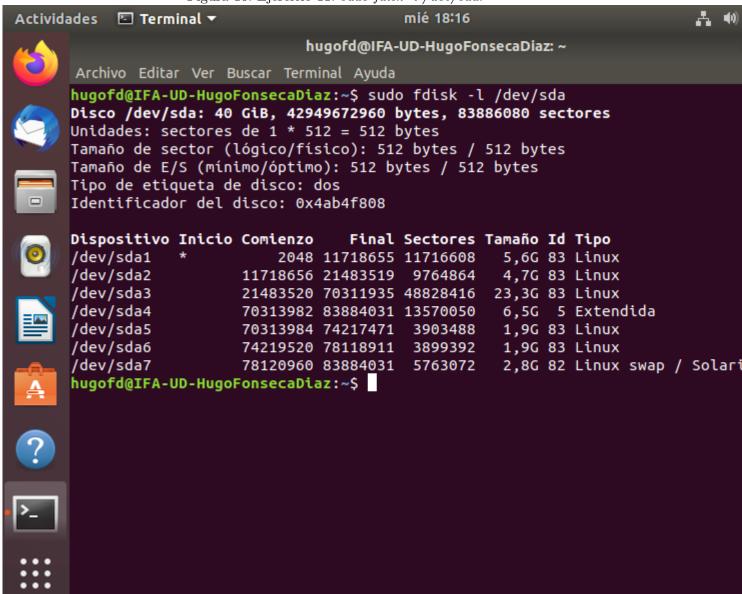
Se puede usar el comando lsblk con la opción f. El comando muestra información de los dispositivos del sistema y la opción f muestra los sistemas de ficheros de los mismos.

Figura 15: Ejercicio 10: lsblk -f.



Para mostrar las particiones del disco sda junto a sus sectores de inicio y fin, se utiliza el comando fdisk con la opción 1, que lista dichas particiones, y pasándole como parámetro el disco que queremos inspeccionar (en este caso /dev/sda). No es necesario especificarle que las unidades del tamaño sean sectores puesto que es el comportamiento por defecto.

Figura 16: Ejercicio 11: sudo fdisk -l /dev/sda.



El fichero donde el kernel almacena las acciones realizadas por cron se encuentra en /var/log/syslog. Puede hacerse un grep con la string cron en dicho archivo para visualizar las acciones, sin embargo, debido al poco espacio en la partición /var, en nuestro caso ese archivo está vacío.

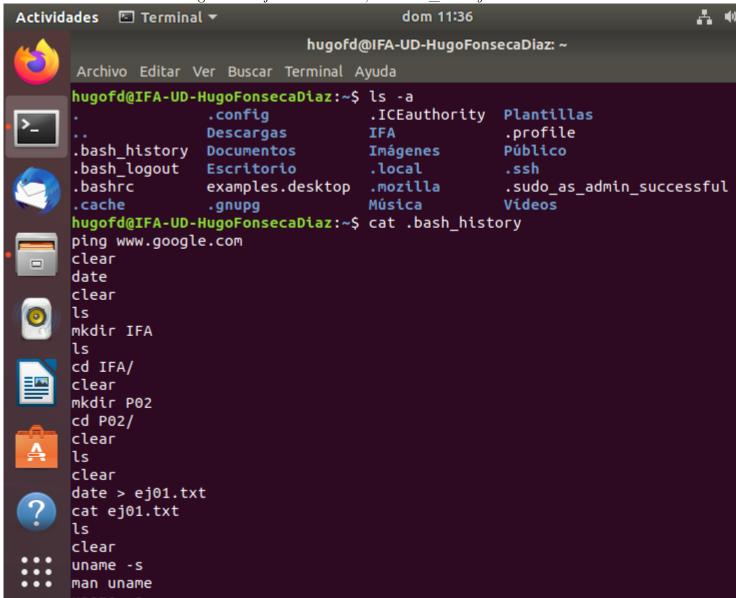
Actividades Terminal ▼ mié 18:30 hugofd@IFA-UD-HugoFonsecaDiaz: ~ Archivo Editar Ver Buscar Terminal Ayuda hugofd@IFA-UD-HugoFonsecaDiaz:~\$ grep cron /var/log/syslog hugofd@IFA-UD-HugoFonsecaDiaz:~\$ cat /var/log/syslog hugofd@IFA-UD-HugoFonsecaDiaz:~\$

Figura 17: Ejercicio 12: grep cron /var/log/syslog.

#### 13. Ejercicio 24

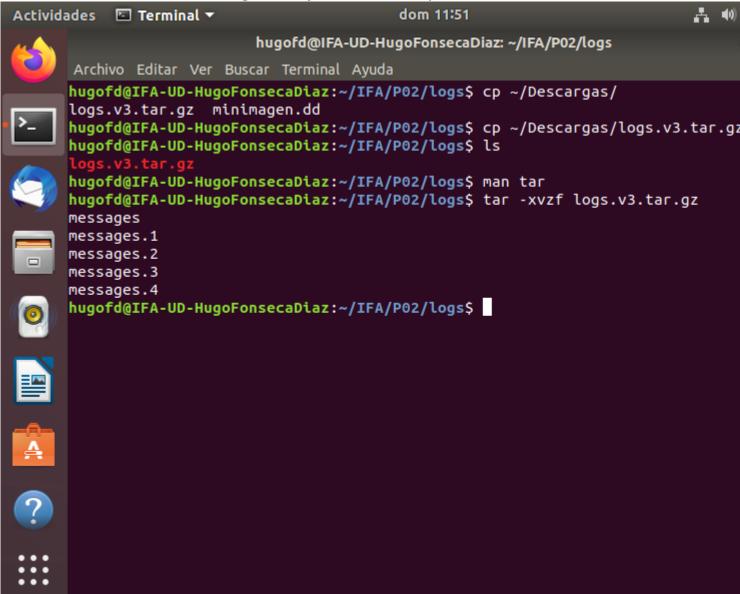
El historial de comandos de bash del usuario se encuentra en un fichero oculto de su carpeta HOME llamado  $bash\_history$ . Se puede utilizar el comando 1s con la flag a para listar todos los archivos, incluidos los ocultos, para comprobar que efectivamente existe el archivo del historial.

Figura 18: Ejercicio 24: ls -a; cat .bash\_history.



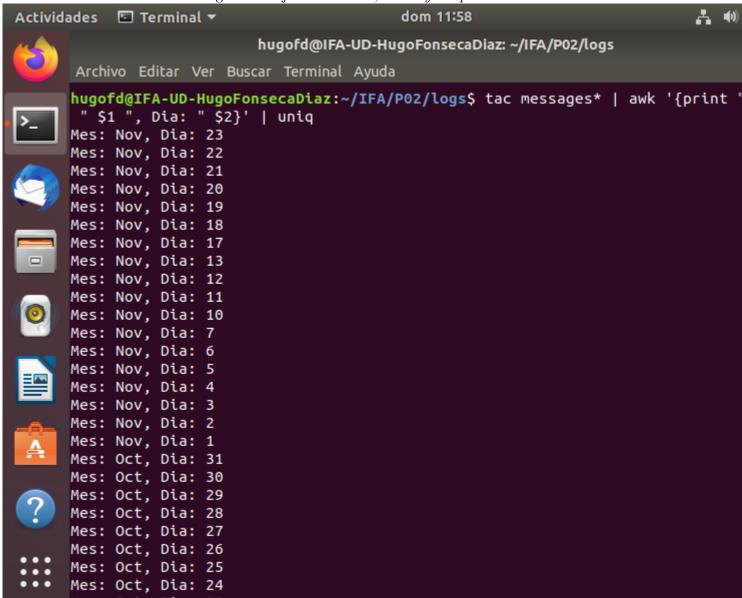
Se descomprime el archivo con el comando tar y las flags xvzf, siendo x una indicación de que se quiere extraer los contenidos del archivo comprimido, v para que lo haga de manera verbosa, z para indicarle al comando que el archivo es un zip y f para pasarle el fichero que se desea extraer al comando.

Figura 19: Ejercicio 27: tar -xvzf.



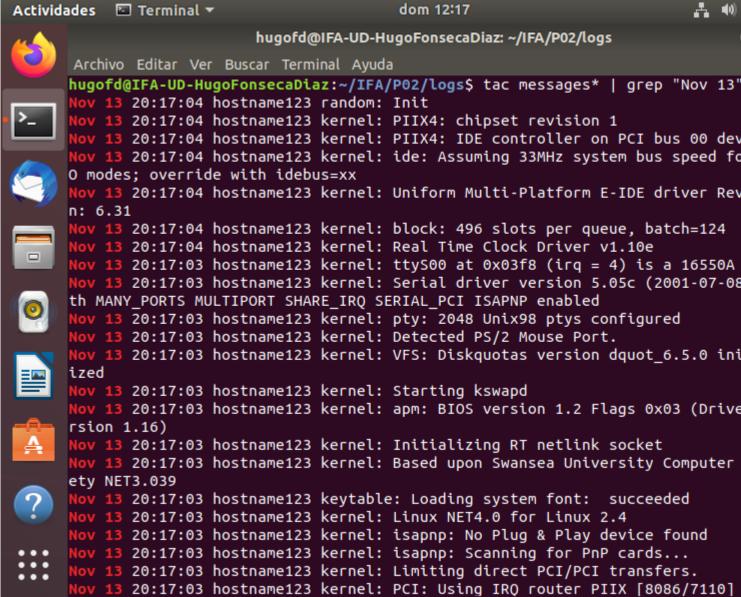
Una vez descomprimidos los ficheros de texto, se procede a utilizar tres nuevas herramientas. Se usa tac para concatenar ficheros de forma inversa (es el comando cat invertido), el lenguaje de programación AWK para procesar texto y el comando uniq para omitir líneas repetidas.

Figura 20: Ejercicio 27: tac, AWK y uniq.



Se usan los comandos tac y grep. El primero se usa para concatenar inversamente los ficheros de los mensajes y el segundo para buscar las líneas donde aparece la cadena de texto "Nov 13".

Figura 21: Ejercicio 28: tac y grep.



#### Referencias