

## Part I

## Monitoratge de registres LOG

Executar un terminal i visualitzar, en temps real, algun dels fitxers de registre del sistema. Veure únicament les noves insercions i indicar els arxius que heu trobat.

Arxius de registre més habituals (poden variar segons la distribució):

- `/var/log/message`: registre de missatges generals del sistema

```
root@user-VirtualBox:/home/user# less +F /var/log/dmesg
```

```

12.850779] kernel: AES CTR mode by software optimization enabled
14.218469] kernel: snd_intelx86 0000:00:05.0: white list rate for 1628:0177 is 48000
16.627924] kernel: audit: type=1400 audit(1616742860.388): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/lsb_release"
16.627924] kernel: audit: type=1400 audit(1616742860.388): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/cups/backend/cups-pdf"
16.790353] kernel: audit: type=1400 audit(1616742860.548): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/cups/snapsnap-confine" pids=515 comm="apparmor_parser"
16.790353] kernel: audit: type=1400 audit(1616742860.548): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/cups/snapsnap-confine" pids=515 comm="apparmor_parser"
16.829966] kernel: audit: type=1400 audit(1616742860.584): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/ppusbkdx"
16.829966] kernel: audit: type=1400 audit(1616742860.584): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/cups/backends/cups-pdf" pids=514 comm="apparmor_parser"
16.858943] kernel: audit: type=1400 audit(1616742860.616): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/cups/backends/cups-pdf" pids=514 comm="apparmor_parser"
16.858950] kernel: audit: type=1400 audit(1616742860.617): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/cupsd"
16.858950] kernel: audit: type=1400 audit(1616742860.617): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/cupsd" pid=514 comm="apparmor_parser"
16.858953] kernel: audit: type=1400 audit(1616742860.618): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/cupsd/nltd party" pids=515 comm="apparmor_parser"
16.858956] kernel: audit: type=1400 audit(1616742860.644): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin/cups-backend" pids=518 comm="apparmor_parser"
16.859490] kernel: audit: type=1400 audit(1616742860.716): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/nvidia_gaodprobe" pid=521 comm="apparmor_parser"
16.859498] kernel: audit: type=1400 audit(1616742860.716): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/nvidia_gaodprobe/kmod" pid=521 comm="apparmor_parser"
25.379307] kernel: kaudtld_printk_skb: 19 callbacks suppressed
25.379307] kernel: audit: type=1400 audit(1616742867.136): apparmor="DENIED" operation="capable" profile="/usr/sbin/cupsbackend" pids=658 comm="cups-backend" capability=caps_cannone=sys_nice
Waiting for data... (Interrupt to abort)

```

- /var/log/auth.log: log d'autenticació

```
root@user-VirtualBox:/home/user# less +F /var/log/auth.log
```

```

Mar 2 13:39:36 user-VirtualBox pkeyexec: pan_unix(polkit:1:session): session opened for user root by (uid=1000)
Mar 2 13:39:36 user-VirtualBox pkeyexec[5772]: user: Executing command [USER=root] [TTY=unknown] [Cwd=/home/user] [COMMAND=/usr/bin/update-notific
er/package-system-locked]
Mar 2 10:14:24 user-VirtualBox systemd-logind[593]: New seat started.
Mar 2 10:14:24 user-VirtualBox systemd-logind[593]: Matching system buttons on /dev/input/event0 (Power Button)
Mar 2 10:14:24 user-VirtualBox systemd-logind[593]: Matching system buttons on /dev/input/event1 (Sleep Button)
Mar 2 10:14:24 user-VirtualBox systemd-logind[593]: Matching system buttons on /dev/input/event2 (AT Translated Set 2 keyboard)
Mar 2 10:17:04 user-VirtualBox CRON[579]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 2 10:17:04 user-VirtualBox CRON[579]: pam_unix(cron:session): session closed for user root
Mar 2 10:17:57 user-VirtualBox udevd[680]: Failed adding user 'vboxadd': data deleted
Mar 2 10:17:57 user-VirtualBox udevd[680]: Failed adding user 'vboxadd': data deleted
Mar 2 10:18:09 user-VirtualBox gdm-autologin: gkr-pam: no password is available for user
Mar 2 10:18:16 user-VirtualBox gdm-autologin[103]: pam_unix(gdm-autologin:session): session opened for user user by (uid=0)
Mar 2 10:18:16 user-VirtualBox gdm-autologin[103]: New session 2 of user user.
Mar 2 10:18:17 user-VirtualBox systemd: pam_unix(systemd:session): session opened for user user by (uid=0)
Mar 2 10:18:17 user-VirtualBox gdm-autologin[103]: gdm: user-gnome-keyring-daemon started
Mar 2 10:19:15 user-VirtualBox dbus-daemon[551]: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=2500ms)
Mar 2 10:19:31 user-VirtualBox gnome-keyring-daemon[1023]: The Secret Service was already initialized
Mar 2 10:20:01 user-VirtualBox polkitd[103]: [103] The MCS21 component was already initialized
Mar 2 10:20:51 user-VirtualBox polkitd[103]: Registered Authentication Agent for unix-session:2 (system bus name: i486 /usr/bin/gn
ome-shell), object path /org/freedesktop/PolicyKit1/AuthenticationAgent, Local e = 5177-0
Mar 2 10:22:18 user-VirtualBox pkeyexec[2505]: user: Executing command [USER=root] [TTY=unknown] [Cwd=/home/user] [COMMAND=/usr/bin/update-notific
er/package-system-locked]
Mar 2 10:23:40 user-VirtualBox sudo: pam_unix(sudo:auth): Couldn't open /etc/security: No existe el archivo o el directorio
Mar 2 10:23:40 user-VirtualBox sudo: user: TtyPath=0 : Pwd=/home/user : USER=root : COMMAND=/usr/bin/su
Mar 2 10:23:40 user-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 2 10:23:40 user-VirtualBox su: (to root) user on pts/5
Mar 2 10:23:40 user-VirtualBox su: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 2 10:30:02 user-VirtualBox CRON[3263]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 2 10:30:02 user-VirtualBox CRON[3263]: pam_unix(cron:session): session closed for user root

```

- `/var/log/kern.log`: registre del kernel

```
root@user-VirtualBox:/home/user# less +F /var/log/kern.log
```

```

[info= same as current profile, skipping] profile=unconfined' names="/snap/snapd/1036/usr/lib/snapd/snap-confine" pid=2785 comm=apparmor_parser
Mar 10 20:23:36 user-VirtualBox kernel: [ 572.934272] audit: type=1400 audit(1616763416.59145): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="/snap/snapd/1036/usr/lib/snapd/snap-confine/mount-namespace-capture-helper"
pid=2785 comm=apparmor_parser"
Mar 10 20:23:37 user-VirtualBox kernel: [ 573.886748] audit: type=1400 audit(1616763417.54346): apparmor="STATUS" operation="profile_load" p
[info= same as current profile, skipping] profile=unconfined' names="/snap/snapd/1036/usr/lib/snapd/snap-confine" pid=2788 comm=apparmor_parser"
Mar 10 20:23:38 user-VirtualBox kernel: [ 574.368425] audit: type=1400 audit(1616763418.02347): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap-update-ns.snap-store" pid=2787 comm=apparmor_parser"
Mar 10 20:23:39 user-VirtualBox kernel: [ 575.641977] audit: type=1400 audit(1616763419.30048): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap.snap-store.snap-store" pid=2792 comm=apparmor_parser"
Mar 10 20:23:40 user-VirtualBox kernel: [ 576.945777] audit: type=1400 audit(1616763420.19449): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap.snap-store.ubuntu-software" pid=2793 comm=apparmor_parser"
Mar 10 20:23:40 user-VirtualBox kernel: [ 576.427374] audit: type=1400 audit(1616763420.08450): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap.snap-store.ubuntu-software-local-file" pid=2794 comm=apparmor_parser"
Mar 10 20:23:50 user-VirtualBox kernel: [ 587.078309] audit: type=1400 audit(1616763430.74051): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap.snap-store.hook.configure" pid=2812 comm=apparmor_parser"
Mar 10 20:23:51 user-VirtualBox kernel: [ 588.924772] audit: type=1400 audit(1616763431.60852): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap.snap-store.snap-store" pid=2813 comm=apparmor_parser"
Mar 10 20:23:51 user-VirtualBox kernel: [ 588.058649] audit: type=1400 audit(1616763431.71253): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap.update-ns.snap-store" pid=2811 comm=apparmor_parser"
Mar 10 20:23:52 user-VirtualBox kernel: [ 588.809745] audit: type=1400 audit(1616763432.47254): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap.snap-store.ubuntu-software" pid=2814 comm=apparmor_parser"
Mar 10 20:23:52 user-VirtualBox kernel: [ 588.924772] audit: type=1400 audit(1616763432.58455): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap.snap-store.ubuntu-software-local-file" pid=2815 comm=apparmor_parser"
Mar 10 20:27:22 user-VirtualBox kernel: [ 798.704577] audit: type=1400 audit(1616763642.20456): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap.snap-store.hook.configure" pid=3020 comm=apparmor_parser"
Mar 10 20:27:22 user-VirtualBox kernel: [ 799.211944] audit: type=1400 audit(1616763642.71257): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap.snap-store.ubuntu-software" pid=3019 comm=apparmor_parser"
Mar 10 20:27:23 user-VirtualBox kernel: [ 799.963400] audit: type=1400 audit(1616763643.46058): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap.snap-store" pid=3021 comm=apparmor_parser"
Mar 10 20:27:23 user-VirtualBox kernel: [ 800.099355] audit: type=1400 audit(1616763643.59659): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap.snap-store.ubuntu-software" pid=3022 comm=apparmor_parser"
Mar 10 20:27:24 user-VirtualBox kernel: [ 800.752915] audit: type=1400 audit(1616763644.24946): apparmor="STATUS" operation="profile_replace"
[info= same as current profile, skipping] profile=unconfined' names="snap.snap-store.ubuntu-software-local-file" pid=3023 comm=apparmor_parser"
Waiting for data... (interrupt to abort)

```

- /var/log/cron.log: registre de crond

```
root@user-VirtualBox:/home/user# less +F /var/log/syslog
```

```

updating /var/run/dbus/system_bus_socket -> /run/dbus/system_bus_socket; please update the unit file accordingly.
Mar 3 10:40:17 user-VirtualBox systemd[1]: Reloading.
updating /var/run/dbus/system_bus_socket -> /lib/systemd/system/dbus.socket:5: ListenStream= references a path below legacy directory /var/run/,
updating /var/run/dbus/system_bus_socket -> /run/dbus/system_bus_socket; please update the unit file accordingly.
Mar 3 10:40:19 user-VirtualBox systemd[1]: Reloading.
Mar 3 10:40:18 user-VirtualBox systemd[1]: /lib/systemd/system/dbus.socket:5: ListenStream= references a path below legacy directory /var/run/,
updating /var/run/dbus/system_bus_socket -> /run/dbus/system_bus_socket; please update the unit file accordingly.
Mar 3 10:40:18 user-VirtualBox systemd[1]: Reloading.
Mar 3 10:40:18 user-VirtualBox systemd[1]: /lib/systemd/system/dbus.socket:5: ListenStream= references a path below legacy directory /var/run/,
updating /var/run/dbus/system_bus_socket -> /run/dbus/system_bus_socket; please update the unit file accordingly.
Mar 3 10:40:21 user-VirtualBox tracker-store[3740]: OK
Mar 3 10:40:21 user-VirtualBox systemd[1010]: tracker-store.service: Succeeded.
Mar 3 10:40:22 user-VirtualBox systemd[1]: Reloading.
Mar 3 10:40:22 user-VirtualBox systemd[1]: /lib/systemd/system/dbus.socket:5: ListenStream= references a path below legacy directory /var/run/,
updating /var/run/dbus/system_bus_socket -> /run/dbus/system_bus_socket; please update the unit file accordingly.
Mar 3 10:43:04 user-VirtualBox systemd-resolved[517]: Server returned error NXDOMAIN, mitigating potential DNS violation DVE-2018-0001, retrying
transaction with reduced feature level UUP.
Mar 3 10:43:12 user-VirtualBox update-notifier.desktop[5869]: /var/lib/dpkg/lock:
Mar 3 10:45:29 user-VirtualBox gnome-shell[1636]: JS ERROR: TypeError: area is null#012padArea@resource:///org/gnome/shell/ui/workspace.js:1101
:9#012.updateWindowPositions@resource:///org/gnome/shell/ui/workspace.js:1334:20#012_realRecalculateWindowPositions@resource:///org/gnome/shell/
ui/workspace.js:1311:14#012_recalculateWindowPositions/this._positionWindowsId@resource:///org/gnome/shell/ui/workspace.js:1286:18
Mar 3 10:45:31 user-VirtualBox gnome-shell[1636]: Object 01.0in (0x5eb7f60070), has been already deallocated - impossible to set any property
on it. This might be caused by the object having been destroyed from C code using something such as destroy(), dispose(), or remove() vfuncs.
Mar 3 10:45:31 user-VirtualBox gnome-shell[1636]: == Stack trace for context 0x5eb7c760710 ==
Mar 3 10:45:31 user-VirtualBox gnome-shell[1636]: #0 7ffff3e30c30 b resource:///org/gnome/shell/ui/iconGrid.js:106 (302af12ed5b0 @ 114)
Mar 3 10:45:31 user-VirtualBox gnome-shell[1636]: #1 7ffff3e30c0f b resource:///org/gnome/shell/ui/iconGrid.js:97 (302af12ed53a @ 94)
Mar 3 10:45:31 user-VirtualBox gnome-shell[1636]: #2 7ffff3e30de0 b resource:///org/gnome/shell/ui/iconGrid.js:851 (302af12f41f0 @ 197)
Mar 3 10:45:31 user-VirtualBox gnome-shell[1636]: #3 7ffff3e31aa0 b self-hosted:1007 (16ee0aee9d30 @ 398)
Mar 3 10:45:38 user-VirtualBox PackageKit: daemon quit
Mar 3 10:45:38 user-VirtualBox systemd[1]: packagekit.service: Succeeded.
Waiting for data... (Interrupt to abort)

```

- /var/log/maillog: registre del servidor de mails

No existeix

- /var/log/qmail/ : registre de Qmail

No existeix

- /var/log/httpd/: registre d'errors i accés a Apache

No existeix

- /var/log/lighttpd: registre d'errors i accés a Lighttpd

```
root@user2021:/home/vib01# less +F /var/log/lightdm/lightdm.log
```

```
Waiting for data... (interrupt to abort)
```

Està buit per que no he tocat lighttpd

- /var/log/boot.log : registre d'inici del sistema  
(al estar en binari no es pot mostrar correctament)

```
root@user-VirtualBox:/home/user# less +F /var/Log/boot.log
```

```

ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (1 of 2) A start job is running for Hold until_0 process finishes up (3min 43s / no
limit)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (1 of 2) A start job is running for Hold until_0 process finishes up (3min 43s / no
limit)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (2 of 2) A start job is running for vboxadd.service (3min 44s / 5min 13s)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (2 of 2) A start job is running for vboxadd.service (3min 44s / 5min 13s)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (2 of 2) A start job is running for vboxadd.service (3min 45s / 5min 13s)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (1 of 2) A start job is running for Hold until_0 process finishes up (3min 45s / no limit)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (1 of 2) A start job is running for Hold until_0 process finishes up (3min 46s / no limit)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (1 of 2) A start job is running for Hold until_0 process finishes up (3min 46s / no
limit)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (2 of 2) A start job is running for vboxadd.service (3min 47s / 5min 13s)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (2 of 2) A start job is running for vboxadd.service (3min 49s / 5min 13s)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (2 of 2) A start job is running for vboxadd.service (3min 50s / 5min 13s)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (1 of 2) A start job is running for Hold until_0 process finishes up (3min 50s / no limit)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (1 of 2) A start job is running for Hold until_0 process finishes up (3min 51s / no limit)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (1 of 2) A start job is running for Hold until_0 process finishes up (3min 51s / no limit)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (2 of 2) A start job is running for vboxadd.service (3min 52s / 5min 13s)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (2 of 2) A start job is running for vboxadd.service (3min 52s / 5min 13s)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (2 of 2) A start job is running for vboxadd.service (3min 53s / 5min 13s)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (1 of 2) A start job is running for Hold until_0 process finishes up (3min 53s / no
limit)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (1 of 2) A start job is running for Hold until_0 process finishes up (3min 54s / no limit)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (1 of 2) A start job is running for Hold until_0 process finishes up (3min 54s / no limit)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m (2 of 2) A start job is running for vboxadd.service (3min 55s / 5min 13s)
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m Finished ESC[0;1;31mESC[0mESC[0;31mESC[0m
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m Starting ESC[0;1;31mESC[0mESC[0;31mESC[0m...
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m Starting ESC[0;1;31mESC[0mESC[0;31mESC[0m...
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m Started ESC[0;1;31mESC[0mESC[0;31mESC[0m...
ESC[0;31mESC[0;1;31mESC[0mESC[0;31mESC[0m Started ESC[0;1;31mESC[0mESC[0;31mESC[0m...
Waiting for data... (Interrupt to abort)

```

No existeix

No existeix

(al estar en binari no es pot mostrar correctament)

```
root@user-VirtualBox:/home/user# less +F /var/log/wtmp
```

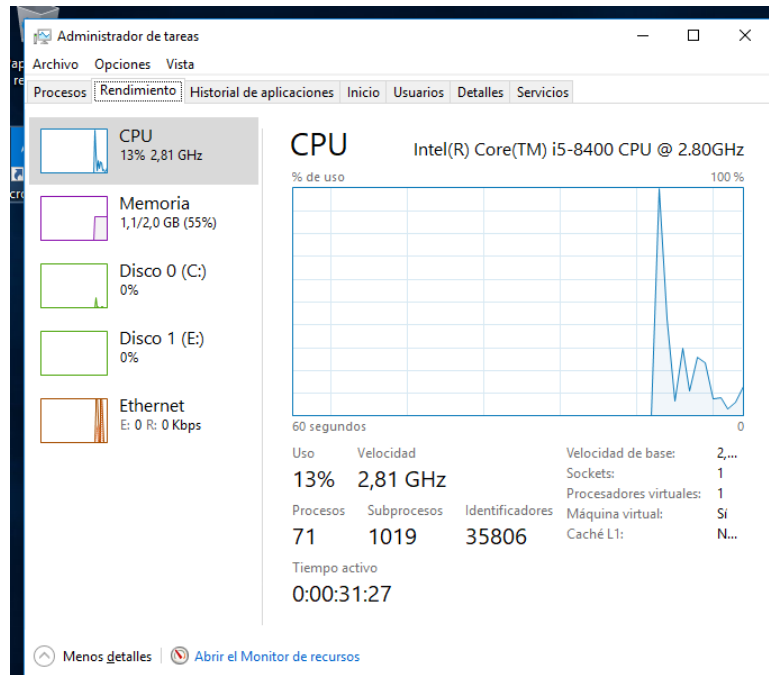
[illegible]

## Part II:

### Rendiment:

#### Windows:

Amb les eines que proporciona Windows 10, analitzar les característiques del vostre sistema segons processos, cpu, discs...



#### Linux:

En el cas de l'Ubuntu incorpora una eina per analitzar el rendiment dels discos. Per accedir a aquesta eina, amb l'opció cerca busqueu "Discs" i en "Més accions" seleccioneu "Test de referència". Analitzeu també les característiques més remarcables.





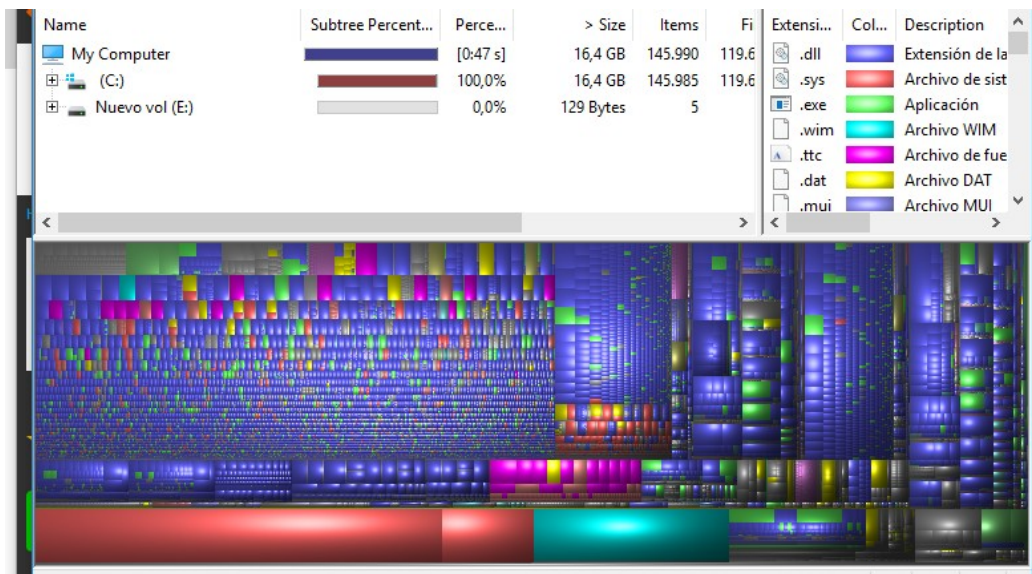
## Estadístiques:

### windows

Analitzar les característiques més remarcables del programari d'estadístiques, amb llicència GPLv2, Windirstat

<http://sourceforge.net/projects/windirstat/>

Permet visualitzar l'ús del disc dur. Veus amb blocs l'ús de memòria, també la memòria total, veure programa per programa quant costa de memòria, i altres funcions..



### Linux

En el cas d'Ubuntu es disposa de l'eina "Baobab" o analitzador de l'ús dels discs. Analitzeu també les característiques més remarcables.

