

# **Actividad 20. Herramientas de Búsqueda en Linux, CMD y Powershell**

[1. Describe las herramientas de búsqueda en Linux, CMD y PowerShell](#)

[2. Realiza los ejercicios propuestos](#)

## **1. Describe las herramientas de búsqueda en Linux, CMD y PowerShell**

Las herramientas de búsqueda son fundamentales en cualquier sistema operativo para localizar archivos, directorios y cadenas de texto.

### **HERRAMIENTAS DE BÚSQUEDA EN LINUX:**

#### **1. *find***

- a. **Objetivo:** Buscar archivos y directorios dentro del sistema de archivos.
- b. **Sintaxis/Ejemplo:** '*find /home/user -name "archivo.txt"*'.

#### **2. *locate***

- a. **Objetivo:** Utilizar base de datos previamente creada para localizar archivos rápidamente.
- b. **Sintaxis/Ejemplo:** '*locate archivo.txt*'.

#### **3. *grep***

- a. **Objetivo:** Buscar cadenas de texto dentro de archivos.
- b. **Sintaxis/Ejemplo:** '*grep "cadena" archivo.txt*'.

#### **4. *which***

- a. **Objetivo:** Mostrar la ruta completa del ejecutable.
- b. **Sintaxis/Ejemplo:** '*which ls*'.

#### **5. *whereis***

- a. **Objetivo:** Localizar el binario, código fuente y páginas de manual de un comando cualquiera.
- b. **Sintaxis/Ejemplo:** '*whereis ls*'.

### **HERRAMIENTAS DE BÚSQUEDA EN CMD:**

**1. dir**

- a. **Objetivo:** Listar archivos y directorios de una ruta específica.
- b. **Sintaxis/Ejemplo:** '*dir C:\Users\Usuario\\*.txt*'.

**2. find**

- a. **Objetivo:** Busca cadenas de texto dentro de archivos.
- b. **Sintaxis/Ejemplo:** '*find "cadena" archivo.txt*'.

**3. where**

- a. **Objetivo:** Mostrar la ubicación de los archivos ejecutables.
- b. **Sintaxis/Ejemplo:** '*where notepad*'.

**HERRAMIENTAS DE BÚSQUEDA EN POWERSHELL:****1. Get-ChildItem**

- a. **Objetivo:** Listar archivos y directorios de una ruta específica.
- b. **Sintaxis/Ejemplo:** '*Get-ChildItem -Path "C:\Users\Usuario" -Filter "\*.txt"*'.

**2. Select-String**

- a. **Objetivo:** Buscar cadenas de texto dentro de archivos.
- b. **Sintaxis/Ejemplo:** '*Select-String -Pattern "cadena" -Path "archivo.txt"*'.

**3. Get-Command**

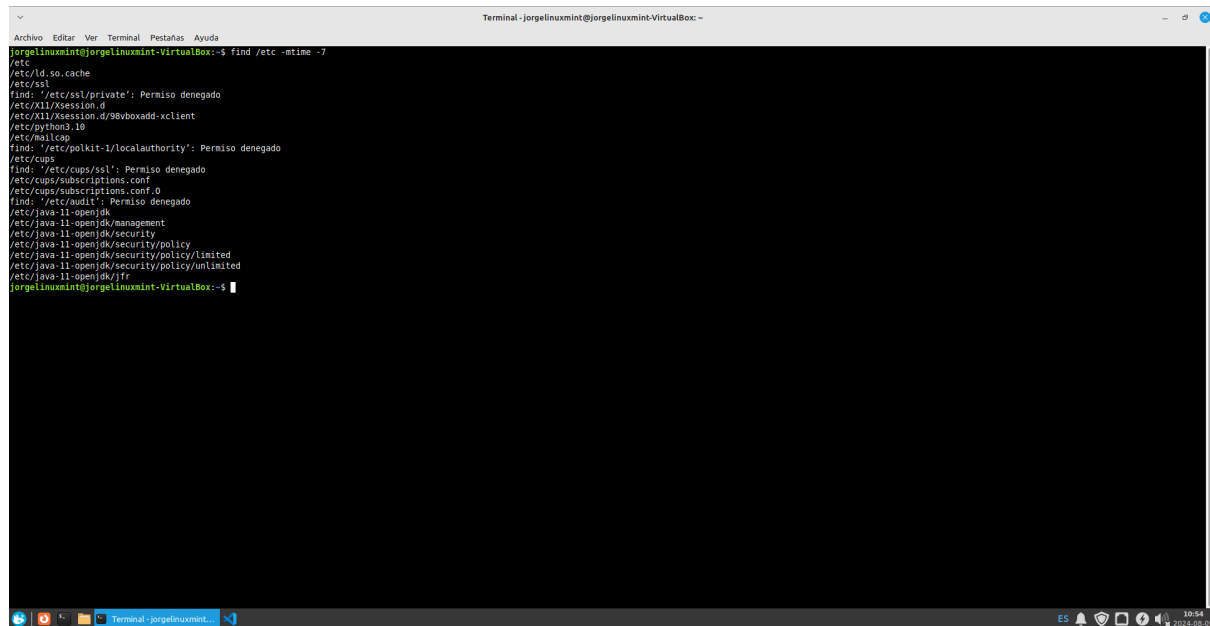
- a. **Objetivo:** Mostrar la lista de comandos disponibles y su ubicación.
- b. **Sintaxis/Ejemplo:** '*Get-Command notepad*'.

**4. Find-Module**

- a. **Objetivo:** Buscar módulos disponibles en el repositorio de PowerShell.
- b. **Sintaxis/Ejemplo:** '*Find-Module -Name AzureRM*'.

**2. Realiza los ejercicios propuestos****LINUX:**

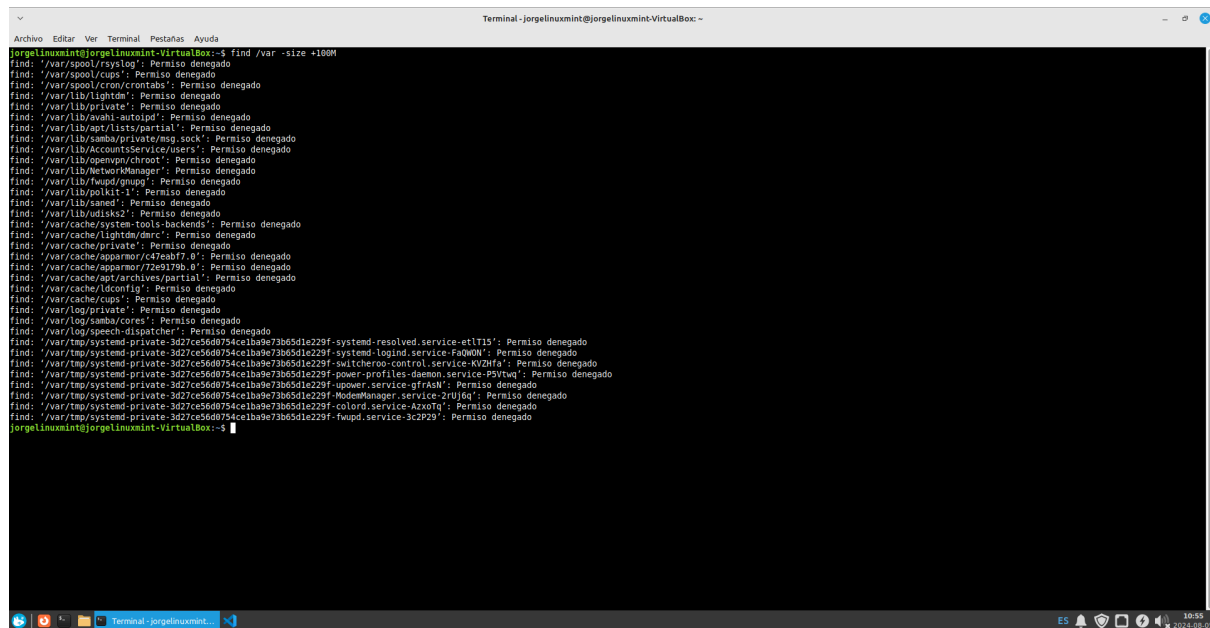
- 1. Buscar archivos modificados recientemente: '*find /etc -mtime -7*'
  - a. Encontrar todos los archivos en el directorio /etc que han sido modificados en los últimos 7 días.



```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ find /etc -mtime -7
/etc
/etc/ld.so.cache
/etc/ssl
find: '/etc/ssl/private': Permisos denegados
/etc/X11/Xsession.d
/etc/X11/Xsession.d/90vboxadd-xclient
/etc/gstom3.10
/etc/mailcap
find: '/etc/polkit-1/localauthority': Permisos denegados
/etc/cups
find: '/etc/cups/ssl': Permisos denegados
/etc/cups/subscriptions.conf
/etc/cups/subscriptions.conf.0
find: '/etc/audit': Permisos denegados
/etc/java-11-openjdk
/etc/java-11-openjdk/management
/etc/java-11-openjdk/security
/etc/java-11-openjdk/security/policy
/etc/java-11-openjdk/security/policy/limited
/etc/java-11-openjdk/security/policy/unlimited
/etc/java-11-openjdk/jfr
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$
```

## 2. Buscar archivos grandes: `find /var -size +100M`

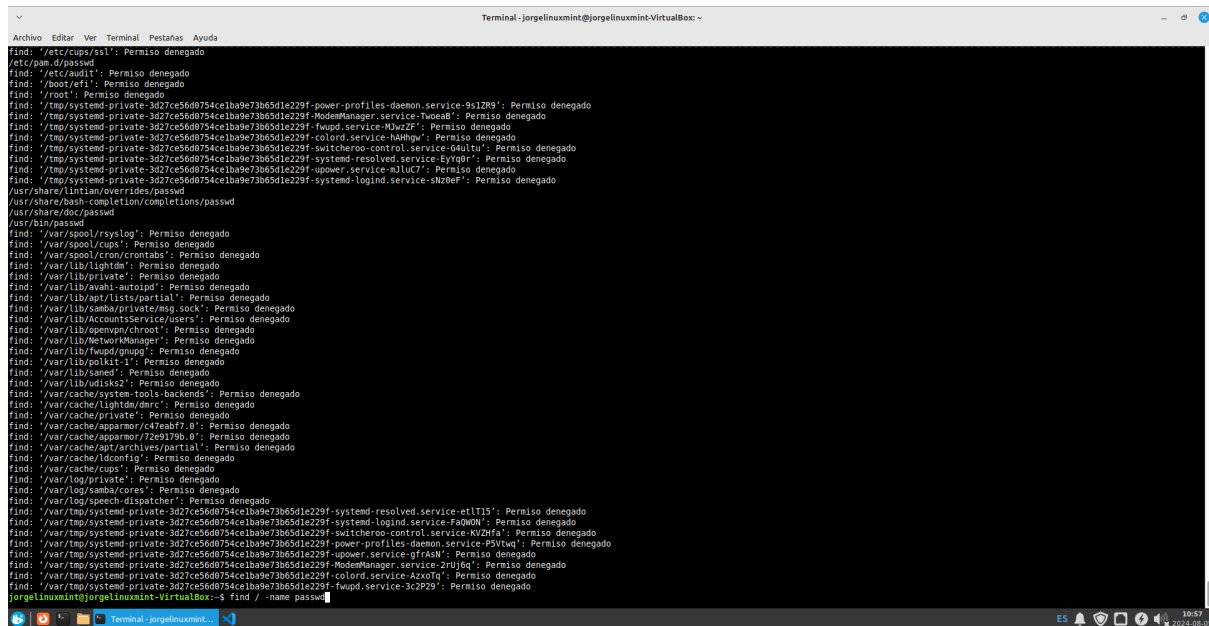
- Identificar todos los archivos en el directorio /var que sean mayores a 100 MB.



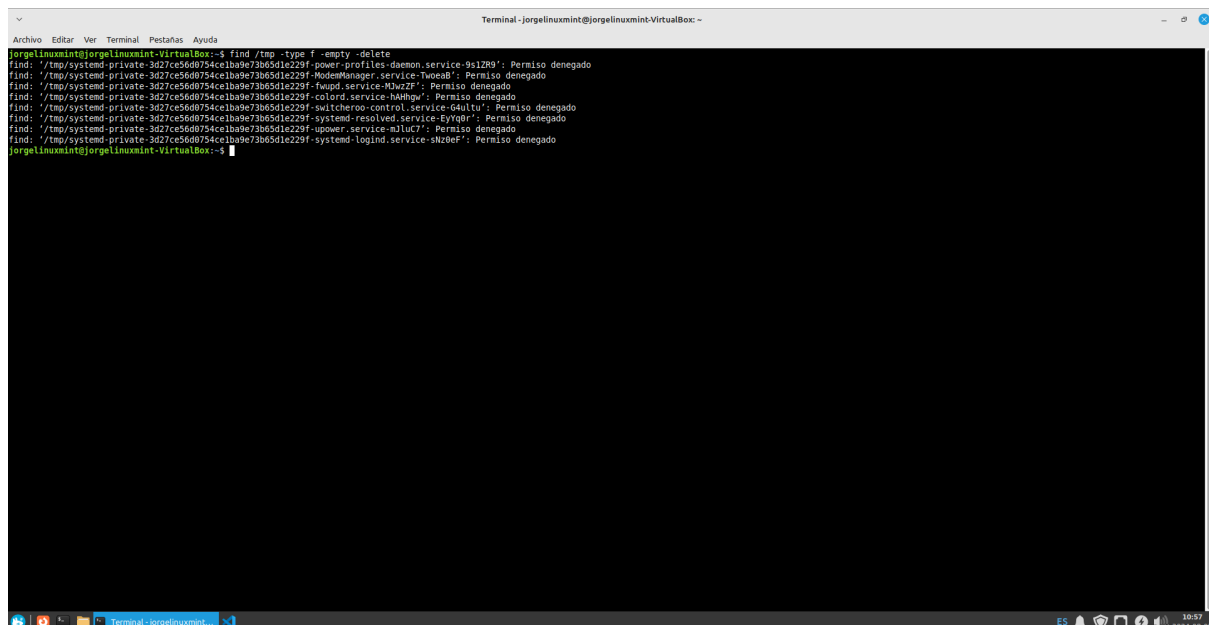
```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ find /var -size +100M
find: '/var/spool/cups': Permisos denegados
find: '/var/spool/cron/crontabs': Permisos denegados
find: '/var/lib/lightdm': Permisos denegados
find: '/var/lib/private': Permisos denegados
find: '/var/lib/avahi-autoipd': Permisos denegados
find: '/var/lib/avahi/hosts/partial': Permisos denegados
find: '/var/lib/samba/private/msg.sock': Permisos denegados
find: '/var/lib/AccountsService/users': Permisos denegados
find: '/var/lib/openssh/ssh-key': Permisos denegados
find: '/var/lib/NetworkManager': Permisos denegados
find: '/var/lib/udev/gnupg': Permisos denegados
find: '/var/lib/polkit-1': Permisos denegados
find: '/var/lib/saned': Permisos denegados
find: '/var/lib/udisks2': Permisos denegados
find: '/var/cache/system-tools-backends': Permisos denegados
find: '/var/cache/lightdm/dmcc': Permisos denegados
find: '/var/cache/private': Permisos denegados
find: '/var/cache/apparmor/c47eb17.0': Permisos denegados
find: '/var/cache/apparmor/72e9179b.0': Permisos denegados
find: '/var/cache/apt/archives/partial': Permisos denegados
find: '/var/cache/ldconfig': Permisos denegados
find: '/var/cache/cups': Permisos denegados
find: '/var/log/private': Permisos denegados
find: '/var/log/samba/cores': Permisos denegados
find: '/var/log/speech-dispatcher': Permisos denegados
find: '/var/tmp/systemd-private-3d27ce56d0754c1ba9e73b65d1e223f-systemd-resolved.service-est115': Permisos denegados
find: '/var/tmp/systemd-private-3d27ce56d0754c1ba9e73b65d1e223f-systemd-logind.service-FdewdM': Permisos denegados
find: '/var/tmp/systemd-private-3d27ce56d0754c1ba9e73b65d1e223f-switcheroo-control.service-KVZfha': Permisos denegados
find: '/var/tmp/systemd-private-3d27ce56d0754c1ba9e73b65d1e223f-power-profiles-daemon.service-P5VtWq': Permisos denegados
find: '/var/tmp/systemd-private-3d27ce56d0754c1ba9e73b65d1e223f-upower.service-gfRAKX': Permisos denegados
find: '/var/tmp/systemd-private-3d27ce56d0754c1ba9e73b65d1e223f-ModemManager.service-2rUJq': Permisos denegados
find: '/var/tmp/systemd-private-3d27ce56d0754c1ba9e73b65d1e223f-colord.service-AzXotq': Permisos denegados
find: '/var/tmp/systemd-private-3d27ce56d0754c1ba9e73b65d1e223f-fwupd.service-3CZP29': Permisos denegados
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$
```

## 3. Buscar archivos por nombre: `find / -name passwd`

- Encontrar todos los archivos con el nombre passwd en el sistema.



4. Buscar y eliminar archivos vacíos: `'find /tmp -type f -empty -delete'`
  - a. Buscar y eliminar todos los archivos vacíos en el directorio /tmp.



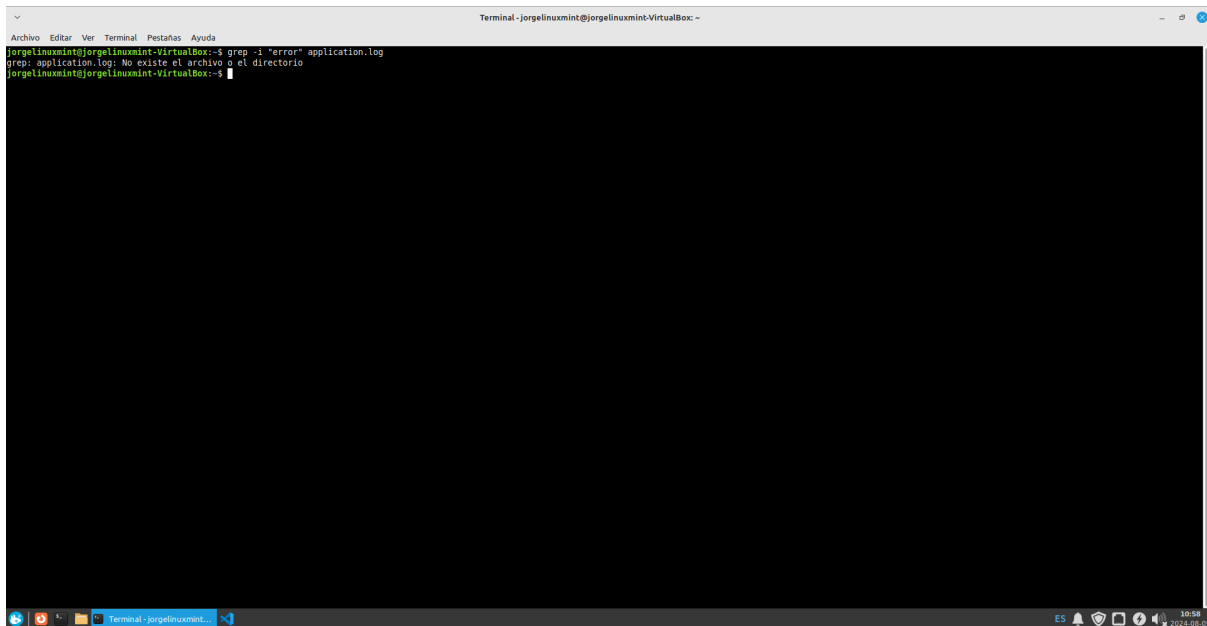
5. Buscar archivos por tipo: *'find /home -type d'*
  - a. Buscar todos los directorios en el directorio /home.

```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -
Archivo Editar Ver Terminal Pestañas Ayuda
/home/jorgelinuxmint/.vscode/extensions/oderwat.indent-rainbow-8.3.1/node_modules/co
/home/jorgelinuxmint/.vscode/extensions/oderwat.indent-rainbow-8.3.1/node_modules/vscode
/home/jorgelinuxmint/.vscode/extensions/oderwat.indent-rainbow-8.3.1/node_modules/vscode/test-web
/home/jorgelinuxmint/.vscode/extensions/oderwat.indent-rainbow-8.3.1/node_modules/vscode/test-web/out
/home/jorgelinuxmint/.vscode/extensions/oderwat.indent-rainbow-8.3.1/node_modules/vscode/test-web/out/server
/home/jorgelinuxmint/.vscode/extensions/oderwat.indent-rainbow-8.3.1/node_modules/vscode/test-web/views
/home/jorgelinuxmint/.vscode/extensions/asvinkumar863.smarty-template-support-2.1.1/snippets
/home/jorgelinuxmint/.vscode/extensions/asvinkumar863.smarty-template-support-2.1.1/server
/home/jorgelinuxmint/.vscode/extensions/asvinkumar863.smarty-template-support-2.1.1/server/dist
/home/jorgelinuxmint/.vscode/extensions/asvinkumar863.smarty-template-support-2.1.1/server/dist/browser
/home/jorgelinuxmint/.vscode/extensions/asvinkumar863.smarty-template-support-2.1.1/server/dist/node
/home/jorgelinuxmint/.vscode/extensions/asvinkumar863.smarty-template-support-2.1.1/syntaxes
/home/jorgelinuxmint/.vscode/extensions/asvinkumar863.smarty-template-support-2.1.1/client
/home/jorgelinuxmint/.vscode/extensions/asvinkumar863.smarty-template-support-2.1.1/client/dist
/home/jorgelinuxmint/.vscode/extensions/asvinkumar863.smarty-template-support-2.1.1/client/dist/browser
/home/jorgelinuxmint/.vscode/extensions/asvinkumar863.smarty-template-support-2.1.1/client/dist/node
/home/jorgelinuxmint/.vscode/extensions/asvinkumar863.smarty-template-support-2.1.1/images
/home/jorgelinuxmint/.vscode/extensions/pflannery.vscode-versionlens-1.14.2
/home/jorgelinuxmint/.vscode/extensions/pflannery.vscode-versionlens-1.14.2/images
/home/jorgelinuxmint/.vscode/extensions/pflannery.vscode-versionlens-1.14.2/images/faq
/home/jorgelinuxmint/.vscode/extensions/pflannery.vscode-versionlens-1.14.2/images/docs
/home/jorgelinuxmint/.vscode/extensions/pflannery.vscode-versionlens-1.14.2/images/docs/suggestions
/home/jorgelinuxmint/.vscode/extensions/pflannery.vscode-versionlens-1.14.2/images/icons
/home/jorgelinuxmint/.vscode/extensions/pflannery.vscode-versionlens-1.14.2/dist
/home/jorgelinuxmint/.vscode/extensions/mintlify.document-2.2.2
/home/jorgelinuxmint/.vscode/extensions/mintlify.document-2.2.2/assets
/home/jorgelinuxmint/.vscode/extensions/mintlify.document-2.2.2/assets/dark
/home/jorgelinuxmint/.vscode/extensions/mintlify.document-2.2.2/assets/light
/home/jorgelinuxmint/.vscode/extensions/mintlify.document-2.2.2/dist
/home/jorgelinuxmint/.vscode/extensions/rapidapi.vscode-rapidapi-client-1.10.2
/home/jorgelinuxmint/.vscode/extensions/rapidapi.vscode-rapidapi-client-1.10.2/assets
/home/jorgelinuxmint/.vscode/extensions/rapidapi.vscode-rapidapi-client-1.10.2/assets/walkthrough
/home/jorgelinuxmint/.vscode/extensions/rapidapi.vscode-rapidapi-client-1.10.2/assets/icons
/home/jorgelinuxmint/.vscode/extensions/rapidapi.vscode-rapidapi-client-1.10.2/assets/icons/active
/home/jorgelinuxmint/.vscode/extensions/rapidapi.vscode-rapidapi-client-1.10.2/assets/icons/light
/home/jorgelinuxmint/.vscode/extensions/rapidapi.vscode-rapidapi-client-1.10.2/assets/screencasts
/home/jorgelinuxmint/.vscode/extensions/rapidapi.vscode-rapidapi-client-1.10.2/dist
/home/jorgelinuxmint/.vscode/extensions/xabikos.javascriptsnippets-1.8.0
/home/jorgelinuxmint/.vscode/extensions/xabikos.javascriptsnippets-1.8.0/snippets
/home/jorgelinuxmint/.vscode/extensions/xabikos.javascriptsnippets-1.8.0/images
/home/jorgelinuxmint/.vscode/extensions/github.codespaces-1.17.2
/home/jorgelinuxmint/.vscode/extensions/github.codespaces-1.17.2/out
/home/jorgelinuxmint/.vscode/extensions/github.codespaces-1.17.2/out/bundle
/home/jorgelinuxmint/.vscode/extensions/github.codespaces-1.17.2/images
/home/jorgelinuxmint/.vscode/extensions/github.codespaces-1.17.2/images/dark
/home/jorgelinuxmint/.vscode/extensions/github.codespaces-1.17.2/images/light
/home/jorgelinuxmint/.vscode/extensions/github.codespaces-1.17.2/dist
/home/jorgelinuxmint/.vscode/extensions/github.codespaces-1.17.2/dist/spec-node
/home/jorgelinuxmint/.vscode/extensions/github.codespaces-1.17.2/dist/spec-node
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ find /home -type d
```

6. Buscar texto en archivos de configuración: `grep -r "network" /etc/*.conf`
- a. Buscar la cadena "network" en todos los archivos de configuración .conf en el directorio /etc.

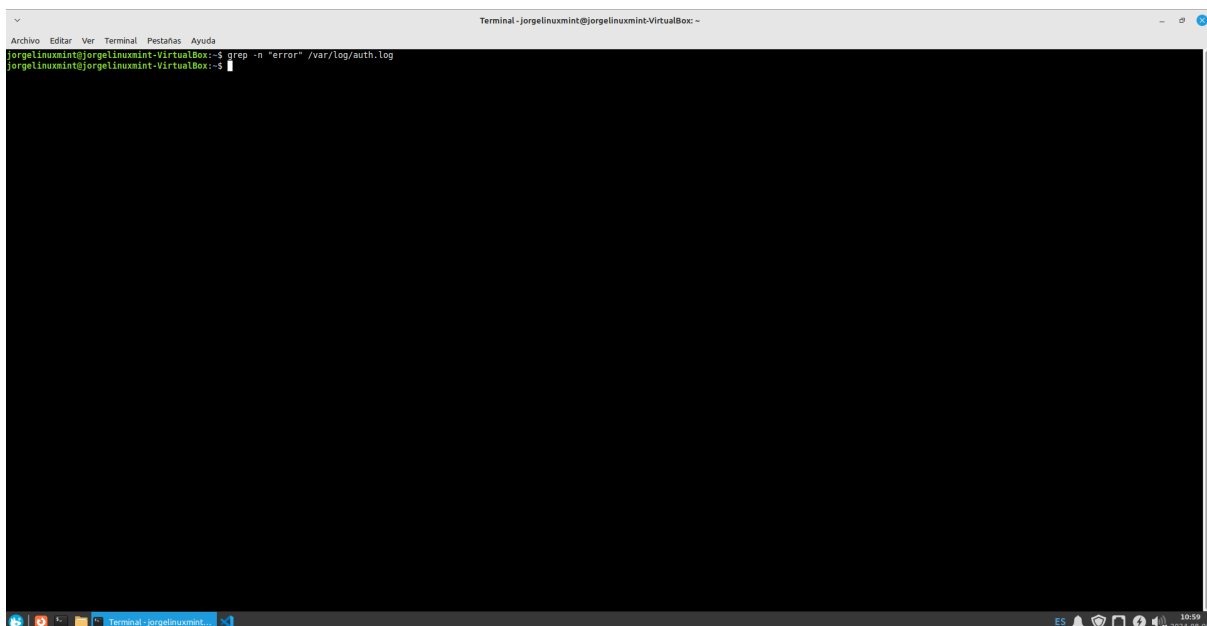
```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -
Archivo Editar Ver Terminal Pestañas Ayuda
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ grep -r "network" /etc/*.conf
/etc/iptables.conf: # over data provided from a network source
/etc/dnsmasq-server-service.conf: # true: Enable the network filtering.
/etc/dnsmasq-server-service.conf: # false: Disable the network filtering.
/etc/traefik.conf: http(in) {insecure=string};
/etc/nsswitch.conf: networks: files
/etc/rygel.conf: # List of network interfaces to attach rygel to. You can also use network IP or
/etc/rygel.conf: # even ESSTID for wireless networks on Linux. Leave it blank for dynamic
/etc/sudo.conf: # By default, sudo will probe the system's network interfaces and
/etc/sysctl.conf: # Additional settings - these settings can improve the network
/etc/sysctl.conf: # security of the host and prevent against some network attacks
/etc/sysctl.conf: # redirection. Some network environments, however, require that these
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$
```

7. Buscar texto ignorando mayúsculas y minúsculas: `grep -i "error" application.log`
- a. Buscar la cadena "Error" o "error" en un archivo específico application.log



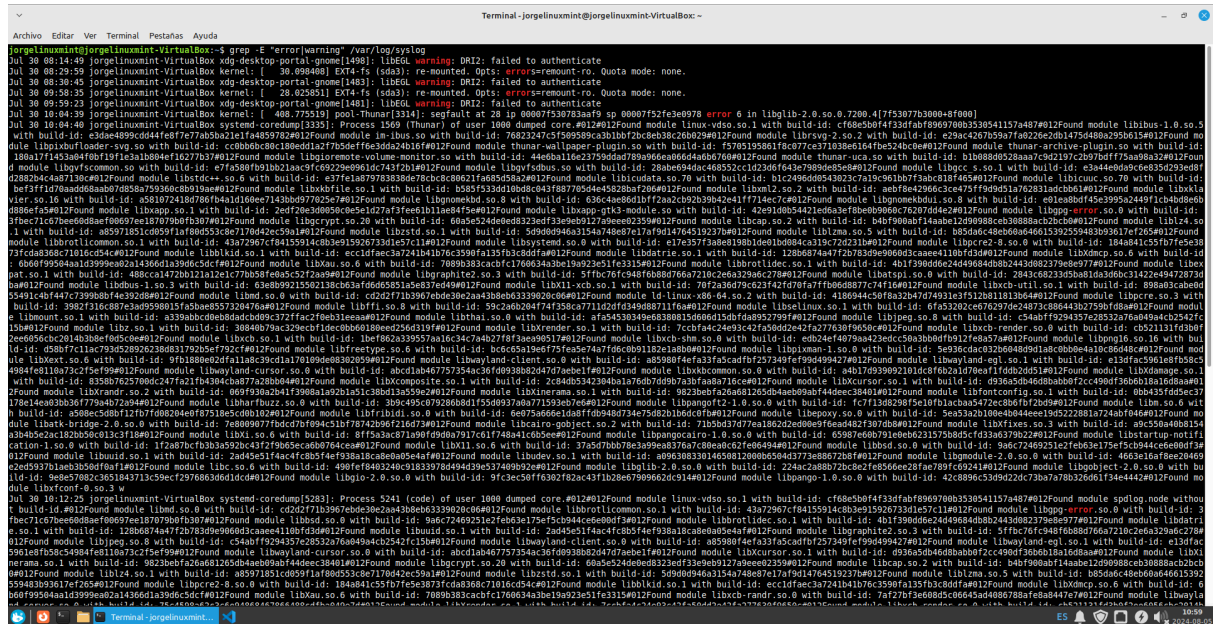
A terminal window titled 'Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -'. The terminal shows a menu bar with 'Archivo', 'Editar', 'Ver', 'Terminal', 'Pestañas', and 'Ayuda'. The command prompt is 'jorgelinuxmint@jorgelinuxmint-VirtualBox:~\$'. The user enters the command 'grep -i "error" application.log'. The output is 'grep: application.log: No existe el archivo o el directorio'. The prompt returns to 'jorgelinuxmint@jorgelinuxmint-VirtualBox:~\$'.

8. Buscar texto y mostrar números de línea: `'grep -n "error" /var/log/auth.log'`
- Buscar la cadena "error" y mostrar las líneas que contienen esa cadena junto con sus números de línea en el archivo auth.log.

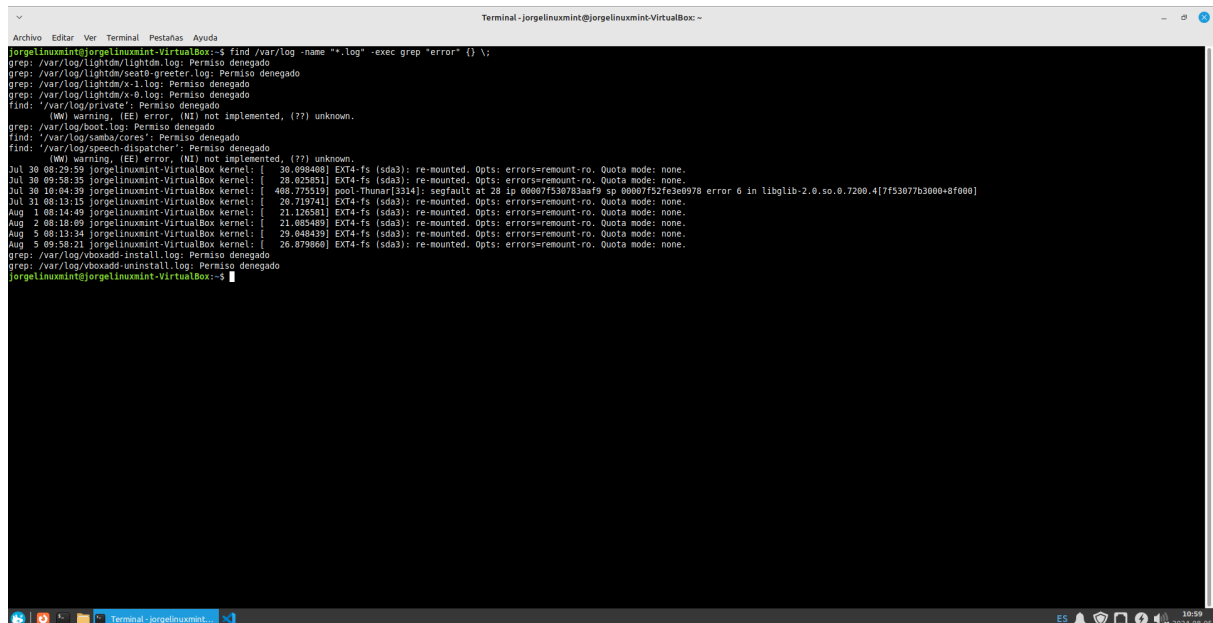


A terminal window titled 'Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -'. The terminal shows a menu bar with 'Archivo', 'Editar', 'Ver', 'Terminal', 'Pestañas', and 'Ayuda'. The command prompt is 'jorgelinuxmint@jorgelinuxmint-VirtualBox:~\$'. The user enters the command 'grep -n "error" /var/log/auth.log'. The output is 'jorgelinuxmint@jorgelinuxmint-VirtualBox:~\$'. The prompt returns to 'jorgelinuxmint@jorgelinuxmint-VirtualBox:~\$'.

9. Buscar múltiples patrones de texto: `'grep -E "error|warning" /var/log/syslog'`
- Buscar las cadenas "error" y "warning" en el archivo syslog.



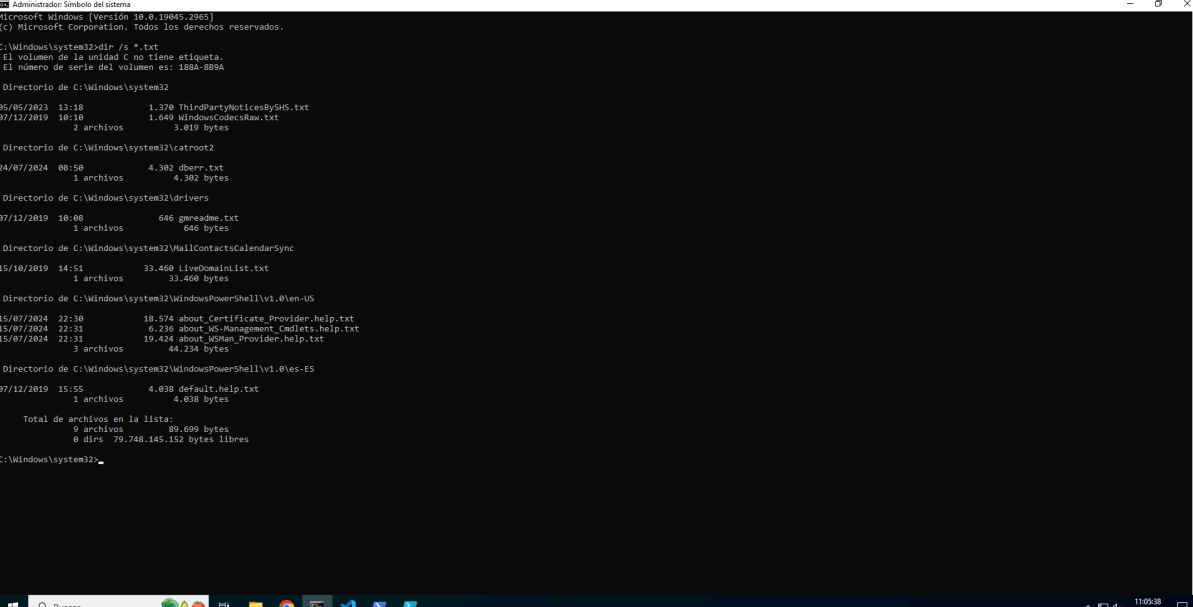
10. Buscar archivos y ejecutar un comando en ellos: `'find /var/log -name '*.log' -exec grep "error" {} \;'`
- a. Encontrar todos los archivos .log en el directorio /var/log y buscar la palabra "error" dentro de esos archivos.



## CMD:

1. Listar archivos con una extensión específica: `'dir /s *.txt'`

- a. Listar todos los archivos con la extensión .txt en el directorio actual y sus subdirectorios.



```
Administrador de símbolos del sistema
Microsoft Windows [Versión 10.0.19045.2265]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>dir /s *.txt
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 188A-889A

Directorio de C:\Windows\system32

05/05/2023  13:18                1.370 ThirdPartyNoticesBySH5.txt
07/12/2019  10:19                1.649 WindowsCodecsRaw.txt
                2 archivos                3.019 bytes

Directorio de C:\Windows\system32\catroot2

24/07/2024  08:50                4.382 dberr.txt
                1 archivos                4.382 bytes

Directorio de C:\Windows\system32\drivers

07/12/2019  10:08                646 gmreadme.txt
                1 archivos                646 bytes

Directorio de C:\Windows\system32\MailContactsCalendarSync

15/10/2019  14:51                33.460 LiveDomainList.txt
                1 archivos                33.460 bytes

Directorio de C:\Windows\system32\WindowsPowerShell\v1.0\en-US

15/07/2024  22:30                18.574 about_Certificate_Provider.help.txt
15/07/2024  22:31                 6.236 about_WS_Management_Cmdlets.help.txt
15/07/2024  22:31                19.424 about_WSMem_Provider.help.txt
                3 archivos                44.234 bytes

Directorio de C:\Windows\system32\WindowsPowerShell\v1.0\es-E5

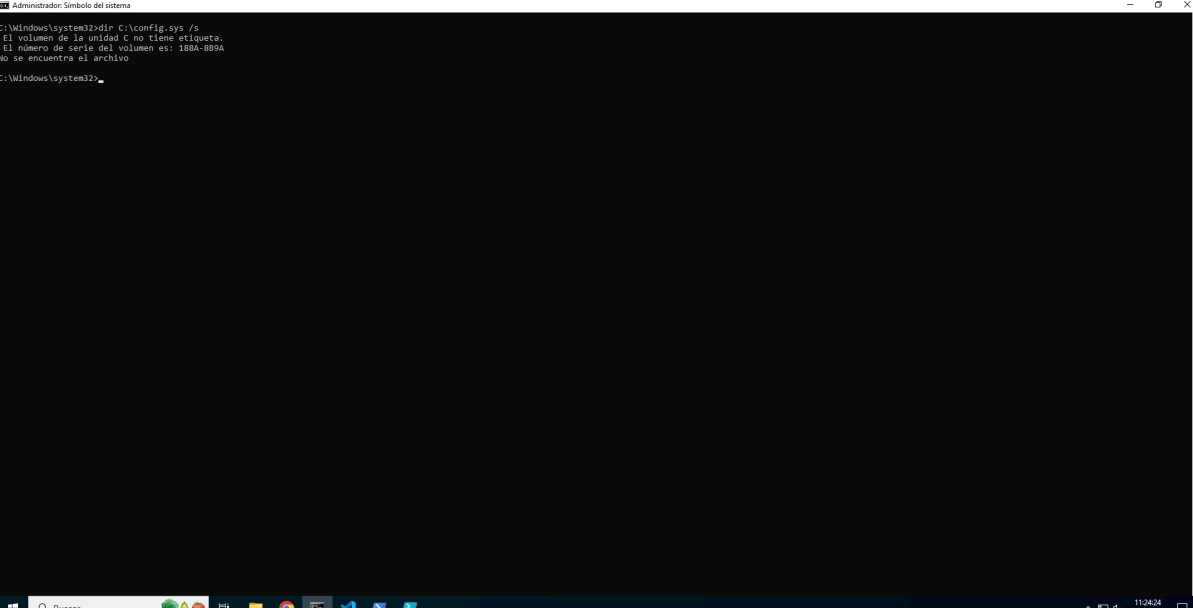
07/12/2019  15:55                4.038 default.help.txt
                1 archivos                4.038 bytes

Total de archivos en la lista:
          9 archivos                80.699 bytes
          0 dirs 79.748.145.152 bytes libres

C:\Windows\system32>
```

2. Buscar archivos por nombre: `'dir C:\config.sys /s'`

- a. Buscar todos los archivos llamados config.sys en el disco C:.



```
Administrador de símbolos del sistema
Microsoft Windows [Versión 10.0.19045.2265]
(c) Microsoft Corporation. Todos los derechos reservados.

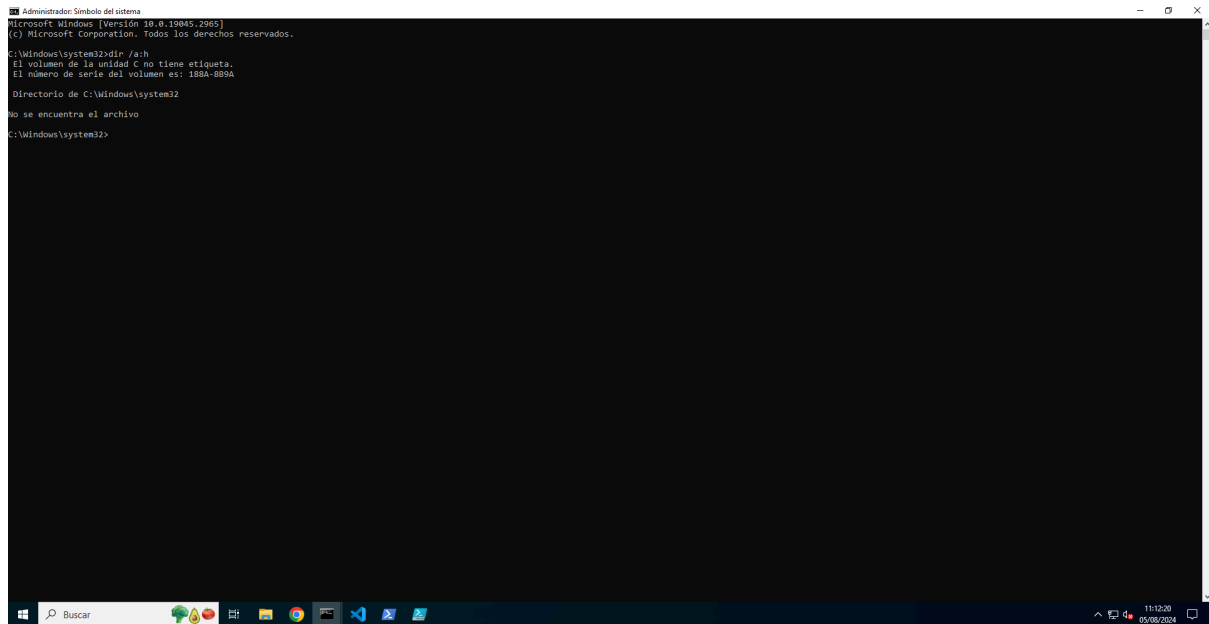
C:\Windows\system32>dir C:\config.sys /s
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 188A-889A
No se encuentra el archivo.

C:\Windows\system32>
```

3. Buscar archivos ocultos: `'dir /a:h'`

- a. Listar todos los archivos ocultos en el directorio actual.





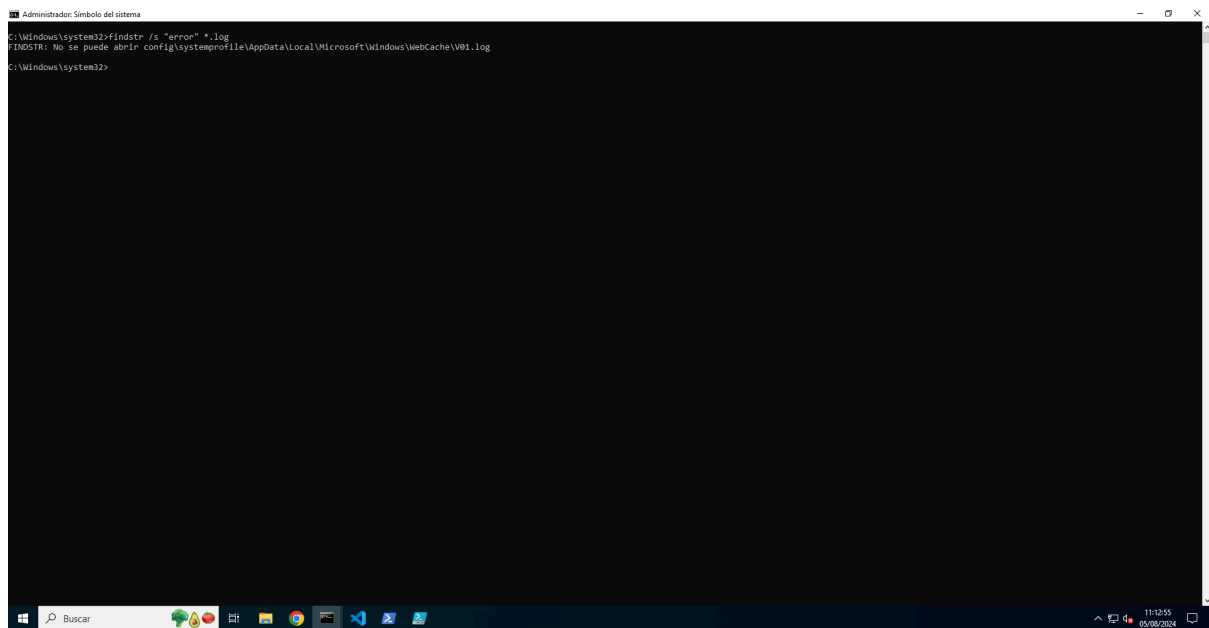
```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.2965]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>dir /aih
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 188A-8B9A

Directorio de C:\Windows\system32

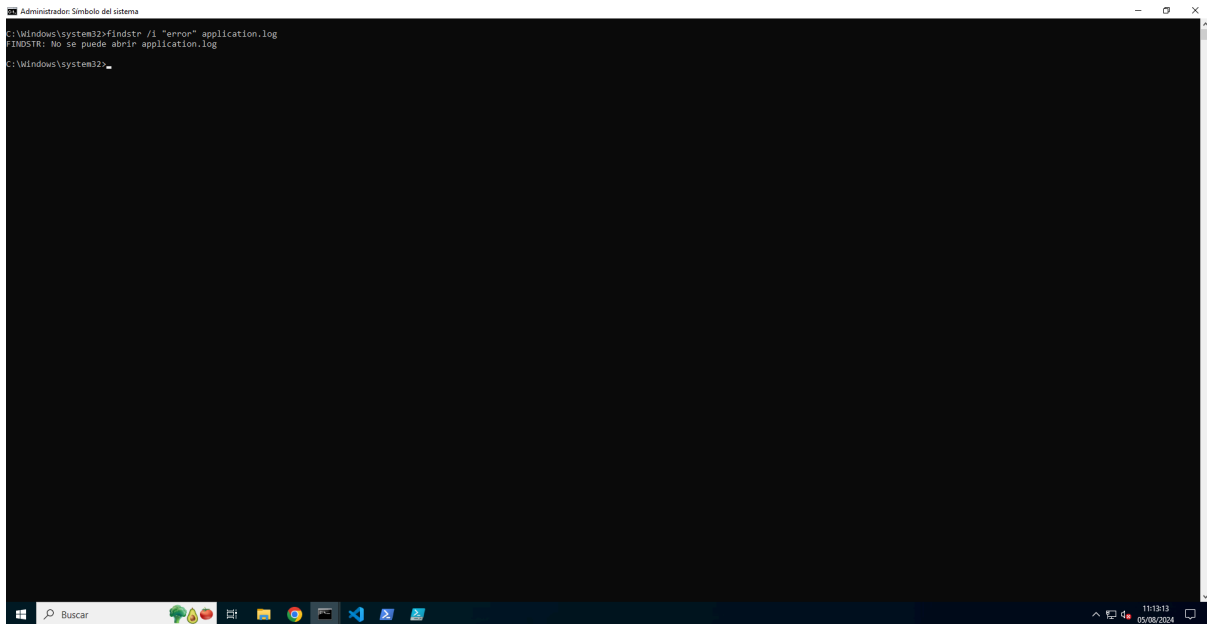
No se encuentra el archivo
C:\Windows\system32>
```

4. Buscar texto en archivos de registro: *'findstr /s "error" \*.log'*
  - a. Buscar la cadena "error" en todos los archivos .log dentro del directorio actual y sus subdirectorios.



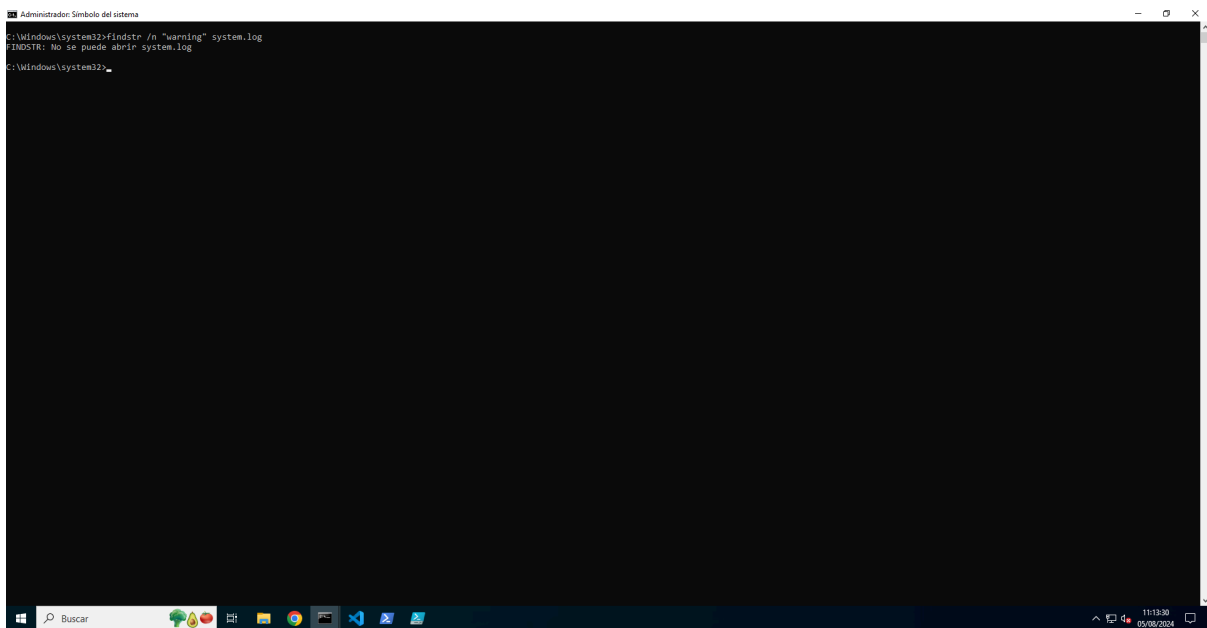
```
Administrador: Símbolo del sistema
C:\Windows\system32>findstr /s "error" *.log
FINDSTR: No se puede abrir config\systemprofile\AppData\Local\Microsoft\Windows\WebCache\WB1.log
C:\Windows\system32>
```

5. Buscar texto ignorando mayúsculas y minúsculas: *'findstr /i "error" application.log'*
  - a. Buscar la cadena "error" o "Error" en un archivo específico application.log.



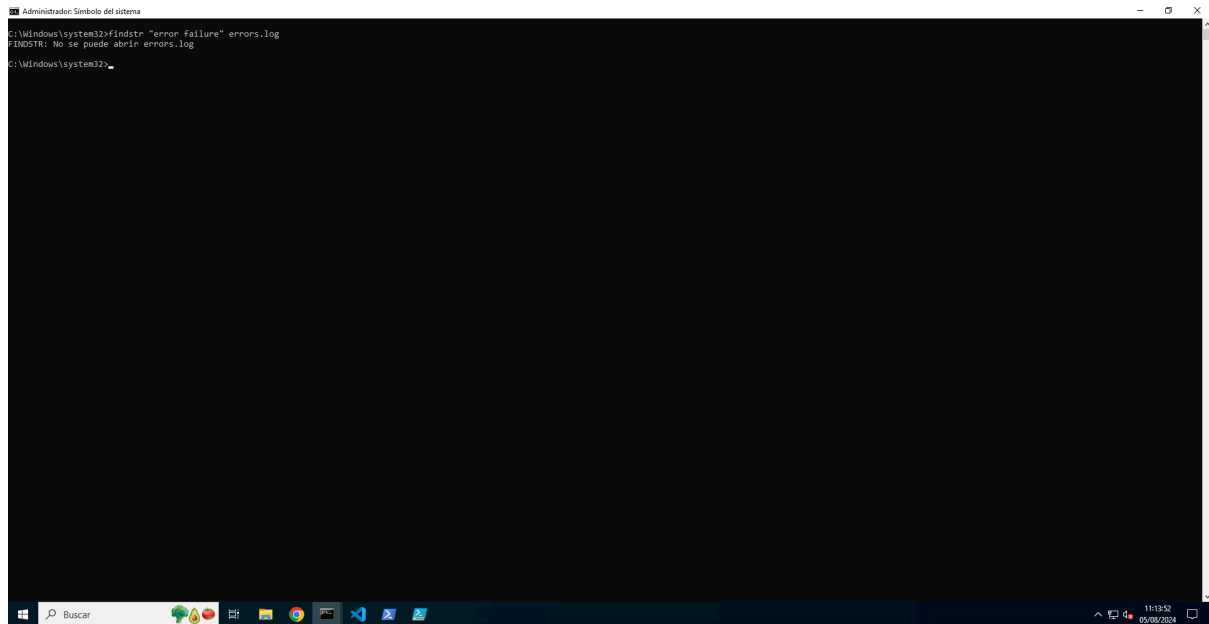
```
Administrador: Símbolo del sistema
C:\Windows\system32>findstr /i "error" application.log
FINDSTR: No se puede abrir application.log
C:\Windows\system32>
```

6. Mostrar líneas con números de línea: *'findstr /n "warning" system.log'*
- a. Buscar la cadena "warning" en el archivo system.log y mostrar las líneas con sus números de línea.



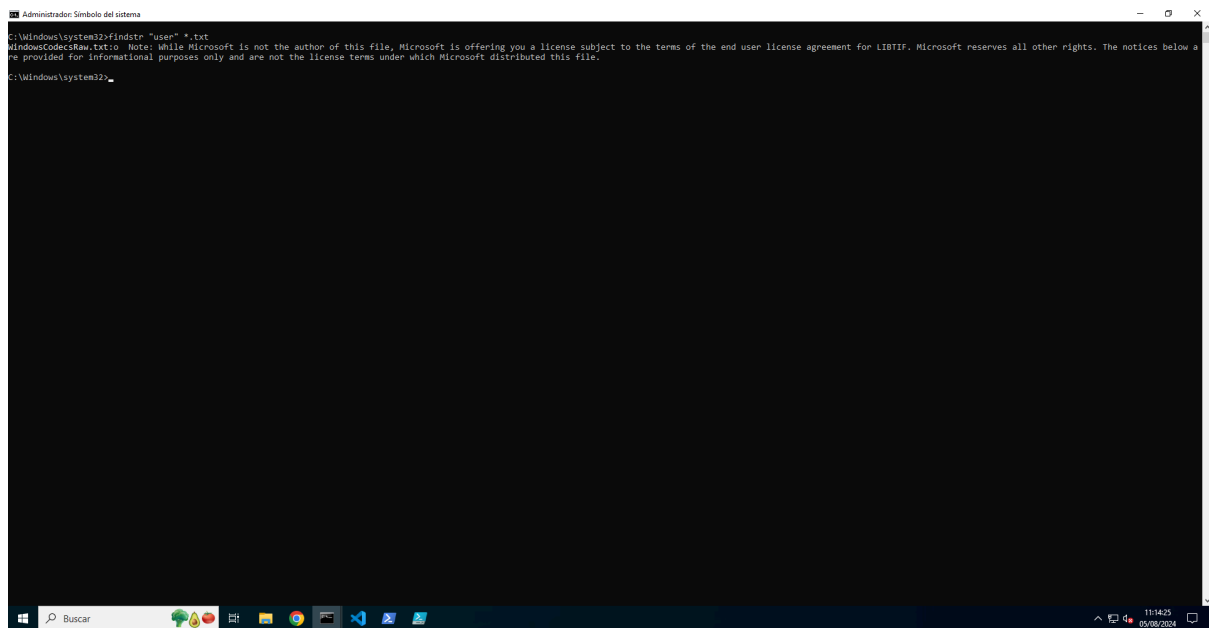
```
Administrador: Símbolo del sistema
C:\Windows\system32>findstr /n "warning" system.log
FINDSTR: No se puede abrir system.log
C:\Windows\system32>
```

7. Buscar múltiples patrones: *'findstr "error failure" errors.log'*
- a. Buscar las cadenas "error" y "failure" en el archivo errors.log.



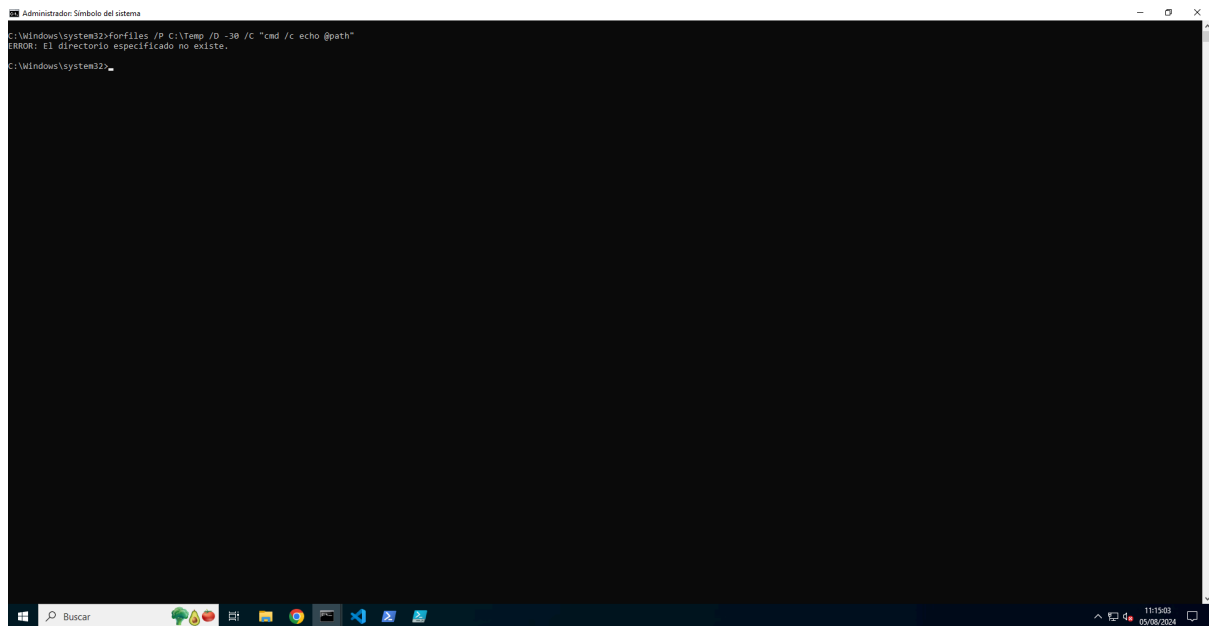
A screenshot of a Windows command prompt window titled "Administrador: Símbolo del sistema". The command entered is `C:\Windows\system32\findstr "error failure" errors.log`. The output shows an error: `findstr: No se puede abrir errors.log`. The prompt is now `C:\Windows\system32>`. The taskbar at the bottom shows the search bar with "Buscar", several application icons, and the system clock displaying 11:13:52 on 05/09/2024.

8. Buscar en un conjunto de archivos: *'findstr "user" \*.txt'*
  - a. Buscar la cadena "user" en todos los archivos .txt dentro del directorio actual.



A screenshot of a Windows command prompt window titled "Administrador: Símbolo del sistema". The command entered is `C:\Windows\system32\findstr "user" *.txt`. The output shows a long block of text, which is a license agreement for the Windows CodeScan tool. The text starts with "WindowsCodeScan.txt: Note: while Microsoft is not the author of this file, Microsoft is offering you a license subject to the terms of the end user license agreement for LIBTIF." and continues with several paragraphs of legal text. The prompt is now `C:\Windows\system32>`. The taskbar at the bottom shows the search bar with "Buscar", several application icons, and the system clock displaying 11:14:25 on 05/09/2024.

9. Buscar archivos y directorios por fecha de modificación: *'forfiles /P C:\Temp /D -30 /C "cmd /c echo @path"'*
  - a. Listar todos los archivos y directorios en el directorio C:\Temp modificados en los últimos 30 días.



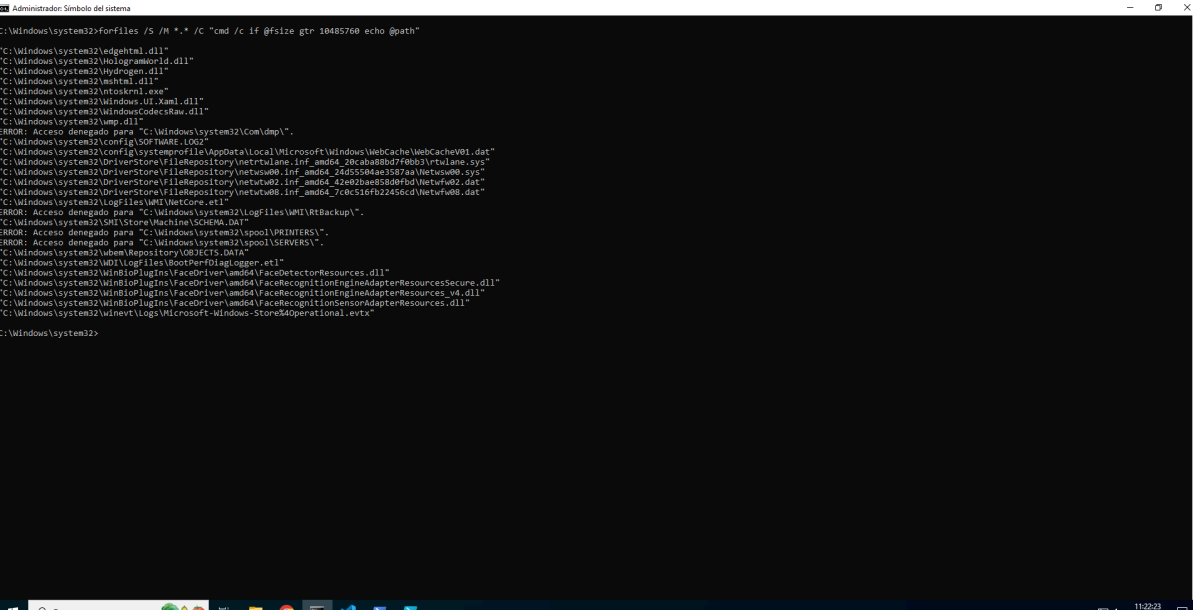
Administrador: Símbolo del sistema

```
C:\Windows\system32>forfiles /P C:\Temp /D -30 /C "cmd /c echo @path"
ERROR: El directorio especificado no existe.

C:\Windows\system32>
```

Windows taskbar at the bottom shows the search bar and system tray with the date 05/08/2024 and time 11:15:03.

10. Buscar archivos con un tamaño específico: *'forfiles /S /M \*.\* /C "cmd /c if @fsize gtr 10485760 echo @path"'*
  - a. Listar todos los archivos mayores a 10 MB en el directorio actual.



Administrador: Símbolo del sistema

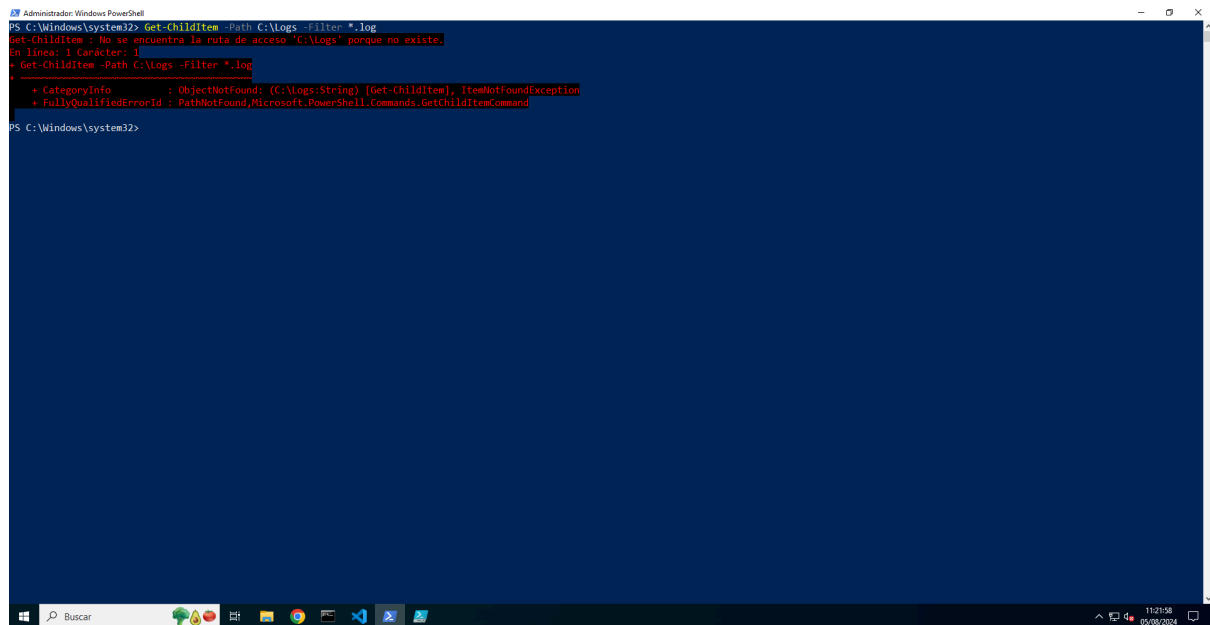
```
C:\Windows\system32>forfiles /S /M *.* /C "cmd /c if @fsize gtr 10485760 echo @path"
"C:\Windows\system32\edgehtml.dll"
"C:\Windows\system32\Hijackprogramorid.dll"
"C:\Windows\system32\Hydregen.dll"
"C:\Windows\system32\mshtml.dll"
"C:\Windows\system32\ntoskrnl.exe"
"C:\Windows\system32\Windows.UI.Xaml.dll"
"C:\Windows\system32\WindowsCodecsRaw.dll"
"C:\Windows\system32\ump.dll"
ERROR: Acceso denegado para "C:\Windows\system32\Com\dmip\".
"C:\Windows\system32\Config\Software\Local\Microsoft\Windows\WebCache\WebCacheV01.dat"
"C:\Windows\system32\Config\SystemAppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat"
"C:\Windows\system32\DriverStore\FileRepository\netrtwlan.inf_amd64_28cab88bd7f80b3\rtwlan.sys"
"C:\Windows\system32\DriverStore\FileRepository\netwtw02.inf_amd64_24d55504ae2587aa\netwtw02.sys"
"C:\Windows\system32\DriverStore\FileRepository\netwtw02.inf_amd64_42e02bae58d0fbd\netwtw02.dat"
"C:\Windows\system32\DriverStore\FileRepository\netwtw02.inf_amd64_7c0c516fb22456cd\netwtw02.dat"
"C:\Windows\system32\LogFiles\WMI\NetCore.etl"
ERROR: Acceso denegado para "C:\Windows\system32\LogFiles\WMI\NetCore.etl".
"C:\Windows\system32\Store\Store\Machine\SCHP.MD"
ERROR: Acceso denegado para "C:\Windows\system32\spool\PRINTERS\".
ERROR: Acceso denegado para "C:\Windows\system32\spool\SERVERS\".
"C:\Windows\system32\WMI\LogFiles\BootPerfDiagLogger.etl"
"C:\Windows\system32\WMI\LogFiles\BootPerfDiagLogger.etl"
"C:\Windows\system32\WinBioPlugins\FaceDriver\amd64\FaceDetectorResources.dll"
"C:\Windows\system32\WinBioPlugins\FaceDriver\amd64\FaceRecognitionEngineAdapterResourcesSecure.dll"
"C:\Windows\system32\WinBioPlugins\FaceDriver\amd64\FaceRecognitionEngineAdapterResources_v4.dll"
"C:\Windows\system32\WinBioPlugins\FaceDriver\amd64\FaceRecognitionSensorAdapterResources.dll"
"C:\Windows\system32\WinBioPlugins\FaceDriver\amd64\FaceRecognitionSensorAdapterResources_v4.dll"
"C:\Windows\system32\WinBioPlugins\FaceDriver\amd64\FaceRecognitionSensorAdapterResources_v4.dll"
C:\Windows\system32>
```

Windows taskbar at the bottom shows the search bar and system tray with the date 05/08/2024 and time 11:22:23.

## POWERSHELL:

1. Listar archivos por tipo: *'Get-ChildItem -Path C:\Logs -Filter \*.log'*

- a. Buscar todos los archivos con la extensión .log en el directorio C:\Logs.

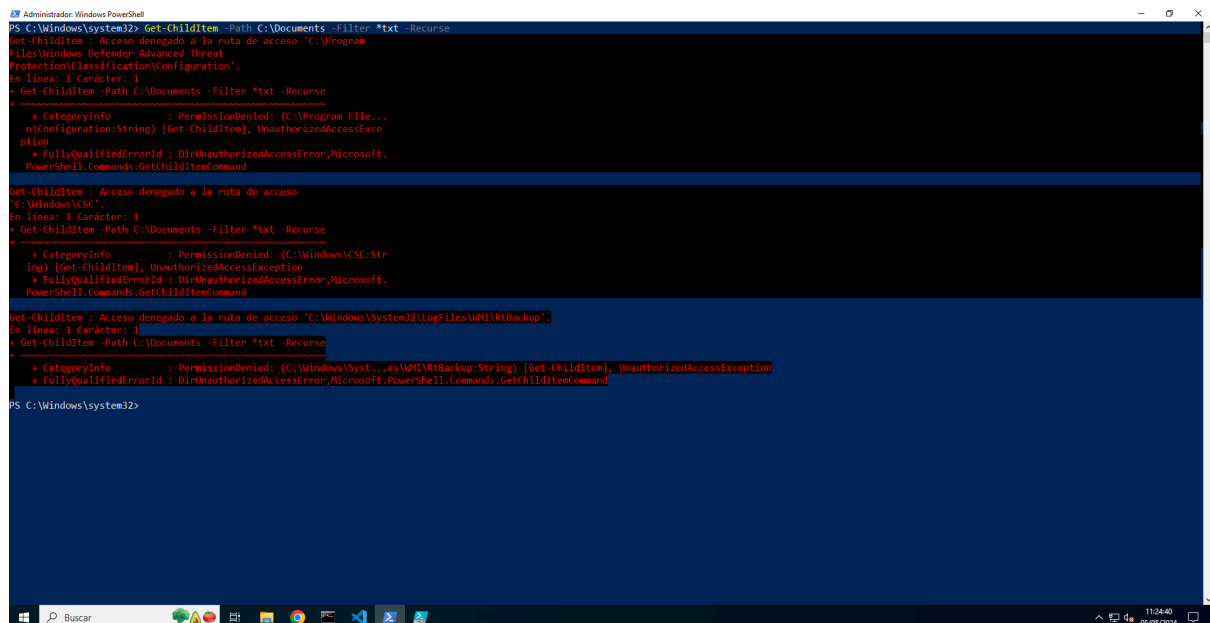


```
Administrador: Windows PowerShell
PS C:\Windows\System32> Get-Childitem -Path C:\Logs -Filter *.log
Get-Childitem : No se encuentra la ruta de acceso 'C:\Logs' porque no existe.
En línea: 1 Carácter: 1
+ Get-Childitem -Path C:\Logs -Filter *.log
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Logs:String) [Get-Childitem], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChilditemCommand

PS C:\Windows\System32>
```

2. Búsqueda recursiva de archivos: *'Get-ChildItem -Path C:\Documents -Filter \*.txt -Recurse'*

- a. Buscar todos los archivos .txt en el directorio C:\Documents y sus subdirectorios.



```
Administrador: Windows PowerShell
PS C:\Windows\System32> Get-Childitem -Path C:\Documents -Filter *.txt -Recurse
Get-Childitem : Acceso denegado a la ruta de acceso 'C:\Program Files\Windows Defender Advanced Threat Protection\Classification\Configuration'.
En línea: 1 Carácter: 1
+ Get-Childitem -Path C:\Documents -Filter *.txt -Recurse
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (C:\Program File...n\Configuration:String) [Get-Childitem], UnauthorizedAccessExce
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChilditemCommand

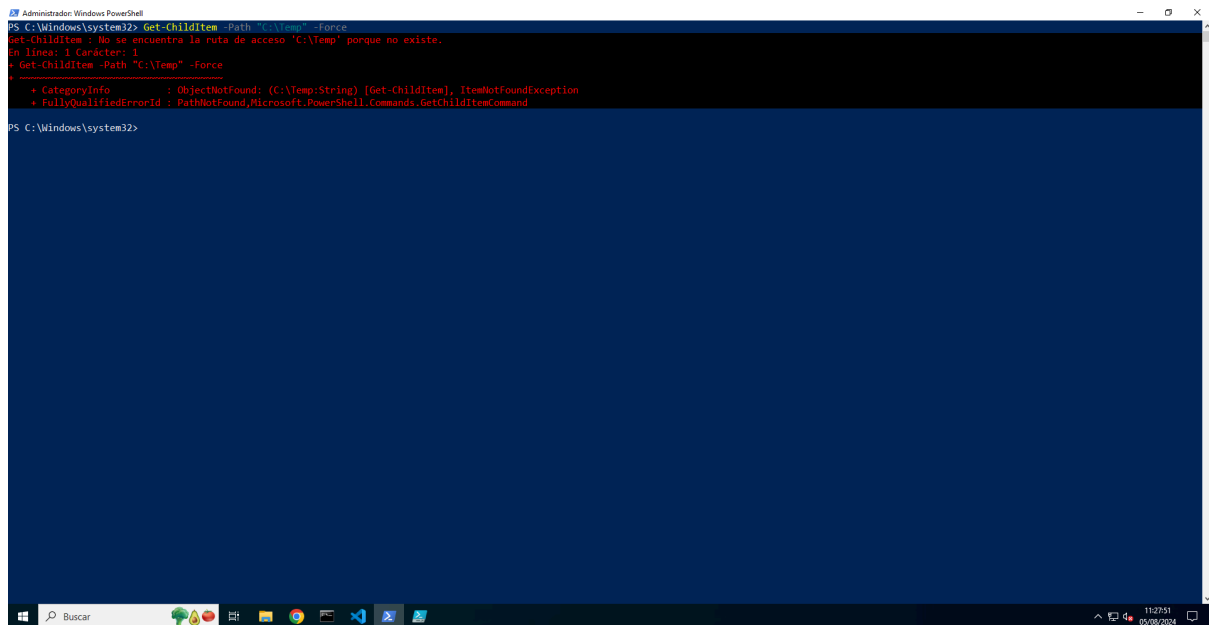
Get-Childitem : Acceso denegado a la ruta de acceso
C:\Windows\CS
En línea: 1 Carácter: 1
+ Get-Childitem -Path C:\Documents -Filter *.txt -Recurse
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (C:\Windows\CS:Str
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChilditemCommand

Get-Childitem : Acceso denegado a la ruta de acceso 'C:\Windows\System32\LogFiles\WMI\RTBackup'.
En línea: 1 Carácter: 1
+ Get-Childitem -Path C:\Documents -Filter *.txt -Recurse
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (C:\Windows\Syst...es\WMI\RTBackup:String) [Get-Childitem], UnauthorizedAccessException
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChilditemCommand

PS C:\Windows\System32>
```

3. Incluir archivos ocultos en la búsqueda: *'Get-ChildItem -Path C:\Temp -Force'*

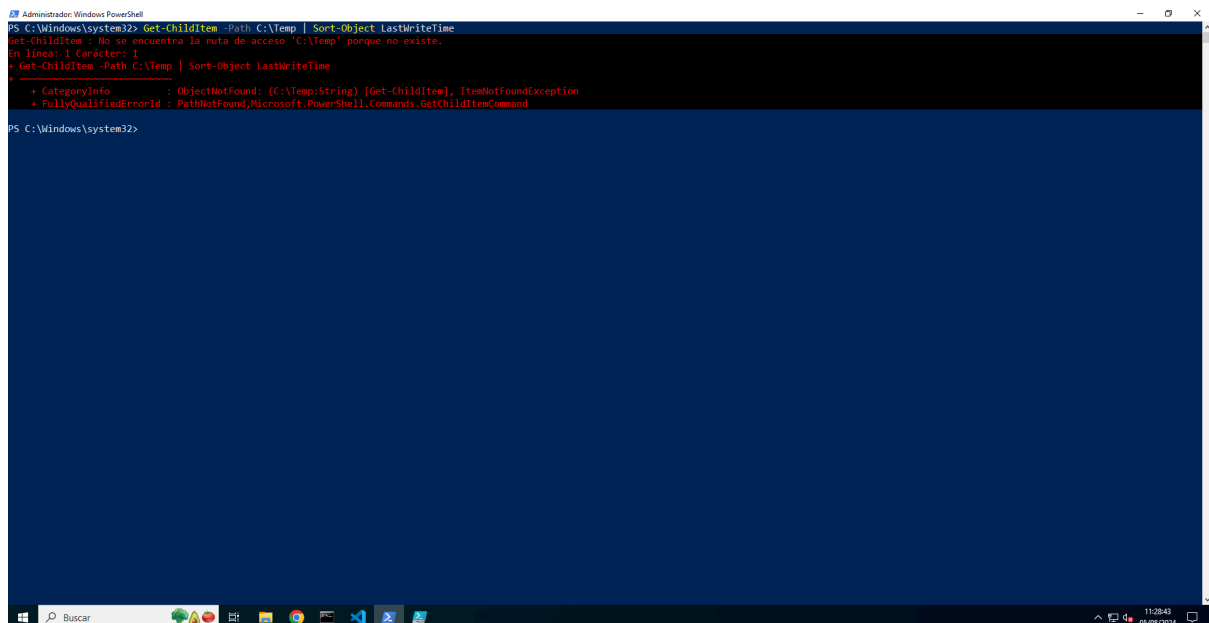
- a. Listar todos los archivos en el directorio C:\Temp, incluyendo archivos ocultos y de sistema.



```
Administrador: Windows PowerShell
PS C:\Windows\System32> Get-Childitem -Path C:\Temp -Force
Get-Childitem : No se encuentra la ruta de acceso 'C:\Temp' porque no existe.
En línea: 1 Carácter: 1
+ Get-Childitem -Path "C:\Temp" -Force
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Temp:String) [Get-Childitem], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChilditemCommand

PS C:\Windows\System32>
```

4. Listar archivos ordenados por fecha de modificación: *'Get-Childitem -Path C:\Temp | Sort-Object LastWriteTime'*
  - a. Listar archivos en el directorio C:\Temp ordenados por fecha de modificación.

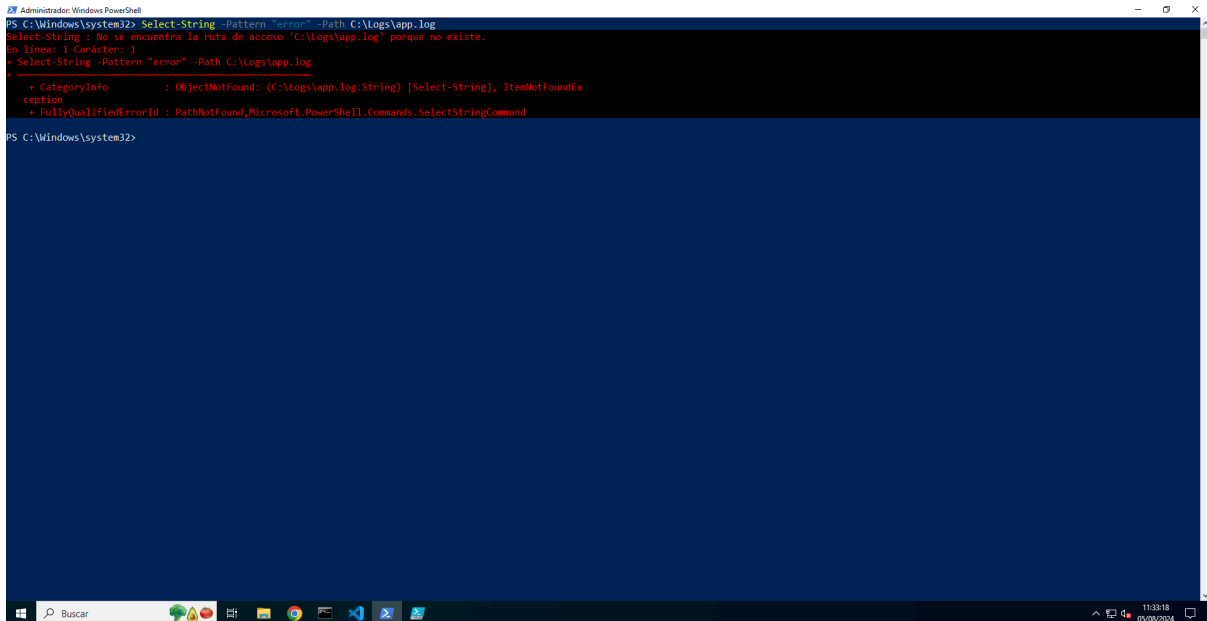


```
Administrador: Windows PowerShell
PS C:\Windows\System32> Get-Childitem -Path C:\Temp | Sort-Object LastWriteTime
Get-Childitem : No se encuentra la ruta de acceso 'C:\Temp' porque no existe.
En línea: 1 Carácter: 1
+ Get-Childitem -Path C:\Temp | Sort-Object LastWriteTime
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Temp:String) [Get-Childitem], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChilditemCommand

PS C:\Windows\System32>
```

5. Buscar texto en archivos: *'Select-String -Pattern "error" -Path C:\Logs\app.log'*

- a. Buscar la cadena "error" en el archivo C:\Logs\app.log.

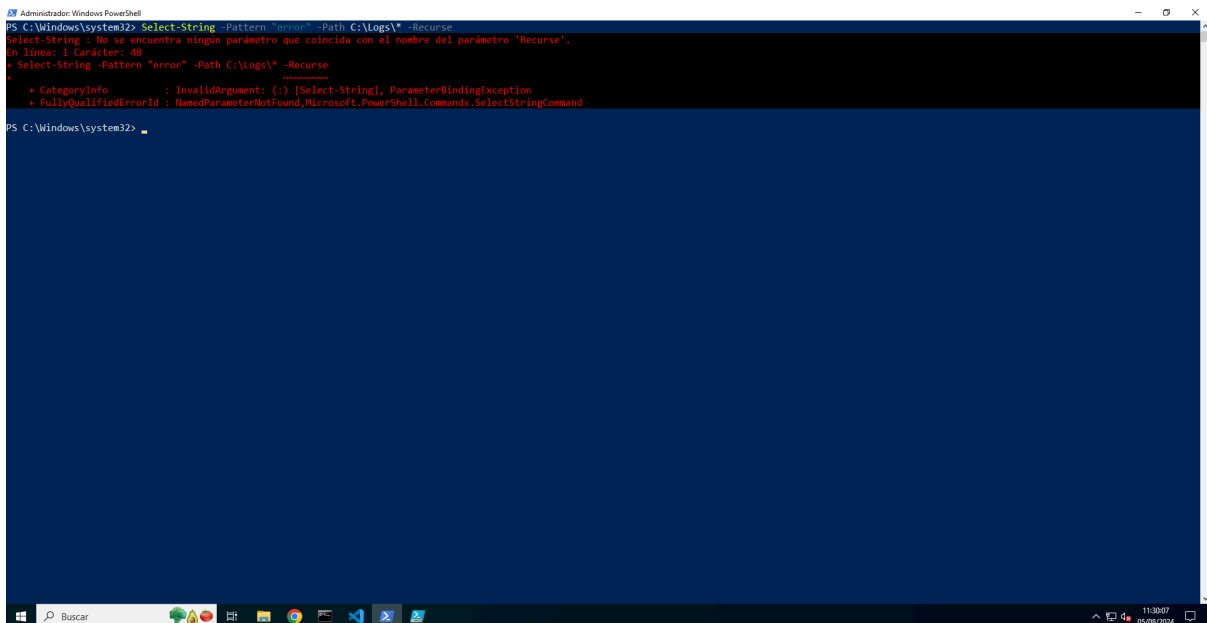


```
PS C:\Windows\system32> Select-String -Pattern "error" -Path C:\Logs\app.log
Select-String : No se encuentra la ruta de acceso 'C:\Logs\app.log' porque no existe.
En línea: 1 Carácter: 1
+ Select-String -Pattern "error" -Path C:\Logs\app.log
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Logs\app.log:String) [Select-String], ItemNotFoundEx
  ception
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SelectStringCommand

PS C:\Windows\system32>
```

6. Buscar texto en archivos recursivamente: *'Select-String -Pattern "error" -Path C:\Logs\\* -Recurse'*

- a. Buscar la cadena "error" en todos los archivos dentro del directorio C:\Logs y sus subdirectorios.

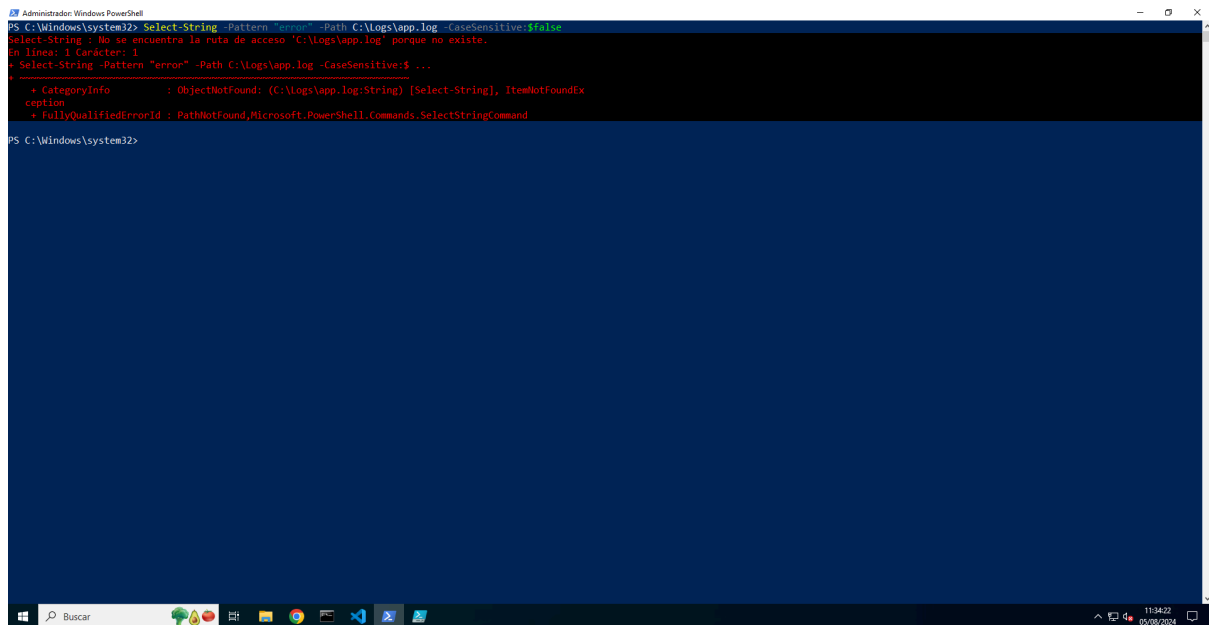


```
PS C:\Windows\system32> Select-String -Pattern "error" -Path C:\Logs\* -Recurse
Select-String : No se encuentra ningún parámetro que coincida con el nombre del parámetro 'Recurse'.
En línea: 1 Carácter: 48
+ Select-String -Pattern "error" -Path C:\Logs\* -Recurse
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Select-String], ParameterBindingException
  + FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.PowerShell.Commands.SelectStringCommand

PS C:\Windows\system32>
```

7. Buscar texto ignorando mayúsculas y minúsculas: *'Select-String -Pattern "error" -Path C:\Logs\app.log - CaseSensitive:\$false'*

- a. Buscar la cadena "error" en el archivo C:\Logs\app.log sin distinguir mayúsculas y minúsculas.

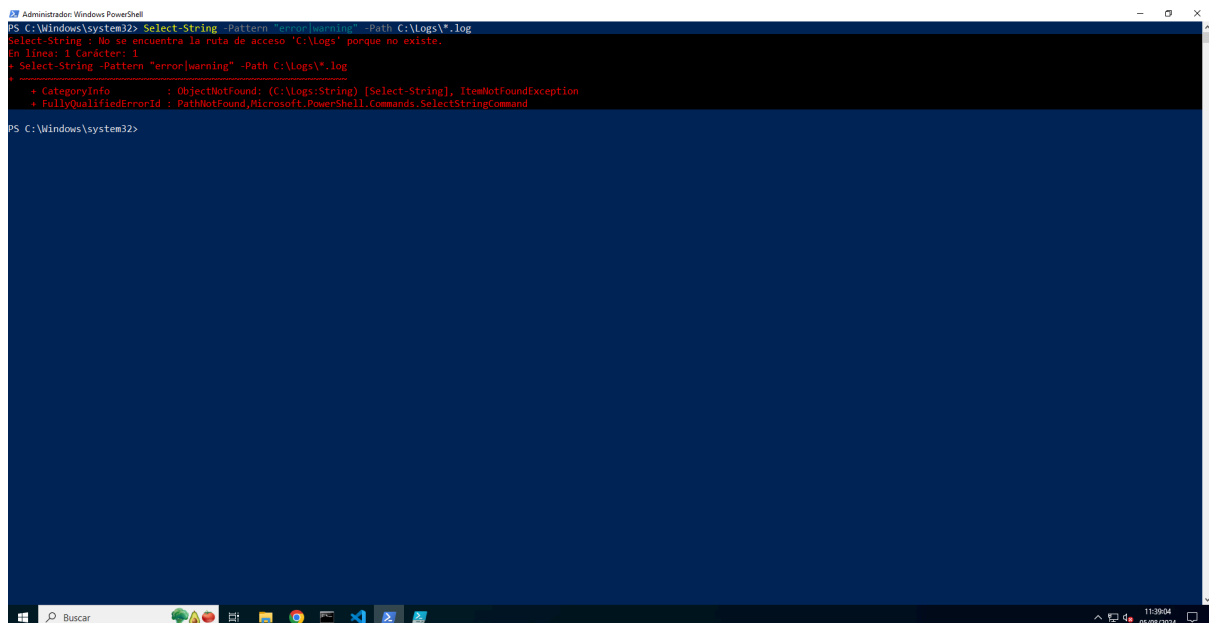


```
PS C:\Windows\system32> Select-String -Pattern 'error' -Path C:\Logs\app.log -CaseSensitive:$false
Select-String : No se encuentra la ruta de acceso 'C:\Logs\app.log' porque no existe.
En línea: 1 Carácter: 1
+ Select-String -Pattern "error" -Path C:\Logs\app.log -CaseSensitive:$...
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Logs\app.log:String) [Select-String], ItemNotFoundEx
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SelectStringCommand

PS C:\Windows\system32>
```

8. Buscar múltiples patrones en archivos: *'Select-String -Pattern "error|warning" -Path C:\Logs\\*.log'*

- a. Buscar las cadenas "error" y "warning" en todos los archivos .log en el directorio C:\Logs.



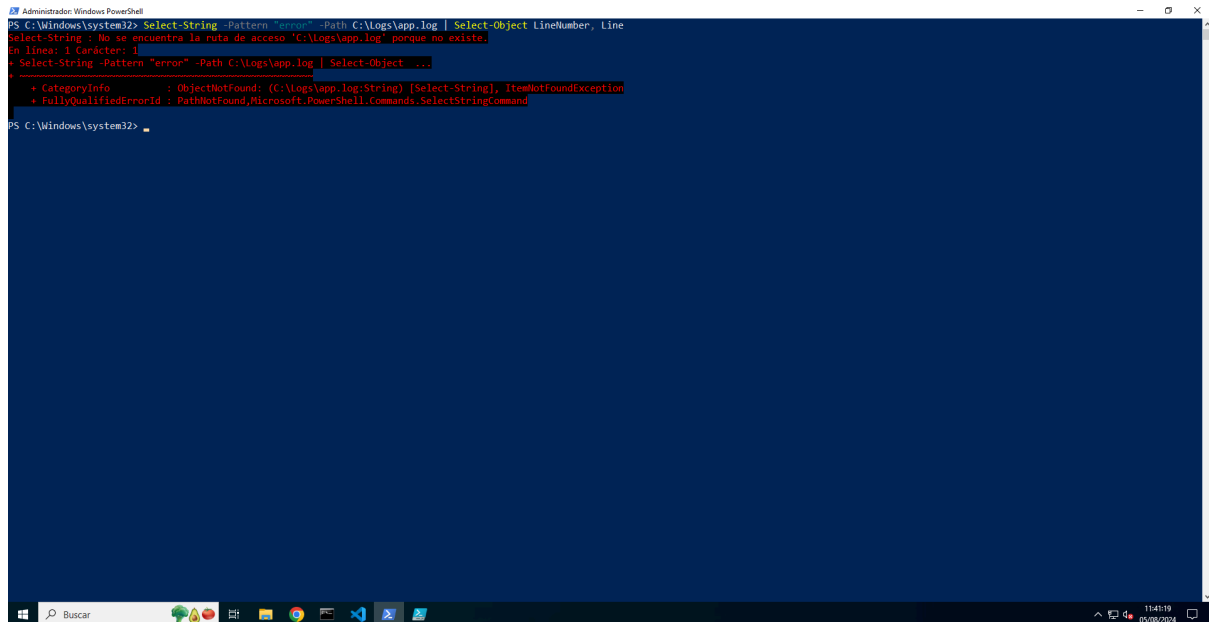
```
PS C:\Windows\system32> Select-String -Pattern 'error|warning' -Path C:\Logs\*.log
Select-String : No se encuentra la ruta de acceso 'C:\Logs' porque no existe.
En línea: 1 Carácter: 1
+ Select-String -Pattern "error|warning" -Path C:\Logs\*.log
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Logs:String) [Select-String], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SelectStringCommand

PS C:\Windows\system32>
```

9. Mostrar líneas con números de línea: *'Select-String -Pattern "error" -Path C:\Logs\app.log | Select-Object LineNumber, Line'*



- a. Buscar la cadena "error" en el archivo C:\Logs\app.log y mostrar las líneas que contienen esa cadena junto con sus números de línea.

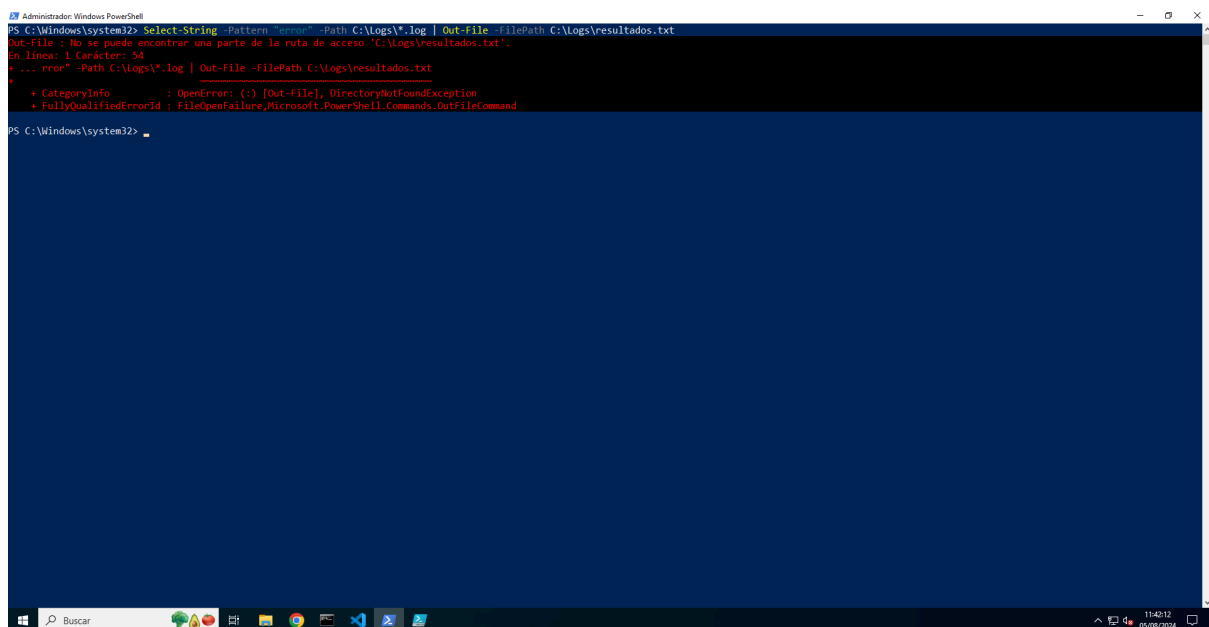


```
PS C:\Windows\system32> Select-String -Pattern "error" -Path C:\Logs\app.log | Select-Object LineNumber, Line
Select-String : No se encuentra la ruta de acceso 'C:\Logs\app.log' porque no existe.
En línea: 1 Carácter: 1
+ Select-String -Pattern "error" -Path C:\Logs\app.log | Select-Object ....
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Logs\app.log:String) [Select-String], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SelectStringCommand

PS C:\Windows\system32>
```

10. Buscar texto en archivos y exportar resultados: *'Select-String -Pattern "error" -Path C:\Logs\\*.log | Out-File -FilePath C:\Logs\resultados.txt'*

- a. Buscar la cadena "error" en todos los archivos .log en el directorio C:\Logs y exportar los resultados a un archivo resultados.txt.



```
PS C:\Windows\system32> Select-String -Pattern "error" -Path C:\Logs\*.log | Out-File -FilePath C:\Logs\resultados.txt
Out-File : No se puede encontrar una parte de la ruta de acceso 'C:\Logs\resultados.txt'.
En línea: 1 Carácter: 54
+ ... rror" -Path C:\Logs\*.log | Out-File -FilePath C:\Logs\resultados.txt
+ ~~~~~
+ CategoryInfo          : OpenError: (:) [Out-File], DirectoryNotFoundException
+ FullyQualifiedErrorId : FileOpenFailure,Microsoft.PowerShell.Commands.OutFileCommand

PS C:\Windows\system32>
```

