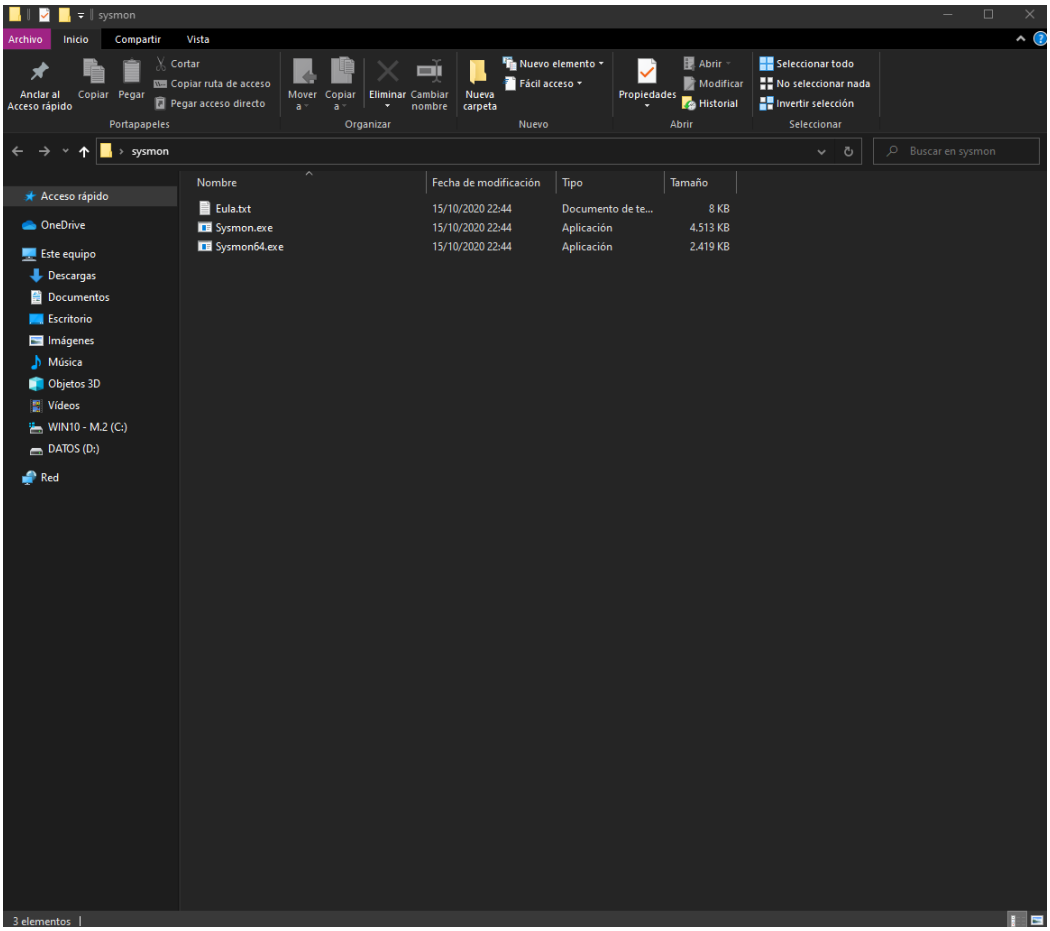
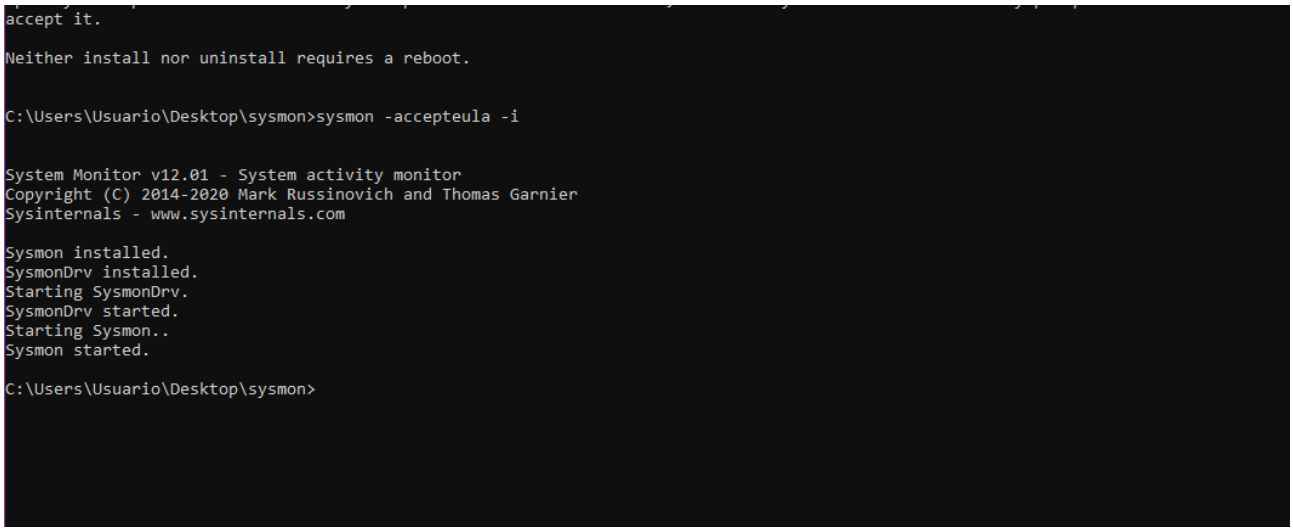
TAREA 5B

Instalación de Sysmon




```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.18363.1139]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>cd C:\Users\Usuario\Desktop\sysmon

C:\Users\Usuario\Desktop\sysmon>sysmon


System Monitor v12.01 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Usage:
Install:                sysmon -i [<configfile>]
Update configuration:   sysmon -c [<configfile>]
Install event manifest: sysmon -m
Print schema:           sysmon -s
Uninstall:              sysmon -u [force]
  -c    Update configuration of an installed Sysmon driver or dump the
        current configuration if no other argument is provided. Optionally
        take a configuration file.
  -i    Install service and driver. Optionally take a configuration file.
  -m    Install the event manifest (done on service install as well).
  -s    Print configuration schema definition of the specified version.
        Specify 'all' to dump all schema versions (default is latest).
  -u    Uninstall service and driver. Adding force causes uninstall to proceed
        even when some components are not installed.

The service logs events immediately and the driver installs as a boot-start driver to capture activity from early in
the boot that the service will write to the event log when it starts.

On Vista and higher, events are stored in "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational". On
older systems, events are written to the System event log.

Use the '-? config' command for configuration file documentation.More examples are available on the Sysinternals
website.

Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to
accept it.

Neither install nor uninstall requires a reboot.
```


accept it.
Neither install nor uninstall requires a reboot.
C:\Users\Usuario\Desktop\sysmon>sysmon -accepteula -i
System Monitor v12.01 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
C:\Users\Usuario\Desktop\sysmon>