Hands-On Lab: OS Processes and Services

To accompany Whitman and Mattord, Principles of Information Security, 7th Ed., 2022, ISBN 9780357506431; OS Processes and Services

Table of Contents

[Introduction 2](#_Toc76732975)

[Objective 2](#_Toc76732976)

[Estimated Completion Time 2](#_Toc76732977)

[Materials Required 2](#_Toc76732978)

[Minimum System Configuration 2](#_Toc76732979)

[Windows Process Assessment 3](#_Toc76732980)

[Reviewing Windows Processes with Task Manager 3](#_Toc76732981)

[Opening Task Manager 3](#_Toc76732982)

[Reviewing Windows Processes with Task Manager 3](#_Toc76732983)

[Reviewing Windows Processes with Process Explorer 9](#_Toc76732984)

[Windows Service Assessment 11](#_Toc76732985)

[Opening Task Manager 11](#_Toc76732986)

[Reviewing Windows Services with Task Manager 11](#_Toc76732987)

[Active Processes and Services Assessment with msconfig 15](#_Toc76732988)

[Opening msconfig 15](#_Toc76732989)

[Reviewing Windows Services 16](#_Toc76732990)

[Service Assessment with Performance and Resource Monitor 17](#_Toc76732991)

[Using the Performance Tab 17](#_Toc76732992)

[Opening Resource Monitor 19](#_Toc76732993)

[Using Resource Monitor 20](#_Toc76732994)

[Self-Reflection and Response 22](#_Toc76732995)

[Instructor’s Response 22](#_Toc76732996)

# Introduction

Part of the job of the information security function is to detect when things are not working as expected, specifically when we have technology that may have been compromised or corrupted so that it cannot be trusted to handle our information without risk of breach of confidentiality, integrity, or availability. While there are many complex tools available that can assist us in detecting unusual activity on a computer, we can also perform some routine evaluations ourselves to detect whether a system has an issue that warrants further investigation.

This lab will discuss the utilities available in Windows 10 that allow the user and administrators of the system to review, identify, and resolve potential issues with running processes and services, and with the current operations of the system

## Objective

Upon completion of this activity, the student will be able to:

* Review available and enabled OS services.
* Review available and enabled OS processes.
* Review current system resource utilization.

These activities will help you complete future labs in this course.

## Estimated Completion Time

If you are prepared, you should be able to complete this lab in 60-90 minutes.

## Materials Required

Completion of this lab requires the following software to be installed and configured on your personal computer:

* Microsoft Windows 10, or another operating system version specified by the lab instructor.

## Minimum System Configuration

To complete the labs included, it is recommended that you operate them from a computer system (desktop or laptop) that is running Windows 10 and has:

* Intel i5 or better CPU
* 8 GB RAM (minimum) - 16 GB RAM (recommended)
* 1 TB Hard Drive with at least 250 GB free (minimum) - 350 GB free (recommended)
* Microsoft Windows 10 or latest version

# Windows Process Assessment

It is important to know what programs and applications are running processes on your system, to be able to detect when a program is malfunctioning, or an application is running that you didn’t authorize. There are several utilities available to allow the user to review the running processes. Once you can review these processes you can determine which are legitimate and which are not.

## Reviewing Windows Processes with Task Manager

One of the first utilities that is integral to Microsoft Windows is the Task Manager, a tool that is native to Microsoft Windows.

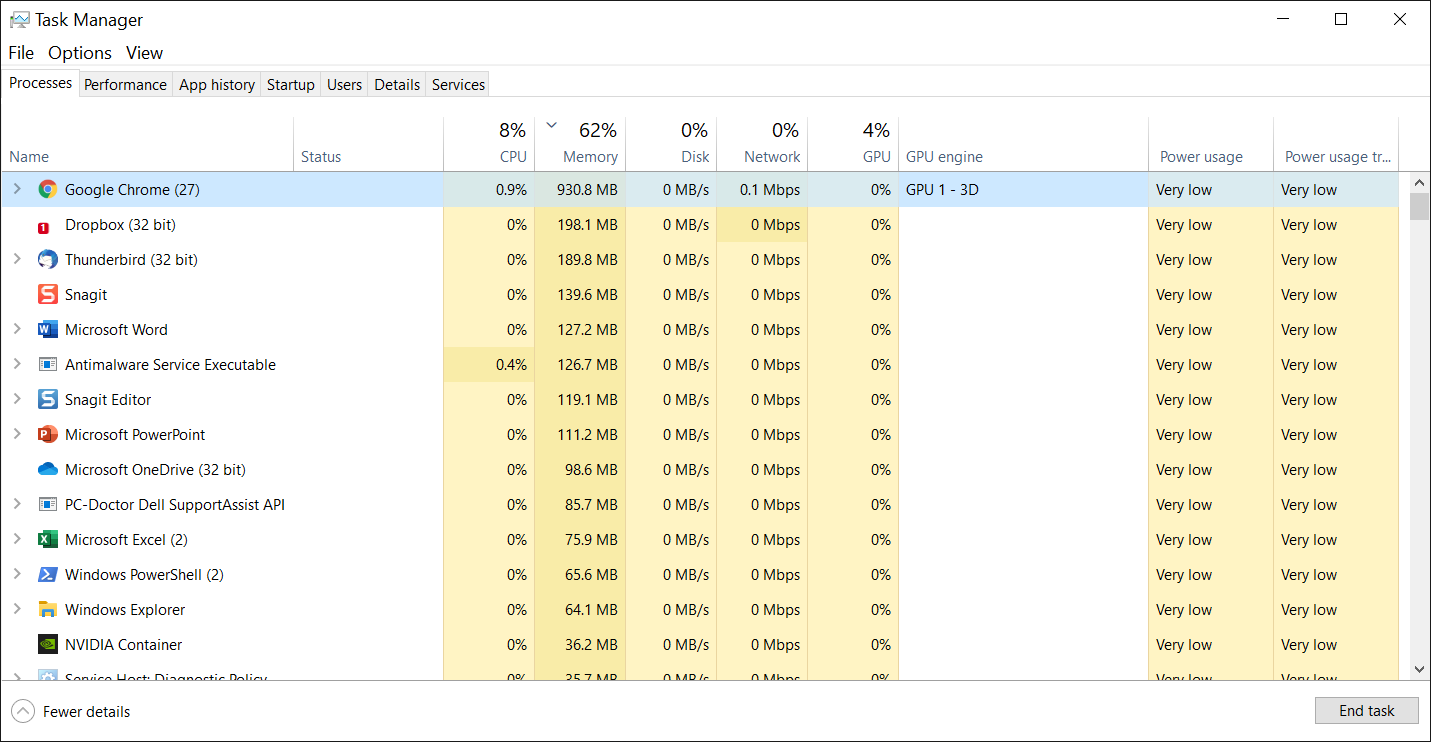
### Opening Task Manager

1. There are a number of ways to access the Windows Task Manager.
   1. In the Windows search bar, type *Task Manager* and click the app.
   2. Right click on the Windows Start button and select *Task Manager*.
   3. Select the **Ctrl + Alt + Del** keys and select *Task Manager*.
   4. You can also select the **Ctrl + Shift + Esc** keys.

Choose one of these ways and open the Task Manager.

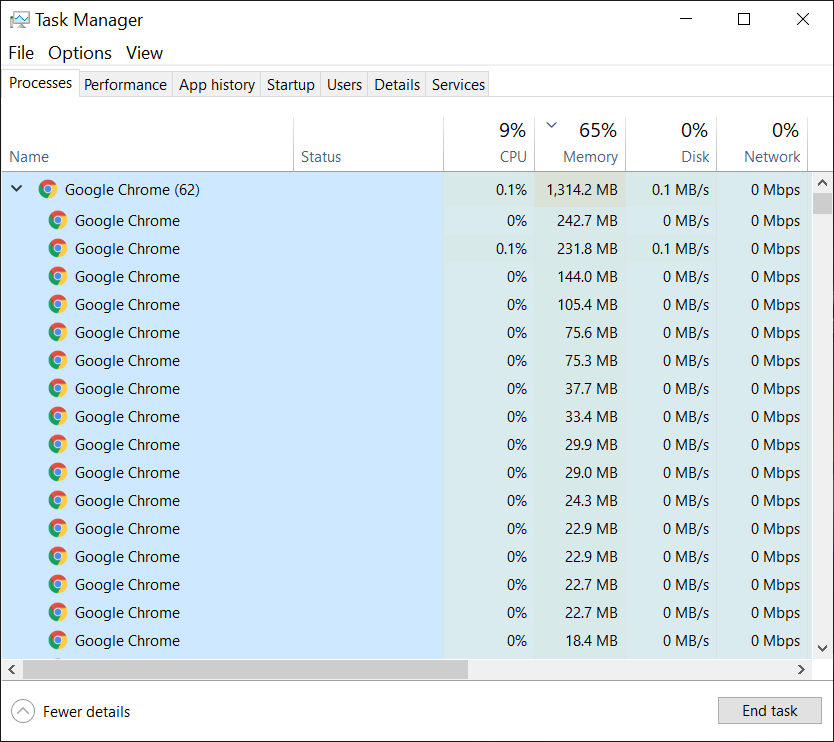
### Reviewing Windows Processes with Task Manager

1. Once open, the default view in Task Manager shows the running processes active on this system. If your view does not look like Figure L06-1 below, click on the **More details** option at the bottom. You may also need to expand the window by dragging on the right edge to see additional columns.



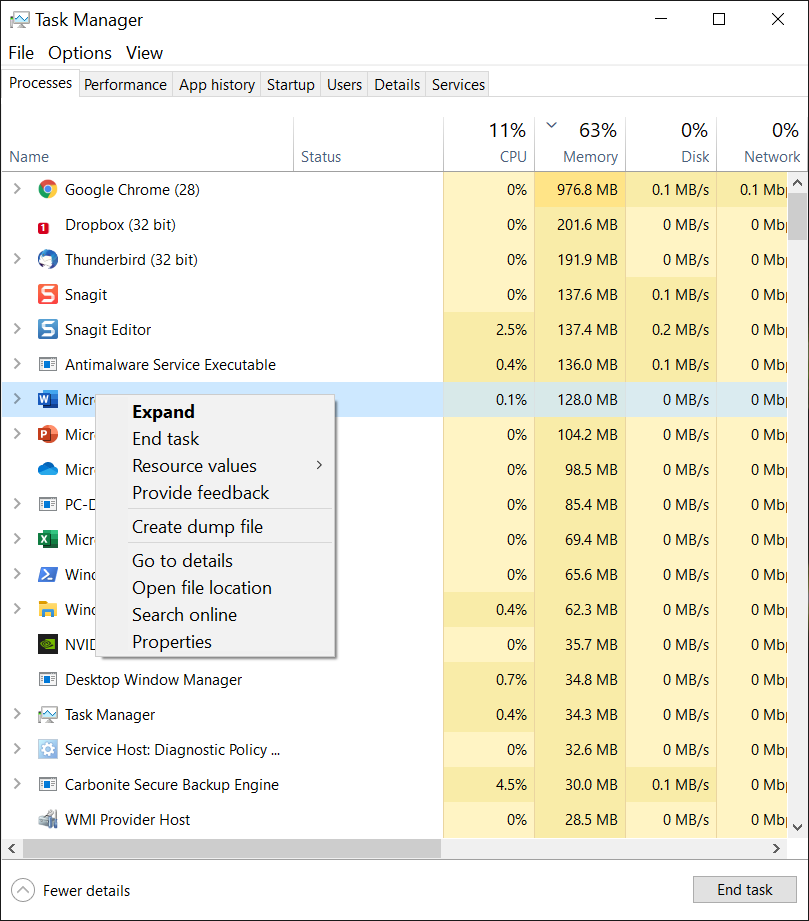
**Figure L06-1** Windows Task Manager

1. Processes are instances of a program or application that are current running on the system. As indicated in Figure L06-1, there are currently many processes associated with Google Chrome running on the example system. You can examine each process individually by clicking the arrow to the left of the process, as shown in Figure L06-2. Each process consumes resources, although inactive processes consume less. The first thing to examine when your system becomes sluggish is whether you have too many processes running, whether they are active or not. In Task Manager, processes are grouped into Applications (programs), Background Processes, and Windows Processes.



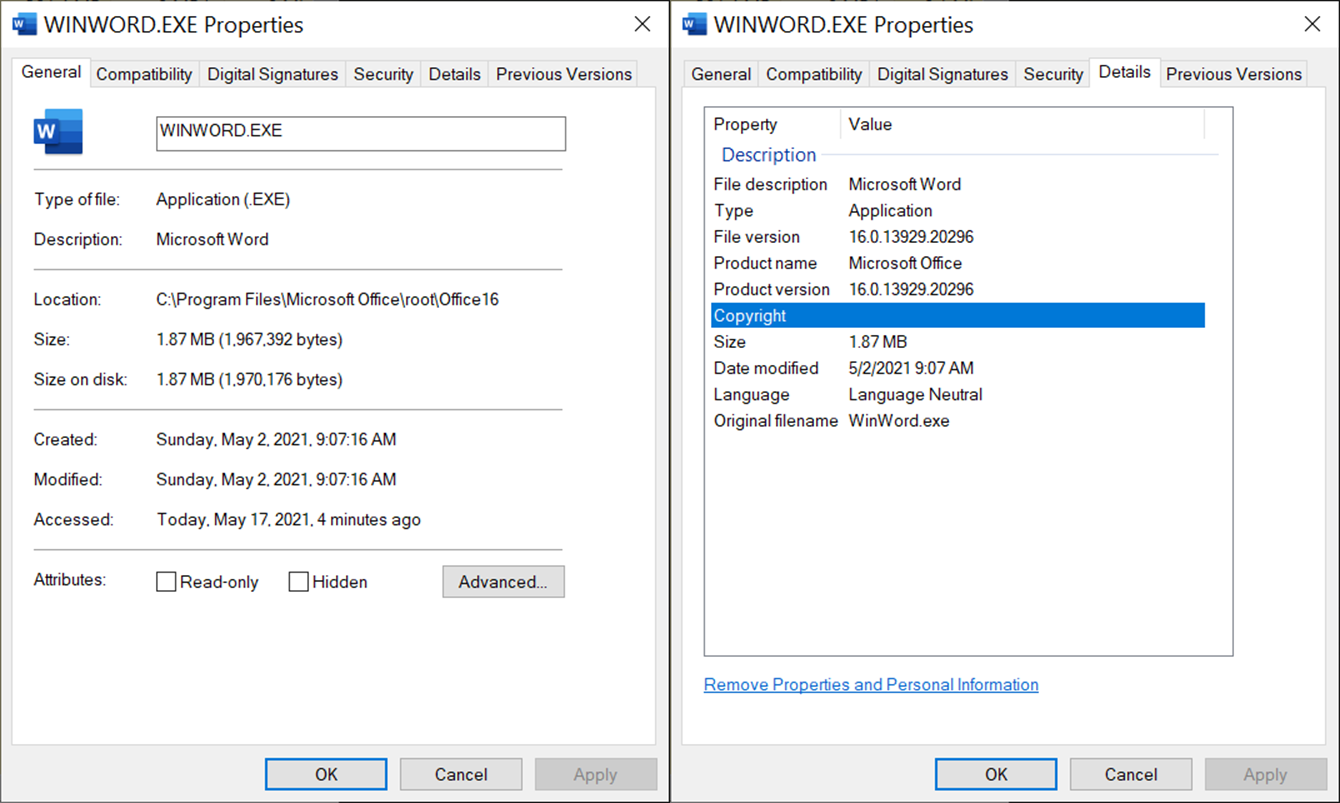
**Figure L06-2** Multiple Google Chrome Processes

1. You can select an individual process and end it by clicking on the process and then clicking on the **End task** button at the bottom. This is especially useful when a process/program becomes unresponsive. You can also view additional details by selecting the process, right clicking, and selecting **details**, or by simply selecting the **Details** tab in the top menu. Look at the details of several processes now.
2. It is important to become familiar with the processes a computer is running by examining this list from time to time. You can learn more about a process by letting Windows look it up for you on the web. Select any process, right click on it, and select **Search Online**. See Figure L06-3 for an example.



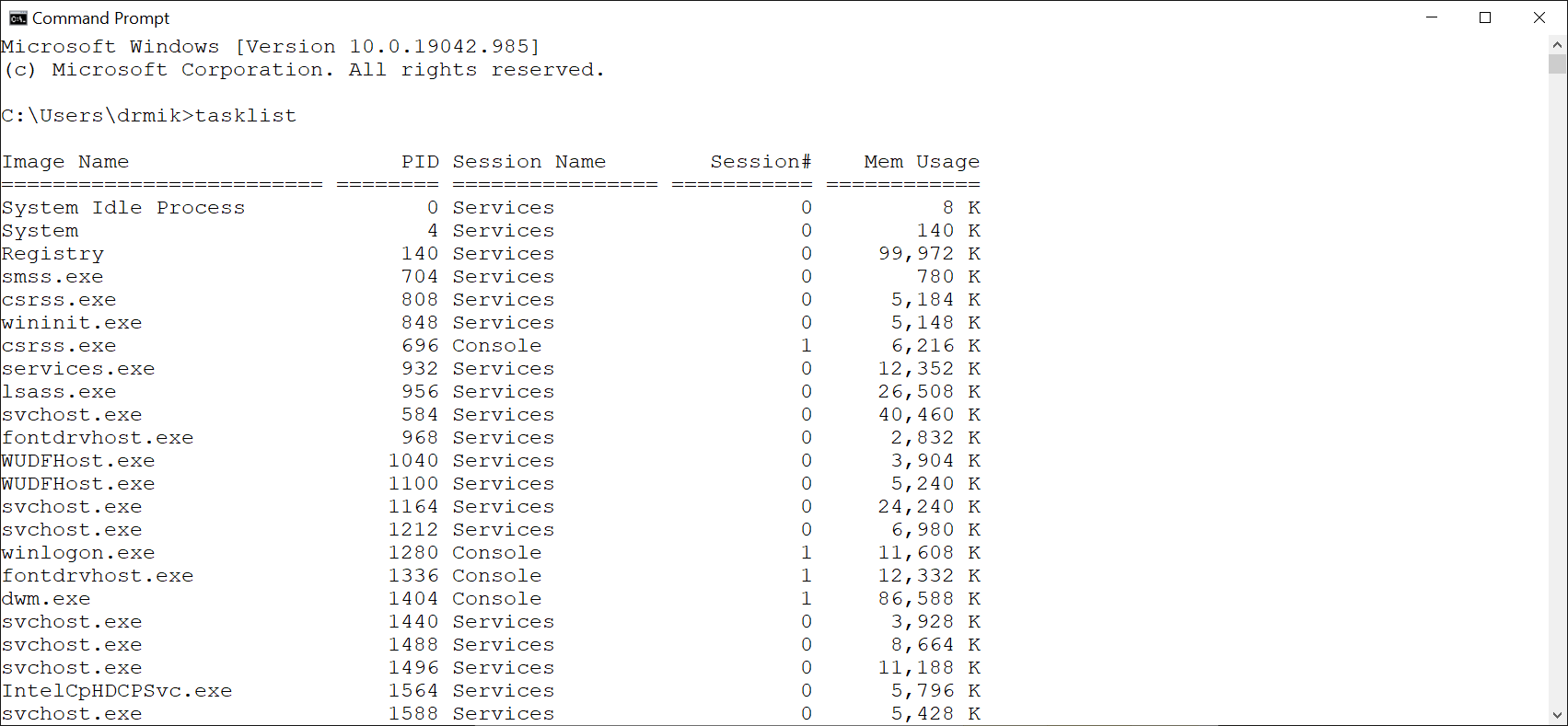
**Figure L06-3** Process Right Click Menu

1. This will allow you to learn more about the process, in case you don’t recognize it. You can also view the properties of the process in the same menu. Examples of the properties window and its corresponding details tab are shown in Figure L06-4.



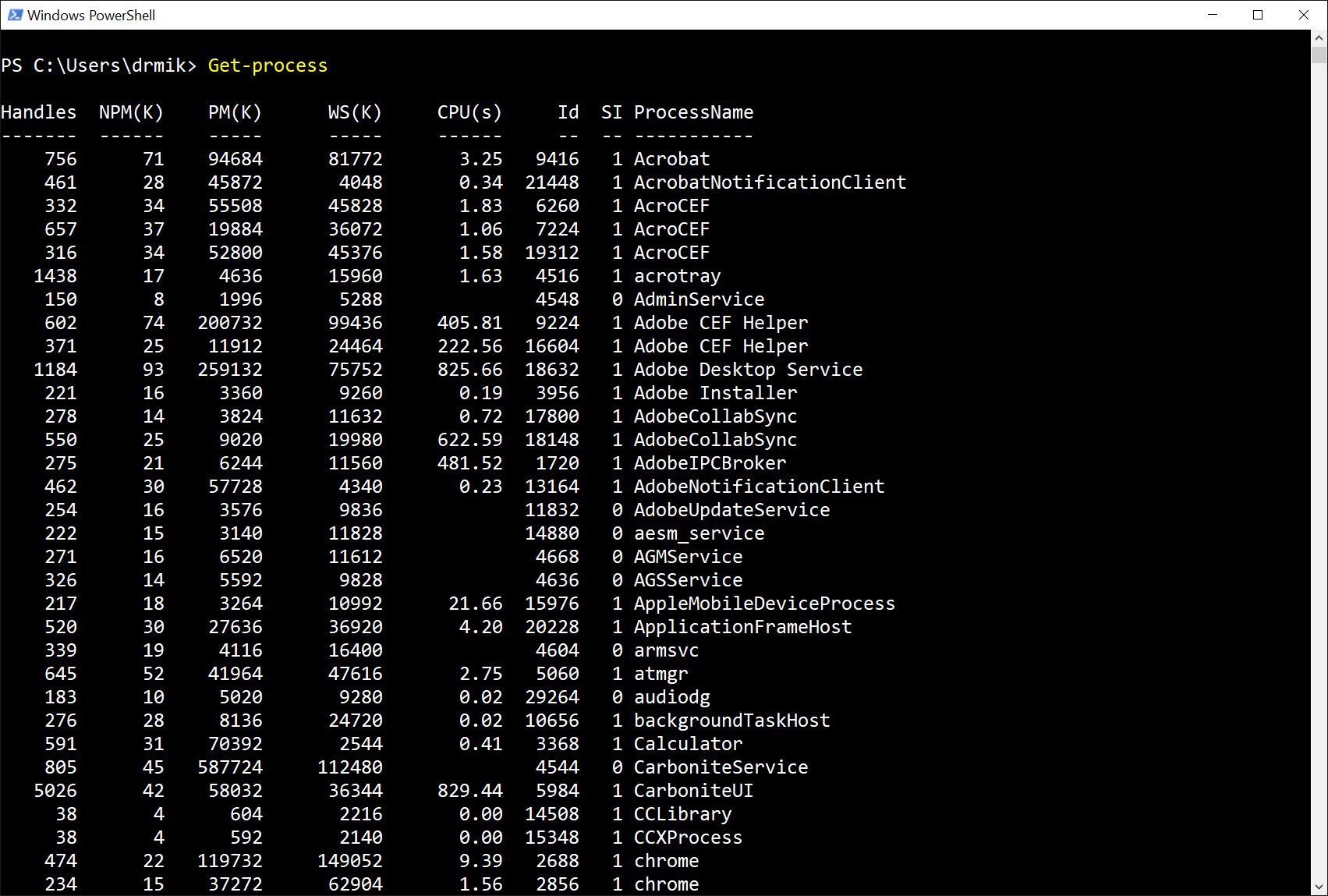
**Figure L06-4** Microsoft Word Process Properties and Details

1. The biggest challenge in managing processes are the numerous processes run on your behalf by the operating system. Scroll down in your list of processes, and you’ll see a group called Windows processes. In that group you’ll see many instances of Service Host – Window’s tool for running services connected to dynamic link libraries (DLL) – resources to support your computer use. The details of these components of the operating system are beyond this lab. There are a number of online references that can help you understand this better. We recommend “How-To Geek: <https://www.howtogeek.com/>.
2. If you want to document the running processes for future reference, you can use a Command window or PowerShell:
   1. Open a command window by typing **cmd** in the window search bar and press **Enter**. Then type **tasklist** at the prompt and press **Enter**. You’ll get a long list on your screen with some basic information as shown in Figure L06-5. To redirect this to a file, repeat the command adding a redirect – **tasklist > processes.txt** and press **Enter**. This will copy the screen output to a text file.



**Figure L06-5** Command prompt display of Windows processes

* 1. You can do the same thing with the PowerShell command. Open a PowerShell session by right clicking the Windows **Start** button on the left side of the task bar and selecting **Windows PowerShell**. In the PowerShell window, type **Get-process** and press **Enter**. Again, you can redirect this to a file by typing **Get-process > processes.txt** and pressing **Enter**.



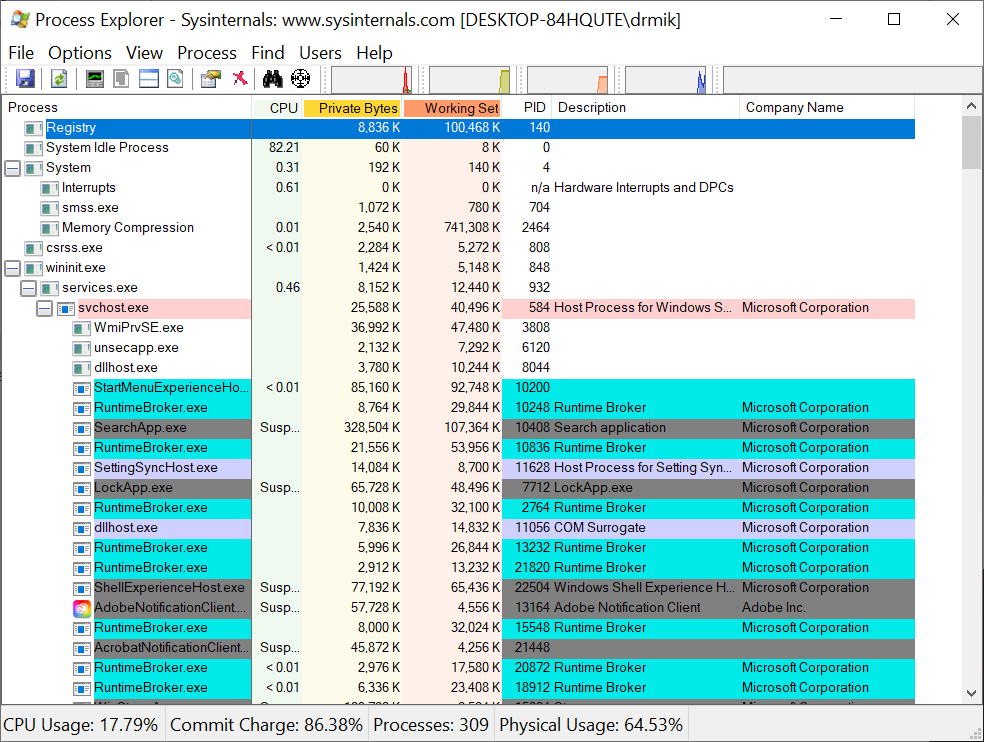
**Figure L06-6** Windows PowerShell Get-process command and results

## Reviewing Windows Processes with Process Explorer

Microsoft has a special utility you can use to learn more about a process, specifically about what resources a process has open. If you’ve ever tried to close a file and received an error message that the file is open or in use, but can’t find an associated application, a process may have it locked as in use.

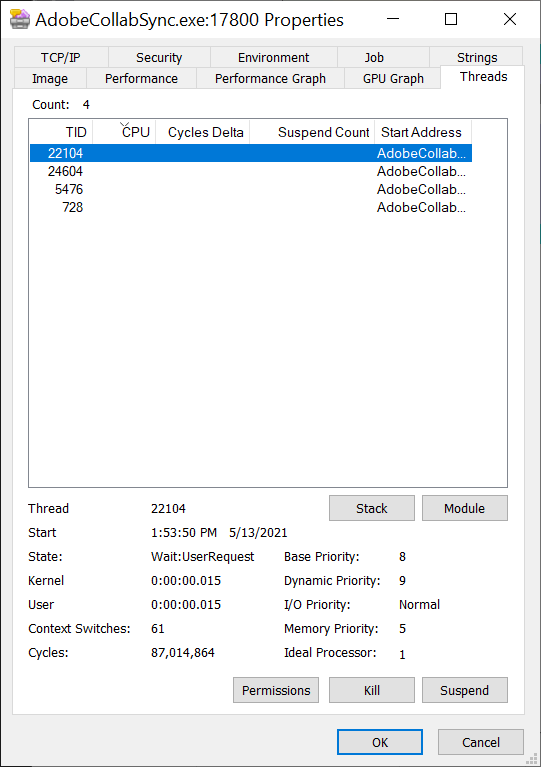
Download Process Explorer

1. First ask your instructor if Process Explorer is already installed. If not, go to <https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer> and click on the Download Process Explorer link at the top of the page. Save the zip file to your local drive and then extract the files to a location you can access.
2. Double click the **proceexp64.exe** file and accept the license agreement. Process Explorer will start as shown in Figure L06-7.



**Figure L06-7** Sysinternals Process Explorer

1. To view a process’ threads (parts of a process) with Process Explorer, select a process and open the process properties by clicking on the process, right click to open a menu, and then select the **Properties** menu item. Then click on the **Threads** tab. As shown in Figure L06-8, you’ll see any threads associated with that process. Note the threads are numbered with an ID (TID) and not named.



**Figure L06-8** Threads associated with a process

1. Here you can see CPU consumption and other information. This information is also color coded with new threads highlighted in green, and threads that exit highlighted in red.

# Windows Service Assessment

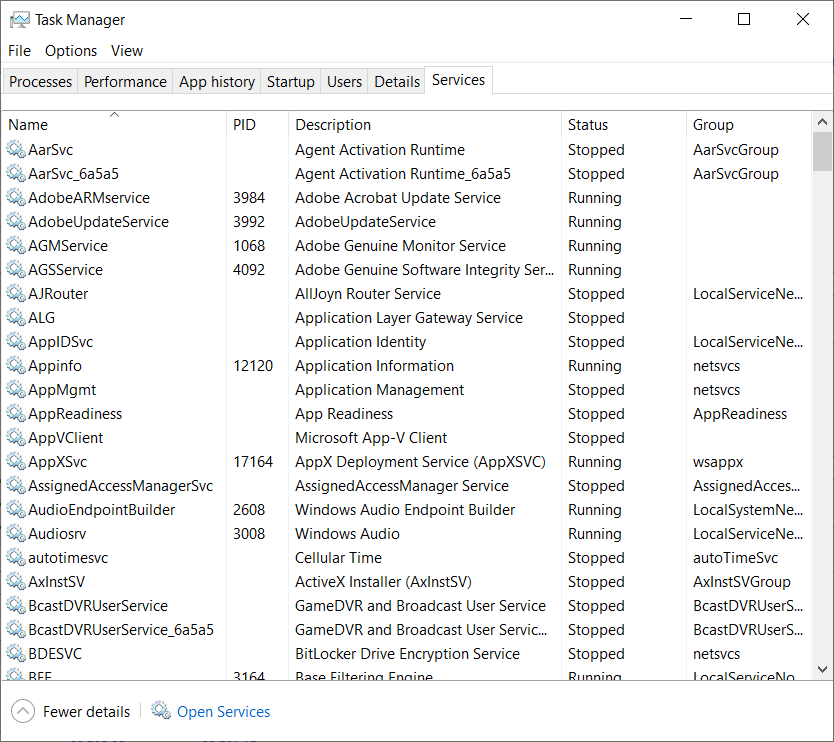
The Windows Task Manager can also be used to examine services. Services are processes that run in the background and don’t directly interact with the user or the desktop.

## Opening Task Manager

1. If you don’t have the Task Manager running already, open it now using one of the following methods:
   1. In the Windows search bar, type *Task Manager* and click the app.
   2. Right click on the Windows Start button and select *Task Manager*.
   3. Select **Ctrl + Alt + Del** keys and select *Task Manager*.

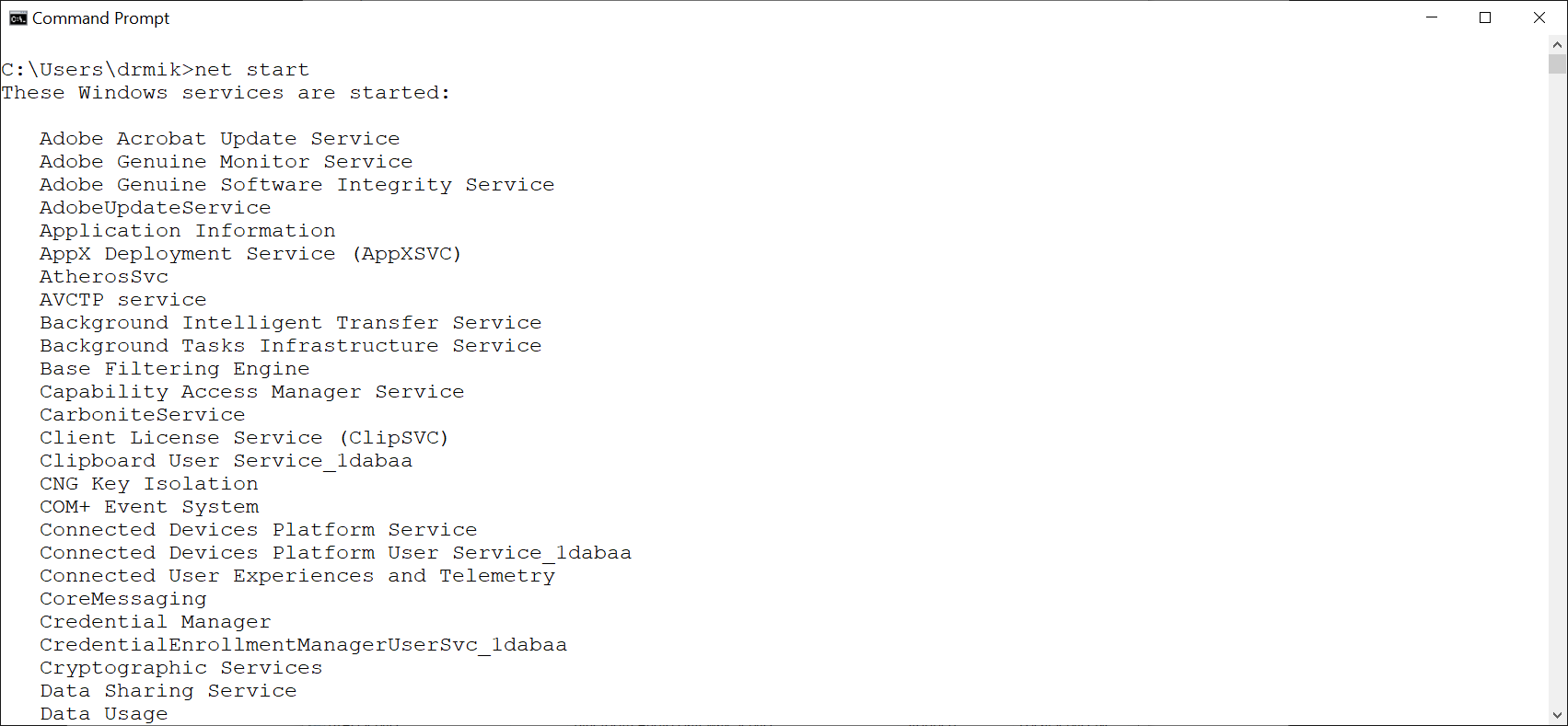
## Reviewing Windows Services with Task Manager

1. Once Task Manager is open, select the **Services** tab at the top. As shown in Figure L06-9, services are listed alphabetically, including a brief description and their status as running or stopped. Since services run in the background, if you don’t review the list, you may never know what is running on your system.



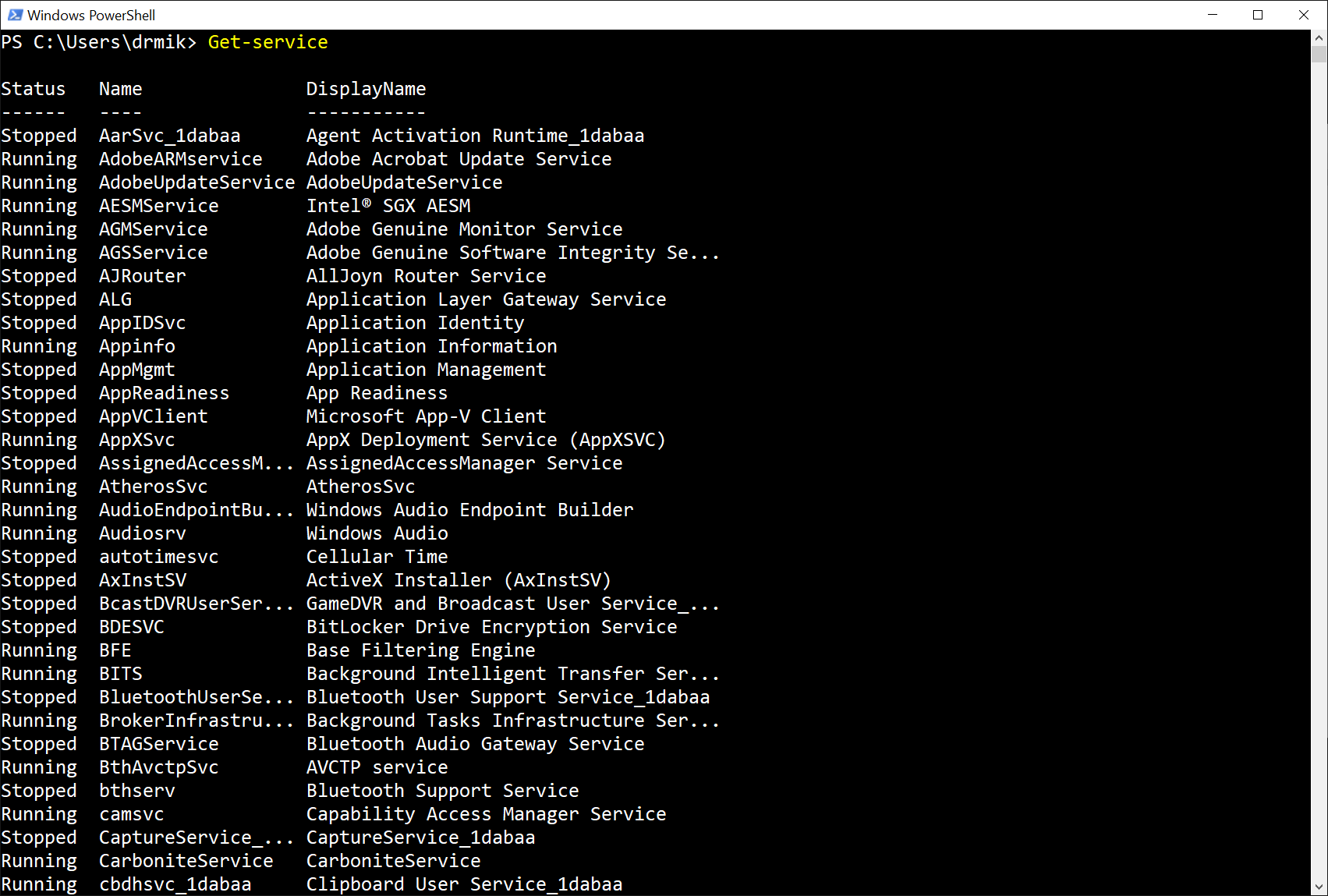
**Figure L06-9** Task Manager Services

1. Just like you could with Processes, you can learn more about a particular service by selecting it and looking at its menu. Right click one of the services running on your system and select **Details**. This brings you back to the Details tab, where both processes and services are listed with additional information.
2. Go back to the **Services** tab, and right click the service again, this time selecting Search online. This will open a web browser with a search on that particular service, allowing you to better understand the service.
3. If you want to document the running services for future reference, you can use a Command window or PowerShell, just like you did with Processes:
   1. Open a command window by typing **cmd** in the window search bar and press **Enter**. Then type **net start** at the prompt and press **Enter**. You’ll get a long list on your screen of just the services that are started and running, as shown in Figure L06-10. To redirect this to a file, repeat the command adding a redirect – **net start > services.txt** and press **Enter**. This will copy the screen output to a text file.



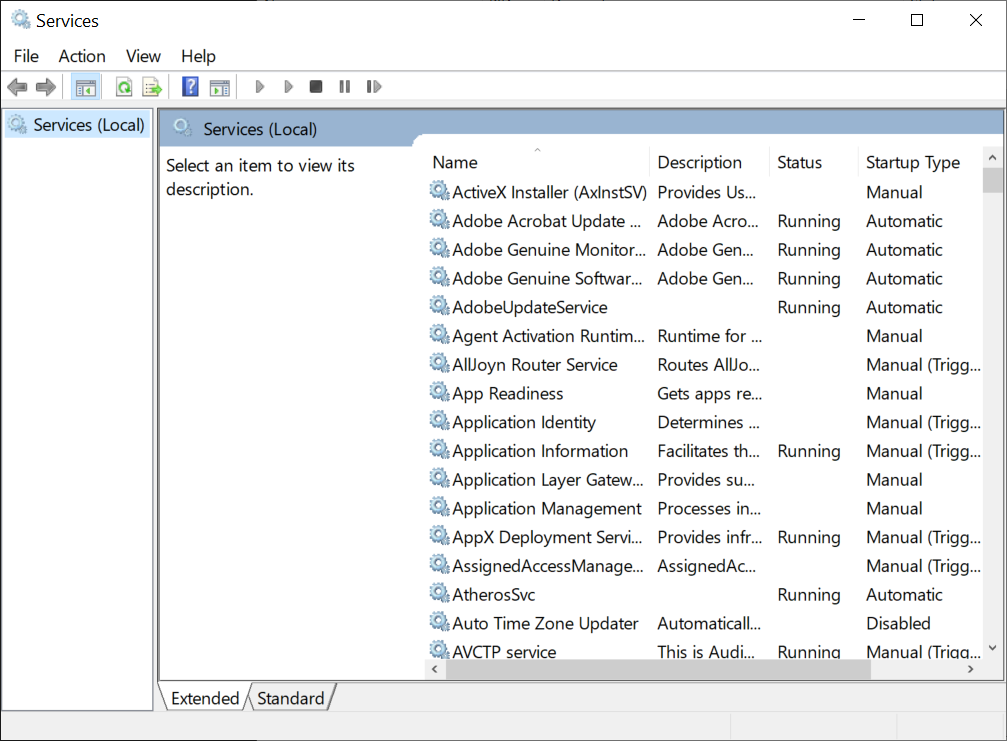
**Figure L06-10** Command prompt display of started Windows services

* 1. You can do the same thing with the PowerShell command. Open a PowerShell session by right clicking the Windows **Start** button on the left side of the task bar and selecting **Windows PowerShell**. In the PowerShell window, type **Get-service** and press **Enter**. Unlike the command window, PowerShell includes all services and their status as stopped or running. Again, you can redirect this to a file by typing **Get-service > processes.txt** and pressing **Enter**.

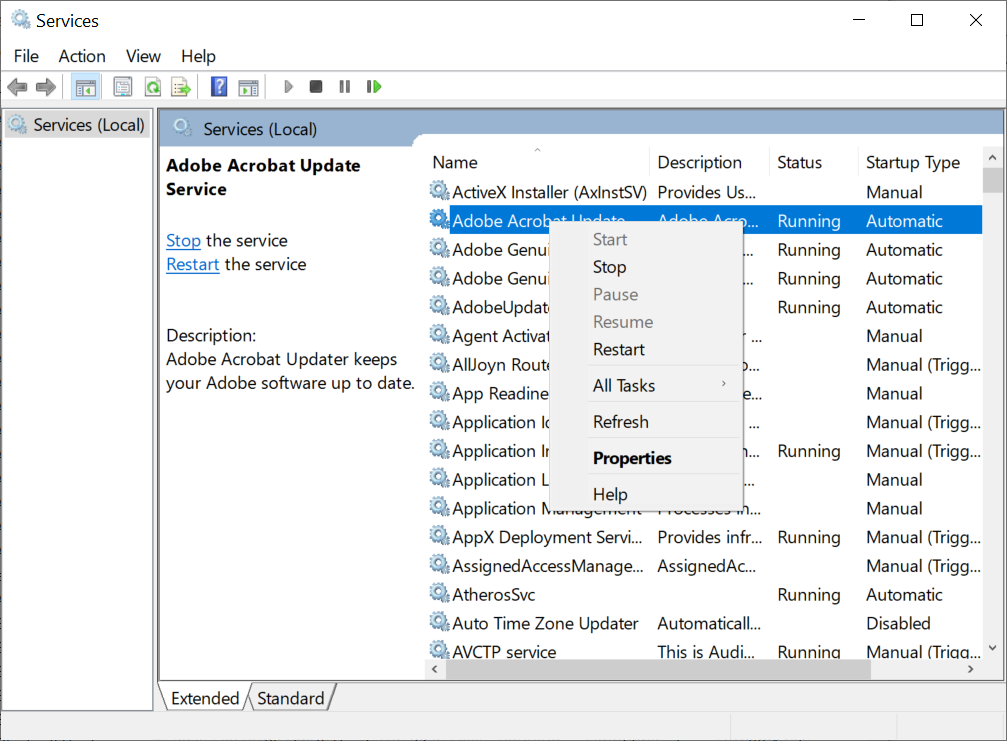


**Figure L06-11** Windows PowerShell Get-service command and results

1. If you wanted to stop a running service or start a service that is stopped, you can do so from the Task Manager. Back at the Task Manager, right click a service, and select **Open Services**. This opens the Services MMC, as shown in Figure L06-12. As shown in Figure L06-13, if you right click a service in the Services MMC, you open a menu allowing you to change the status of a service and look at its properties.

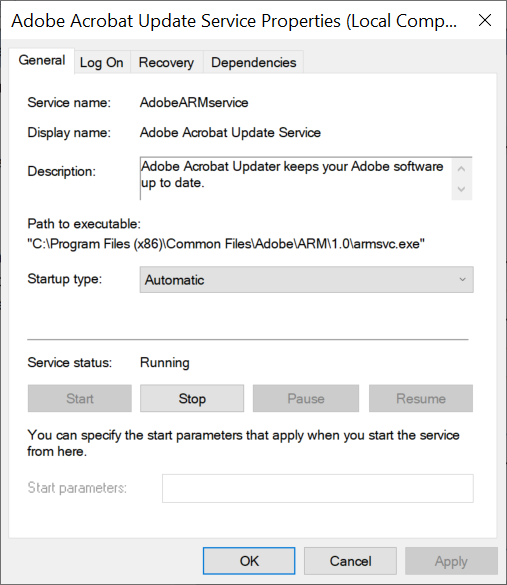


**Figure L06-12** WIndows Services MMC



**Figure L06-13** Windows Service Sub-menu

The properties include its dependencies on other services, drivers, etc. (see Figure L06-14.) Review the properties on a few services to become more familiar with this information.



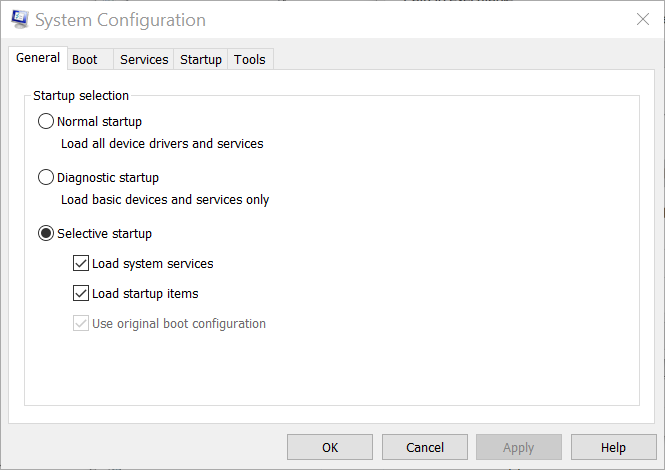
**Figure L06-14** Service Properties Screen

## Active Processes and Services Assessment with msconfig

Windows System Configuration Utility, better known as msconfig, is a utility used to troubleshoot issues with a windows system. It includes service information, just like task manager, but also includes information on system boot and other useful information.

### Opening msconfig

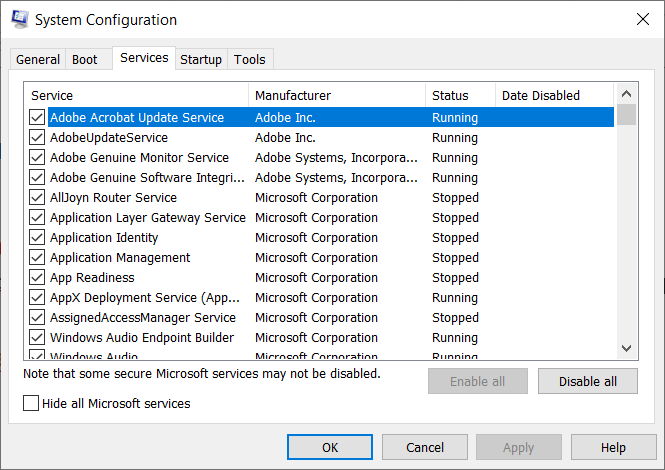
1. In the Windows task bar search field, type **msconfig** and press **Enter**. You should see the Systems Configuration utility as shown in Figure L06-15.



**Figure L06-15** Windows System Configuration Utility (msconfig)

### Reviewing Windows Services

1. Click on the **Services** tab. This tab shows much of the same information shown in Task Manager and Services MMC, as shown in Figure L06-16. From this tab, you can directly enable or disable (start or stop) multiple services at once, by unchecking (to stop) or checking (to start) the services and clicking the Apply button. Since these can have an unwanted impact on the function of your system, it is not recommended unless you know a service to be malicious.

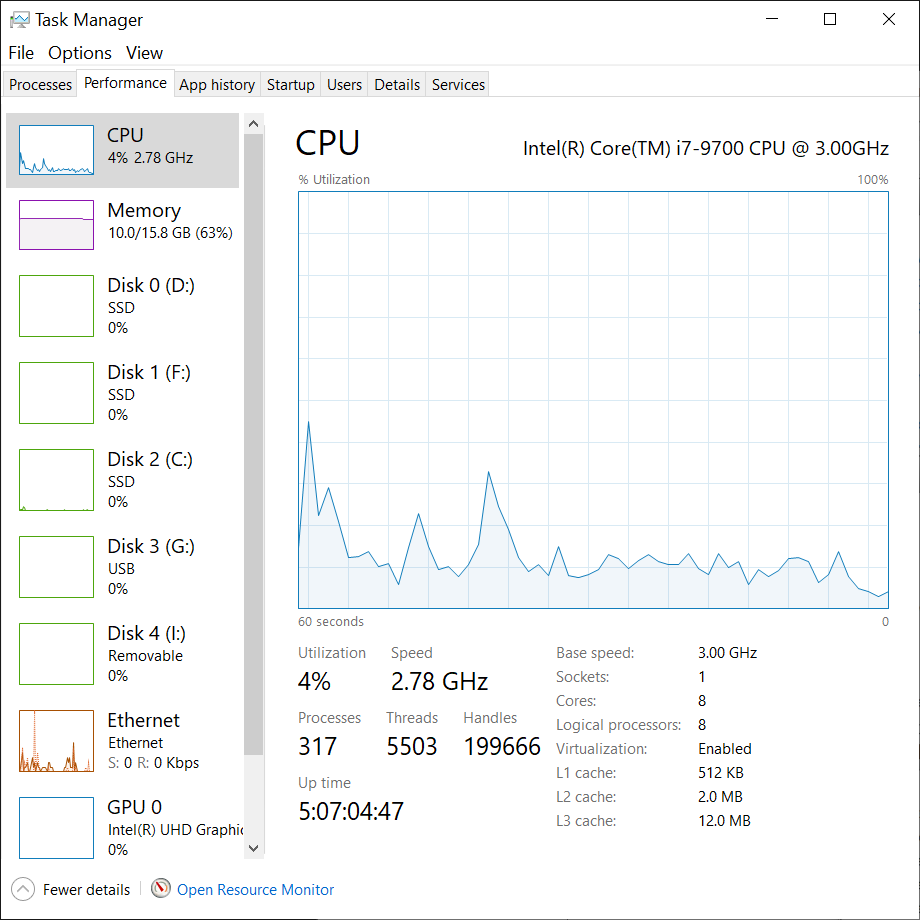


## Service Assessment with Performance and Resource Monitor

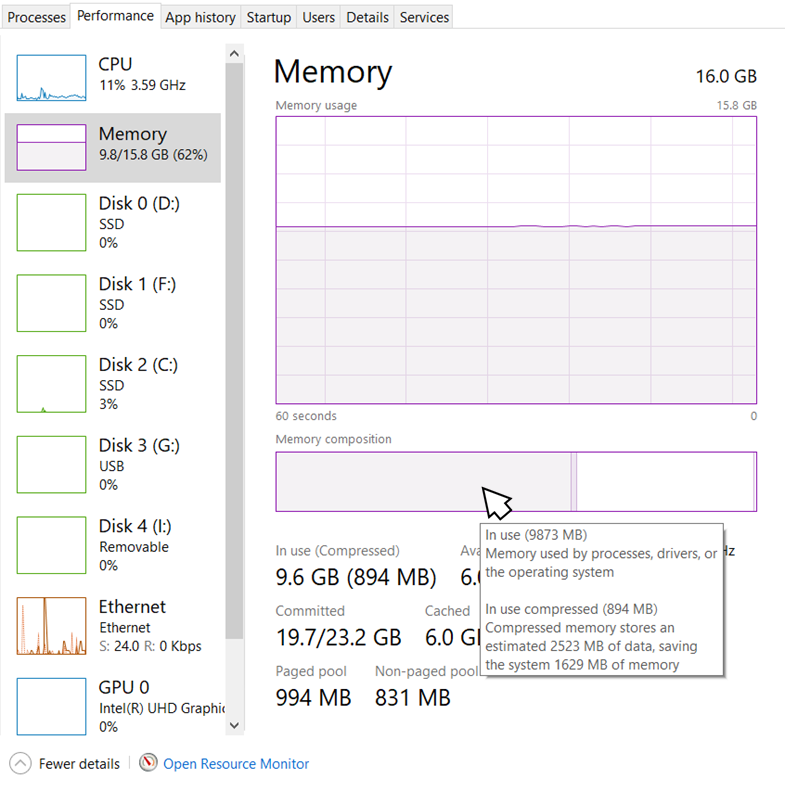
The last utilities we’ll look at are the Windows Task Manager Performance tab and the Windows Resource Monitor.

### Using the Performance Tab

1. Open your Windows Task Manager as described in a previous lab assignment. Select the **Performance** tab. Here you will see an overview of how your system is using its resources like the Central Processing Unit (CPU), Memory, Drives and Internet connection, as well as Graphical Processing Unit (GPU), as shown in Figure L06-16. You can select the different categories on the left side of the utility to review each. You can also hover your mouse over parts of the screen to see additional information (See Figure L06-17). However, this still doesn’t provide a lot of detail. For that we’ll need the Resource Monitor.



**Figure L06-16** Windows Task Manager Performance Tab

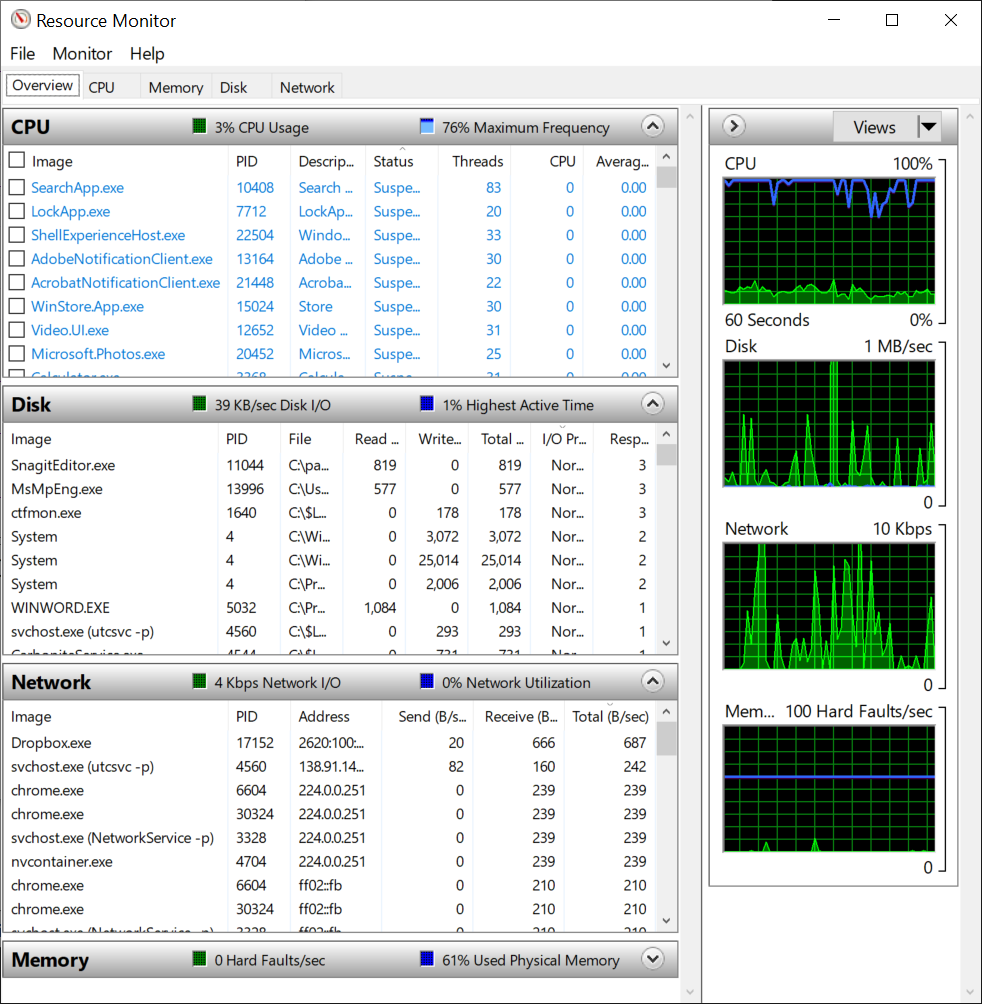


**Figure L06-17** Task Manager Performance Tab additional information

### Opening Resource Monitor

1. There are several ways to open the Resource monitor:
   1. Select the **Open Resource Monitor** link at the bottom of the Task Manager Performance tab, as shown in Figure L06-16 and -17 above.
   2. Type **Resource Monitor** in the Windows task bar search field and then click on the app.
   3. Click the Windows **Start** button, then, select **All Apps**, then **Windows Administrative Tools**, then **Resource Monitor**.
   4. Open the msconfig utility as described previously, and select **Resource Monitor** from the *Tools* tab.

Resource Monitor will open, as illustrated in Figure L06-18.



**Figure L06-18** Windows Resource Monitor

### Using Resource Monitor

1. As you can see in Figure L06-18 above, Resource Monitor provides a lot more detail than the Task Manager Performance tab does. The processes and services that are running are shown in the CPU window at the top. Each can be right clicked to reveal a sub-menu, allowing stopping, and **Searching Online** for more information. Select a few entries and use the *Search Online* feature to examine in more detail.
2. Below the CPU window are entries for Disk (drive), Network, and Memory. If one of these categories doesn’t have anything below it, click on the down arrow button. That should “unhide” the entries for that category. On the right side of the Resource Monitor are several graphical representations of systems use. Some power users like to keep this running on their desktop, just to see what applications are demanding the most systems resources. High resource use could be an indicator of something unwanted, especially if you’re not actively engaging in a program that you would expect to have this impact, like watching a streaming video, playing an online computer game, or opening 62 Google Chrome tabs. Applications that are sending and receiving data, when you’re not active online, can also indicate the presence of applications that might be stealing your information, or they could just be your backup program, Dropbox or Microsoft OneDrive updating synchronized records. It’s important for you to get familiar with what SHOULD occur in the normal course of using your system, to make it easier for you to detect what SHOULD NOT occur.

# Self-Reflection and Response

What is the difference between a process and a service in the Windows operating system?

|  |
| --- |
| Processes are controlled by the user and normally run in conjunction with an application or program that a user has started. Services, on the other hand, are started by the OS and run in the background to help the system run correctly. |

Can you think of why you would need to be able to determine which processes are running on your Windows computer?

|  |
| --- |
| A good reason to see what processes are running on your system is to make certain there are no rogue programs running on your system. Another instance where a user may be interested in knowing what processes are running is to determine the amount of system resources that are in use. |

Can you think of why you would need to be able to determine which services are running on your Windows computer?

|  |
| --- |
| Determining which services are running on the system is a way to determine if there are any instances of malware or suspicious background items running. |

## Instructor’s Response

|  |
| --- |
|  |