# Objectives

* + You will use the most common features of **Task Manager** and the related PowerShell commands to gather resource information about running applications and services.

## Skills Reviewed

* + Starting applications.
  + Opening multiple tabs on a browser.
  + Use PowerShell pipeline.
  + Use **Sort-Object** cmdlet

## New Skills

* + End task with Task Manager.
  + End process with Task Manager.
  + Modify the view in Task Manager.
  + Use Task Manager to identify that a bottleneck exists.
  + User **Get-Service**, **Get-Process**, **Stop-Process**, **Measure-Object** cmdlets.

# Initial Conditions

Your virtual machine should be in this state prior to beginning this guided practice:

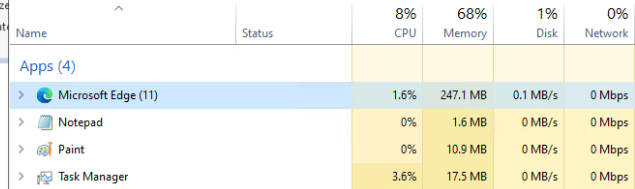
* + Guided practice **Installing Windows 10** and **User Accounts** are complete.

# Final Conditions

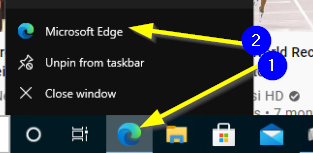
No configuration changes made to system.

# Instructions

1. Log on to **CLIENT1** as **Ann Fellows**.
2. Open applications for use in evaluating performance issues.
   * 1. Open **Microsoft Edge** and open tabs for the following web sites:
     2. <http://www.facebook.com>
     3. <https://www.google.com>
     4. <http://grvl.ecpi.net>
     5. <https://youtube.com>
     6. Open **Notepad.**
     7. Open **Microsoft Paint.**
3. View the running applications with **Task Manager.** Open **Task Manager** by right-clicking taskbar and selecting **Task Manager**.
   * 1. **Task Manager** opens.
     2. On the **Processes** tab, click **View** and verify that **Group by** **type** is checked.
     3. Note that the processes are group into three sections: **Apps**, **Background processes** and **Windows Processes**.
     4. Capture a snippet of the data on the **Processes** tab in **Task Manager** that shows the processes in the **Apps** groups. The snippet should contain **CPU**, **memory**, **Disk** and **Network** columns and should be like the image below. Save the image as **TaskManager\_*studentID*.png** (where ***studentID*** is your assigned studentID).



* + 1. Note that **Microsoft Edge** has anumber in parenthesis (11). This is now many processes are running for **Microsoft Edge**. You have 4 web sites open, why are there more than 4 processes?
    2. On the **Taskbar**, right click **Microsoft Edge** and select **Microsoft Edge**. A new window opens for **Microsoft Edge**. Did additional **Microsoft Edge** processes appear in **Task Manager**?



* + 1. On the **Taskbar**, right click **Microsoft Edge** and select **New InPrivate Window.** A new window opens for **Microsoft Edge**. Did additional **Microsoft Edge** processes start in **Task Manager**? Explain the difference between opening a new session and opening **InPrivate Window**.

1. Viewing processes with **PowerShell**.
   * 1. Open PowerShell.
     2. Use the **Get-Process** cmdlet to view the running processes.
     3. Compare the output to the list of processes in **Task Manager**. Is the list the same? Shift to the **Details** tab in **Task Manager** and compare the list to the output of the **Get-Process** cmdlet.
     4. How many processes are running? Execute the **Get-Process | Measure-Object –Line** command in PowerShell. This counts the number of objects passed through the pipeline.

> get-process | Measure-Object -Line

Shows 64 lines

1. Stop a non-responding application with **Task Manager.**
   * 1. In **Task Manager**, on the **Processes** tab, right click the **Paint** application and select **End Task**. What happens in **Task Manager**? What happened to **Paint** application?
2. Stop a non-responding application with **PowerShell.**
   * 1. Issue the **Get-Process n\*** command to list running processes that start with the letter **n**. The **Id** column lists the **Process ID** (PID).

> Get-Process n*

ID column in output is highlighed

* + 1. Use the **Stop-Process <id>** command to stop the **notepad** process (**<id>** is PID). The PID on your system may be different from the PID in the images.

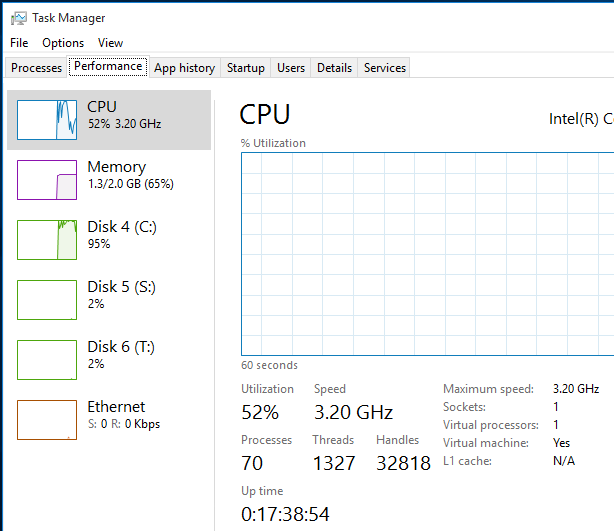
> stop-process 5960

* + 1. Shift to **Task Manager**, is the **Notepad** app still running?
    2. Open **Notepad**.
    3. Issue the **Stop-Process –Name notepad** command. What happens?

1. In **Task Manager**, if the application will not stop when you click the **End Task** button then you can kill the process using **End Task**.
   * 1. On the **Process** tab, right click on **Microsoft Edge** application, and select **Go To details**.
     2. This will take you to the **Details** tab with the associated **Microsoft Edge** process highlighted.
     3. To stop the **Microsoft Edge** process, click the **End Task** button.
     4. You will receive a message indicating that you may lose information, click the **End Process** button.
2. Modifying the **Process** tab view in **Task Manager**.
   * 1. Right-click any column name and select the additional items:
        1. **PID** - Process ID - can be used to kill (stop) a process.
        2. **Command Line** - can see additional options used when starting the command and used to see where the executable is located. Viruses often use the same name as system commands but run from odd locations.
     2. To determine which processes are using the most resources you can click the column headings to sort in ascending or descending order.
3. Viewing the status of a service using **Task Manager.**
   * 1. In **Task Manager**, select the **Services** tab.
     2. Click the column header to sort the services by **Name** and then view the status column to see if the service is running or stopped.
     3. To perform additional configuration of a service, click the **Open** **Services** link at the bottom of the window to open the **Service** console.
4. Viewing the status of a service using PowerShell.
   * 1. Issue the **Get-Service** command. The output shows all services registered with the system.
     2. Use the **Sort-Object** cmdlet to sort the output of the **Get-Service** cmdlet
        1. **Get-Service | Sort-Object Name**
        2. **Get-Service | Sort-Object Status**
        3. **Get-Service | Sort-Object Status, Name** (sort by Status, then by Name)
5. Viewing system performance using **Task Manager**.
   * 1. In **Task Manager**, select the **Performance** tab.
     2. You will see **CPU**, **Memory**, **Disk**(s) and **Network** graphs. The number of each item depends on the specific hardware (or virtual hardware) in your system.
        1. On the **Processes** tab, you may see **Disk** at 33%. This does not indicate an issue. When you switch to the **Performance** tab, you see **Disk 0** at 100%, **Disk 1** and 0% and **Disk 2** at 0%, you have then identified an issue, **Disk 0** is being over utilized while **Disk 1** and **Disk 2** are being underutilized.

# Document Work

1. With Task Manager open to the Performance tab, take a snippet, and save as **TaskPerform\_studentID.png** (where ***studentID*** is your assigned studentID). The snippet should contain the small graphs for CPU, Memory, Disk and Ethernet and show the utilization, speed and maximum speed of the CPU and the uptime of the system. The snippet should be like the image below.



Event viewer

# Objectives

* + You will use Event Viewer to extract information from Windows 10.

## Skills Reviewed

* + Use Computer Management.
  + Restarting services.
  + Use pipeline in PowerShell.
  + Use **Select-Object**, **Where-Object**, and **Format-List** cmdlets

## New Skills

* + Filtering event logs.
  + Extracting data from event logs.
  + Use **Get-EventLog** cmdlet.
  + Add a Task to an Event.

# Initial Conditions

Your virtual machine should be in this state prior to beginning this guided practice:

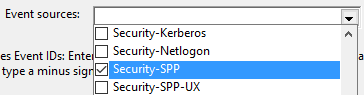
* + Windows 10 client activated through KMS server.

# Final Conditions

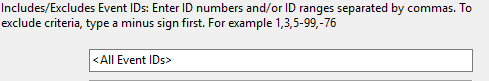
No configuration changes are made.

# Instructions

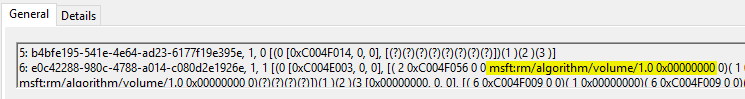
1. Log onto **CLIENT2** with your administrative account.
2. Open **Computer Management**. Expand **System Tools > Event Viewer > Windows Logs** and click on **Application**. The **Application** log opens.
3. Use filtering to modify the list of possible events.
   * 1. In the **Action** pane, click **Filter Current log…Filter Current Log** dialog opens. In **Event sources:** dropdown scroll down and select **Security-SPP** (SPP is Software Protection Service) and then click **OK**.

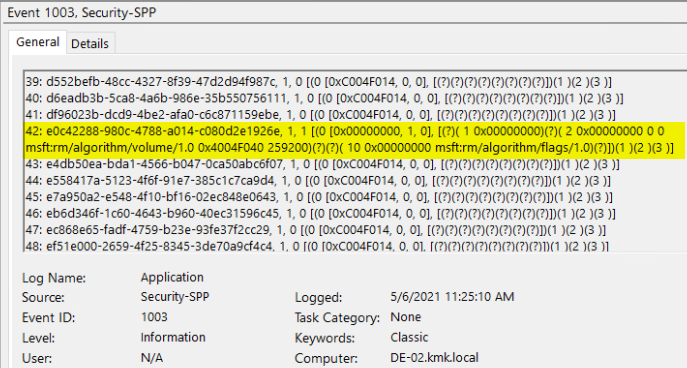


* + 1. Note the **Source** column has only **Security-SPP**. In the **Action** pane, click **Filter Current log…**
    2. **Filter Current Log** dialog opens. Note that the previous selection for **Event Sources:** remains. In the **<All Event IDs>** text box, enter **1003,** and click **OK**.



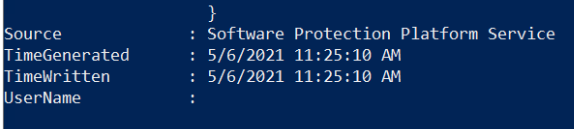
* + 1. Note that all columns now display the same information. You will now need to look in the **General** to find the specific data you are seeking. Scroll to the earliest event in the filtered list and click on the event. See image below. **msft:rm/algorithm/volume/1.0 0x00000000** is highlighted. This event is from a time when the system was not activated.



1. Scroll to the latest event in the log and double-click on the event. Note that the **General** section display size is larger. Identify the row that **msft:rm/algorithm/volume/1.0** is located. You are tasked with finding when the system was activated, this equates to the first entry that has **msft:rm/algorithm/volume/1.0 0x4004F040**. You might need to search through many, many records to find the one ou are looking for. In this case, its best to find the record with PowerShell and then verify the data in the Event Log. Do not close the **Event Vewier**, you will need to return
2. Use **PowerShell** to find the first entry that has **msft:rm/algorithm/volume/1.0 0x4004F040**. Open **PowerShell** with administrative rights and issue the command:

Get-EventLog Application | Where-Object {$\_.Message -Like '\*msft:rm/algorithm/volume/1.0 0x4004F040\*'} | Select-Object -Last 1 | Format-List

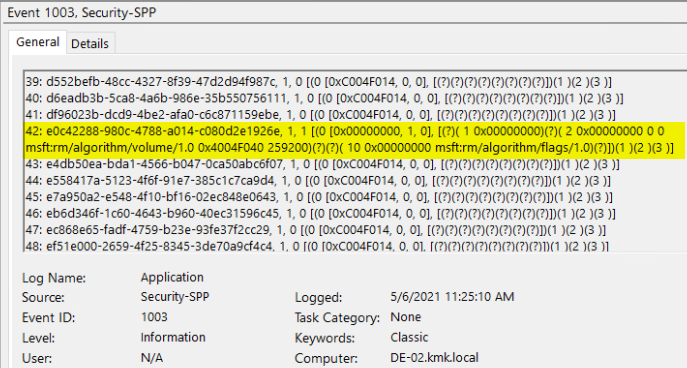
Note that the time extracted by **PowerShell**.

****

1. Return to the Event Viewer. the scroll arrows on the right side of the **Event Properties** dialog box to scroll to event with the exact date/time as noted in the PowerShell command. Note the time of the first event. They time will be the same.

# Document work

1. Capture a snippet showing the activation time for the earliest entry in the event log for **msft:rm/algorithm/volume/1.0 0x4004F040**. The snippet should be like the image below showing the logged date/time and activation **msft:rm/algorithm/volume/1.0 0x4004F040**. Save the snippet as **CIS245\_EventViewer*\_studentID*.png** (where ***studentID*** is your studentID).



Resource monitor

# Objectives

* + Use graphical and command line tools to gather resource usage information about running application and services.

## Skills Reviewed

* + Using IE and opening multiple tabs

## New Skills

* + Open **Resource Monitor** using **resmon** command
  + Filter processes on Resource Monitor
  + View how individual processes affect CPU, Memory, Disk and Network resources
  + Identify the ports open on a system.

# Initial Conditions

Your virtual machine should be in this state prior to beginning this guided practice:

* + Windows 10 client installed.

# Final Conditions

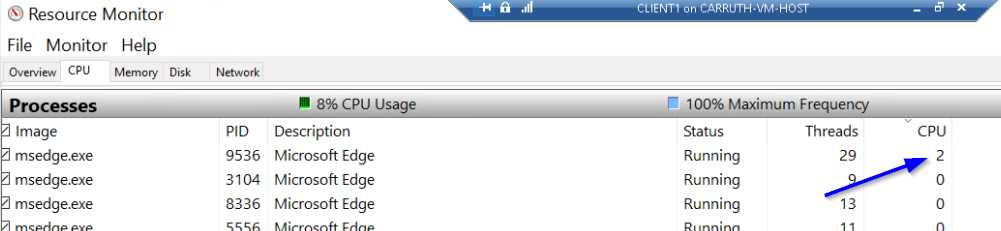
No changes made to system.

# Instructions

1. Login to **CLIENT1** using your administrative account.
2. Start **Edge** and browse to <https://sourceforge.net>.
3. Open **Resource Monitor** by executing **resmon** in **Run** dialog box.
4. **Resource Monitor** opens. You should see tabs for **CPU**, **Memory**, **Disk** and **Network** across the top and graphical representation down the right side.

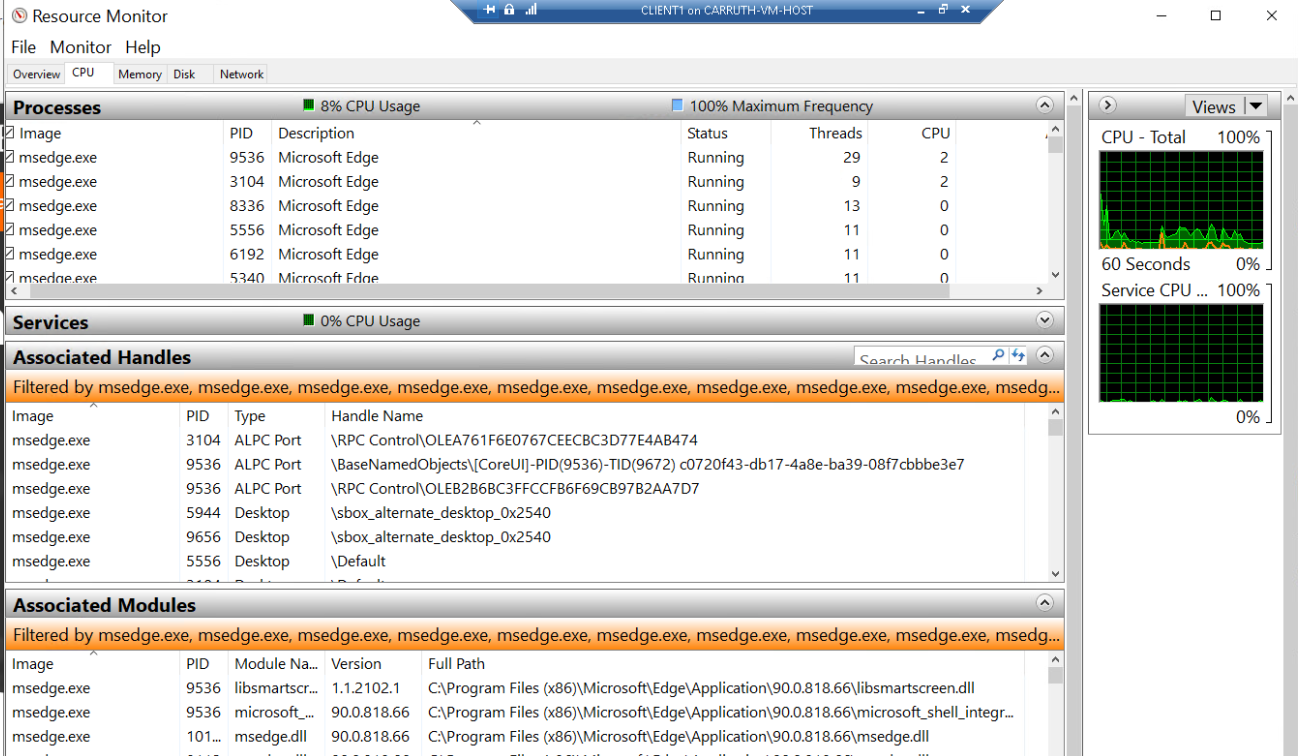
shows Overview, CPU, Memory, Dislk and Network tabs

1. Monitoring CPU Usage
   * 1. Click the **CPU** tab
     2. Expand all the sections.
     3. This view breaks out the CPU usage by applications and services.
        1. In the **Processes** section, all the running processes are listed, but none are checked.
        2. In the **Services** section, system services are listed showing the CPU usage by each.
        3. The **Associated Handles** section shows files, registry keys, kernel objects, and other resources that the selected application is accessing.
        4. The **Associated Modules** section shows the DLLs (libraries) or other programs that the selected process is using.
        5. Note the message in **Associated Handles** and **Associated Modules** sections, “Select a process”. Nothing appears in this section unless action is taken by the user.
     4. To identify the applications using the most memory, click on the **CPU** column to sort by CPU usage as shown below.



* + 1. Note the down arrow in the **CPU** column; this shows that the column is sorted in descending order by CPU usage.

1. Viewing Handles and Modules being accessed by **Edge**.
   * 1. Click the **Image** column header to sort the processes by **Image** name in ascending order (a-z)
     2. There should be several Microsoft **Edge** processes shown (**msedge.exe**). Select them all. Your screen should look similar to the one shown below.



* + 1. You can now see information displayed in the **Associated Handles** and **Associated Modules** section of **Resource Monitor.** Also note that no services are listed in the **Service** section.
    2. Click the **Memory**, **Disk** and **Network** tabs. Do you see **msedge.exe** selected in each? If not, refresh **Edge** and then click on each tab.

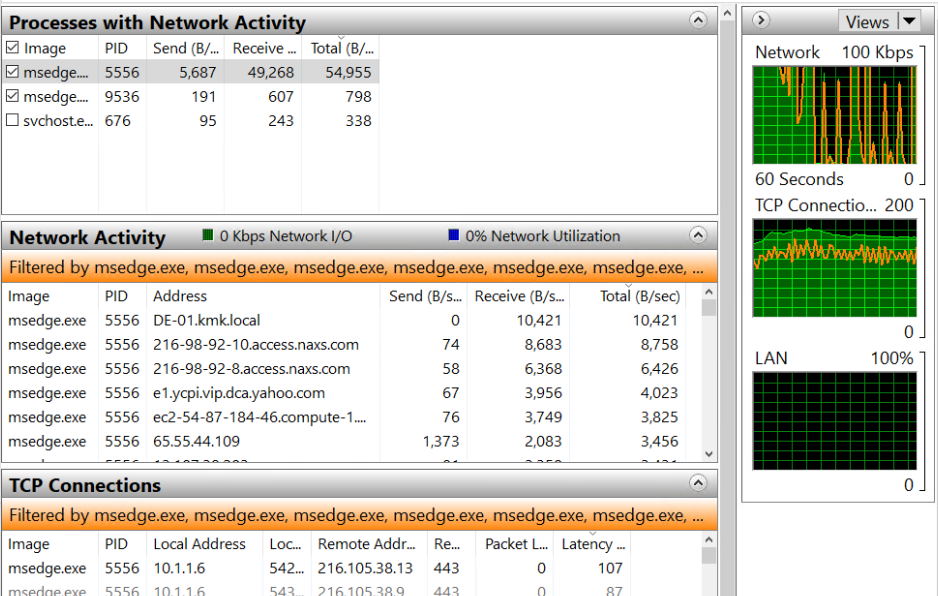
1. Monitoring Memory Usage
   * 1. Click on the **Memory** tab
     2. Record the amount of memory:
        1. In Use
        2. Modified
        3. Standby
        4. Free
     3. In **Edge**, open additional tabs <http://ecpi.edu> . What happened to the memory usage?
     4. Record the amount of memory:
        1. In Use
        2. Modified
        3. Standby
        4. Free
     5. How and why did the values change?
2. Monitoring Disk usage
   * 1. Select the **Disk** tab.
     2. This view will display all the processes that are accessing the disk.
     3. Open additional tabs and browse to **google.com** and **msn.com.**
     4. Select **msedge.exe** in the **Process** **with** **Disk Activity** section
     5. Notice that in the **Disk Activity** window you can see the actual files that are being accessed.
     6. The storage section shows the logical disks on the system and various information about these. In this section, the disk queue length shows the number of applications that are waiting to access the disk. If this number remains high, is a good indicator that you may need additional disk drives or perhaps should move the paging file to another drive.
3. Monitoring Network Usage and Activity

When you are having issues with your network, it is helpful to be able to see the programs that are accessing the network and how much traffic each is generating. You may be at home and wonder how much bandwidth Netflix is taking or be at work and wonder how much bandwidth the roaming profiles are using. The Network tab of the Resource Monitor can be used for these tasks.

* + 1. Select the **Network** tab.
    2. This view will display all the processes that are accessing the Network.
    3. Expand all the sections.
       1. The **Processes with Network Activity** section displays the processes that are making connections to other devices or are allowing incoming connections.
       2. The **Network Activity** section shows how much traffic is being sent and received and between which programs and remote locations.
       3. The **TCP Connections** shows the TCP connections between the computer and remote computers. It displays the local (source) and remote (destination) ports in use. It also shows the Packet Loss and Latency which can be used to troubleshoot network issues that are causing packets to be dropped (Packet Loss) or delayed (Latency).
       4. The **Listening Ports** section shows the ports on which your computer is listening. These normally indicate a service that you are providing.

# Document Work

1. With the Resource monitor open with the tabs still open, capture a snippet of the Resource Monitor showing the Network tab with Network Activity and three graphs. You may need to make the Windows size smaller. The PID for each process should be readable in the snippet. Save the snippet as **ResMon\_*studentID*.png** where (***studentID*** is your assigned studentID). The image should be like the one below.



# Questons you should be able to answer

1. What happens to available memory when multiple browser tabs are open? How can this affect the operation of the computer?
2. How can **Resource Monitor** assist in identifying the bottle neck?
   1. Memory
   2. Disk
   3. CPU
   4. Network
3. What approximate values would indicate a bottleneck?
   1. Memory
   2. Disk
   3. CPU
   4. Network

Performance monitor

# Objectives

* + Use Performance Monitor real time performance counters and performance counters from a data collector set.

## Skills Reviewed

* + Use **run** to open tools.

## New Skills

* + View real time counters with Performance Monitor.
  + Add counters to Performance Monitor.
  + Highlight a single counter in Performance Monitor.
  + Run Data Collector Set.
  + Create Data Collector Set.

# Initial Conditions

Your virtual machine should be in this state prior to beginning this guided practice:

* + Windows 10 installed.

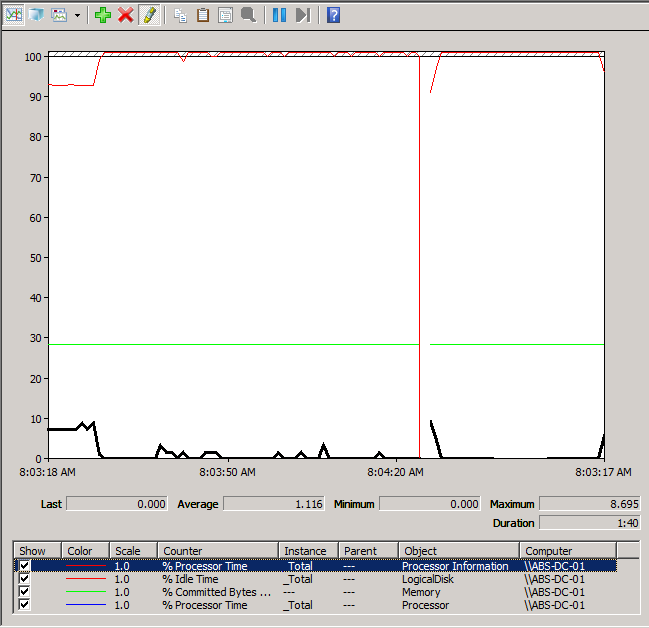
# Final Conditions

At the end of this exercise, you will have:

* + One user defined **Data Collector Set** created, and reports generated.

# Instructions

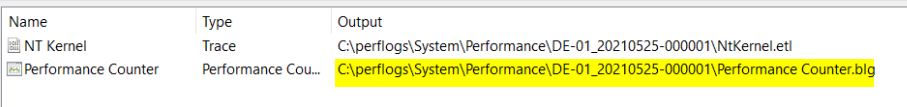
1. Login to **CLIENT1** using your administrative account.
2. Open **Performance Monitor** by executing **perfmon** in Run as Administrator.
3. **Performance Monitor** opens. In **System Summary**, the four potential areas for a bottle neck are identified: **Memory**, **Network**, **Physical Disk**, and **Processor**. Which counters are selected for each item? Note that the values are changing as this is real time data.
4. Viewing Real time performance counter data.
   * 1. Click on **Performance Monitor** in the console tree.
     2. **Performance Monitor** opens. You see a single counter, the **%Processor** Time counter. The counter name and other information are displayed at the bottom.
     3. Add additional counters for disk, memory, processor, and network.
        1. Click on the green **+** symbol on the tool bar in the results pane.
           1. The **Add Counters** dialog box opens. Note that there is an option to display counters from other computers. In this guided practice, we will only choose counters from the local machine.
           2. Check the **Show Description** check box at the bottom of the dialog box.
           3. In the **Available** counters, scroll down to the **Logical Disk** object and expand the object. Notice all the counters are highlighted by default. Choose **% idle time,** in the **Instance of selected object:**  box, select **C:** drive, and then click the **Add** to add the counters. Collapse **Logical Disk** object.
           4. Scroll to the **Memory** object and expand it. Choose the **% Committed Bytes in Use** and click **Add** to add it to the display. Collapse the **Memory** object.
           5. Scroll to the **Processor** object and expand it. Choose the **% Processor Time,** in the **Instance of selected object:**  box, select **\_Total,** and then click **Add** to add the counter to the display.
           6. Click **OK** on the **Add Counters** dialog box to view the real-time data.
        2. The Performance Monitor window should appear like image below.



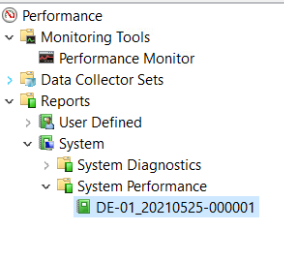
* + - 1. Press **Ctrl+H**. This will allow you to identify a single counter. Click on each of the counters at the bottom of the results pane and observe that counter in real time. Open **Microsoft Edge** and observe counters change.

1. Using data collector sets
   * 1. In **Performance Monitor** tool, in the console tree, expand **Data Collector Sets** > **System**. Right click **System Performance** and select **Start**.
     2. This will start the data collector set. You should now see a green arrow in the **System Performance** data collector set icon and you will now see a file in the output column of the details pane.
     3. The default duration for this data collector set is one minute. Wait until you see the report stop and the icon change. This indicated the data collector set completes its collection.
2. Analyzing a performance report.

In the previous step, you ran a data collector set. When this is done, the operating system will write the results to files located in the **C:\perflogs** directory. The exact location and file name can be seen in the output column of the details view of the data collector set. A separate file is created for the performance counter, event trace, and configuration information. This information is compiled into a report that can be viewed in the **Reports** node in the console tree.



* + 1. In **Performance Monitor**, in the console tree, expand **Reports > System > System Performance**. Click on **System Performance**.
    2. You should see a report with the name of your computer in the title along with the date similar to the one shown below.

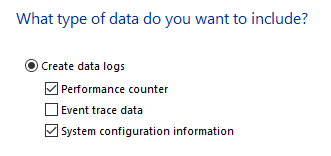


* + 1. Click the report and then look in the details pane.
       1. Notice the information provided in the summary screen. It identifies **CPU** and **Memory** utilization and the processes using the most of each.
       2. Note in the **Resource** view, it gives a green light (icon) for **CPU**, **Network**, and **Disk** indicating that these do not appear to be a problem. The report would show a yellow or red light to indicate a potential problem.
       3. Browse through the remaining parts of the report to view what information is available.

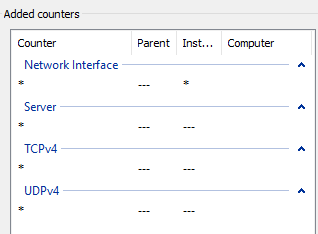
1. Create a custom data collector set.

There may be times when you wish to collect specific types of performance data. You may be troubleshooting a RAID array or a specific program. At these times, you may wish to create a custom data collector set.

* + 1. In **Performance Monitor** > **Data Collector Sets** right click **User Defined** select **New > Data Collector Set**.
       1. The **Create New Data Collector Set** wizard opens. In the **Name:** text box input ***studentID*-Network Diagnostics** (where ***studentID*** is your student ID), select **Create Manually (Advanced)** and then click **Next**.
       2. On the **What type of data do you want to include?** page, select **Create data logs,** and then select **Performance counter** and **System configuration information** and then click **Next**.



* + - 1. On the **Which performance counters would you like to log?** page, add the following objects/counters:
         1. Network Interface/\*
         2. Server/\*
         3. TCPv4/\*
         4. UDPv4/\*

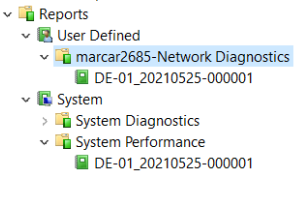


* + - * 1. After all counters are added, click **OK**.
        2. Note the **Sample Interval.**
      1. Click the **Next** button.
      2. On the **Which registry keys would you like to record?** page, click **Next**.
      3. On the **Where would you like the data to be saved?** page, review the path in **Root directory**: text box. What is **%systemdrive%**? Accept the default location and click **Next**.
      4. On the **Create the data collector set?** page, select the **Open properties for this data collector set** and then click **Finish**.
      5. The ***StudentID* - Network Diagnostics Properties** pagewill open. Note that all the configurations that you made in the wizard can be modified here on one tab or another. Some additional configurations are also available. Review the configurations on the **General, Directory**, **Security,** and **Schedule** tabs.
         1. Click the **Stop Condition** tab. Check the **Overall duration:** check box and input **2** in the textbox, in **Units:** select **minutes**, and then click **OK**.

1. Run the ***StudentID* - Network Diagnostics Data Collector Set.**
   * 1. How long will the data collect set run after starting?
     2. How many data points will the data set have? (**Hint**: Internal 15 seconds)

# Document work

1. After the data collect set stops, take a snippet showing the reports for the **User Defined** and **System performance**. Save the snippet as **DataCollectorReports*\_studentID*.png** (where ***studentID*** is your studentID).



1. Take a snippet showing report created when the ***StudentID* - Network Diagnostics Data Collector Set** was ran. At least the bottom 20% of the graph and all data points visible on the tool should be shown in the snippet. Save the snippet as **UserDefinedReport\_studentID.png** (where ***studentID*** is your studentID).

