Laboratory 1 - Windows 10 Administration

In this laboratory exercise you will review a number of essential methods for managing and controlling your computer running the Windows 10 operating system. We will be using some of these methods in other laboratory projects in this course.

Introduction - Windows 10 is the latest version of Microsoft operating systems for desktop and laptop computers. Operating systems provide the user with efficient ways load and store data on the hard drive and to run application programs. The computer programmer must be familiar with the host operating system in order to properly design and debug software. There are a number of third-party (i.e. not created or maintained by Microsoft) software tools to support the proper management of computers running Windows 10. As part of this lab we will become familiar with a few of these tools.

Open the Control Panel and select System (this is most easily done if the control panel is in the *small icons* display mode), and answer the following questions: [Note: the answers will depend on the particular computer you are running].

1. What service pack are you running? ____

2. Provide the following information about your computer:

Manufacturer: ____________________ Rating: ____________________

Model: ____________________ Processor: ________________

RAM: ____________________ System Type: ______________

Computer Name: __________________ Prod. ID: __________________

3. Clicking on Windows Experience index gives more details about the performance rating for your computer. Give the rating values for the following:

Processor: ___________________ Memory(RAM): ______________

Graphics: ___________________ Gaming graphics: ____________

Primary HD: ___________________

Open the Control Panel and select Folder Options, select the View tab. Uncheck the Hide Extensions for Know File Types option (if it is checked), and then click OK.

4. Verify that file extensions are now visible. YES NO

Accessing Command-Line Tools - Many of the tools provided in Microsoft's disk operating system (DOS) are still available and useful for systems administration. To open a console window click on the start icon, type cmd into the Search Programs and Files textbox and select cmd.exe (which appears at the top of the search list under the heading Programs ( ).

From within the console window type the word help and press enter. This will give you a list of some of the DOS commands with a brief description of their use. You can get more information about a particular command by typing its name followed by a space and /?.

Some DOS commands available to you are not in this list however. You can find more complete lists of available DOS commands online at sites such as http://ss64.com/nt/.

5. Use the DOS command ping to determine the average time to access www.google.com from your computer.

ping www.google.com _______ _______ _______ _______ avg time = _______

Another common DOS command for networking is the trace route command. Perform a trace route for www.google.com by entering the following:

```
tracert www.google.com
```

This command will indicate the intermediate nodes through which you are connected to the google server farm. If the number of hops does not exceed 30 (the max permitted by tracert) the last IP listed will be the IP of google.

6. Provide the following information from you google trace route.

How many hops? _____________

Node with largest round-trip times (RTTs) ___________________

IP address of www.google.com ________________

Let's take a closer look at what tracert is telling us. The first line is my address the max # hops and the size of the packets being sent. Each additional line indicates a server system or a router in the path between our system and the destination system. The time shown are the round-trip times (RTTs) to move a data packet between consecutive nodes. It is typical for each packet to be sent three times so we get three RTTs for each step. Asterisks (*) indicate that a particular server/router is not providing the requested information (for example Solaris systems typically show an asterisk instead of the second or third RTT. Timeouts do not necessarily indicated a lost packet since there are three chances (probes) for each packet.

When an IP address is shown without a name it usually means that the DNS lookup failed. If the tracert fails there will be an indication of the problem such as...

!H - host unreachable
!N - network unreachable
!P - protocol unreachable
!S - source route failed (router is blocking source-routed packets)
!F - fragmentation needed (indicates that the router is misconfigured)
!X - the administrator has blocked traceroute at this router

You may see a TTL (time-to-live) warning which means that a reply packet had an unexpected value, which is usually not a concern.

7. There are Web sites that provide a google map position of the approximate geographic location of a computer based on its IP address. Use the IP address of google to locate their servers. On of these geolocator Web is http://www.ip-adress.com/ip_tracer/

Physical address of google.com ____

Choosing a DNS Server - Every website is hosted on a server with a unique IP address. Currently we are using IPv4 protocol which is a set of four bytes (each byte has a range of 0-255). Although we can access a Web site directly using the IP address of the server. For example google.com has IP address 209.85.153.104. We can reach google by entering the IP address into a browser's location bar but more commonly we use the URL (unified resource locator) which is easier to remember. The URL is sent to a DNS (domain name service) server where the associated IP is looked up similar to a phone number on a phone book. The default setting for Microsoft is to let Windows 7 and 10 automatically choose the DNS server, but this choice can result in slower Internet response.

Open the control panel and select *Network and Sharing Center*, click on *Change Adapter Setting*s, right-click the icon for your Internet connection and press the *Properties* button.

On the Networking tab highlight the line for Internet Protocol Version 4 (TCP/IPv4) and click Properties. Choose Use the following DNS server addresses: and enter the following IP addresses for OpenDNS. Click OK and close the Sharing Center.

OpenDNS preferred IP:	208.67.222.222
OpenDNS alternate IP:	208.67.220.220

8. Ping www.google.com again and compare the new results with those in question 5.

ping www.google.com _______ _______ _______ _______ avg time = _______

Organization of the Registry - The Registry is organized into five major sections called hives. Each hive is stored in its own system file on the hard drive.

HKEY_CLASSES_ROOT. Contains information about registered applications, including file associations and OLE object classes. (This hive displays the same settings as the HKEY_LOCAL_MACHINE\ Software\Classes key.)

HKEY_CURRENT_USER. This hive is a subset of the HKEY_USERS hive, pertaining to the current user of the PC. It contains all attributes for the desktop environment and network connections.

HKEY_LOCAL_MACHINE. Contains most of the settings for your PC’s hardware, system software, and individual applications.

HKEY_USERS. Contains subkeys corresponding to the HKEY_CURRENT_USER hives for all users of the PC, not just the current user.

HKEY_CURRENT_CONFIG. Contains information gathered when Windows first launches, such as settings pertaining to your PC’s display and printers. The data stored in this hive is not permanently stored on disk, but rather is regenerated each time your PC boots.

Editing the Registry - We can edit the registry using the apply named editing tool regedit.exe. To run regedit, click the Start button and type regedit into the Search Programs and files textbox, then click on regedit.exe when it appears at the top of the search window.

CAUTION: Editing the registry incorrectly may not be easy to fix. The values are changed as soon as they are entered and there is no undo button. THERE BE DRAGONS.

To become familiar with the process of editing the registry we can do a few relatively simple (and fairly safe) things to improve our computer's performance. These are not a required part of this laboratory exercise.

Speeding Up Window's Menus - This edit removes the delay that is normally present between clicking a menu and Windows displaying the contents of that menu.

1. Open the Registry Editor

2. Navigate to the HKEY_CURRENT_USER\Control Panel\Desktop key (for the key value do not attempt to expand the folder, rather click on its name to reveal is value set in the right pane.

3. Right-click the MenuShowDelay item and select Modify.

4. Change the current value (probably 400) to 100. (Notice: setting this parameter to a value that is too close to zero (0) can cause erratic behavior).

5. Click OK.

Disabling Low Disk Checking - Windows frequently checks the amount of free hard drive space if available. While is a good idea to know when you are about to run out of space, its not very efficient to have the OS continuously taking up CPU time checking the drive. In any event you probably are aware of the amount of free space and will know when your drive is getting full. You can disable the low disk checking by adding a new registry value as shown here:

1. Open the Registry Editor

2. Navigate to the HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Policies key.

3. Right-click in the right-hand pane and select New, Key. Name this new key Explorer, and then select it.

4. Right-click in the right-hand pane and select New, DWORD (32-bit) Value.

5. Name the new DWORD NoLow DiskSpaceChecks.

6. Right-click the new LoLowDiskSpaceChecks item and select Modify.

7. In the Edit DWORD dialog box, change the value to 1.

8. Click OK.

Moving the Windows Kernel Into Memory - Another way to speed up Windows is to move the OS kernel into RAM using the following registry edit:

1. Open the Registry Editor.

2. Navigate to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ Session Manager\Memory Management key.

3. Right-click the DisablePagingExecutive item and select Modify.

4. In the Edit DWORD dialog box, change the value to 1.

5. Click OK. (You must reboot for changes to take effect)

Using Remote Desktop - This Windows 10 tool allows you to take control of a remote computer using your computer's keyboard, monitor, and mouse.

On the machine being accessed remotely...Select *Start* - *Control Panel* - *System and Security* - *System*. Click *Remote Settings* in the left pane. On the *Remote* tab of *System Properties*, choose *Allow Connections From Computers running Any Version Of Remote Desktop*.

On the making the connection...Start - All Programs - Accessories - Remote Desktop Connection. Enter the Username and Password you would use to access the remote computer.

Verify that you can control the remote machine from within a window on your computer, as you answer the following questions.

9. Can you run applications on the remote machine? YES NO

10. Describe the performance of a computationally intensive application. _______________

____

11. Describe the performance of a graphically intensive application ____________________

____

12. Can you transfer a file from the remote machine to the local machine? YES NO

Resource Monitor - In Windows 10 the Resource Monitor has its own dialog box which can be accessed in a number of ways. We will find and open the Resource Monitor using *Search Programs and Files* under *Start*. The *Resource Monitor* application is also called *resmon*.

Overview Tab - Provides information about the performance of the four major subsystems CPU, Disk, Network, and Memory.

CPU Tab - Displays the individual processes running on the machine, the process ID's (PID), the status of each running process, the number of threads controlled by the process, and average CPU utilization.

Memory Tab - Shows the process information as displayed on the CPU tab with an overview of memory allocation in the form of a graphical representation. It also shows the number of hard faults (attempts to access memory not in RAM).

Disk Tab - Used to display the disk activity, showing the Processes With Disk Activity, disk Activity, and Storage. Also maintains a graph of disk transfer in KB/sec and disk queue length (the amount of data currently waiting for transfer to RAM for processing).

Network Tab - Provides information about network communications with your computer including all the connections by and to your machine through the LAN and the Internet.

13. How many CPU's are listed by the Resource Monitor of your computer? ___________

14. How much active memory is *in use*___________, *free* __________ on your computer?

15. List the top three Processes with Network Activity __________ ___________ __________

Performance Monitor - Using the *Performance Monitor* (aka *perfmon.exe*) you can create your own real-time counter or collect and record counter data for any OS subsystem. From *Start* find and run *perfmon.exe*.

In the left pane of perfmon, choose the Performance Monitor item and add a new counter using the following procedure.

1. Click the Add button on the toolbar (a green +).

2. Make sure *that Select Counters From The Computer* is displaying <Local Computer>. (Later we will make use of the remote monitoring capability).

3. Select a performance object from the drop-down list. All Windows 7 and 10 system resources are tracked. These include Cache, Memory, Paging file, Process, and Processor.

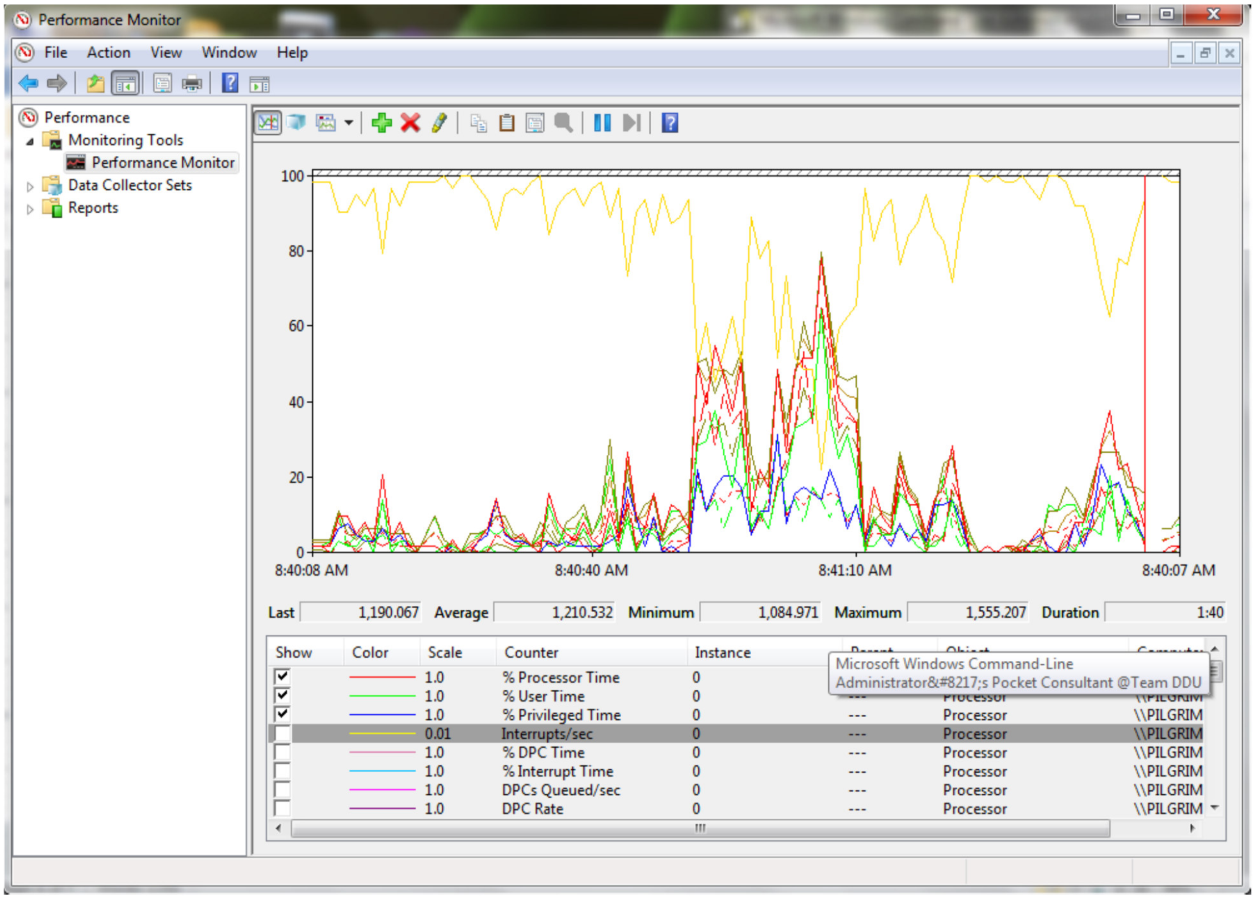
4. Select the counter(s) within the selected performance object you want to track. For now you can add *Processor* to the monitor.

5. Select < All Instances> to track all the associated instances or pick specific instances from the list box.

6. Click the Add button to add the counters for the selected performance object.

7. Repeat 2 through 6 to include any additional counters you would like to track. Then click OK.

After you've added counters, you can select a specific counter by highlighting it in Performance Monitor. To highlight a counter, click it and then click the Highlight button (which looks like a highlighter) on the Performance Monitor toolbar, or select the counter and press Ctrl+H. To stop showing data for a counter, deselect the check box under Show for that counter. To remove a counter, highlight it in Performance Monitor and click the Delete button on the toolbar. The Delete button looks like a red X.



Last 1,190.067 Average 1,210.532 Minimum 1,084.971 Maximum 1,555.207 Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	—	1.0	% Processor Time	0			
☑	—	1.0	% User Time	0	---	Processor	\\PILGRIM
☑	—	1.0	% Privileged Time	0	---	Processor	\\PILGRIM
□	—	0.01	Interrupts/sec	0	---	Processor	\\PILGRIM
□	—	1.0	% DPC Time	0	---	Processor	\\PILGRIM
□	—	1.0	% Interrupt Time	0	---	Processor	\\PILGRIM
□	—	1.0	DPCs Queued/sec	0	---	Processor	\\PILGRIM
□	—	1.0	DPC Rate	0	---	Processor	\\PILGRIM

Microsoft Windows Command-Line Administrator&#8217;s Pocket Consultant @Team DDU

16. Turn off all counters except %Processor Time, %User Time %Privileged Time and %Idle Time for your processor(s) as you answer the following questions.

a. What is the effect on %Processor Time of rapidly scrolling through a document such as a .pdf file?

____

b. If you have more than one processor/core being monitored. How do the %Processor Times compare during the active described in (a)?

____

c. Run a graphics-intensive applications (such as a video) while monitoring your Processor(s) %User Time. Describe the result.

____

d. Run two or more videos and describe the changes you see.

____

____