**SYS140 - Week 12 Lab 1**

**Instructions: (Follow instructions carefully!)**

**Hasan Hashim**

**SYS-140**

**Week 12 Lab 1**

**10/19/2020**

**Leave this document intact and respond under each question.**

## Objective

In this lab you run some of the Windows Sysinternal tools dealing with processes, files and disks. Before running the tools you should read the pertinent sections in the [Windows Sysinternals Administrators Reference Book](http://proquest.safaribooksonline.com.cobalt.champlain.edu/book/operating-systems-and-server-administration/microsoft-windows/9780735662728).

Download and run the tools and answer the questions for each tool. The Download site for SysInternals is <https://docs.microsoft.com/en-us/sysinternals/>.

**Submission items for this lab will be formatted like this.**

Processes

## Process Explorer

Sometimes it is necessary to look at what is happening with processes that are running on Windows. Viewing the CPU processes and determine which ones are using the most memory is a very common task. Some rogue malware may use a lot of CPU but those are the aggressive Fake AV and ransomware. The malware written by professionals may not be so easily detected or use hardly any CPU. Spambots can send dozens of emails in a few seconds without any noticeable performance problems.

There have been times when an svchost.exe process was using 99% of the CPU at startup, but there were about 30 svchost processes running. How do you tell what is really going on? Process Explorer is a great tool to use.

**Preparation:**

Download Process explorer on your Windows 10 VM

Run Process Explorer with administrative rights in your Windows 10 VM. Answer the following questions (1 point each):

1. **Which process (other than System Idle) is using the most CPU? How much is it using?**

AVG Secure Browser it uses 62.1%

1. **Which Process is using the most memory (Private Bytes and Working Set combined)? How much of each?**

AVG Secure Browser is uses 305.7 MB 3.057 bytes

1. **What are “Private Bytes” and “Working Set?” How are those relevant to the question in this assignment?**

Private Bytes are what the app has actually allocated and it includes pagefile usage. Also Private Bytes is the total virtual address space occupied by the all process.

Working sets are the total physical memory used by the process.

It is important to talk about it because they tell us the total virtual address space and the total physical memory that is used by the process.

**\*\*CITE the source(s) where you found the response to the question above.\*\***

<https://stackoverflow.com/questions/1984186/what-is-private-bytes-virtual-bytes-working-set#:~:text=Private%20Bytes%20are%20what%20your,Private%20Bytes%20and%20standby%20list.>

1. **What options does Process Explorer offer that Task Manager does not?**

The Process Explorer offers more features that are not in the Task Manager. Some of them are: it shows us every process with detailed information about it, CPU usage trake, tells us which process has loaded a DLL file, gives you the access to kill or suspend a process from working.

## Autoruns

There are a lot of programs that autostart when you load Windows. Some are required, but others are loaded by the manufacturer that you didn’t even know existed.

Malware, the garden variety kind, will put itself into the startup folder so it can be reactivated on a reboot so this tool is useful for capturing that information..

**Preparation:**

Download Autoruns on your Windows 10 VM

Extract and run the Autoruns file (Autoruns64) and select the Everything Tab.

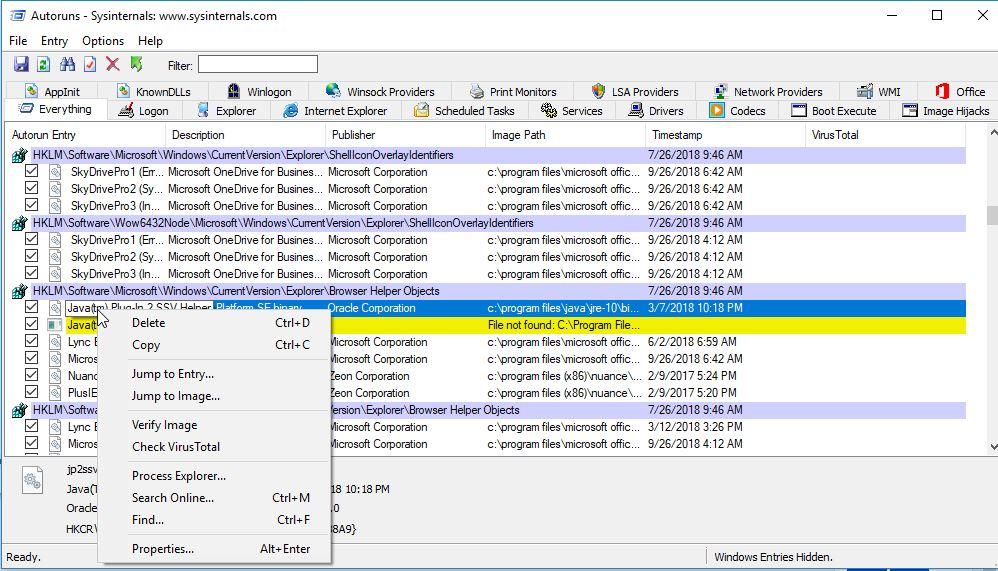
1. Look through the entries.
2. Click the Logon Tab. How many “Auto Entry” results do you see?

9

1. **Look through all of the entries that startup at Logon. Find three to do some research on. What information can you find out about those processes after performing an online search? (3 points)**

**\*\*CITE the source(s) where you found the response to the question above.\*\***

1. Right-click on a startup entry. What options are available to you? What do they mean? In the screenshot below, I did a right-click on the entry “Java” the questions “What do they mean?” is asking what the options in the context menu mean (“Delete”, “Copy”, etc.)



1. **Export the results of autoruns into a CSV file. Upload the CSV file as a separate file along with your submission of this document (1 point).**
2. **Why is it important to save the data to a CSV file? (1 point)**

Because it saved the data as a table so the data will be clear to the reader to understand.

## Disk Utilities

Have you ever found that your hard drive is running out of space and you can’t figure out which directory is using the most data? Du can come to your rescue, but you need to run it from the command prompt.

**Preparation:**

1. Download DU from the sysinternals website
2. Run a command prompt as administrator. Change directory (cd) to where the file has been downloaded. Paste the following line into the command prompt:

du –c “c:\Program Files\\*”

1. **What information does this give you? How useful is this? Only handwritten submissions are required here. (1 point)**

It gives information about how much space I have in the file. It is important because it gives us the power to track the file and the directories.

1. Add a 2 level search by adding “–L 2” to the command line as follows.

1. **Is this more useful? How would you use this tool to track down where your disk is filling up? (1 point)**

This is really useful. I usually make a google search for it and there should be a way to solve the problem. I am really glad that I used this tool to track the problem on the disk.

**SUBMISSION SUMMARY:**

* **Answers to questions #1 through #4 in ‘Processes’**
* **Answer to questions #3 and #6 in ‘Autoruns’**
* **CSV file from question #5 in ‘Autoruns’**
* **Answers to questions #3 and #5 in ‘Disk Utilities’**