**SYS-140 - Week 9 Lab 2**

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

**Hasan Hashim**

**SYS-140**

**Week 9 Lab 8b**

**11/9/2020**

**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 System Internals Administrators Reference](https://learning.oreilly.com/library/view/windows-sysinternals-administrators/9780735662728/).

Download and run the tools and answer the questions for each tool. The Download site for SysInternals is: <https://technet.microsoft.com/en-us/sysinternals/bb545021.aspx>

Preparation:

1. Run the tools within your Windows 10 Virtual Machine

**Networking**

**TCP View**

TCP View allows you to look at the TCP and UDP connections or streams that have been run on your system. It also allows you to look at the process name and ID associated with the connection on your end. The application is different from Wireshark because it shows more low-level information such as which process is using the open socket. That is very, very valuable information. For every open port and process on your computer, you want to know the process that has it open and the path to the process (where the executable exists on the disk).

**Preparation**

Download TCP View from the Sysinternals website

Run TCP-View with administrative rights and answer these questions.

**SUBMISSION (4 points): Find the connection which has sent the most bytes and identify the following:**

* **Process Name: Chrome.exe**
* **Process ID: 16212**
* **Protocol: UDP**
* **Remote Address: \***
* **Remote Port:\***
* **Approximate Bytes Sent: 158011**
* **Approximate Bytes received: 141480**

**Include all of this information in your lab submission.**

**WhoIs**

**Preparation**

Download Whois from the Sysinternals website

WhoIs is a mature Internet program (typically Unix) that uses the DNS to lookup information about a domain name.

Open cmd.exe as an administrator and run *whois champlain.edu.*

**SUBMISSION (3 points): Find the following in your Champlain whois query:**

**Name of Administrative Contact: Chris North**

**Email of Administrative Contact: cnorth@champlain.edu**

**Name of Technical Contact: Wayne Buttles**

**Phone number of Technical Contact: +1.8028602710**

**Primary Name Server: NS.CHAMPLAIN.EDU**

**When the Domain Name expires: 31-Jul-2021**

**Include this information in your lab submission.**

**SUBMISSION (1 point): Run whois google.com. Note whether there is more or less information presented here than in the Champlain whois record. Include this answer in your lab submission.**

**There are more information in the google.com than champlain.edu**