**CSC 547/747 Network Forensics & Investigation Fall 2017**

**Assignment 4**

**Andrew Burden**

1. (10 points) From the Run window, type in regedit.exe and press Enter. In the resulting UI, what is the left pane called and what is the right pane called? Is there a registry key that shows the mounted logical registry keys and their derivative hive files?

**The left is the key pane and the right is the value pane. Yes, they can be found in HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist. The path for the keys are all shown for except for \HARDWARE, it has a dynamic key created at boot that doesn’t have a hive file.**

1. (15 points) During a network investigation, you want to know which commands your suspect may have typed from the Run window. Where can you find this information, and which tool might you use to find it?

**The key for the hive file, NTUSER.DAT, would show this search history at Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU. Registry Viewer is a program that could help in finding it.**

1. (10 points) During a network investigation, you encounter a registry in which there are eight control sets. Which control set do you examine as the current control set?

**The key for the system hive file can be found at HKLM\SYSTEM\Select. The correct key would be found in the value named “Current”.**

1. (15 points) During an investigation you find that it is significant to determine if deleted files passed through the Recycle bin (the default behavior) or if they were deleted immediately without going to the Recycle bin. Which Registry key may tell you this information? (Assumed that your os is Windows 7 and you use ProcMon)

**If you run ProcMon you can go to the recycle bin properties and select the option to “remove files immediately when deleted.” You can see the corresponding value changed in the registry and find the corresponding hive file.**