**Forensics**

**Assignment 15%**

The registry is a database in Windows Operating System that contains important information about system hardware, installed programs and settings, and profiles of each of the user accounts on your computer. Windows continually refers to the information in the registry. Normally users should not need to make manual changes to the registry because programs and applications typically make all the necessary changes automatically. An incorrect change to your computer's registry could render your computer inoperable. However, if a corrupt file appears in the registry, you might be required to make changes. It is strongly recommended that you back up the registry before making any changes and that you only change values in the registry that you understand or have been instructed to change by a source you trust. In this assignment you will be required to perform and document the following tasks in a report no greater than 5 pages:

1. Windows maintains a separate history of all the programs launched on your computer, including details like the number of times they have been run, and the last execution date and time. This information is stored in the Registry (HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist). What useful Forensics information can found in the registry hive above? Include a screen shot of some of the programs in your report. Using tool called CCleaner demonstrate how you can delete records from your registry.

(3 marks)

1. List the devices serial number, friendly names, last write time, volume name, and the volume serial number associated with USB devices that have been used in your computer, this information will be found in your Windows registry.

(3 marks)

1. Demonstrate the Forensics use of Windows jump lists (<http://articles.forensicfocus.com/2012/10/30/forensic-analysis-of-windows-7-jump-lists/>) or Link files (LNK Files).

(3 marks)

1. When an individual connects to a wireless network, the service set identifier (SSID) is logged as a preferred network connection. Locate the registry hive where this information can be found. List all the Wifi networks and mac address of the wireless access points to which have you have been connected. Note: in the interest of your privacy change around this data.

(3 marks)

1. It is possible to hide evidence intentionally in the registry. Using Windows Operating System hide evidence in the registry. Detail how you have done this

(3 marks)

**References**

1. Carvey, Harlan. Windows Forensic Analysis 2E. (Burlington, MA: Syngress, 2009).
2. Carvey, Harlan. Windows Registry Forensics. (Burlington, MA: Syngress,
3. 2011).
4. <http://sentinelchicken.com/data/TheWindowsNTRegistryFileFormat.pdf>
5. Carvey, Harlan. Windows Forensics Analysis 3E. (Waltman, MA: Syngress, 2012).
6. Andy Cobb and Jason Hale, Data Exfiltration and Forensic Analysis in a Microsoft Windows Environment, ISSA Journal, volume 11, issue 11, November 2013, page 18-23
7. http://www.sans.org/reading-room/whitepapers/forensics/wireless-networks-windows-registry-computer-been-33659