**Laboratory Exercise – Windows Registry Forensics Analysis**

Name:

**1. Overview**

This exercise provides hands-on experience applying concepts learned during the Windows registry forensics discussion.

**2. Resources required**

This exercise requires a virtual machine with Regripper software installed. Cyber Range users should use the Introduction to Digital Forensics environment. This virtual environment includes various forensics software, as well as digital artifacts required for this exercise.

The following filesystem image is provided for this exercise and other exercises in this module:

* Win7\_Laptop.tar.gz

**3. Initial Setup**

Log in to your account on the Cyber Range and access the *Introduction to Forensics* exercise environment.

The filesystem image listed above are on the Desktop in the ‘Cases/01\_Filesystems’ folder or in an alternate location specified by your instructor. If you haven’t already done so, open a Terminal and expand the image using the following command:

**$ cd /home/student/Desktop/cases/01\_Filesystems**

**$ tar -xvf ./Win7\_Laptop.tar.gz**

**4. Tasks**

**Windows Registry Forensics**

Examine Windows 7 Registry Hives . . .

**# cd /home/student/Desktop/cases/01\_filesystems/Win7\_Laptop**

1. What service pack level is the Windows 7 computer and when was it installed?
2. List the users and SIDs on the system
3. Are there any programs designated to run at system startup? If so, list them here.
4. Is the system a workstation or a server (hint, see producttype plugin)
5. Have any USB devices been used on the system? List them here.
6. When was the system last shut down?
7. Is the computer set up to listen for Remote Desktop (RDP) connections? If so, what port is it listening on?
8. Which URLs did the user Dug visit using Internet Explorer?
9. Did the user Dug open any .txt files (what are the filenames)?
10. What else can you find out about Dug’s activities on the system?