# **CIT 430 – Forensic Activity #1.3 – Windows Registry Walkthrough**

## **Introduction**

In this activity, you or in a team will determine which registry key contains evidence needed for a forensic investigation. Use the resources on Canvas and/or Google to help complete the questions below.

### **Things to Note:**

· This is a Windows XP system

· The answers to the questions will be found in the HKEY \_LOCAL\_MACHINE

#### **Case Background**

On 09/20/04, a Dell CPi notebook computer, serial # VLQLW, was found abandoned along with a wireless PCMCIA card and an external homemade 802.11b antennae. It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect. It is suspected the device owner gets within range of Wireless Access Points (like Starbucks and other T-Mobile Hotspots) to intercept internet traffic, attempting to get credit card numbers, usernames & passwords.

##### **Investigation Tasks**

As a forensic investigator intern, your boss has tasked you with finding the following information:

Partners: Brithany, Kaleb, Brad

|  |  |
| --- | --- |
| **Time zone the and Greenwich Mean Time (GMT) the device is configured to use** | Timezone -KEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation  GMT  -HKLM/SOFTWARE/Microsoft/Windows NT/Current Version/Time Zones/UTC/Display |
| **The registered owner of the device** | · HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion  · Double click on registered owners  · Double click on registered organization to define the organization information    · |
| **The number of user accounts on the device** | KEY\_LOCAL\_MACHINE\SAM\Domains\Accounts\Names |
| **The last logged on user account** | · HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System  · Select system folder  · Click on DWORD  · Display last login info |
| **The last time the device was shutdown** | HKEY\_LOCAL\_MACHINE\software\nv version\prefetcher\exittime |