Lab 12: User Profiles and the Windows Registry

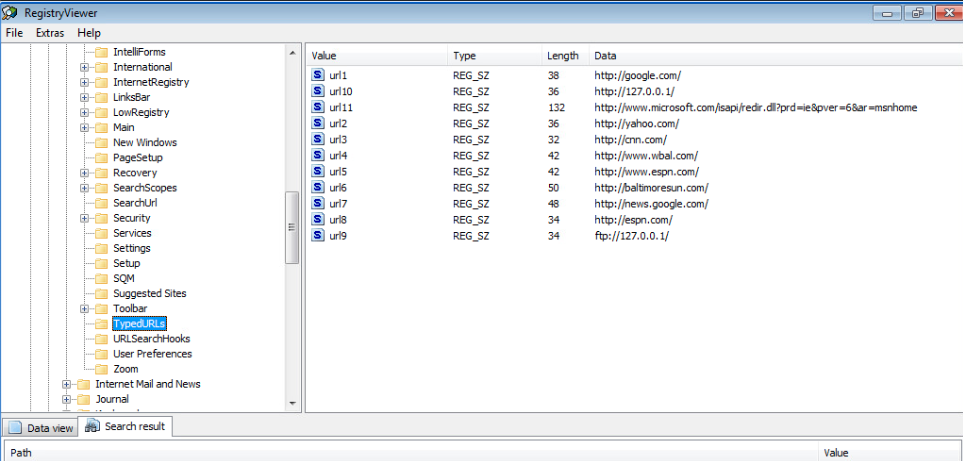
Lab 12 report Name: Kevin Ubilla

This Lab is extra credit for Unit 10. It is worth 15 points. The Challenge Flags are worth 2.5 Extra Credit points.

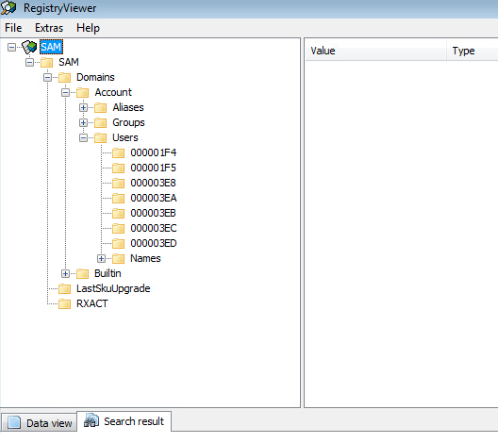
1. **Obtaining a Live Windows Registry, Step 9.**  You are in the process of obtaining the Password and registry files and ready to push the “browse” button and notice that the dialog box is giving you a warning. What is the forensic significance of this warning?

**→** This warning means that the next steps taken might modify the actual system files and not just the duplicated image. As the name implies, it is a live capture of the victim’s computer. **←**

1. **Analyzing the Registry Hives Using RegViewer, Examining a User’s Profile, Step 14.**  You have clicked on “**TypedURLs**” under Internet Explorere in the view of the registry gained by the Registry Viewer. Please capture the list of URLs that results from this and paste it below.

**→ ←**

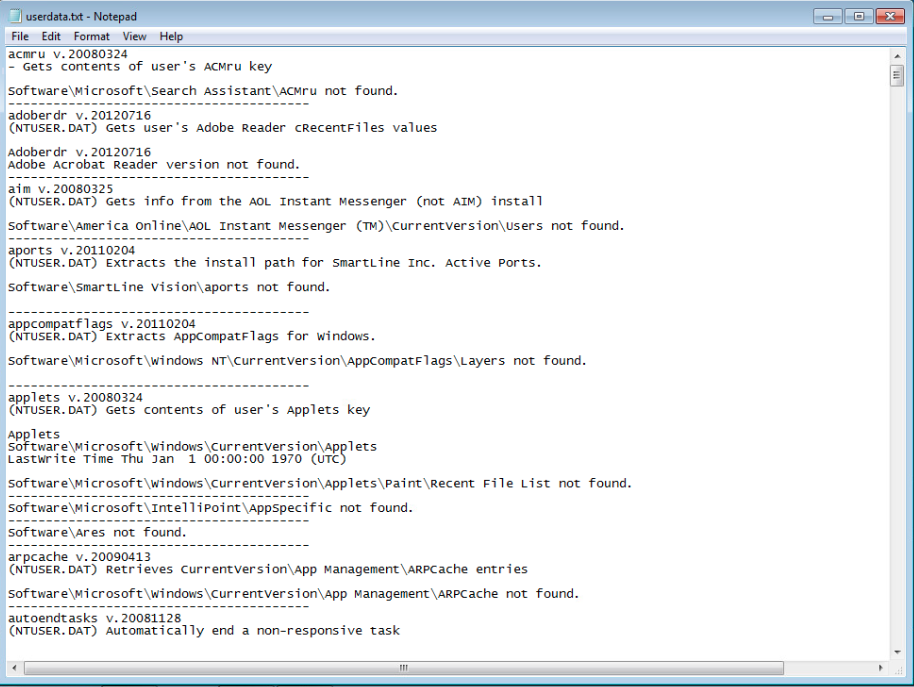
1. **Analyzing the Registry Hives Using RegViewer, Exploring the SAM File, Step 7.** Once you have drilled down to the Names within Users in the SAM file, capture the window that shows the hierarchy of users with their RID values listed (5 layers) and paste it below.

**→  ←**

1. **Analyzing the Registry Hives Using RegViewer, Exploring the System Registry Hive, Step 11.** You have opened a screen by expanding **CurrentControlSet01\Control\Windows** and found a 64 bit Shutdown Time value. How do you make sense of that value? Please type your answer below.

**→ 64 bit values are interpreted as UTC time. It is 1:09:11 UTC ←**

1. **Analyzing the Registry Hives Using RegRipper, Step 9.** You have used RegRipper to generate a report named **userdata.text**. Open it using Notepad, capture the report and display it below.

**→ ←**

**If you encountered any issues, either positive or negative, with this Lab, please let me know by commenting here. (This IS an experiment, after all.) I am tuning this according to what you say.**

**→ ←**