## CIT 430/530

## Lab #2 – Windows Registry Analysis

In this activity you will parse a Windows XP registry for specific information. In a forensic investigation, performing a registry analysis is part of a full investigation and the collecting registry data is “simply part of the story.”

### Resources

[1] Carvey, Harlen. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry. 2011. Burlington, MA. Elsevier, Inc.

## Regedit

Registry Editor is the face of the registry and is the way to view and make changes to the registry, but it's not the registry itself. Technically, the registry is the collective name for various database files located in the Windows installation directory. (Source: Tim Fisher – [What is the Windows Registry?](https://www.lifewire.com/windows-registry-2625992))

Start regedit from the terminal with the following command

**$ regedit**

The GUI may take a few moments to fully load. Once it does, select the HKEY\_CURRENT\_USER folder, then drill down using the path shown below to view current configurations and settings for your SIFT workstation.

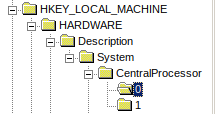
HKEY\_CURRENT\_USER 🡪 Software 🡪 Microsoft 🡪 Windows 🡪 Internet Settings 🡪 ZoneMap 🡪 ProtocolDefaults

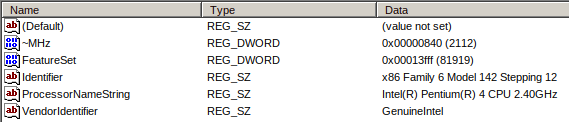
* **What protocols are used for network communications by default?**
  + **@ivt, file, ftp, http, https**

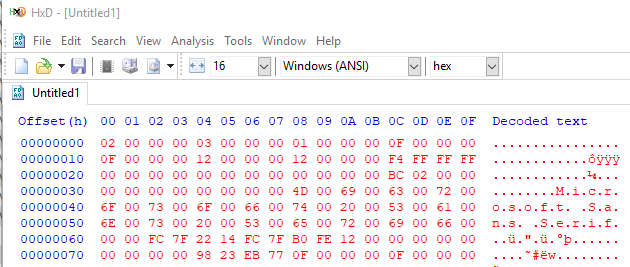
Next, select the Volatile Environment folder directly below the Software in the HKEY\_CURRENT\_USER registry

* **What server is accessed when you start your SIFT workstation?**
  + **logonserver**

Take a moment to explore the other hives and registry folders listed. As your move around you’ll notice that many of the values are blank (i.e. not configured) or have hexadecimal data or legible text, as shown in the figure below. While this information can be useful in a forensic investigation, manually parsing the registry can be overwhelming.





****With that said, a search of the Registry should still be performed as part of the digital forensic process, particularly when you need to verify configuration settings (e.g. autorun of scripts, installed or uninstalled programs, etc.). Without a deep understanding of how the Registry works, finding and interrupting this information can be difficult.

In the above figure, the HKEY\_USERS\.DEFAULT\Control Panel\Appearance\Schemes key value was exported. The highlighted portion says that the Sans Serif font would be used if the Control Panel was configured with a scheme of Spruce.

There are a number of forensic programs that can automate the tasks of searching through a Registry. For example, the Windows-based Nirsoft program will read registry values, then export the information as to a hex editor as shown below. While GUI versions of Registry viewers work well enough, using a CLI version is often more efficient.

In the next section of the lab, you’ll use the Linux version of RegRipper to find registry values and interpret the output to answer questions. Some of the output from the commands is long, so you will need to scroll up in the terminal to view all details. Be sure to carefully review the output to make sure you can answer the lab questions carefully. Note: Some values will be not be returned, this is ok.

### Registry Analysis using RegRipper

RegRipper is a flexible open source tool that can facilitate registry analysis with ease. It contains pre-written Perl scripts for the purpose of fetching frequently needed information during an investigation involving a Windows box. We are using RegRipper because of the simplicity of the tool and the availability of numerous plugins that capture specific information from the registry. (Source: Pranshu Bajpai – [Windows Registry Forensics using ‘RegRipper’ Command-Line on Linux](https://resources.infosecinstitute.com/registry-forensics-regripper-command-line-linux/#gref))

Some of the output from the commands is long, so you will need to scroll up in the terminal to view all details. Be sure to carefully review the output to make sure you can answer the lab questions carefully. Note: Some values will be not be returned, this is ok.

Open a new terminal and change to the RegFiles2 directory

**$ cd Downloads/RegFiles2**

#### Software Registry File

* Contains installed program settings and associated usernames and passwords
* Can contain system information

**# rip.pl -r Software -p product**

**# rip.pl -r Software -p producttype**

**# rip.pl -r Software -p winver**

**# rip.pl -r Software -p networkcards**

**# rip.pl -r Software -p nic**

**# rip.pl -r Software -p ssid**

**# rip.pl -r Software -p installer**

Based on the outputs from the commands above, answer the following questions

* **What OS does this system use?** 
  + **Microsoft Windows XP**
* **What information is potentially collected from using the ssid plugin?** 
  + **The potential information that can be collected using the ssid plugin is being able to see the server name in which you can possibly connect to or join.**
* **Where else can NIC information be found using RegRipper?** 
  + **You can also use networkcards to find network interface cards (nic)**
* **How many installed programs are reported?** 
  + **10**
* **Are these user installed or system installed?** 
  + **System installed**

#### System Registry Files

* Contains additional computer system settings (e.g. drive letter designations, system name, hardware/software configuration)
* Help ID a computer and any storage devices that were mounted on a system

**#** **rip.pl -r System -p compname**

**# rip.pl -r System -p shutdown**

**# rip.pl -r System -p timezone**

**# rip.pl -r System -p usb**

**# rip.pl -r System -p usbstor3**

**# rip.pl -r System -p mountdev2**

**# rip.pl -r System -p devclass**

**# rip.pl -r System -p services | less**

* **What time was this system last shutdown?** 
  + **Mon Sep 17 14:00:59 2018**
* **When was this system shutdown in Eastern Standard Time?** 
  + **Mon Sep 17 17:00:59 2018**
* **At one point there was a 2.0 USB device used on this system. Does the number 36bdf51d relate have any significance?** 
  + **Yes, the significance of this value is that this is the 2.0 USB device number in which it is identified as.**
* **What drive letter was assigned to the USB when it was mounted on the system?** 
  + **E**
* **A remote user could easily establish an unsecure connection to this system based on the reported status of the Telnet service?** 
  + **Yes**
* **If a USB device were inserted into this system and it had a malicious executable installed, would it automatically run?** 
  + **No, typically a file that is downloaded cannot simply run itself. There is other actions or processes that need to take place to start the virus in said file.**

#### SAM Registry Files

* Contains information on user accounts, password hashes
* Contains information on Groups and domains
* Lists GUIDs (Globally Unique IDs)

**#** **rip.pl -r SAM –p samparse**

**# rip.pl -r SAM –p samparse\_tln**

**# rip.pl -r SAM -p profilelist**

**# rip.pl -r Software –p profilelist**

**Based on the output from commands answer the following questions**

* **Of the total accounts (from the previous question), which has the most logons?** 
  + **The most logons were 5**
* **How many accounts are related to system and services accounts?** 
  + **7**
* **How many accounts have administrative access on this system?** 
  + **3**
* **In the Administrators group, what user account names are associated with the given SSIDs?**
  + **Sally Baker, Billy Baker, and nkucs**

#### NTUSER.dat Registry File

* Contains user-specific information (e.g. desktop settings, most recently used (MRU) files)
* All user accounts on a system have their own ntuser.dat file

**# rip.pl -r ntuser.dat -p yahoo\_cu**

**# rip.pl -r ntuser.dat -p olsearch**

**# rip.pl -r ntuser.dat -p winrar\_tln**

**# rip.pl -r ntuser.dat -p mpmru**

* **Based on the output from the commands above, was useful information collected? Why or Why not?** 
  + **This information was not useful at all in this lab. Most of the commands we entered are for files and folders that do not exist or have no context for these specific users.**

**# rip.pl -r ntuser.dat -p internet\_explorer\_cu**

**# rip.pl -r ntuser.dat -p typedurls**

**# rip.pl -r ntuser.dat -p wallpaper**

**# rip.pl -r ntuser.dat -p filehistory**

**# rip.pl -r ntuser.dat -p shellfolders**

**# rip.pl -r ntuser.dat -p recentdocs**

* **When a user opens IE, what’s displayed?** 
  + [**http://microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome**](http://microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome) **– start page**
* **How many actual files were accessed on 4/17/2019?** 
  + **6 files were accessed**
* **What user was logged in to the system when the registry files were collected?** 
  + **Sally Baker**