CSCE 4555/5555 – Computer Forensics

Lab 03 Project (Chapter 5)

Working with Windows and CLI Systems

STUDENT ID: 11647576

The Windows registry is the central repository that contains all the settings and data for the Windows environment. The registry is divided into five folders, or hives, and they are located in the C:\Windows\System32\Config folder. Each registry hive provides specific data such as passwords, desktop settings, hardware and software configurations, and other valuable forensic information that may be useful during an investigation.

Examining the Windows XP SAM Hive

The Security Account Manager (SAM) contains information about the user accounts and their associated password hashes, as well as group definitions and domain associations. The actual passwords are not stored for security purposes, but many forensic tools can decrypt password hashes and allow investigators to gain access to password-protected areas of the computer. The SAM registry file stores information using Globally Unique IDs called GUIDs. GUIDs are 32-character hexadecimal tags that are stored as 128-bit integers and are used to identify operating system data such as usernames or hashed password locations. In this part of the lab, you will examine a forensically secured Windows XP SAM registry file to locate useable forensic information.

1. Start **AccessData Registry Viewer** on your workstation, and click **Yes** in the User Account Control dialog box. Click **OK** in the CodeMeter.exe dialog box and then click **OK** in the Registry Viewer dialog box (this message will appear each time the Registry Viewer is launched).
2. Click the **File** tab and select **Open**. Navigate to the **SAM.dms** file and select **Open**. Maximize the window to fill the entire desktop.
3. Click each **+** to expand the SAM, Domains, Account, and Users folders.
4. Click the first folder (**000001F4**), and locate the Key Properties folder in the lower-left window. Drag the window boundaries to display all the data.
5. The Key Properties window displays the information contained in each key folder. Click the scroll bar on the right side of the Key Properties to view all the attributes. The SID unique identifier field contains values that indicate the type of account and whether the account is a default account that is created automatically when the OS is installed. The 500, 501, and 1000 values indicate default accounts that were automatically created. Identify the following information for this account:
   - **a.** What is the User Name? **Administrator.**
   - **b.** Is it an Active or Disabled Account? **Active Account.**

c. Is it a Default or Created Account? **Default Account.**

6. Click the fifth folder (**000003EB**), and locate the Key Properties folder in the lower-left window. Identify the following information about this account:

d. What is the User Name? **User.**

e. Is it a Default or Created Account? **Created Account**

f. How many times has account been accessed? **24**

g. When was last logon date/time? **5/14/2007 23:32:53 UTC**

h. When was date/time password last changed? **5/29/2009 21:10:02 UTC**

7. Click the sixth folder (**000003EC**), and locate the Key Properties folder in the lower-left window. Identify the following information for this account:

i. What is the User Name? **jsmith**

j. What is the Full Name of account owner? **John Smith**

k. When was last logon date/time? **5/15/2007 0:18:16 UTC**

l. When was date/time password last changed? **5/31/2009 6:04:24 UTC**

m. Is a Password Required? **False**

8. Click the sixth folder (**000003EE**), and locate the Key Properties folder in the lower-left window. Identify the following information for this account:

n. What is the User Name? **sworth**

o. What is the Full Name of account owner? **Steve Worth**

p. When was last logon date/time? **Never**

q. When was date/time password last changed? **5/31/2009 6:08:45 UTC**

9. Expand the **Names** folder. Note the user account names, and click the **jsmith** account. Note the Last Written Time indicates that this account was accessed on 5/31/2009, whereas the Last Logon Time indicated for this account above has a different date 2 years earlier. Why do you think this discrepancy exists? *Hint: Think in context of an investigation.*

I believe only the password was changed and the file not accessed.

10. Expand the **Builtin** folder located under the Domains folder, expand the **Aliases** folder, and then expand the **Members** folder to reveal two folders, one of which has a long number (the GUID). Windows uses GUID to hide actual names that might be used to locate critical information such as password hashes. Expand the folder with the GUID.

s. Select the folder for the **jsmith** account. What is the Folder Name? **000003EC**

t. The hex data in the lower-right window represents the hashed password data. Write this information here. **21 02 00 00 20 02 00 00**

11. Answer the following review questions about this activity.

    u. How many user accounts are listed in the SAM hive? **7**
    v. How many user accounts are disabled? **3**
    w. How many Built-in accounts are disabled? **2**
    x. How many users have never logged onto this computer? **5**
    y. How many user accounts require a password? **4**

12. Click the **File** tab and select **Close** to close the **SAM.dms** file, but leave the application open.

Examining the Windows XP System Hive

The SYSTEM registry hive contains drive letter designations for internal and external storage devices, the system name, and the configuration data for the system's hardware and software. This hive is very important because it can help identify on a specific computer any storage devices that may have been mounted onto the operating system. The SYSTEM hive also contains information about when the Windows partition was created and activated. The Product ID Key (PID) is a unique identifier that can act as an electronic fingerprint uniquely identifying this Windows operating system. In this part of the lab, you will add a Windows XP SYSTEM registry file to locate potential forensic information.

13. Click the **File** tab and select **Open**. Navigate to the **system.dms** file and select **Open**.

14. Click the **+** symbol next to the **ControlSet001** folder to expand it, and click the **+** symbol to expand the **Control** folder. Next, click the **+** symbol next to the **ComputerName** folder to expand it, and then click the **ComputerName** child folder to display the name in the upper-right window.

    z. Write the ComputerName indicated in the Data field. **USER-6AF329E100**

15. Drag the scroll bar on the right side of the upper-left window down to view the **TimeZoneInformation** folder, and click it to display the computer's time zone bias. The time zone identification is critical because time stamp information is based on the time zone bias.

    aa. What is the StandardName time zone? **Eastern Standard Time**

16. Under the **ControlSet001** folder, click the **Enum** folder, and expand it to view the subfolders. Select the **IDE** folder, and expand all the subfolders. This folder contains all the IDE (Integrated Drive Electronics) storage devices, which include the CD-ROM and hard disk drive and their associated signatures.

    bb. How many storage devices are connected to the IDE interface? **2**

    cc. What is the FriendlyName of the CD-ROM Drive? **HL-DT-ST RW/DVD GCC-4240N**

    dd. What is the FriendlyName of the Disk Drive? **HITACHI_DK23AA-60**

17. Click the **USBSTOR** folder, and expand the folder to display all the USB storage devices that have been plugged into the computer. Each storage device has a unique serial number so that it can be identified underneath the top-level sub-folder that identifies the device type and driver. In addition, the Last Written Time is listed for each USB flash drive.

    ee. How many different USB devices have been plugged into the computer? **3**

    ff. What is the serial number of the USB flash drive last written to? **27005402893046**

    gg. What is its Last Written Time? **7/26/2009 18:36:45 UTC**

18. Click the **MountedDevices** folder. This folder lists every storage device that has been mounted in the OS along with its associated drive letter.

    hh. How many mounted devices have assigned drive letters? **3**

    ii. Could more than one USB flash drive have been mounted (i.e., plugged in) at the same time? Why or why not?

    Not more than one, as each USB flash drive, has a unique last-written time.

19. Expand the **WPA** folder. This folder contains the information on this unique copy of Windows. The **Key-CJ27J3P2XV9J9JCPB4DVT** folder contains the ProductID (PID) for this copy of Windows. The **SigningHash-6KCM6KFTX6MD62** folder contains the activation hash along with the Last Written Time. This information indicates when Windows was first installed and activated.

    jj. What is the ProductID (PID) for this copy of Windows? **76487-770-9755187-2286**

    kk. What date/time was this copy of Windows activated? **5/29/2009 21:10:10 UTC**

    ll. Does this information agree with the user account data found earlier? Why or why not?

    No, the last login time was two years prior to the time when windows were activated.

20. Click the **File** tab and select **Close** to close the **system.dms** file, but leave the application open.

Examining the Windows XP NTUSER.DAT Hive

The NTUSER.DAT registry hive contains user-specific information such as the desktop, Windows, software, and file settings. In addition, this registry hive stores the most recently used files and devices. The forensic information stored in this area can help investigators tie together documents, Internet searches, and recently used storage devices. The NTUSER.DAT file in Windows XP is located in the C:\Documents and Settings\Username folder, and there are separate folders and NTUSER.DATA files for each account holder in Windows. Many password decryption tools require both the NTUSER.DAT file and the SYSTEM registry hive to retrieve a user password. In this part of the lab, you will add a Windows XP NTUSER.DAT registry to locate potential forensic information.

21. Click the **File** tab and select **Open**. Navigate to the **NTUSER.DAT** file and select **Open**.

22. Click the **Edit** tab and click **Find**. In the Find dialog box, type **recent files** and press the Enter key. In the upper-right window, recently opened documents will be displayed along with the path to the files.

    mm. How many files were found from this search? **2**

    nn. What type of files is listed in the recent files key? **(REG_SZ) xls file**

    oo. What is the file name of the first file listed (File1)? **Tech stock portfolio.xls**

23. Select the top-level **NTUSER.DAT** file, click the **Edit** tab, and select **Find**. In the find dialog box, type **jsmith** and click **Find Next** to search for the keys containing information about John Smith.

    pp. What is the name of the key returned from this search? **44BBA840-CC51-11CF-AAFA-00AA00B6015C**

    qq. When was this user account created (i.e., Last Written Time)? **6/1/2009 0:36:08 UTC**

24. Press the **F3** key to search for the Logon User Name. Note that you may have to repeat this several times.

    rr. What is the Last Written Time for this key? **5/15/2007 0:26:39 UTC**

25. Select the top-level **NTUSER.DAT** file, click the **Edit** tab, and select **Find**. In the find dialog box, type **email** and click **Find Next**. Click the **F3** function button to locate e-mail account information for jsmith. Note the lower-right window displays the e-mail username in hex. Use the arrow keys to scroll through the POP, SMTP, and password keys, and look for the text information in the hex area. The e-mail password is encrypted as displayed in hex (ASCII characters).

    ss. What is John Smith's e-mail username and domain?

    jsmith954@comcast.net

    (username:jsmith954, Domain: comcast.net)

    tt. What is the POP3 Server name? **pop.comcast.net**

26. Select the top-level **NTUSER.DAT** file, click the **Edit** tab, and select **Find**. In the find dialog box, type **typedurls** and click **Find Next** to locate any URLs that were typed by jsmith. Data is listed in both the upper data window and the lower hex data area.

uu. How many web sites did jsmith search? **1**

vv. On what date/time did jsmith go to the Microsoft site? **6/1/2009 0:36:05 UTC**

27. Click the **File** tab and select **Exit** to close the **Registry Viewer** when you are finished.

You are to submit this document with your answers through the **Lab 03** dropbox on Canvas by the due date and time.