Lab Assignment 2A – Windows Registry Analysis

Background

Students will continue to analyze the image and triage artifacts collected from Lab Assignment 1A in order to practice parsing the Windows registry for system configuration information and evidence of user activity.

Scenario: The Shield SOC received a network alert for a download for BitTorrent and a Privacy Cleaner utility over the weekend. Both tools are against the company's acceptable use policy and may be potentially unwanted programs (PUPs). The incident response team identified the system of interest and requested that the forensic team image the system and perform an analysis.

Objectives

- Become familiar with Windows common registry parsing and analysis tools
- Parse system registry hives for user accounts, configuration settings, and installed applications
- Parse and analyze user registry hives to identify user and account activity

Exercise Preparation

Forensic Workstation Preparation

Part of this preparation was completed during Lab Assignment 1A, but if you deleted Lab 1A evidence or reverted to an earlier snapshot, this step must be performed again.

1. Download and unzip FTK Imager on a host system or virtual machine
2. Download and unzip Registry Ripper 3.0 on a host system, virtual machine, or external drive
3. Download and Install AccessData Registry Viewer on a host system (Demo Mode)
4. Download and unzip the Lab 1 contents from OneDrive ("Imaging and Triage Lab.zip" archive from Lab 1A and "Lab Assignment 2B" archive)

OneDrive 2A Evidence Link:
https://northeastern-my.sharepoint.com/:f:/g/personal/e_booker_northeastern_edu/EgjF7jqB2m1MgHBQxMMm1fYBha6WztkXrFt6_d9IrAJzwg?e=XZYVew

OneDrive Forensic Tools Link:
https://northeastern-my.sharepoint.com/:f:/g/personal/e_booker_northeastern_edu/Es9N9lw4pthBr1iAX6vypiEB-y4isrST1PkQCTuRnGhM-A?e=UPlS09

System Registry Analysis

Parse system, software and account registry hives for initial triage and forensic analysis of configuration settings (**SYSTEM, SOFTWARE and SAM** registry hives) using Registry Ripper (regripper 3.0).

Note: The next two processes require the registry hives extracted in Lab Assignment 1A.

User Registry Analysis

Parse user-specific registry hives for triage and forensic analysis of user activity to answer forensic questions. These items will include program execution, file knowledge, file access, and other evidence of user actions (**NTUSER.DAT** registry hives; **USRCLASS.DAT** will be analyzed during Module 4).

Exercise – Questions

Forensic Workstation Preparation

1. Not applicable

System Registry Analysis

1. PATHS (with LOG1 and LOG2)
    a. **NONAME [NTFS]/[root]/Windows/System32/config/SAM**
    b. **NONAME [NTFS]/[root]/Windows/System32/config/SYSTEM**
    c. **NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE**
    d. **NONAME [NTFS]/[root]/Users/srogers/NTUSER.DAT**
2. Parse the SAM hive as illustrated in the lecture and answer the following questions based on content, locations and directions in the PowerPoints:
    a. What is the Relative ID (RID) for the **"srogers"** account (hint: last for digits of a Security Identifier – SID)?

    Embedded RID : 1001

    b. What is the complete SID of the srogers account that includes the RID above?

    S-1-5-21-263698462-3103634936-1936700066-1001

    c. When was the **"srogers"** account created (date/time)?

    Account Created : 2019-01-19 03:11:57Z

    d. When was the last login date/time?

    Last Login Date : 2019-01-21 18:56:51Z

e. How many times has this account been logged into?

Login Count : 10

f. Has the user ever entered an incorrect password, if so when (date/time)?

Pwd Fail Date : 2019-01-20 19:46:19Z

3. Parse the SYSTEM hive as illustrated in the lecture and answer the following questions based on content, locations and directions in the PowerPoints:
   a. What is the COMPUTERNAME?

ComputerName = AVENGERS01

   b. What is the current system time zone?

TimeZoneKeyName-> Eastern Standard Time

   c. What date/time was the system last shutdown?

ShutdownTime : 2019-01-20 21:11:38Z

4. Parse the SOFTWARE hive as illustrated in the lecture and answer the following questions based on content, locations and directions in the lecture material:
   a. What is the operating system install date? (CTRL+F and search for winver and look at **InstallDate**)

InstallDate 2019-01-19 03:06:56Z

   b. Can you identify any system autostart programs? If so, what are they, where are they located, and what are these applications?

LastWrite Time 2019-01-20 21:12:14Z
SecurityHealth - %ProgramFiles%\Windows Defender\MSASCuiL.exe
VMware User Process - "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
LastWrite Time 2019-01-20 21:17:39Z
Dropbox - "C:\Program Files (x86)\Dropbox\Client\Dropbox.exe" /systemstartup
LastWrite Time 2019-01-20 21:17:37Z
GrpConv - grpconv -o

Refer to the lecture material for specific intent, locations, and interpretation of these values that can be found for related users within their NTUSER hive.

1. Often when applications are installed, they include an uninstaller. This is a valid way to look for evidence of items installed, while providing another location to corroborate evidence. Can you find any installed applications under various "uninstall" keys? If so, what are the results and the date/time stamps?

   uninstall v.20200525
   (Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT hives

   Uninstall
   Software\Microsoft\Windows\CurrentVersion\Uninstall

   2019-01-20 21:27:13Z
   BitTorrent v.7.10.4.44847

   2019-01-20 02:46:39Z
   Microsoft OneDrive v.18.240.1202.0004

2. Identify the most recent six folders accessed by this account and the last write time of the last folder accesses (…\RecentDocs\Folder)

   Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
   LastWrite Time 2019-01-21 19:16:10Z
   MRUListEx = 3,5,2,4,1,0
   3 = Personal
   5 = USB Backup
   2 = Shield Documents
   4 = This PC
   1 = Shield_USB (E:)
   0 = The Internet

3. What were the two most recently accessed .xlsx files?

   Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.xlsx
   LastWrite Time 2019-01-21 19:16:10Z
   MRUListEx = 1,0
   1 = Random Accounting Spreadsheet.xlsx
   0 = Confidential Alloy Expense Accounts.xlsx

4. What were the two most recently accessed .pptx files?

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pptx
LastWrite Time 2019-01-21 05:07:00Z
MRUListEx = 1,0
1 = Presentation with Sensitive IP.pptx
0 = Alloys.pptx

5. What was the last .docx file accessed?

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx
LastWrite Time 2019-01-21 05:06:25Z
MRUListEx = 0
0 = S. Rogers Resume.docx

6. Were there any .jpg files accessed? If so, what were they?

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg
LastWrite Time 2019-01-21 05:23:13Z
MRUListEx = 1,0
1 = Cap-2.jpg
0 = Cap-1.jpg

7. Under the "userassist" key showing evidence of program execution, what applications may be of concern from an investigation or policy violation standpoint? List the application name and the last written timestamp showing last execution.

2019-01-21 05:10:14Z
C:\Users\srogers\Downloads\torbrowser-install-win64-8.0.4_en-US.exe (1)
…
2019-01-20 21:26:03Z
C:\Users\srogers\Downloads\BitTorrent.exe (1)

Exercise—Key Takeaways

- Parsing the registry in temporal order provides a repeatable process for forensic investigations
- Analysis of the system registry hives provides system evidence for all users on a system
- Analysis of user hives can provide a significant amount of evidence and insight into user behavior, knowledge, and actions

***Please submit the final complete assignment as a single .PDF and any applicable reports as a .ZIP file.**
**Screenshots may also be added to this document when appropriate.

Lab Assignment 2B – Additional Registry Analysis

Background

Students will use AccessData's Registry Viewer to analyze the registry and be exposed to another registry utility that might be more user-friendly, but allow for the verification and validation of forensic evidence identified using other tools to corroborate initial findings.

Objectives

- Become familiar with a Windows Graphical User Interface (GUI) analysis tool
- Identify types of evidence found in various registry hives and their location
- Learn to interpret registry values and their meaning for forensic investigations

Exercise Preparation

Examining the SAM Hive

The Registry is the central repository of settings and data for the Windows environment. It's divided into five hives, three of which are in the C:\Windows\System32\Config folder. Each hive contains specific data, such as passwords, desktop settings, hardware and software configurations, and other valuable forensic information. The Registry files most useful to forensics investigators are the Security Accounts Manager (SAM) and SYSTEM hives and the ntuser.dat file (which is in the C:\Users*username* folder and is unique for each user). The SAM hive stores information on user accounts and their password hashes as well as group definitions and domain associations by using globally unique IDs (GUIDs). In this assignment, students will copy Registry files from a Windows image with FTK Imager and view the SAM hive with AccessData Registry Viewer 2.0.0.

OneDrive 2B Evidence Link:
https://northeastern-my.sharepoint.com/:u:/g/personal/e_booker_northeastern_edu/ETljYp9EbBBJhpm4bOdDW5YB0xos3-x3NfDExtRenMOMnw?e=DZg0HG

Students will examine the SAM hive to determine the user accounts on a seized computer:

1. Download the **Lab Assignment 2B.zip** to your work folder. Extract the folder to the same location.
2. Ensure you've downloaded and installed the latest version of AccessData's Registry Viewer
3. Start FTK Imager. If necessary, click **Yes** in the UAC message box. Click **File**, **Add Evidence** Item from the menu. In the Select Source dialog box, click the **Image File** option button, and then click **Next**. In the Select File dialog box, click **Browse**, navigate to and click your work folder, click the

LabAssignment2B.img file, and then click **OK** to enter this source path. Click **Finish** to open the image in FTK Imager.

4. In the top left pane (Evidence Tree), click to expand **LabAssignment2B.img** , **6gb [NTFS]**, **[root]**, and **Users**. Click the **Denise** folder, and then right-click the **ntuser.dat** file in the File List pane and click **Export Files**. In the Browse For Folder dialog box, navigate to and click your work folder, click **Make New Folder**, and type **Lab2B** for the new name. Click **OK** to copy the file, and click **OK** in the Export Results message box.
5. In the top left pane (Evidence Tree), click to expand **Windows** and **System32**, and then click **config**. In the File List pane, Ctrl+click **SYSTEM**, **SOFTWARE**, **SECURITY**, **SAM**, and **DEFAULT**. Right-click one of these selected files and click **Export Files**. Navigate to and click the **Lab2B** subfolder of your work folder, and click **OK** to copy the files. Click **OK** in the Export Results message box, and then exit FTK Imager.
6. Start Registry Viewer, and if necessary, click **Run as administrator**. If necessary, click **Yes** in the UAC message box. Click **Yes** in the ERROR dialog box, click **Cancel** in the Security Device Settings dialog box, and click **OK** in the Registry Viewer dialog box to start Registry Viewer in demo mode.
7. Click **File**, **Open** from the menu. Navigate to the **Lab2B** subfolder of your work folder, and in the File List pane, click **SAM**, and then click **Open**.
8. In the top left pane, click to expand the **SAM**, **Domains**, **Account**, and **Users** folders. Click the **000001F4** folder, and enlarge the Key Properties pane at the lower left. Notice the last logon time and the SID unique identifier field, which indicates the type of account and whether it's created automatically when the OS is installed. Values of 500, 501, and 1000 show default accounts (created automatically). This user account is Administrator, and it has been logged on to three times.
9. Click the **000003E9** folder. The jfriday account has been logged on to seven times, and the SID value 1001 indicates that this account was created.
10. Click the **000003EC** folder. The Denise Robinson account was created but has never logged on to the computer.
11. Click to expand the **Names** folder, and then click the **jfriday** folder. The Last Written Time entry indicates that this account was accessed on 2/6/2014 when the password was changed.
12. Leave Registry Viewer open as you answer the exercise questions below. When you're finished, close the SAM hive by clicking **File**, **Close** from the menu. In the Registry Viewer dialog box, click **Yes**, and leave Registry Viewer running for the next step of the assignment.

Examining the SYSTEM Hive

The SYSTEM Registry hive contains drive letter designations for internal and external storage devices, the system name, and configuration data for the system's hardware and software. This hive is important because it can help identify a computer and any storage devices that might have been mounted in the OS. It also contains information on when the Windows partition was created and activated. The product ID (PID) key in the SYSTEM hive is a unique identifier that can act as an electronic fingerprint to identify a legally activated Windows OS.

Students will examine the SYSTEM hive to see how it manages connected devices on a computer:

1. In Registry Viewer, click **File**, **Open** from the menu. Navigate to the **Lab2B** subfolder of your work folder, click the **SYSTEM** file, and then click **Open**.
2. In the top left pane, expand the **ControlSet001**, **Control**, and **ComputerName** folders, and then click the **ComputerName** folder to display the name at the upper right.

3. Scroll down and click the **TimeZoneInformation** folder in the left pane to display the computer's time zone information. This information is critical because timestamps for files, folders, and logs are based on the time zone.
4. Scroll down the left pane, and expand the **Enum** folder and the **IDE** folder, which contains IDE storage devices, such as the CD/DVD drive. Expand the **USB** folder to see all USB storage devices plugged into the computer. Each storage device has a unique serial number and a Last Written Time entry in the Key Properties pane.
5. Click the **MountedDevices** folder, which lists every storage device that has been mounted in the Windows OS along with its associated drive letter and GUID value. This information can be used to associate hard drives with a Windows computer.
6. Leave Registry Viewer open as you answer the exercise questions below. When you're finished, close the SYSTEM hive by clicking **File**, **Close** from the menu. In the Registry Viewer dialog box, click **Yes**, and leave Registry Viewer running for the next step in the assignment.

Examining the NTUSER.DAT Hive

The ntuser.dat Registry file contains user-specific information, such as personalized settings for the desktop, software, and e-mail accounts as well as the most recently used (MRU) files and devices. The forensic information in this file can help investigators discover Internet searches and recently used storage devices, for example. The ntuser.dat file is in the C:\Users\username folder, and each account holder in Windows has a separate ntuser.dat file.

Students will look for forensic evidence in the ntuser.dat file belonging to a suspect's user account:

1. In Registry Viewer, click **File**, **Open** from the menu. Navigate to the **Lab2B** subfolder of your work folder, click the **ntuser.dat** file, and then click **Open**.
2. Click **Edit**, **Find** from the menu. In the Find dialog box, type **Denise** and press **Find Next or Enter**. The first Registry key associated with Denise is displayed at the upper right.
3. Press the **F3** key to search for the next Registry key containing a reference to Denise. Notice the GUID associated with the username account information. Press **F3** again to find the next key, and notice the e-mail account for Denise along with her full name.
4. Click **Edit**, **Find** from the menu. In the Find dialog box, type **jfriday** and press **Enter** to search for any Registry keys associated with this suspect. A message is displayed stating that Registry Viewer couldn't find any keys associated with this user. This happened because each ntuser.dat file is associated with only one user account.
5. Leave Registry Viewer open as you answer the exercise questions below. When you're finished, exit Registry Viewer.

Exercise – Questions

Examining the SAM Hive

UID	RID	User Name	Disabled	Last Password Change Time (UTC)
000001F4	500	Administrator	True	9/30/2013 4:07:13
000001F5	501	Guest	True	Never
000003E9	1001	Jfriday	False	2/6/2014 18:44:26

000003EB	1003	HomeGroupUser$	False	Never
000003EC	1004	Denise	False	3/4/2014 11:53:06

1. The Registry contains how many hives?

   The SAM hive containers 5 registries (above) of Administrator, Guest, jfriday, HomeGroupUser$ and Denise

2. How many user accounts are disabled?

   2 Disabled Accounts: Administrator and Guest

3. The SAM hive uses PIDs to store information on user accounts. True or False?

   False – PIDs do not show when searching in "Edit > Find > Find what: "

4. Name two SID values that indicate whether an account was created automatically.

   User RIDs of 500 and 501 show default accounts (created automatically). There was no User with RID 1000 which would be created automatically. The valid RIDs that were created automatically in this hive are the Administrator and Guest accounts which are disabled. Their paths are under:

   SAM\SAM\Domains\Account\Aliases\Members\S-1-5-80-2375682873-768044350-3534595160-1005545032

   SAM\SAM\Domains\Account\Aliases\Members\S-1-11-96-3623454863-58364-18864-2661722203-1597581903-1858740627-2803279481-1352708721-4128937580

5. The Key Properties pane in Registry Viewer shows when user accounts have changed their passwords. True or False?

   True, When in the path "SAM\SAM\Domains\Account\Users\(USER_ID)" the Key Properties show information that includes the "Last Password Change Time"

Examining the SYSTEM Hive

1. What's the computer name of this system?

   Found in the path "SYSTEM\ControlSet001\Control\ComputerName\ComputerName" the ComputerName is "mnmsrvc"

2. What's the time zone setting for this computer?

   Found in the path "SYSTEM\ControlSet001\Control\TimeZoneInformation" The TimeZoneKeyName is "Pacific Standard Time"

3. How many mounted devices on this system have assigned drive letters? What are the letters assigned?

Found in the path "SYSTEM\MountedDevices" There are two devices mounted on the system with letters "C" and "D"

4. What information is stored in the Enum folder?

   "The Enum tree is reserved for use by operating system components, and its layout is subject to change. Drivers and user-mode device installation components must use system-supplied functions, such as IoGetDeviceProperty, CM_Get_DevNode_Registry_Property, and SetupDiGetDeviceRegistryProperty to extract information from this tree." - https://learn.microsoft.com/en-us/windows-hardware/drivers/install/hklm-system-currentcontrolset-enum-registry-tree

   Operating System Components are stored in the "HKLM\SYSTEM\CurrentControlSet\Enum" Registry Tree

   a. User account information
   b. Password information
   c. File locations
   d. Hardware and software values

5. The SYSTEM hive contains configuration data for passwords. True or False?

   True located at path "SYSTEM\ControlSet001\Control\Terminal Server\DefaultUserConfiguration"

   Password is not set for the SYSTEM

Examining the NTUSER.DAT Hive

1. The ntuser.dat file contains information on multiple account holders. True or False?

   False. *"each ntuser.dat file is associated with only one user account."*

2. What's the e-mail account for the user Denise?

   Found in Path:
   Computer\HKEY_CURRENT_USER\Software\Microsoft\IdentifyCRL\UserExtendedProperties

   Denise's email is: denise.robinson5@outlook.com

3. The ntuser.dat file contains information on which of the following? (highlight all that apply.)

   a. Drive letter designations
   b. Personalized desktop settings
   c. PID key
   d. MRU devices

4. Password decryption tools often need which of the following to retrieve user passwords? (highlight all that apply.)

a. SYSTEM hive
b. SAM hive
c. ntuser.dat file at Path "NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\HomeGroup\Roaming\{39B34448-0E32-4644-8FA9-5C339284F3D6}"
d. Enum folder

5. The ntuser.dat file is in which of the following paths?
   a. C:\Windows\System32\Config
   b. C:\Documents and Settings\Users
   c. C:\Users*username*
   d. C:\SYSTEM

Exercise—Key Takeaways

- Utilize GUI registry tools to analyze registry hives and compare output to command line tools
- Parse SAM, SYSTEM, AND NTUSER hives for initial triage and forensic evidence
- Understanding the structure of hives, keys, subkeys, and values is critical for forensic analysis

***Please submit the final complete assignment as a single .PDF and any applicable reports as a .ZIP file.**
**Screenshots may also be added to this document when appropriate.