|  |  |
| --- | --- |
| Course | Computer Forensic |
| Lab | Lab 06 |
| Name of the Student | Maisha Khatoon |
| Student ID | 100899259 |

# **LAB: 06**

This lab focuses on Windows forensics registry analysis.

**Objective:**

* **Learn windows registry**

**Leaning Activities:**

At the end of these activities, you should understand:

* Windows registry
* Understand how to navigate registry keys
* Regedit display of Windows Registry hive
* How to collect artifacts

**Tools to use:**

-Mantooth.e01

- Regedit

- Registry Viewer

**Note: Please include a screenshot of each step. Corp your screenshot to show relevant information only. Uncropped screenshots will result in a 10% deduction from your marks.**

**Task 1:**

* 1. First download Mantooth.e01
  2. Open new case in Autospy
  3. Add data image file Mantooth.e01

1.4 Autospy will process the image file as evidence source (This might take few minutes)

Let’s start by finding registry hives with the imager file

* 1. In the Autospy go to Windows/System32/config
  2. Now you will see a list of file, select System
  3. Autospy will parse the registry file into the pane in the bottom (under Application) You

will see a list of folders

* 1. Open ‘ControlSet001->Control->TimeZoneInformation’, Select the ‘TimeZoneInformation’

The configuration information will be parsed in the Metadata pane.

What is the time zone? \_\_\_\_\_\_\_\_Mountain Standard Time\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Take a screenshot of this result)

A screenshot of a computer

Description automatically generated

**Task-2:**

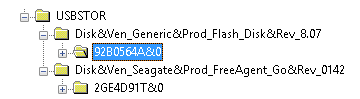
**Track USB serial number**

2.1 Navigate to the System Hive (Windows/System32/config)

2.2 Select ControlSet0001→ Enum→ USBSTOR

You will see a lot of information regarding to connected USB devices, Scan disks, IPods +etc. There are sub keys listed, the number indicate the serial number (if it has one).

Ex:



*Here you can see two USB Devices have been installed on this machine, a Seagate FreeAgent device and a Generic device (Generic device is not that uncommon, the Serial number will help you to track the USB device through the artefacts).*

*Both of these devices have a unique serial from their respective manufacturers. This can be seen by the &0 or &1 at the end of the serial number. If instead the second character is an & then the device does not have a unique serial number and Windows has issued one which is unique to the local system only.*

A screenshot of a computer

Description automatically generated with medium confidence

2.3 Select ControlSet0001→ Enum→ USB

There are Vendor ID and Product ID are listed (Ex: VID\_05DC&PID\_A410)

A screenshot of a computer

Description automatically generated with medium confidence

**Task 3:**

**Track USB drive letter**

3.1 Navigate to the Software Hive, then go to Microsoft→ Windows Portable Devices→ Devices

3.2 Find what drive letter was associated to the USB drive with label ‘WASHER’? \_\_(E:) & (F:)\_\_\_\_\_\_

(Take a screenshot of this result)

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

Why is it important to know the Drive number/letter (like F:) of a connected device? \_\_ When conducting tasks like file management, data access, and troubleshooting, knowing the drive number or letter of a connected device is vital since it enables you to precisely identify and reference the item in question. It gives you the ability to traverse the file system, run commands, and modify settings that are unique to the device, which guarantees that your interactions will be effective and focused. \_\_\_\_\_\_\_\_\_

Where could this come in handy during a forensic investigation? \_\_\_\_\_ When conducting a forensic investigation, it is essential to be aware of the drive number or letter of each connected device in order to correctly identify and access the storage media that is the subject of the inquiry. It makes it possible for investigators to carry out activities such as imaging, data extraction, and analysis on the particular device that is of interest. During the course of the inquiry, having knowledge of the drive letter or number makes it easier to keep correct paperwork and to keep track of the chain of custody. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Task 4:**

**Track networks**

4.1 Navigate to the Software Hive, then go to Microsoft-->Windows NT -->CurrentVersion->NetworkList-->Signatures-->Managed and highlight the key, on the right we should see a Dns Suffix.

(Take a screenshot of this result)

A screenshot of a computer

Description automatically generated with medium confidence

4.2 Now, select Unmanaged Managed and highlight the key, on the right we should see a Dns Suffix

(Take a screenshot of this result)

A screenshot of a computer

Description automatically generated with low confidence

A screenshot of a computer

Description automatically generated with medium confidence

*Note:*

*managed = computer on a domain*

*unmanaged = computer not on a domain*

4.3 Make a note on the “DefaultGatewayMac’, Are the MAC address same? \_\_\_No, the MAC addresses are not the same, they are different.\_\_\_\_

Why?

Because every network interface device has its own unique mac address. When conducting a forensic investigation, it is essential to be aware of the drive number or letter of each connected device in order to correctly identify and access the storage media that is the subject of the inquiry. It makes it possible for investigators to carry out activities such as imaging, data extraction, and analysis on the particular device that is of interest. During the course of the inquiry, having knowledge of the drive letter or number makes it easier to keep correct paperwork and to keep track of the chain of custody.

**Task 5:**

**Track Recent activities**

5.1 Navigate to /img\_Mantooth.E01/vol\_vo2/Users/WesMantooth/AppData/Roaming/Microsoft/Windows/Recent

5.2 Now, Scroll through some of the recent files listed here, see if you can find any which are

associated to USB drives. (Take a screenshot of this result)

A screenshot of a computer

Description automatically generated with medium confidence

5.3 Are there any files that may be of interest during our forensic investigation? \_\_Bill\_Gates.gif.lnk can be of some interest because this file seems deleted.

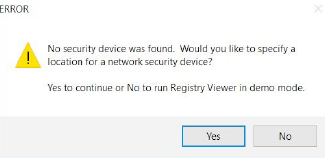
**Task 6:**

**Registry Analysis with Registry Viewer**

The Windows registry provides a lot of information about the system, the machine, and the users. Now we will work to select and extract the most useful elements for the purposes of our analysis.

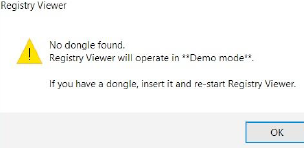
6.1 Download Access Data, Registry Viewer (<https://accessdata.com/product-download/registry-viewer-2-0-0>)

6.2 Once installed, you can launch the program and a window will appear with the following warning:



Click No and run Registry Viewer in demo mode.

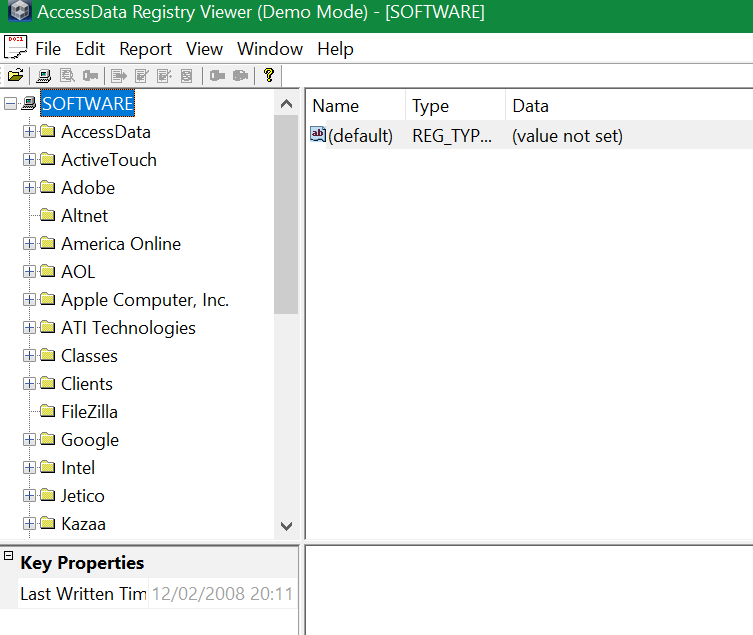
In the new window that will open, click OK and finally you will have access to the operating interface of the tool.



6.3 In this task, we will need to export registry hives from Autopsy in Task1. Export the following registry hives:

* **SYSTEM**
* **SOFTWARE**
* **SECURITY**
* **NTUSER.DAT**

6.4 To import a file just click on File→Open and select an extracted hive file.



6.5 We choose the Software file previously extracted with FTK Imager to continue our analysis.

6.6 To import a file just click on File→Open and select an extracted hive file.

6.7 In the upper left panel, note the hive Software represented as a PC and, under it, the keysrepresented as folders. In the lower left, Key Properties are shown. Note the Last Written Timeproperty, which corresponds

to 12/02/2008 20:11:57.

If we scroll down and select the key Arcobat Reader and the subkey Installer, we can see the stored values, specifically, version, the installation path and the default directory of the tool.

*You may have noticed that we are using the demo version of the Registry Viewer. This is because although the features are obviously more limited than the full version (no Common Areas shown and the inability to generate reports), Registry Viewer demo is still a powerful and very useful tool for analyzing the registry.*

6.8 What is the OS version? \_\_\_\_\_\_\_\_\_\_\_\_\_6.0\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Hint: SOFTWARE\Microsoft\WindowsNT\CurrentVersion)

6.9 When was this OS installed? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Tue Feb 27 19:22:03 2007\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6.10 Who is the registered owner?\_\_\_\_\_\_\_\_\_Wes Mantooth\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6.11 What is the model and manufacturer? \_\_\_\_\_\_value not set\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Hint: SOFTWARE\Microsoft\Windows\CurrentVersion\OEMInformation)

6.12 To find useful information about the installed printers, you can look at the subkeys stored at this path:

SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\

What is the printer driver name?\_\_\_\_\_Epson stylus photo rx420 (m)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Note: To verify it, just highlight the hexadecimal value stored in the Shutdown- Time value and then right-click and select Show Hex Interpreter Window.*

6.13 What is the computer name? \_\_\_\_\_WESMANTOOTH-PC\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Hint: SYSTEM\ControlSet001\Control\ComputerName\ComputerName)

6.14 What is the time zone? Mountain Standard Time

(Hint: SYSTEM\ControlSet001\Control\TimeZoneInformation)

6.15 When is the last shutdown time?\_\_\_\_2006-11-02 12:48:34\_\_\_\_\_\_\_\_\_\_\_\_

(Hint: SYSTEM\ControlSet001\Control\Windows\)

**Task 7:**

The SAM hive can provide some interesting statistical information about the local users and the machine’s use.

To see how many accounts are recorded, we can move to the SAM\Domain\Account\Users and count the subkeys present. Each subkey represents a user, its name is formed by four zeros followed by the hexadecimal

representation of the user’s relative identifier (RID): the Administrator account has a RID of 500, so the stored key is named 00001F4, where 01F4 is the hexadecimal translation of 500, the first user’s account created has a RID of 1001, so the stored key name is 0309 and so on.

A screenshot of a computer

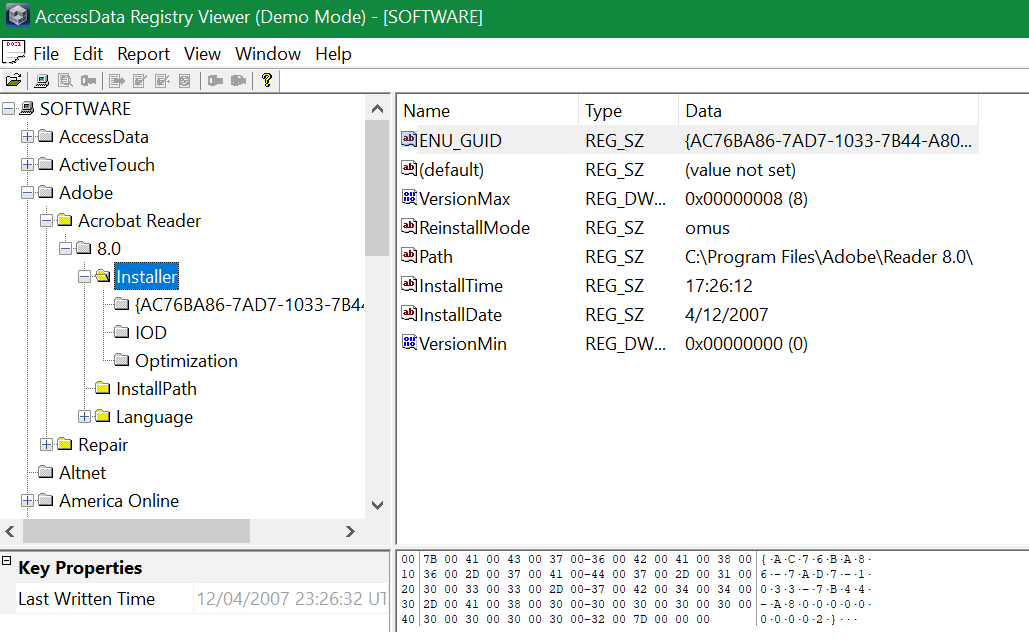
Description automatically generated

**Task 8:**

If we want to collect as much data as possible from an installed application, we must look at the following key:

SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\

We will see a list of subkeys identified by the application’s product code GUID. If we need to find a certain application, we can select the key Uninstall on Edit→Find and type a specific term to make a search only restricted to our key. For example, let’s try to find some information about the AOL.



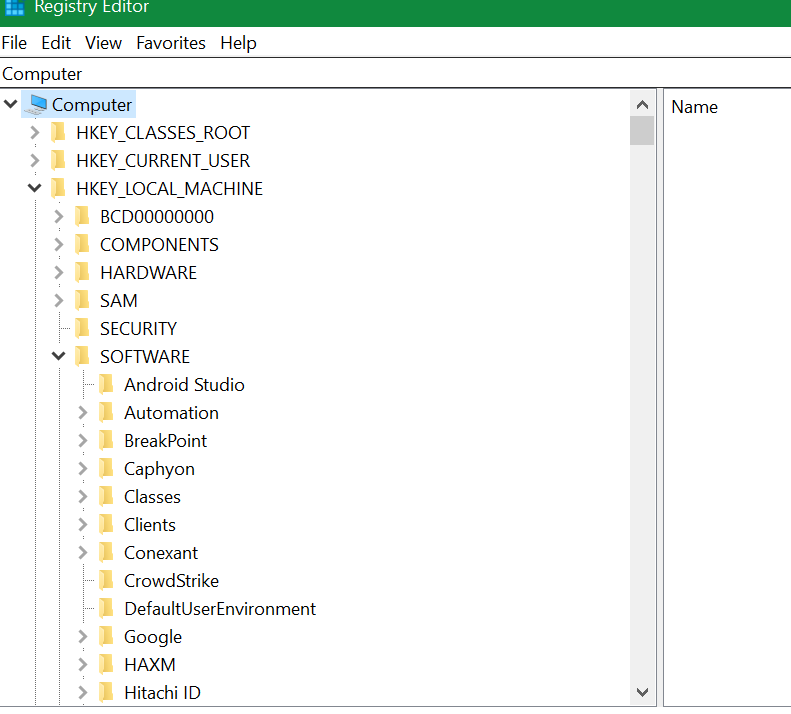
**Task 9:**

Registry Analysis with Registry Viewer

Windows Registry extraction with FTK Imager or Regedit

There are several ways to perform an extraction from the Windows Registry, let’s see some of the most useful. On a running machine, you can perform a backup of the registry using the Windows Graphical Interface or using the command shell or PowerShell. In the first way, just launch the regedit command in the cmd shell to open the graphical version of the registry.

9.1 To export the entire registry right-click on the computer icon and select “export” to save a .reg file in a folder of your choice.



9.2 Open “Access Data FTK Imager"

9.3 Click on “Add Evidence Item” button

9.4 Select “Logical Drive” radio button

9.5 Select source drive.

9.6 Scan “MFT” by expanding “Evidence Tree”.

Go to windows/system32/config/.

9.7 Export registry file by clicking “Export Files” button. Select the destination folder of your choice.

A screenshot of a computer

Description automatically generated

**Reflective statements (end-of-exercise):**

You should reflect on these questions:

1. Which registry key holds the list of URLs the currently logged on user typed into Internet Explorer?

HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\TypedURLs

|  |  |
| --- | --- |
|  |  |

1. Which registry key would you use to discover the SID associated with a particular user?

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \ProfileList

1. Which registry hives holds information about installed applications, settings; along with information about any hardware that has ever been connected to the computer including the type of bus, total size of available memory, list of currently loaded device drivers and information about Windows?

HKEY\_LOCAL\_MACHINE

1. Assume you have copies of the registry files, SAM, SECURITY and SOFTWARE, In other words these files are NOT in an image. Which program would you use to inspect the files?

Access Data Registry Viewers5re

**References**

1. <https://microsoft.fandom.com/wiki/Windows_Registry>
2. <https://www.howtogeek.com/school/using-windows-admin-tools-like-a-pro/lesson5/>
3. <https://en.wikipedia.org/wiki/Windows_Registry>
4. <https://cloudblogs.microsoft.com/industry-blog/en-gb/technetuk/2016/07/15/13-epic-registry-hacks/>