UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LAB 7 – Examining the Windows Registry

Objective

- Gain understanding of Windows registry
- Use Windows registry editor (regedit or regedt32)
- Create copies of Windows registry for later analysis
- Use Forensics Software to examine the saved copy of a Windows registry

File Required:

GCFI-Win98.eve

Tools:

Pro-Discover Basic & FTK Registry Viewer

In-Lab Exercise: Complete the tasks in a team of two of your choice. However, be sure to submit report of your own.

Task 1

Locate registry files of your windows system (Windows XP or later). For this task, you need to complete the table with the following format:

No.	Filename and Location	Purpose of File	File Size (Bytes)	File Date and Time	Screen Shot
1		For your username: User-protected storage area; contains the MRU files list and desktop			
2		Contains the computer's system settings			
3		Contains user account management and security settings			
4		Contains the computer's security settings			
5		Contains installed programs settings and associated usernames and passwords			
6		Contains additional computer system settings.			

Task 2

Use Windows registry editor to change start-up program settings. In this task, you are to examine
HKLM\SOFTWARE\MICROSOFT\Windows\CurrentVersion\Run and
HKCU\SOFTWARE\MICROSOFT\Windows\CurrentVersion\Run.
Complete the following,

1. Add a string value to
   HKLM\SOFTWARE\MICROSOFT\Windows\CurrentVersion\Run
   and set the value to the notepad program and the notepad program opens a text file called "Banner.txt" that you need to create as the user warning banner of your imaginary company.
2. Log out and log back in.
3. You should observe that the notepad program is running and the program opens the "Banner.txt". If you do not observe this behavior, you must make necessary correction until you observe the behavior.
4. Add a string value to
   HKCU\SOFTWARE\MICROSOFT\Windows\CurrentVersion\Run and
   a. set the value to the Windows Media Player and the player plays a selected audio clip.
5. Log out and log back in.
6. You should observe that the Windows Media Player is playing the selected audio clip upon logging in.
7. Answer the following question,

   How do
   HKLM\SOFTWARE\MICROSOFT\Windows\CurrentVersion\Run
   and
   HKCU\SOFTWARE\MICROSOFT\Windows\CurrentVersion\Run
   affect Windows behavior differently?

Task 3

Examine a saved copy of the Windows registry using a forensics software. For this task, you are to complete the steps below. The files needed in this lab can be found in ULearn under Lab 7/during the lab session.

Task 3.1: To extract Registry files with ProDiscover Basic

1. Start ProDiscover Basic with the **Run as administrator** option. If the Launch Dialog dialog box opens, click **Cancel**.
2. Click **File, New Project** from the menu.
3. In the New Project dialog box, type **InChap06** in the Project Number text box and the Project File Name text box, and then click **OK**.

4. In the tree view of the main window, click to expand **Add** and then click **Image File**.
5. In the Open dialog box, navigate to your work folder, click the **GCFI-Win98.eve** image file, and click **Open**. Click **Yes** in the Auto Image Checksum message box, if necessary.
6. Click the **Search** toolbar button. In the Search dialog box, click the **Content Search** tab. Click the **Search for files named** option button, and in the Search text box, type **system.dat** and **user.dat**. Under Select the Disk(s)/Image(s) you want to search in, click the image file (see Figure 1), and then click **OK**.

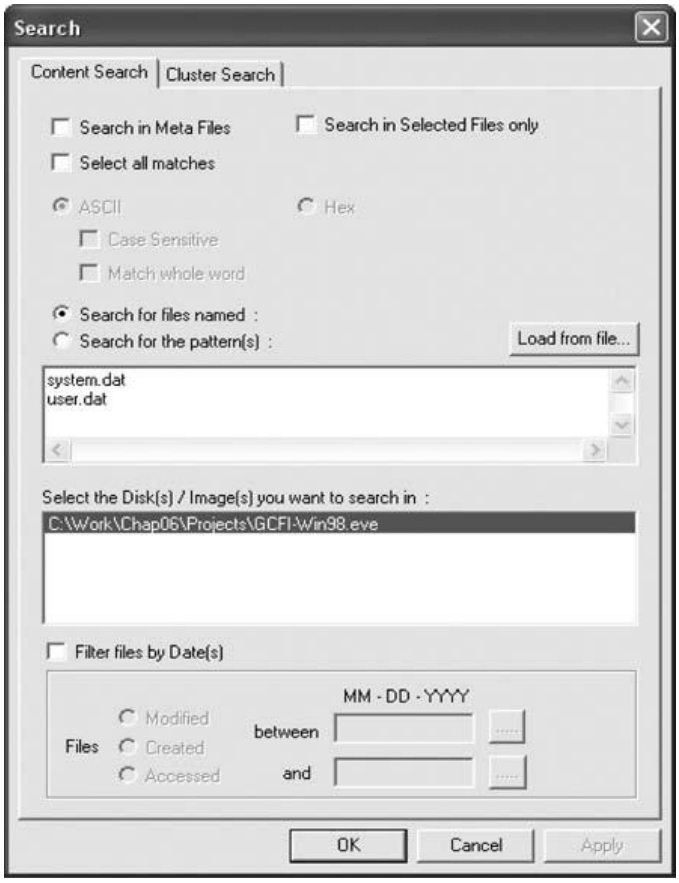

Figure 1 Searching for registry files

7. In the search results, click the check box next to the SYSTEM.DAT file. When the Add Comment dialog box opens, type **Registry files to extract**, click the **Apply to all items** check box, and then click **OK** (see Figure 2).

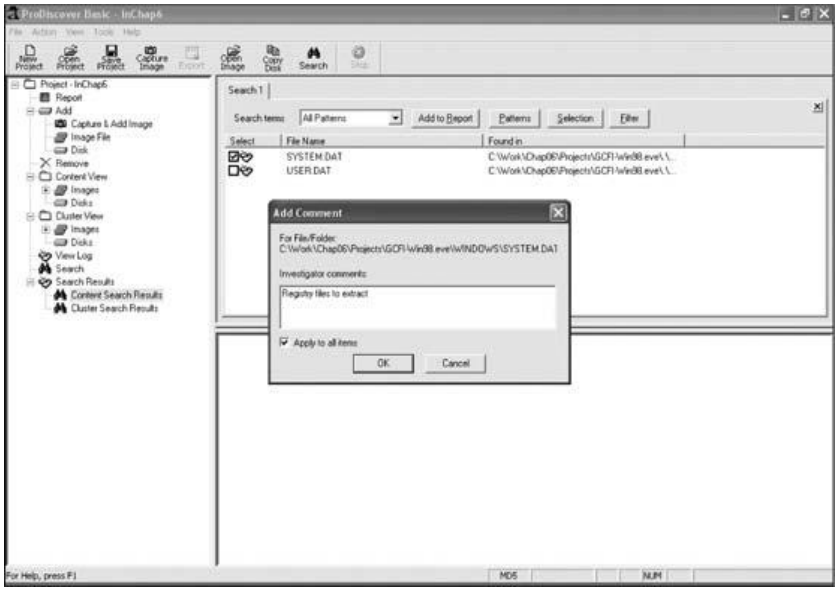

Figure 2 Selecting Files in the search results

8. Click the check box next to the USER.DAT file, and then click **Tools, Copy Selected Files** from the menu. In the Choose Destination dialog box, click **Browse**. In the Browse for Folder dialog box, navigate to and click your work folder, and then click **OK**. Click **OK** again in the Choose Destination dialog box.
9. Exit ProDiscover Basic, saving the project if prompted.

Task 3.2: To examine extracted Registry files using AccessData Registry Viewer

1. Start Notepad or another text editor.
2. Start Registry Viewer (operate in "Demo Mode")
3. In Registry Viewer's main window, click the **Open** toolbar button and navigate the location where you save your work for Task 3.1 **(…\GCFI-Win98.eve\Windows**). Click **USER.DAT** and then click **Open**.

> **Note: When ProDiscover extracts Registry files, it creates a subfolder with the image file's name and the suffix Recovered, followed by the folder path where the file was recovered. In the previous activity, the Registry files were originally located on the suspect's drive at C:\Windows. ProDiscover maintains this directory path prefaced by the image filename.

4. Click Edit, **Find** from the menu. In the Find dialog box, type **superior** in the Find what text box (see Figure 3), and then click **Find Next**.

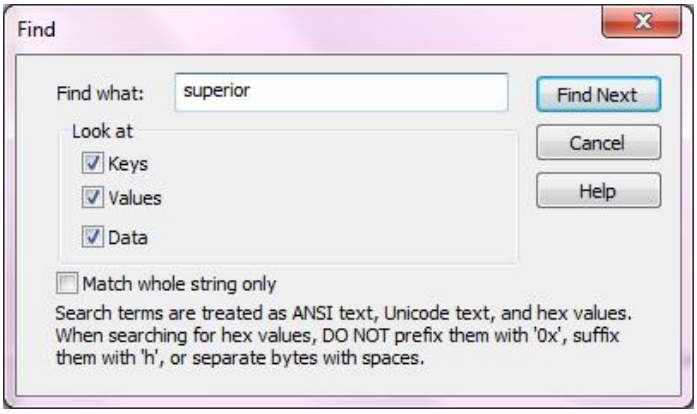

Figure 3 Entering a search term in Registry Viewer

5. When the search results are displayed, right-click the folder in the left pane containing the key and click **Copy Key Name** (see Figure 4). Paste it into Notepad.

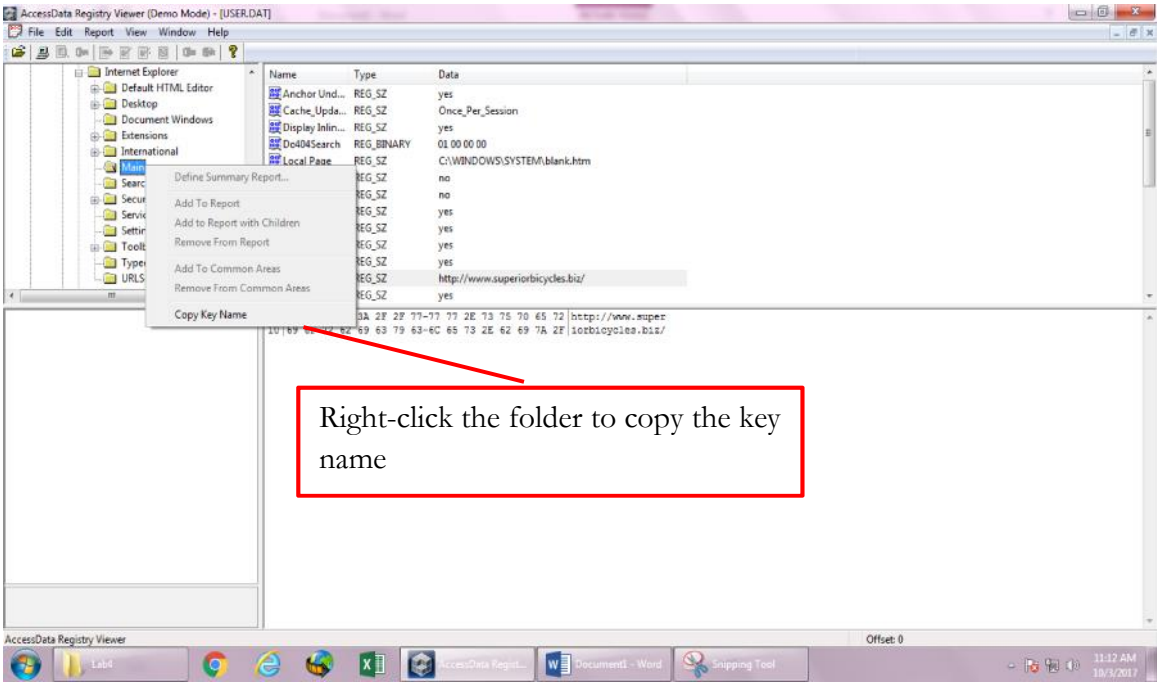

Figure 4 Copying a key name in Registry Viewer

6. Back in Registry Viewer, press **F3** to search for the next occurrence of the keyword "superior," and copy and paste the key name as before. Repeat this step until you find no more occurrences.
7. Click **USER.DAT** in the left pane, and then click **Edit, Find** from the menu again. This time, type **denise** in the Find what text box and click **Find Next**.
8. When the search results are displayed, right-click the folder in the left pane containing the key, click **Copy Key Name**, and paste it into Notepad. Press **F3** to search for the next occurrence of the keyword "denise," and copy and paste the key name as before. Repeat until no more occurrences are found.

9. Exit Registry Viewer by clicking **File**, **Exit** from the menu, and then clicking Yes in the Exit Registry Viewer dialog box.
10. Delete any redundant folder names in Notepad (refer to Figure 5), and save this text document as **InChap6-reg-search.txt**. Exit Notepad.

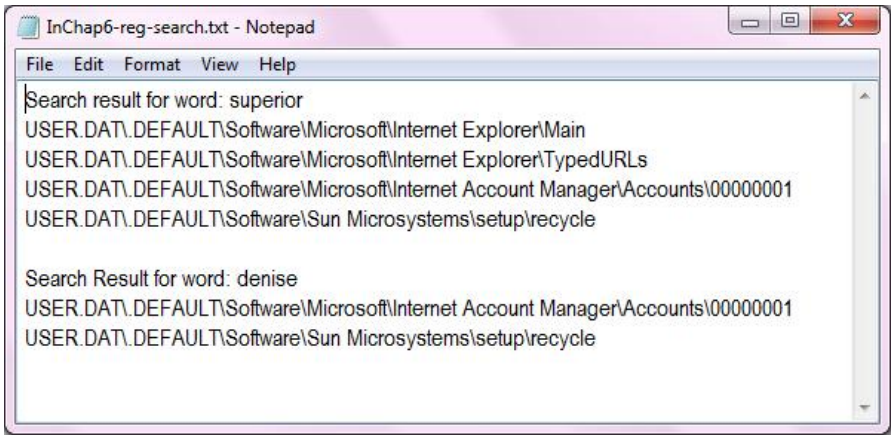

Figure 5 The search result showing paths for keys of interest

Task 4

For conduct forensics analysis, you must create bit-stream copies of the Windows registry of the computer you are investigating (other than the registry of the Windows you are using as a forensics workstation). Complete the following:

1. On a windows machine, can you copy the registry files you identified in Task 1? If you attempt to copy them, what do you observe?
2. Device a plan to create bit-stream copies of the registry files and make the bit-stream copies.
3. Save the bit-stream copies of the registry file in a folder. Name the folder using a meaningful name. Create a zip archive of the folder. Then generate a MD5 checksum for the zip archive.

Submission:

- A concise written report that explains each task.
  - Which computer is your workstation?
  - Did you complete the task? What evidence or test result do you have? What is the comparison results if you are asked?
- Beside the plan, upload the zip archive to ULearn at the end of the lab session.

Please Take Note:

a. Add your name and matric number at the top of your report
b. Plagiarism is strictly prohibited.
c. Late submission will be unaccepted