CSCE 4555/5555 – Computer Forensics

Lab 07 Project (Chapter 10)

VM Forensics, Live Acquisitions, and Network Forensics

Due: 11:59 PM on Tuesday, November 15, 2022

Student ID:11647576

Using a Live Acquisition Tool to Capture Evidence

You have used AccessData's Forensic Toolkit (FTK) Imager to image storage devices, provide preliminary forensic information, and analyze several file system partitions. However, FTK Imager can also be used to acquire the contents of virtual memory and the Windows registry. The virtual memory and Windows registry contain useful information that may be related to any computer crimes committed on that machine. For example, virtual memory holds data temporarily as the operating system processes instructions. Often information about recently attached devices such as physical storage devices, external storage devices, or computer hardware may be found in the registry.

1. Start **FTK Imager** on your workstation. If prompted to allow the program to make changes to your computer, click **OK** or **Yes**. When FTK Imager has finished loading, click the **File** tab, and click **Obtain Protected Files**.
2. In the Obtain System Files dialog box, click **Password recovery and all registry files** under the Options area. Click **Browse**, and navigate to your desired work folder in the Browse For Folder dialog box. Click **Make New Folder**, and type **Registry** in the edit name box. Click **OK**, and the path you created will be displayed in the Destination for obtained files box. Click **OK** in the Obtain System Files dialog box, and the registry files will be copied.
3. In Windows Explorer, find and open your Registry folder.
   a. What are the names of the two files in all capital letters? SAM, SECURITY
4. Click the **File** tab, and click **Capture Memory**. In the Memory Capture dialog box, click **Browse**, and navigate to your desired work folder in the Browse For Folder dialog box. Click **Make New Folder**, and type **RAM** in the Folder text box. Click **OK** to add the path in the Memory Capture dialog box, and click **Capture Memory**. This may take several minutes depending on the size of your installed RAM. When the Status indicates [100%] in the Memory Progress dialog box, click **Close**. This procedure is used to acquire the contents of the virtual memory or RAM.
5. In Windows Explorer, find and open your RAM folder.
   b. What is the file name extension of the virtual memory in your RAM folder? .mem
6. Click the **File** tab in FTK Imager, and select **Exit** to close FTK Imager. Be sure to close any open windows on your forensics Windows VM desktop.

7. These files will not be used for analysis, so once you have completed this activity, delete your Registry and RAM folders including all of their contents and be sure to empty the Recycle Bin to ensure there is enough space in the forensic Windows VM for others to work. We will use supplied files for the next part of the lab.

Unfortunately, none of the forensics tools available to us in this course can perform static analysis on virtual memory, but full-versioned forensics software such as FTK and OSForensics can process a virtual memory capture performed on a live computer as we did in the last activity.

Analyzing Windows Registry

The Windows registry controls the operating system environment, and it is the central repository for all information regarding users, passwords, connected devices, and physical hardware. The data contained in the registry can be searched for evidence using the Microsoft Regedit tool or forensics tools such as AccessData's Registry Viewer. The Registry Viewer tool provides much more information that Regedit when viewing areas that contain user account names and their unique identity attributes. Windows does not display user information in a naturally reliable fashion. Instead, every item listed in the registry that must be secure uses a 128-bit name called a globally unique ID (GUID). The GUIDs contain information that can be searched and linked to a particular user such as the last login or last storage device accessed. Therefore, information in the Windows registry can also reveal details regarding computer-related crimes. In this lab, you will examine registry hives (folders) for evidence using the Registry Viewer.

8. Download the **Registry.zip** file from Canvas into your desired work folder. *Note that this file is being supplied from the textbook, not the file that you obtained in the previous activity.*

9. Right-click the **Registry.zip** file located in your desired work folder and select **Extract All** from the context menu. Click **Extract** to unzip the compressed Registry folder, and close the window after the process completes.

10. Right-click the **AccessData Registry Viewer** application, and select **Run as administrator**.

11. Click **Yes** in the User Account Control dialog box. If no security device was found, click **No** to run Registry Viewer in demo mode. Click **OK** in the Registry Viewer dialog box warning that no dongle was found.

12. Then click the **File** tab and click **Open**. Navigate to your desired work folder and double-click the **Registry** folder.

13. Click the **SAM** file, and click **Open** in the dialog box.

14. Click the **+** symbol next to the SAM folder to expand it, and view the subfolders. Expand the **Domains**, **Account**, and **Users** folders to see the user account details.

15. Click the **000001F4** account registry key, and view the information on the Administrator account including the Last Logon Time. Note the details in the lower-left Key Properties window. The unique System Identifier (SID) is listed as 500, indicating that this is the Windows built-in account created when the operating system was installed.

    c. How many times did this user logon to this account? 8

    d. Is this account disabled? Yes

16. Click the **000001F5** folder, and note the SID unique identifier for the Guest account is 501. This also indicates that the Guest account is a built-in account created during the Windows installation. Both Administrator and Guest are built-in accounts.

    e. How many times has this account been used? 1

    f. Is this account disabled? false

    g. What is the last access date for this account? 04/28/2010 3:20:12 UTC

17. Click the **000003E8** folder. Note that the accounts with SID unique identifiers 1000 and higher were created by the administrator, and they are not built-in accounts. They belong to users who have accounts on the computer.

    h. What is the user name for this account? John Smith

    i. What is the SID (RID) unique identifier associated with this account? 1000

    j. What was the last time this user logged into the computer? 5/3/2010 17:19:37 UTC

18. Click on all of the user folders to answer the following questions.

    k. How many total users with accounts have never logged into this computer? 2

    l. Which users have never logged into this computer? Andrew and Willian Smith

19. Click the **File** tab, click **Close**, and click **Yes** in the Registry Viewer dialog box to clear the current registry file from the Registry Viewer.

20. Click the **File** tab, and select **Open**. Double-click the **system** registry hive to load it into the Registry Viewer.

21. Expand the **ControlSet001**, **Enum**, and **STORAGE** folders. Expand the **Volume** folder located below the STORAGE folder to see all the storage devices that have been or are currently attached to the computer. This section includes both external and internal storage devices. Drag the edges of the window if necessary to view all the information.

    m. How many total storage devices have been attached to this computer? 7

22. Expand the USBSTOR folder to reveal all the USB devices that have been or are currently attached to this computer. The entries here are only USB-type external storage devices. This information is useful for investigators looking for additional storage devices that may not be attached to the computer, but were at one time.

    n. How many USB storage devices have been connected to this computer? 6

    o. How many internal hard drives have been attached to this computer? 2

23. Click the **MountedDevices** folder. This subkey stores the database of mounted devices that matches the device to a given drive letter or volume.

    p. What is the maximum number of storage devices that have been attached to this computer at one time? 12

24. Click the **File** tab, and select **Exit**. Click **Yes** in the Registry Viewer dialog box to close the program.

You are to submit this document, with your solutions, to the **Lab 07** dropbox on Canvas by the due date and time.