DIGITAL FORENSICS LAB SERIES

Lab 13: User Profiles and the Windows Registry

(DF7774)

Document Version: 2014-02-07 (Beta)

Organization: Moraine Valley Community College
Authors: Jesse Varsalone and Kevin Vaccaro

The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

Contents

Introduction 3
Objective: Explain the purpose of Registry editing 3
Lab Topology 4
Lab Settings 5
1 Obtaining a Live Windows XP Registry 6
1.1 Using FTK® Imager 6
1.2 Conclusion 10
1.3 Discussion Questions 10
2 Analyzing the Registry Hives using RegViewer 11
2.1 Examining a User's Profile 11
2.2 Tracking a User's Behavior 16
2.3 Exploring the SAM file 21
2.4 Exploring the System Registry Hive 25
2.5 Examining the SECURITY Hive 30
2.6 Exploring the Software Hive 33
2.7 Conclusion 36
2.8 Discussion Questions 36
3 Analyzing the Registry Hives using RegRipper 37
3.1 Using RegRipper 37
3.2 Conclusion 40
3.3 Discussion Questions 40
References 41

Introduction

This lab is part of a series of lab exercises intended to support courseware for Forensics training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, the student will capture the registry hives of the Windows operating system using a free, commercial tool called FTK Imager. Students will then analyze the registry hives using two open source tools, RegRipper and RegViewer.

This lab includes the following tasks:

1. Capturing a live Windows XP registry
2. Analyzing the registry hives using RegViewer
3. Analyzing the registry hives using Regripper

Objective: Explain the purpose of Registry editing

The Windows registry contains all of the settings for a system. Everything from the application software that is installed to usernames and passwords are tracked in the registry. The devices that are connected to the system, connections to networks, and browser history are just a few of the many settings that the registry keeps track of.

Windows incorporates a tool called regedit (registry editor) to allow an administrator to directly change the settings within the registry. However, the regedit tool does not allow detailed analysis of the registry because it masks important information--even the administrator of the system is limited. Open source tools go beyond the capabilities of the utilities included within the Windows environment. In this lab, we will take a look at the information that can be gathered from the registry hives in the Windows XP registry. Information can be gathered manually as well as automatically.

FTK Imager – FTK Imager allows you to image a disk or a logical drive.

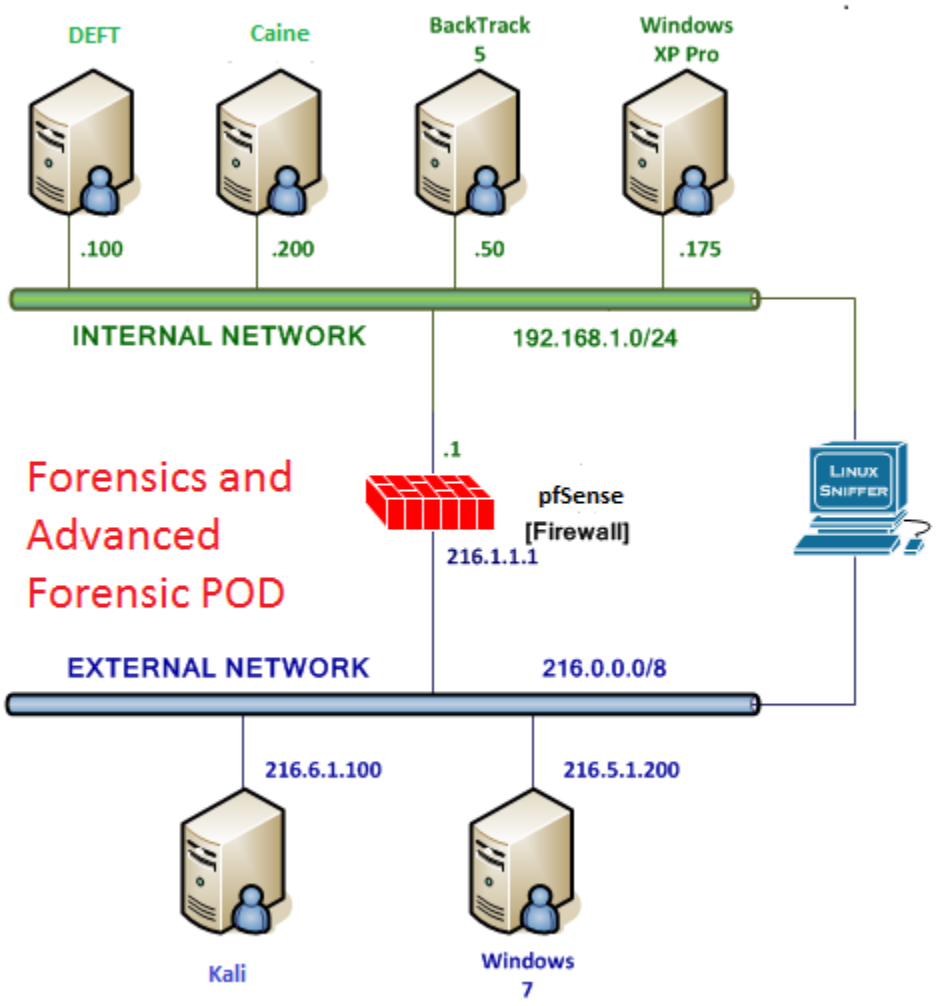
RegViewer – a registry analysis tool that can open Windows Registry files. The free tool can be downloaded from this link: http://www.gaijin.at/en/getitpage.php?id=regview

RegRipper – a tool that extracts and analyzes registry information.

Regedit – A built in program that for viewing registry keys on the Windows operating system

Windows Registry – A database that contains user and computer settings for a Windows OS.

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Windows XP Pro Internal Machine	192.168.1.175		

1 Obtaining a Live Windows XP Registry

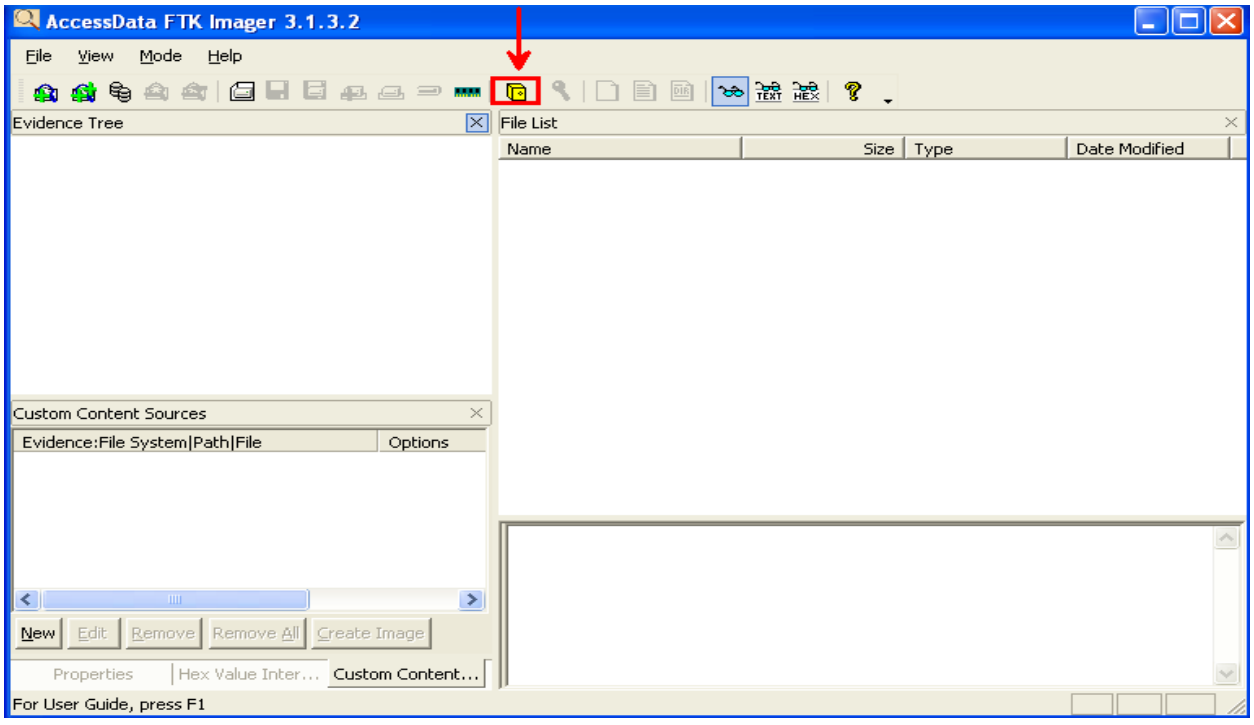
The first task is to obtain a copy of the Windows registry from the system that is running Windows XP and is using the registry to provide the system environment. This method gives you a snapshot of the current registry state.

1.1 Using FTK® Imager

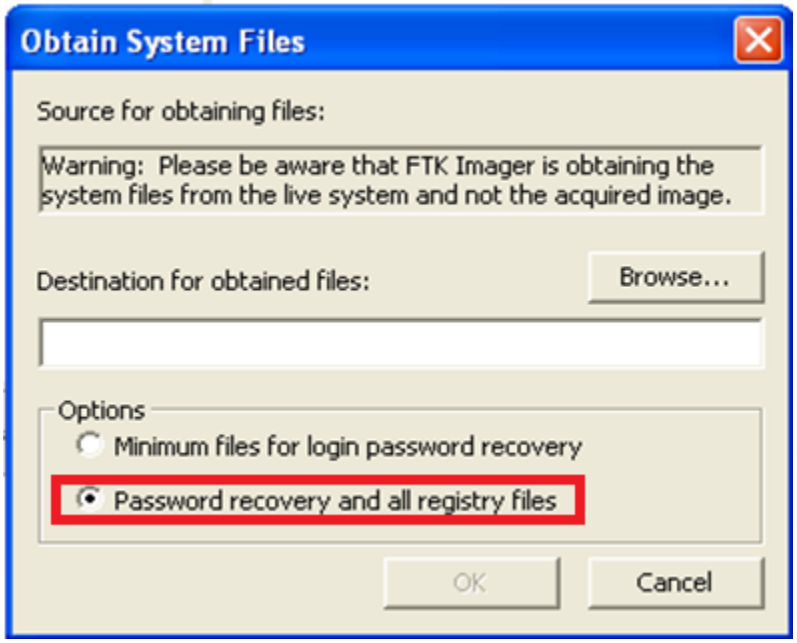
FTK® Imager is installed on the Windows XP Professional machine.

1. Open FTK® Imager by double-clicking the shortcut on the desktop.

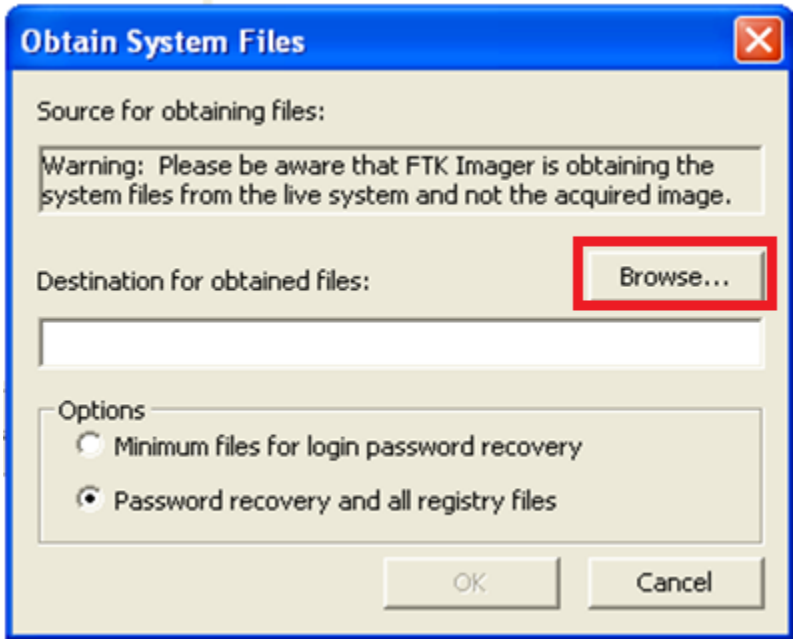
2. Click the Golden locker icon on the FTK® toolbar to obtain the system registry files.



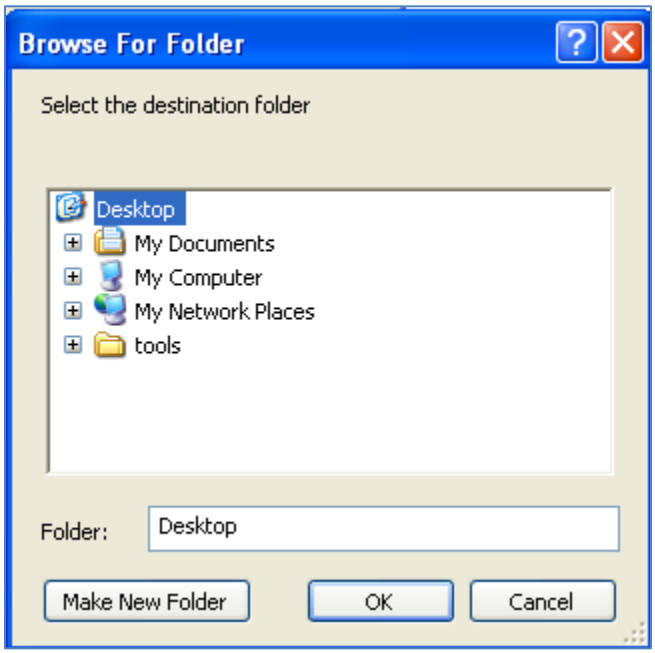
3. At the Obtain System Files screen, choose the **Password Recovery and all registry files** option (To obtain a full registry including the NTUSER.dat file). The **Minimum files for password recovery** will only provide access to the SAM and Security hives.



4. To choose the destination for the obtained files, click the **Browse** button.

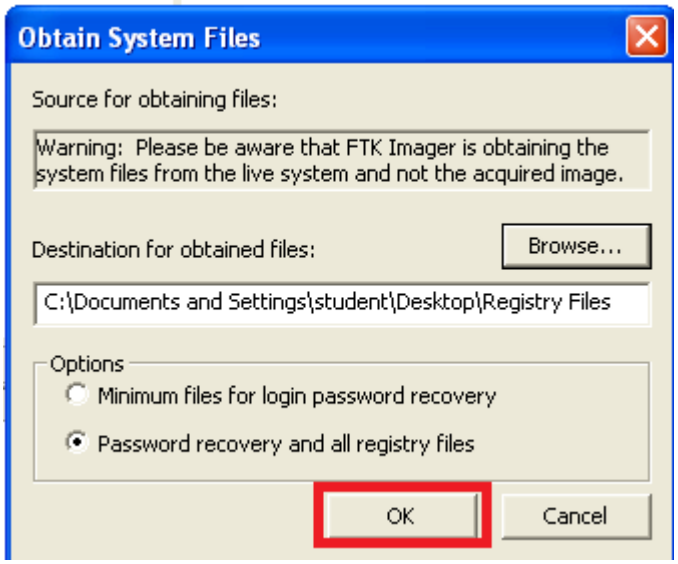


5. Select the **Desktop** from the browser window.

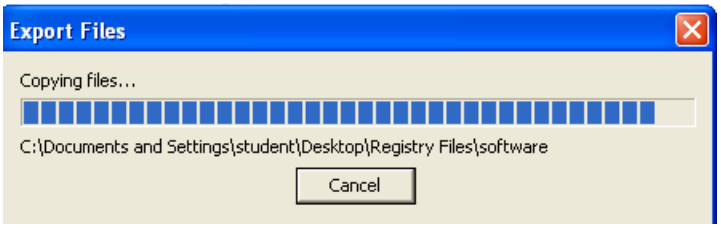


6. Click **Make New Folder** and name the folder **Registry Files**. Click OK.

7. Click **OK** again to capture the registry files.

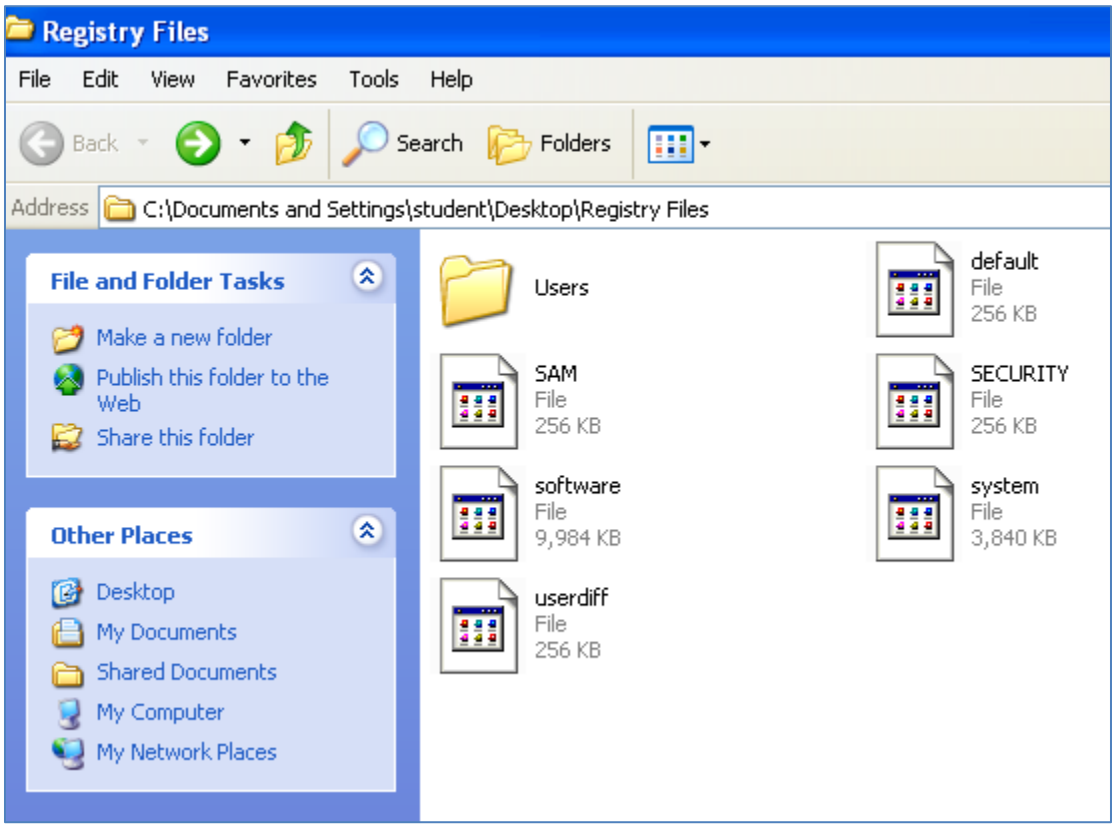


8. FTK imager will provide you with a status bar indicating the export progress.



9. Close FTK Imager by clicking the red X in the top-right corner of the program.

10. Open the **Registry Files** folder on the desktop. There are 6 registry files and a folder.



1.2 Conclusion

Each registry key holds information we can explore about the computer. In the **Users** folder, all users on the machine and their profiles are captured. Within each of the users' profiles, there is a file, NTUSER.dat. The NTUSER.dat file provides information about a user.

1.3 Discussion Questions

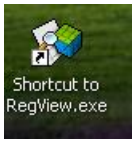
1. What are the names of the main registry files?
2. Where are the registry files located on a Windows machine?
3. What does each registry file contain?
4. What button is used to export the Registry files within FTK Imager?

2 Analyzing the Registry Hives using RegViewer

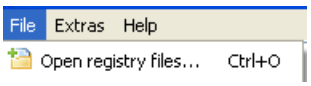
Registry Viewer opens Windows Registry files in a file structure that is similar to the regedit tool. Folders, keys, and values can all be searched for information. The free tool can be downloaded from this link: http://www.gaijin.at/en/getitpage.php?id=regview

2.1 Examining a User's Profile

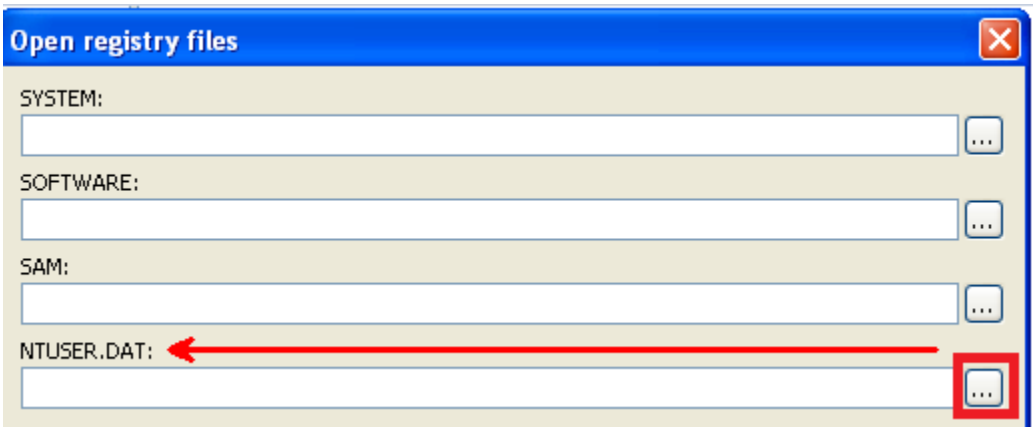
1. Double-click the **RegView** shortcut icon on the desktop.



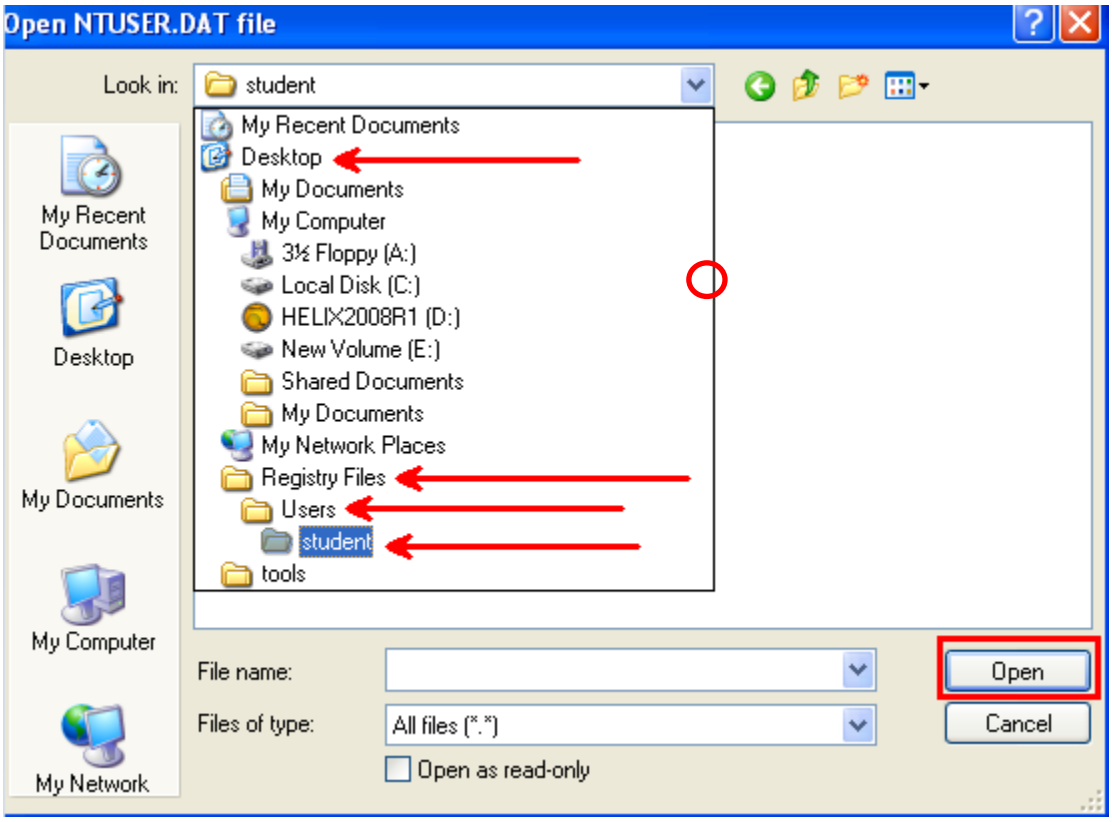
2. To examine a user's profile, select **File > Open registry files.**



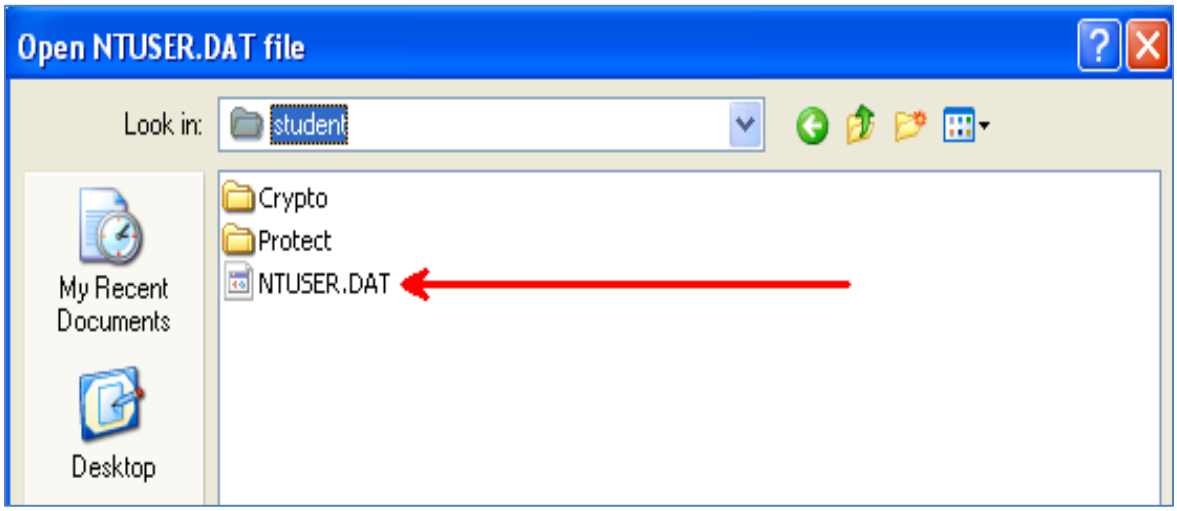
3. In the Open registry files box, click on the browse icon for **NTUSER.DAT.**



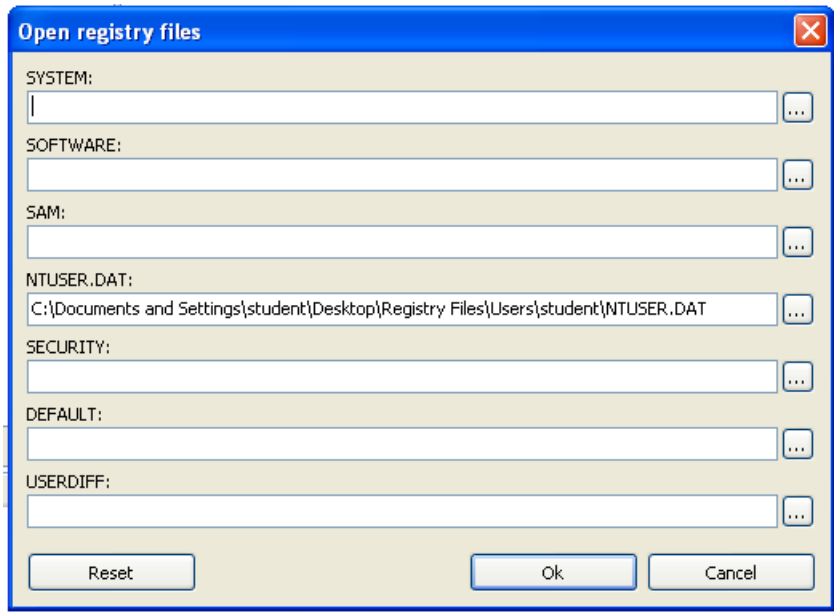
4. Select **Desktop > Registry files.** Double-click on the **Users** folder and select **student**.



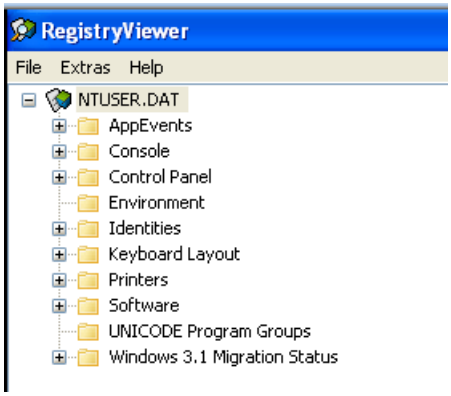
5. Within the **student** folder, select the **NTUSER.DAT** file and click **Open**.



6. The path of the file appears under the NTUSER.DAT heading. Click **OK**.

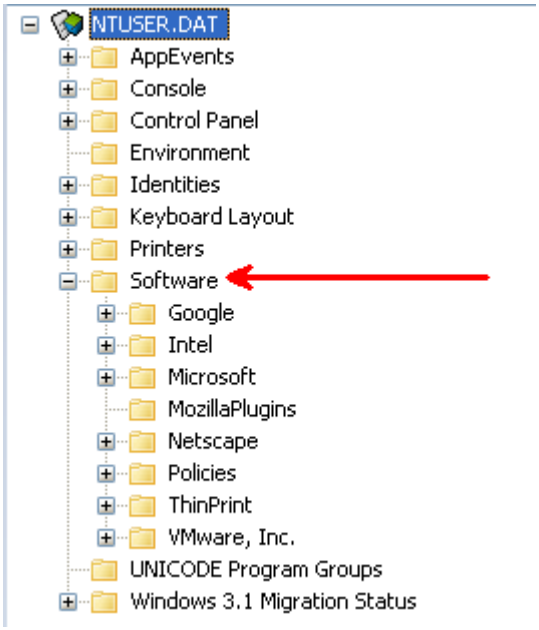


7. You are now examining the user's profile on the machine. This view is not normally seen on a running machine. We will look at some common artifacts in this user's profile.

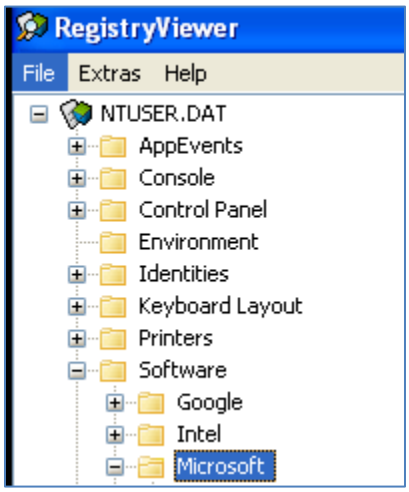


8. We will start with any URLs that the user browsed to in Internet Explorer. Click on the **+** symbol next to the **Software** folder.

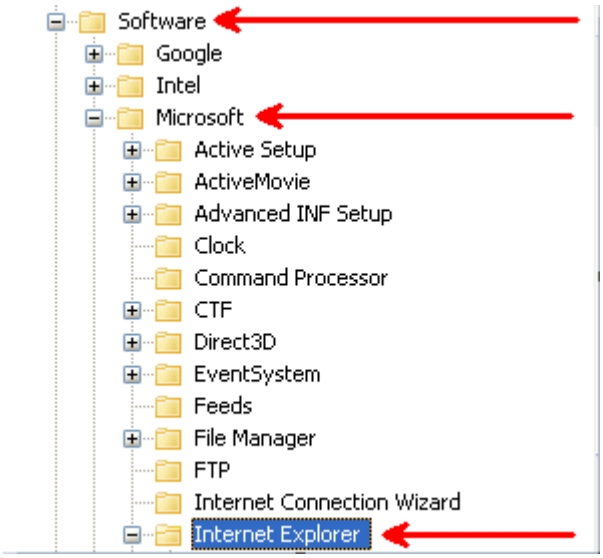
Be aware that the Window's registry does ***not*** track Firefox or Chrome browsing history.



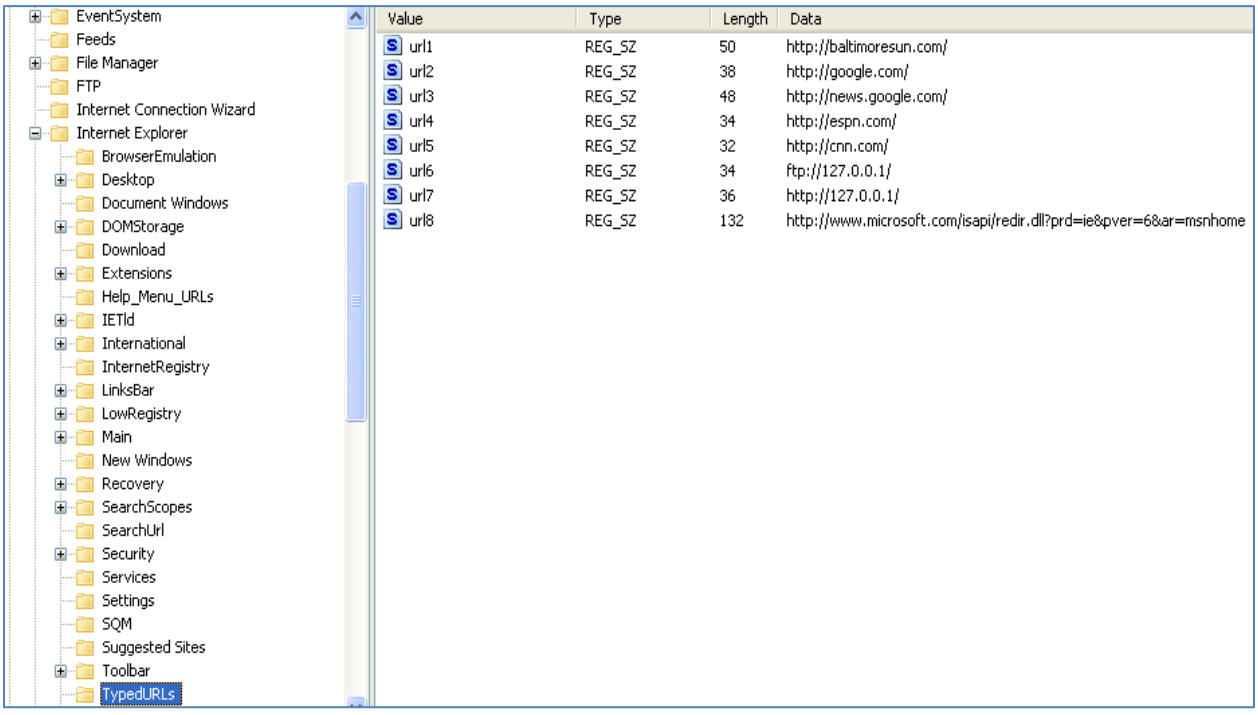
9. Start to drill down by clicking the **+** symbol for **Microsoft**.



10. Next, under the category of Software, expand **Internet Explorer.**



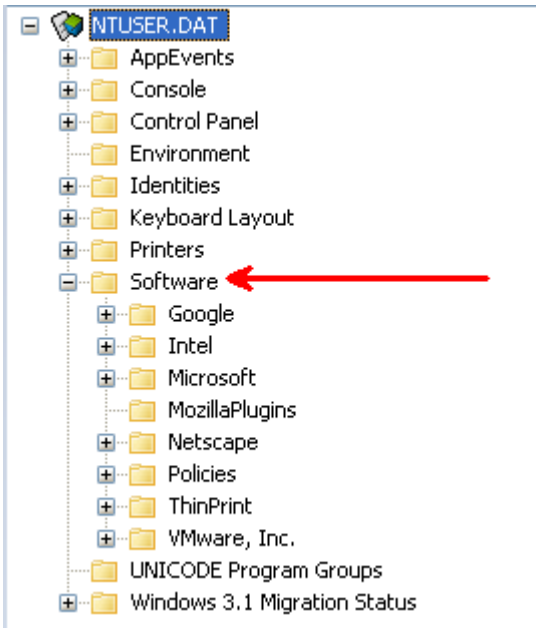
11. Next, expand **TypedURLs** under **Internet Explorer.** This user has typed 8 URLs into the Internet Explorer URL bar. The registry records up to 25 entries with the latest URL appearing at the top of the list.



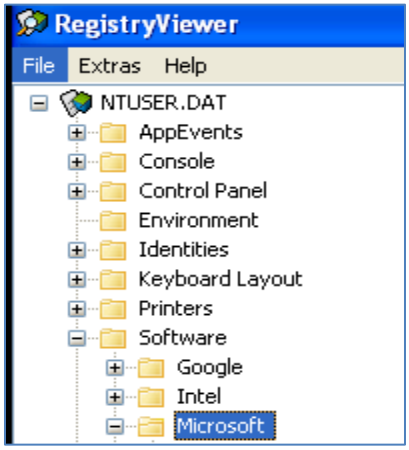
2.2 Tracking a User's Behavior

To track whether a user has used the **Open** and **Save As** dialog boxes for Windows utilities, look at the **Most Recently Used (MRU)** value in the ComDLG32 (Common Dialog).

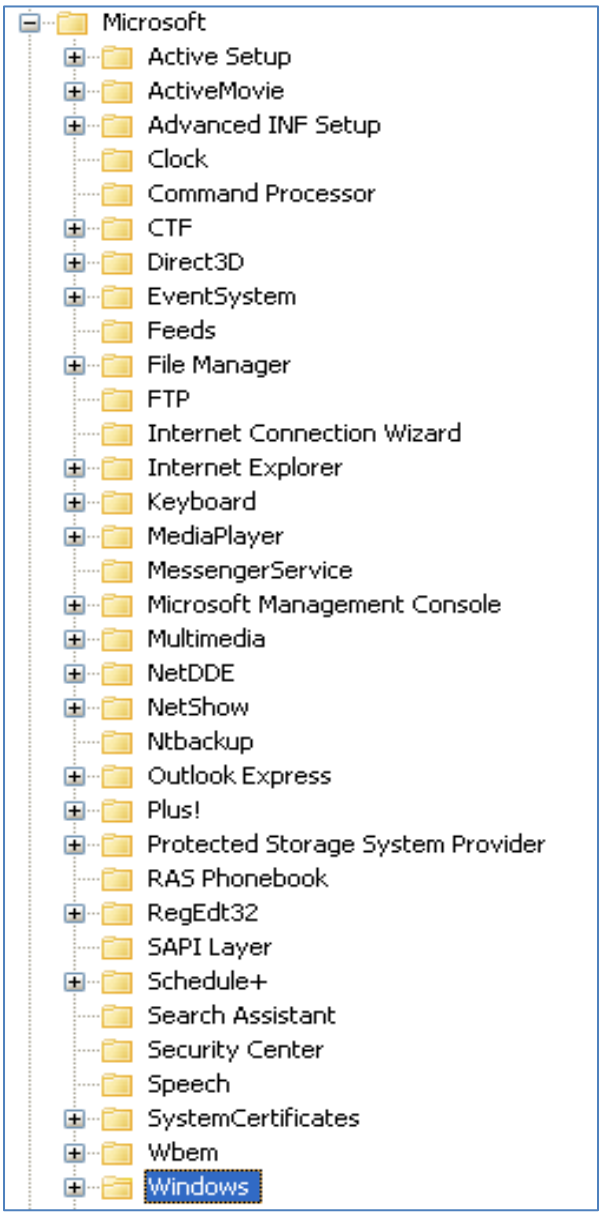
1. Expand the following: Click on the **+** symbol next to the **Software** folder.



2. Start to drill down by clicking the **+** symbol for **Microsoft**.

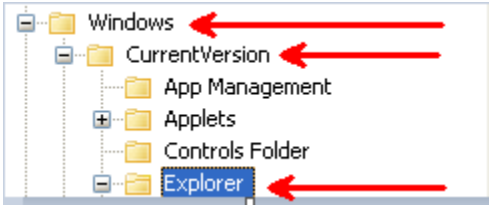


3. Next, expand **Windows.**

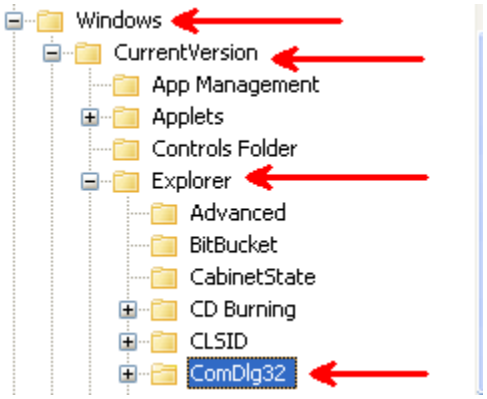


4. Under the Windows folder, expand the CurrentVersion folder.

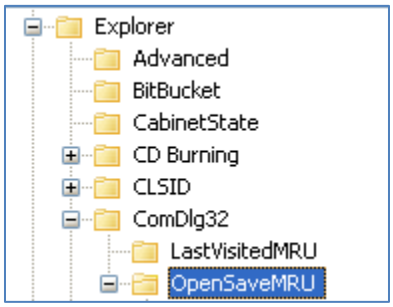
5. Under the **CurrentVersion** folder, expand the **Explorer** folder.



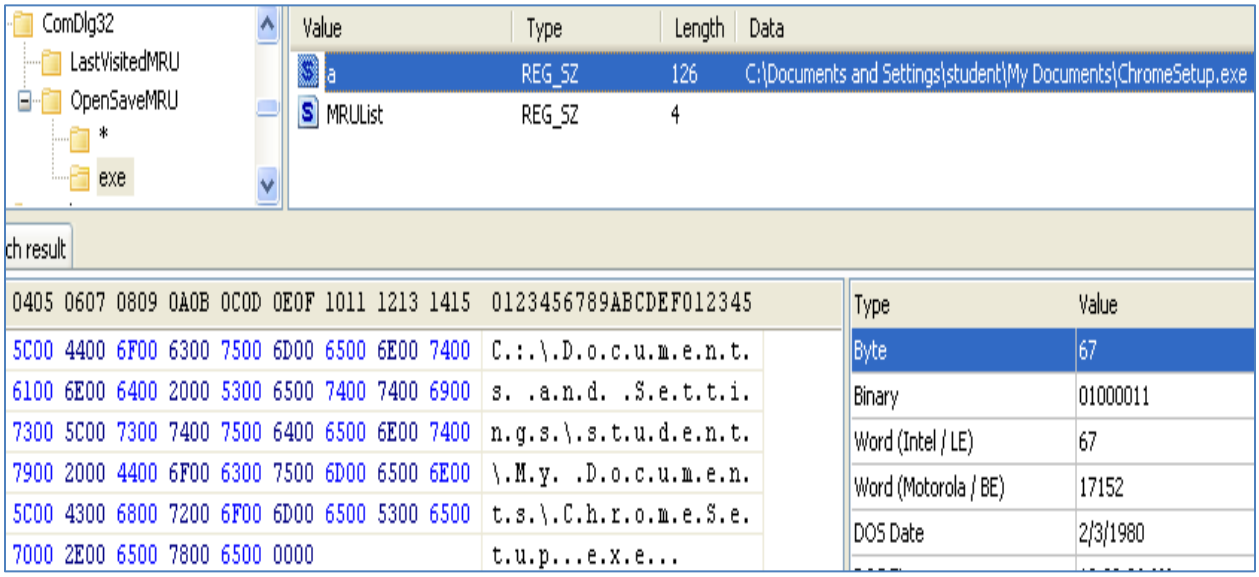
6. Under the **Explorer** folder, expand the **ComDLG32** folder.



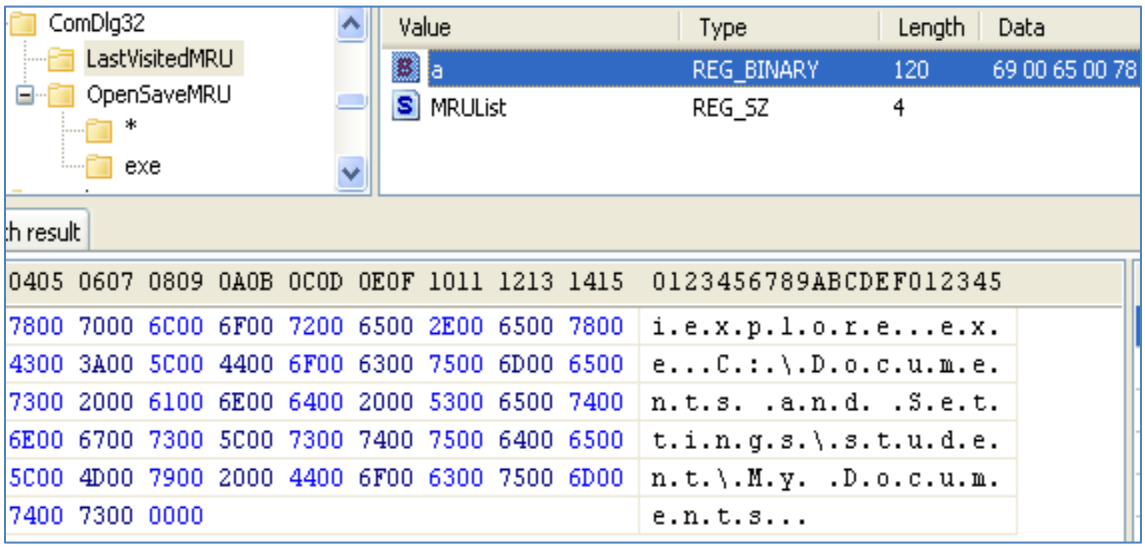
7. Under the ComDLG folder, expand the OpenSaveMRU folder.



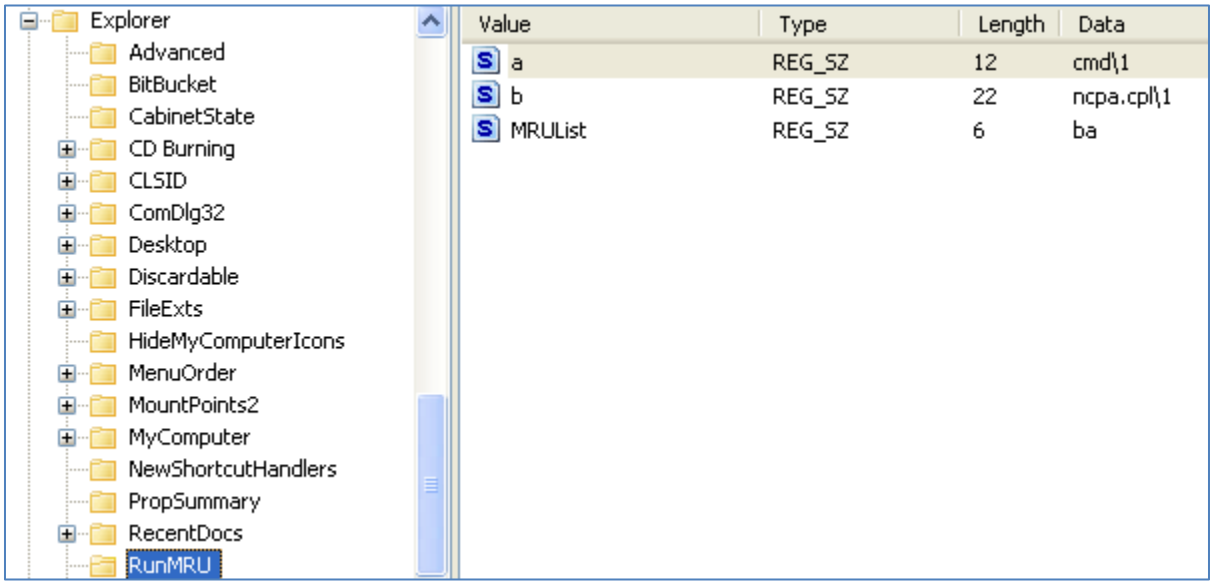
8. Under OpenSaveMRU folder, expand exe. Under exe, highlight **a** on the right to show the last open the user performed. This shows that the last open and save action that the user performed was a download of ChromeSetup.exe



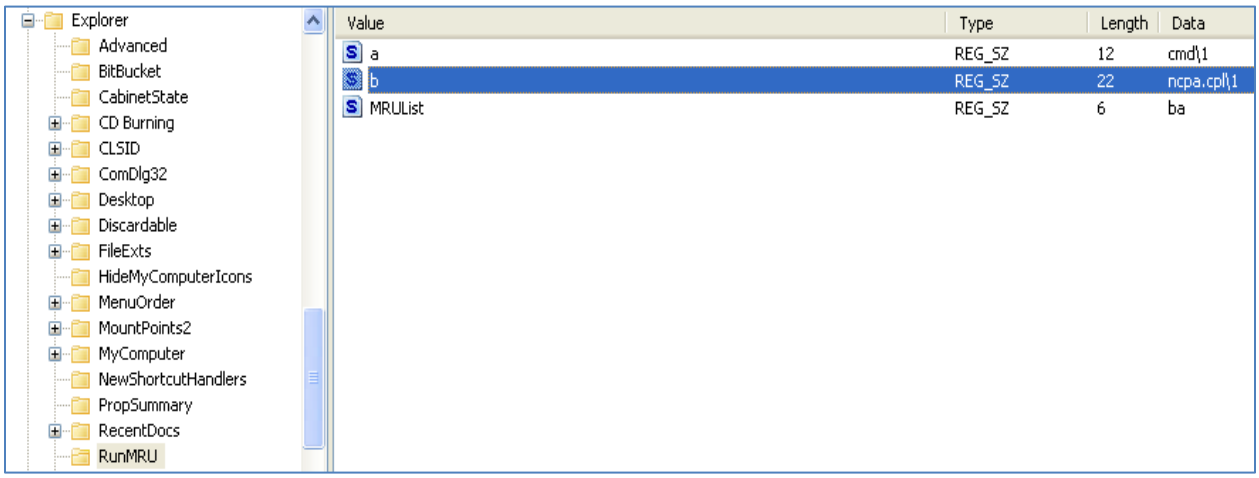
9. Under the ComDLG folder, expand the LastVistedMRU folder. Highlight **a** on the right to show the program used to download of ChromeSetup.exe (OpenSaveMRU).



10. Under the Explorer folder, expand the RunMRU folder. To examine the last command run from the **Start > Run** dialog box, look at the data value for **a**. The command **cmd.exe** was the last command entered in the **Start > Run** dialog box.



11. Highlight **b**. The ncpa.cpl command, which opens the network connections dialogue box, was also run on the system. This registry key tracks up to 26 entries.

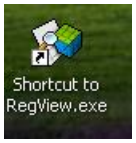


12. Close the Registry Viewer program so the information from NTUSER.dat will be cleared.

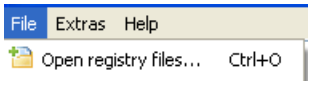
2.3 Exploring the SAM file

The SAM Registry file holds all the account information for the users of the computer.

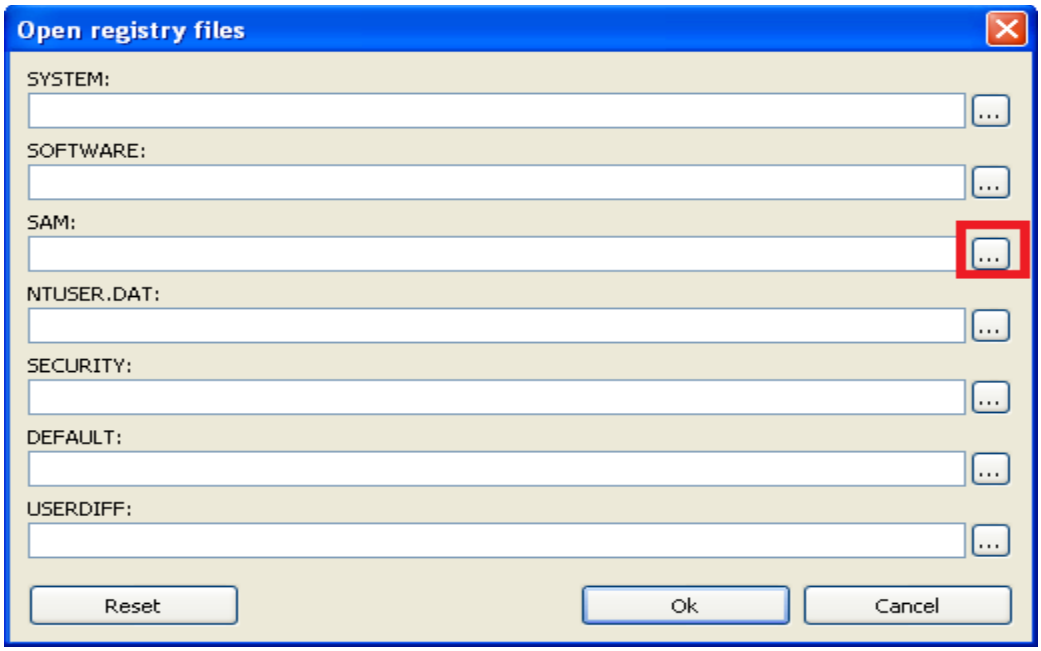
1. Double-click the **RegView** shortcut icon on the desktop.



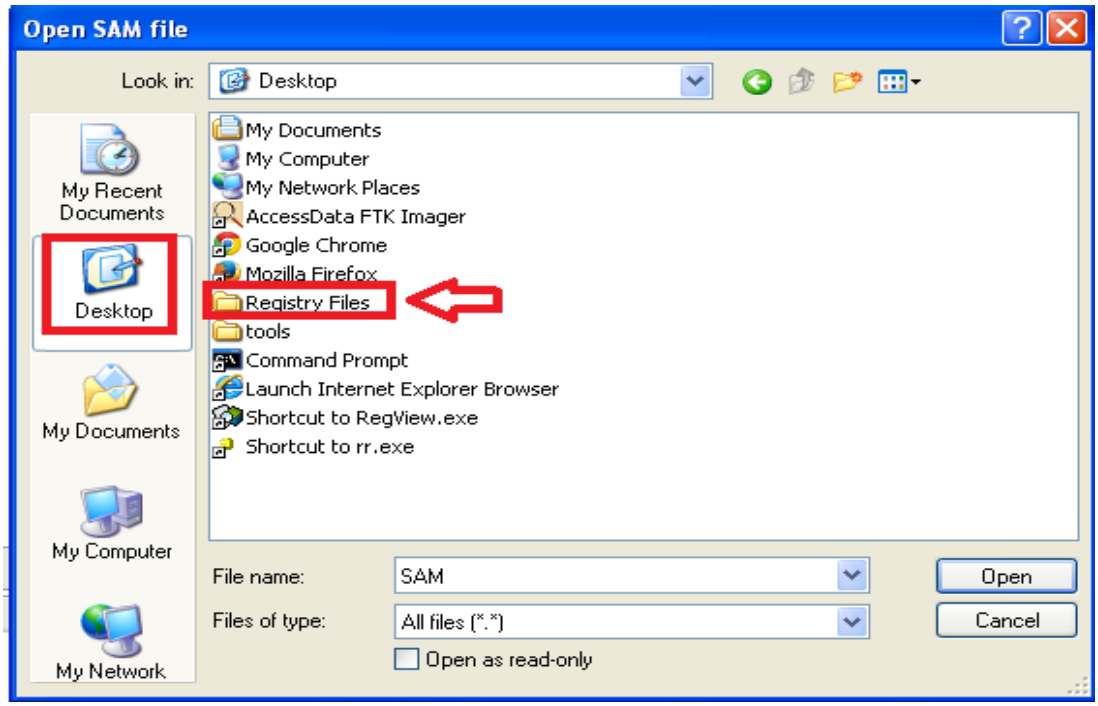
2. To examine a user's profile, select **File > Open registry files.**



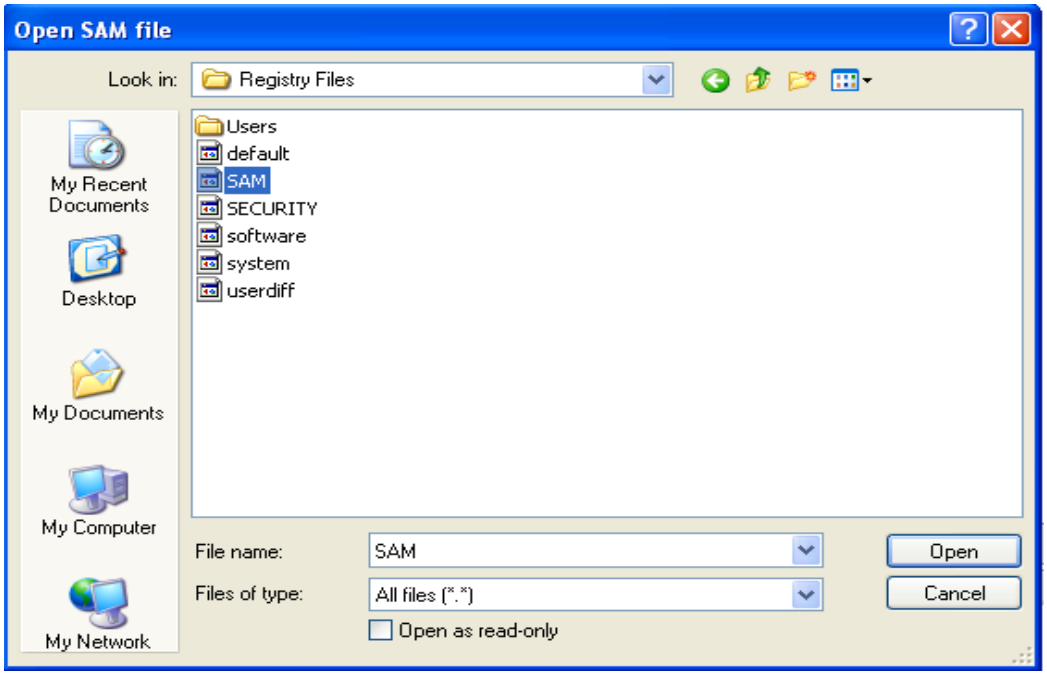
3. In the Open registry files box, click on the browse icon for SAM



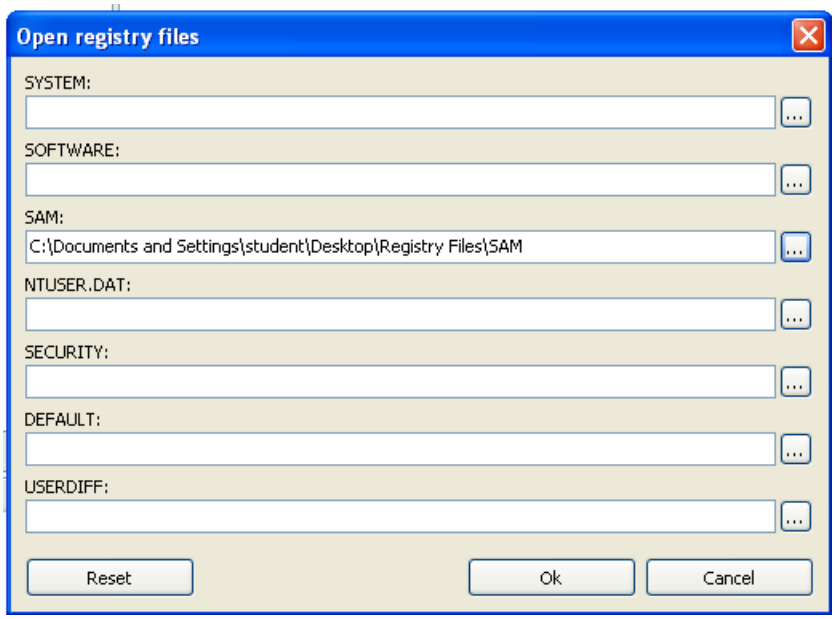
4. Browse to the **Registry Files** folder on the Desktop.



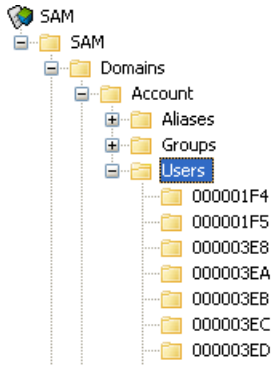
5. Double-click on the **SAM** file to open the file in Registry Viewer.



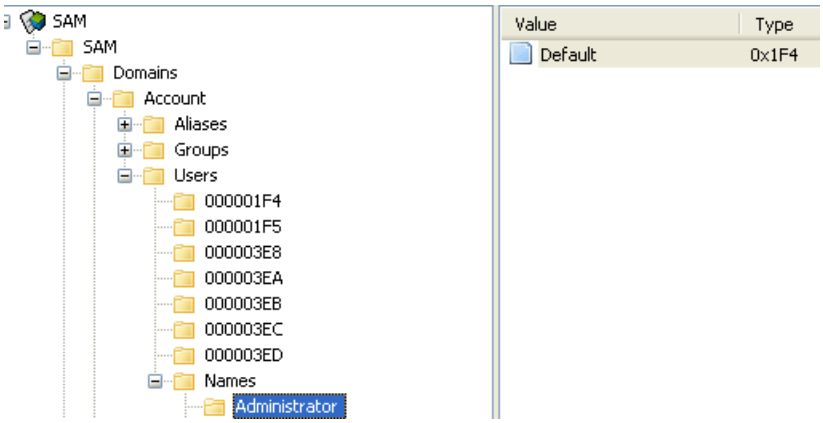
6. Examine the full path to the SAM file and click OK to open the file.



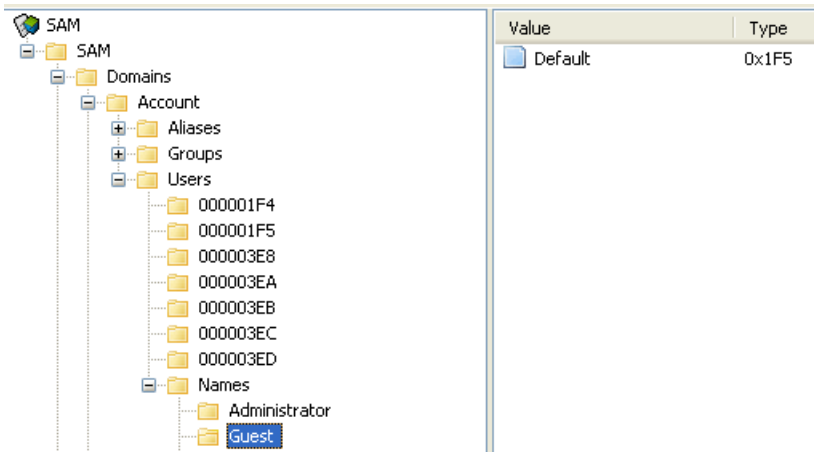
7. Expand the **+** sign next to **Domains** and drill down to **Account > Users > Names**. Both the Relative Identifier (RID), a unique, sequential value assigned by Windows to each account, and the user name is shown. If an account is deleted, there is a gap in numbering. The system does not reuse RID values. The first RID value is **000001F4**.



8. The hex value 000001F4 equals 500 in decimal. This is the default RID, or Relative Identifier, value for the Administrator account. The Administrator account always has a value of 500.



9. The next hex value is 000001F5, which equals 501 in decimal and is the Guest account. User accounts begin with 000003.



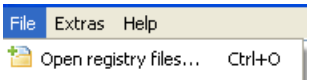
13. HelpAssistant is the first user account and has a hex value of 000003E8 (1000 is the decimal equivalent). Follow the sequence of user accounts created. If an account were deleted, there would be a missing number. Notice you can find the RID value at offset 48-49 and it is in little endian. The least significant bit is first, so F401 is read as 01F4.
14. Close the RegView program.

2.4 Exploring the System Registry Hive

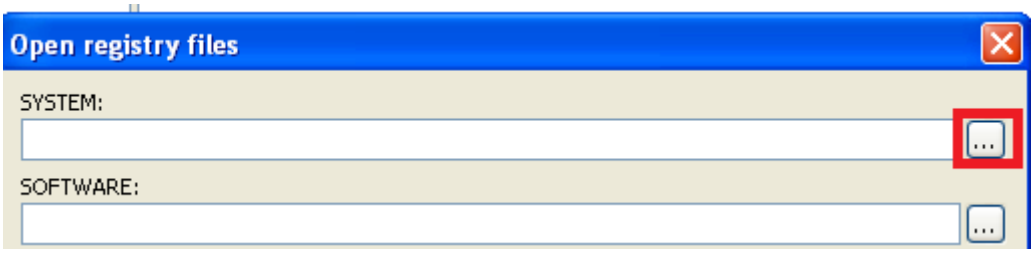
The System registry hive holds all of the computer startup parameters, device driver configurations, OS behavior, and hardware configurations.

1. Double-click the **RegView** shortcut icon on the desktop.

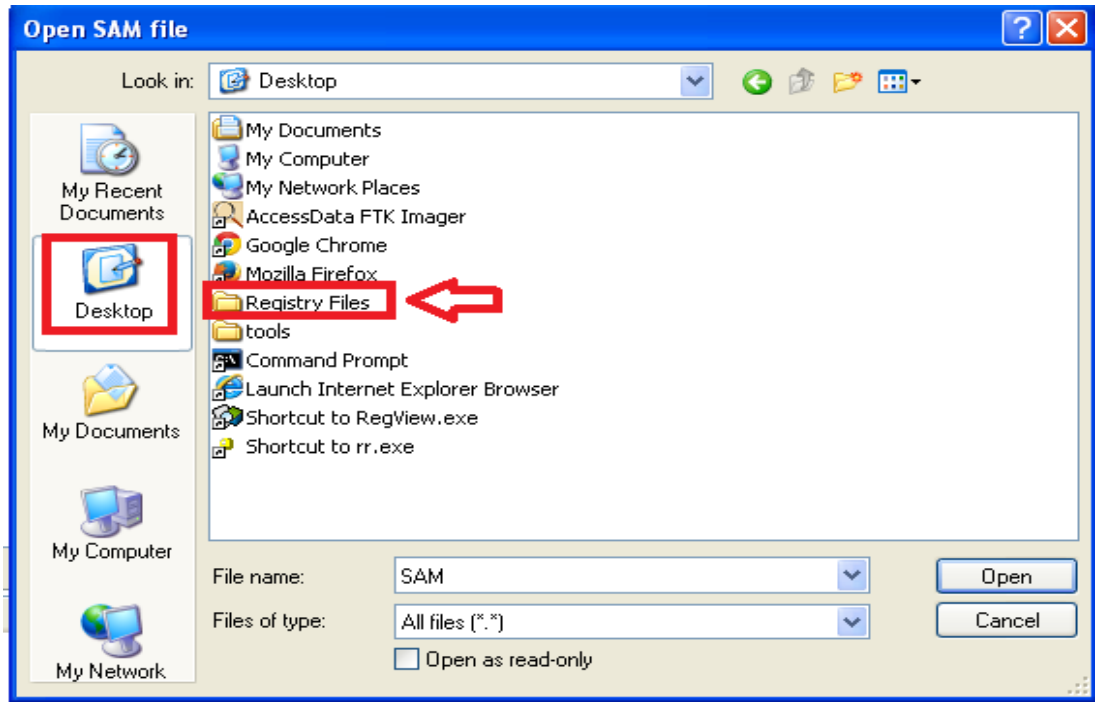
2. To examine a user's profile, select **File > Open registry files.**



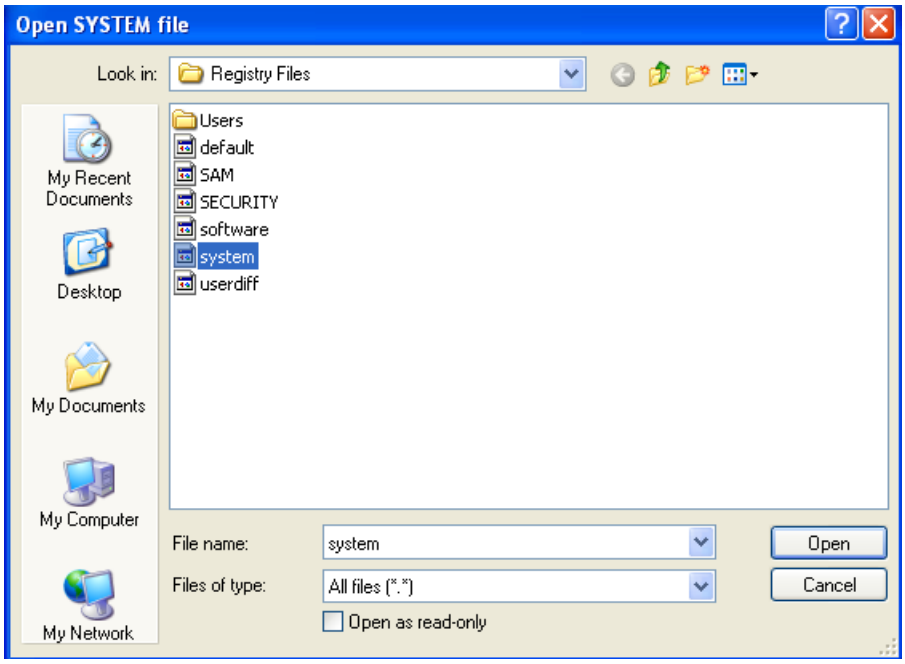
3. In the Open registry files box, click on the browse icon for SYSTEM.



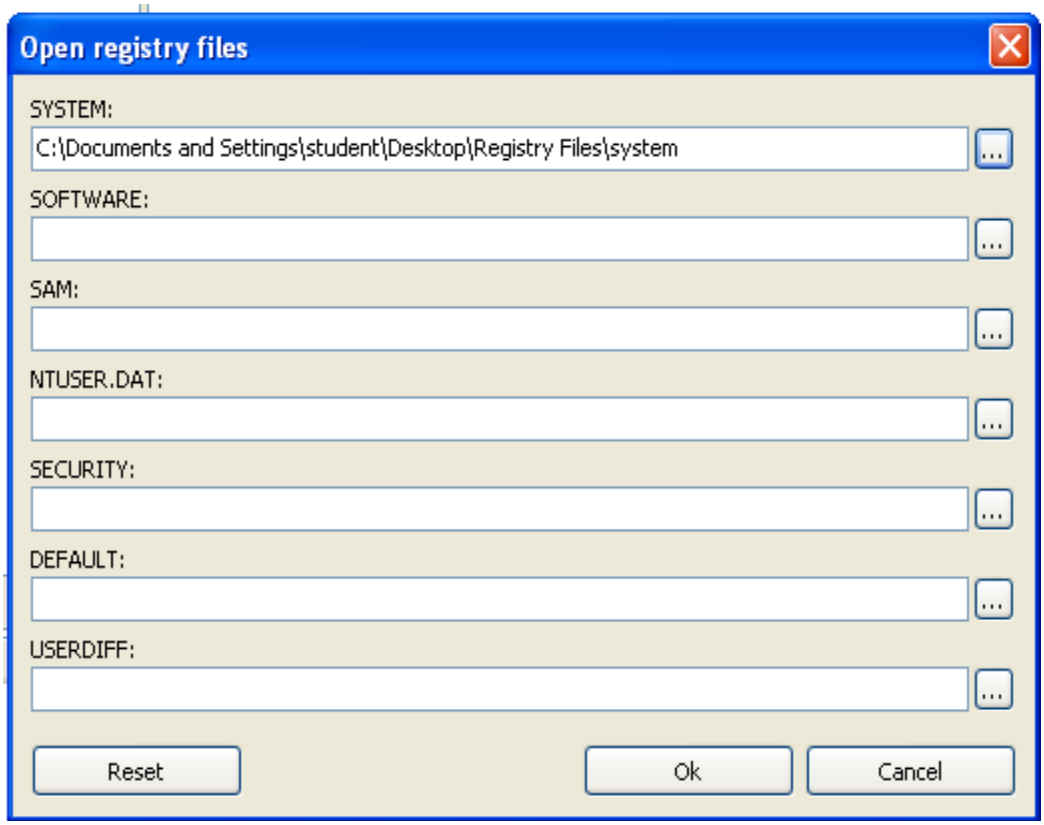
4. Browse to the **Registry Files** folder on the Desktop.



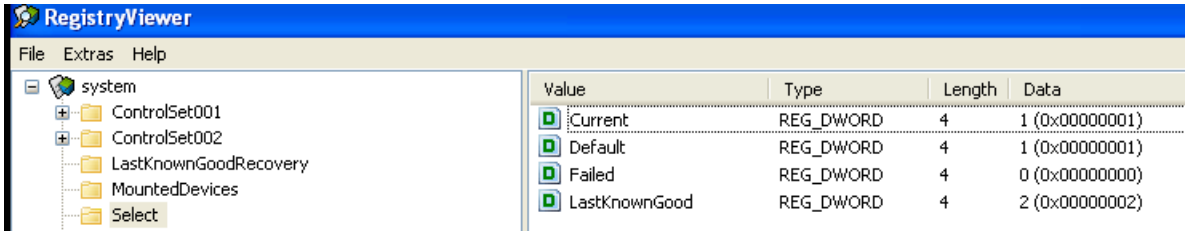
5. Double-click on the **system** file to open the file in Registry Viewer.



6. Examine the full path to the SYSTEM file and click Ok to open the file.

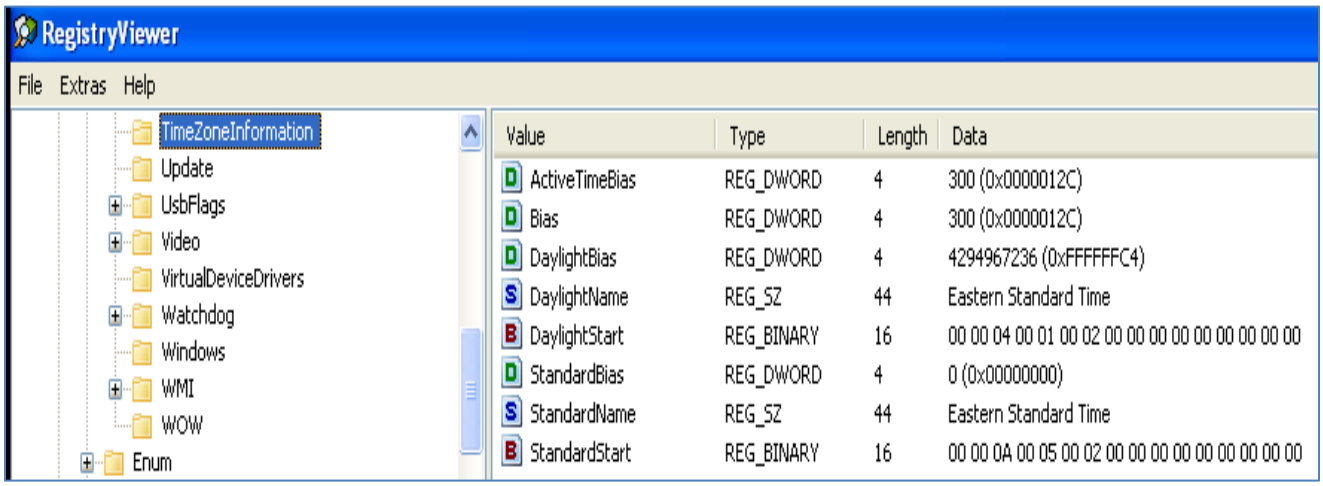


7. Choose the **Select** folder located under system. View the entry for Current in the right pane, which will show the control set that was active when the machine was running and the registry was captured. The value of one for **Current** indicates that **ControlSet001** was the active configuration.

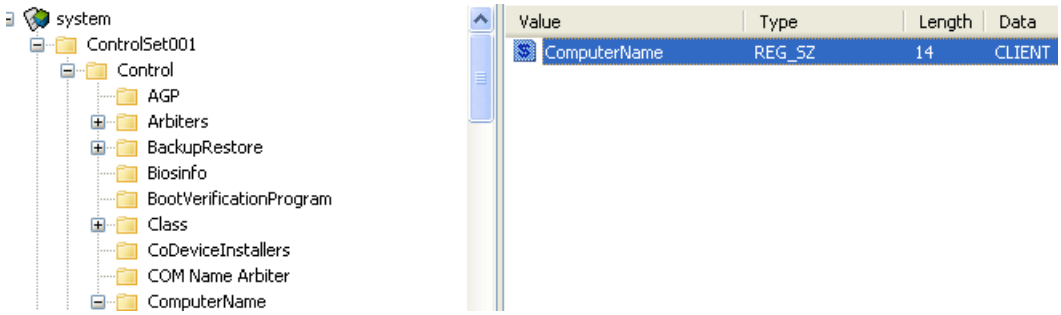


8. Under CurrentControlSet01, Click the **+** sign next to the **Control** and navigate down to **TimeZoneInformation**. This machine was set to **Eastern Standard Time** with a Bias value of 300. Bias measures the difference in minutes from Coordinated Universal Time, or UTC time. In this case, the Bias is 300 minutes or +5 hours. Therefore, the time is UTC +5. Time zone information can be critical in computer forensic cases, since the investigator will often establish a timeline of events.

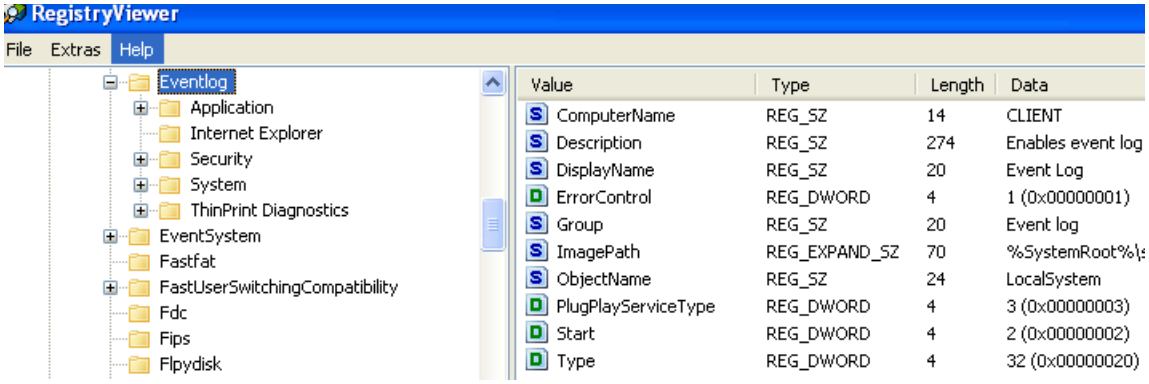
The current time zone for the machine is a very important value to capture, in order to determine the time zone the machine was set to use.



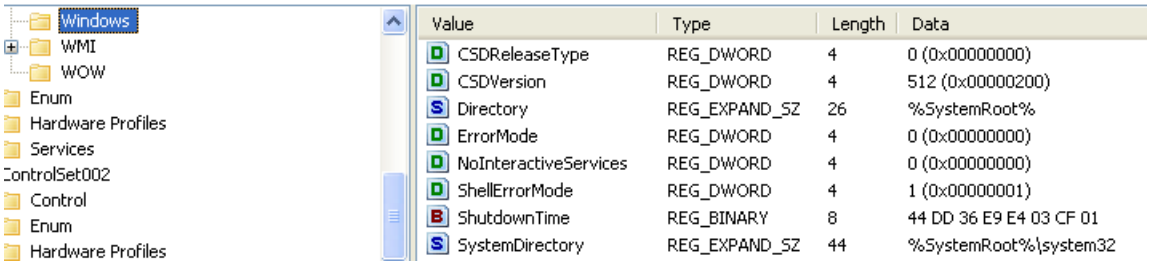
9. For ControlSet001, drill down through **Control > ComputerName > ComputerName** to identify the system's Computer Name.



10. A second location to find the computer name on a Windows XP machine is **CurrentControlSet01\Services\Eventlog\ComputerName.**

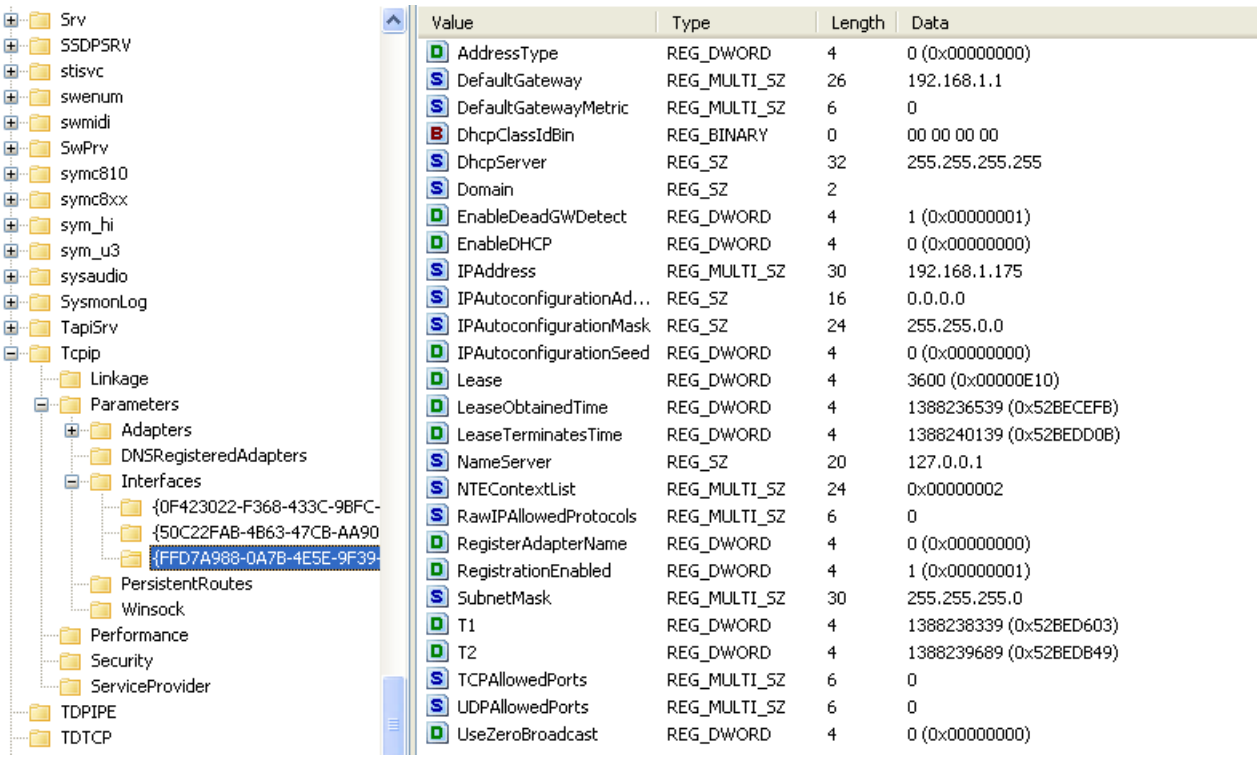


11. Find out when the machine was last shutdown by expanding CurrentControlSet01\Control\Windows. The Shutdown Time value is a 64-bit value that is interpreted in the lower part of Registry Viewer as UTC time.



12. To view the devices that were mounted on the machine, select **MountedDevices**. The standard drive letters, A, C, and D, and the volume headers for each are displayed.

13. To find out how the machine is configured for TCP/IP, go to **CurrentControlSet01 > Services > Tcpip > Parameters > Interfaces.** Look through each interface for any network data.

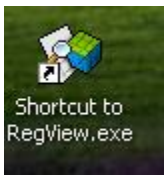


14. Close the RegistryViewer program so the SYSTEM Registry file is no longer displayed.

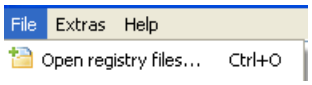
2.5 Examining the SECURITY Hive

The SECURITY hive stores local security policies including User rights, password policy, user account memberships, a link to the SAM file for updates, and a user interface through User Manager.

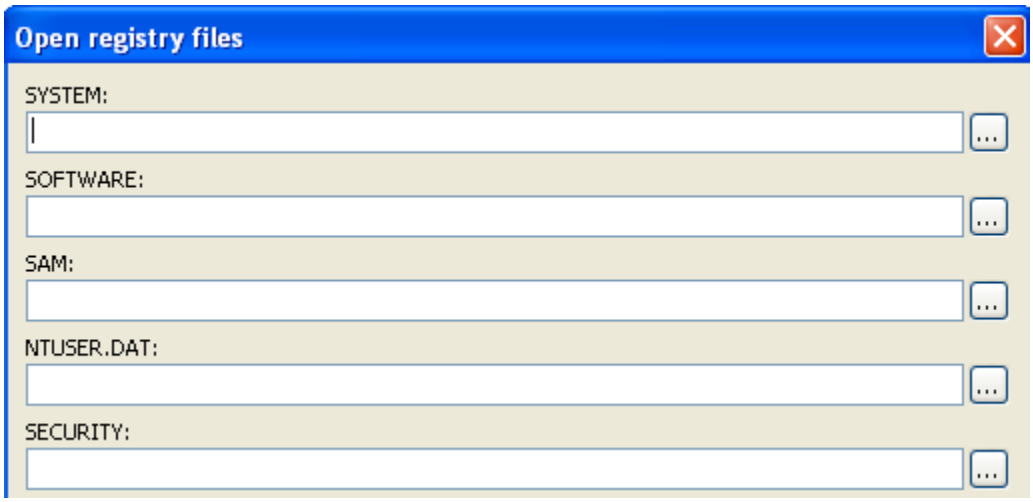
1. Double-click the **RegView** shortcut icon on the desktop.



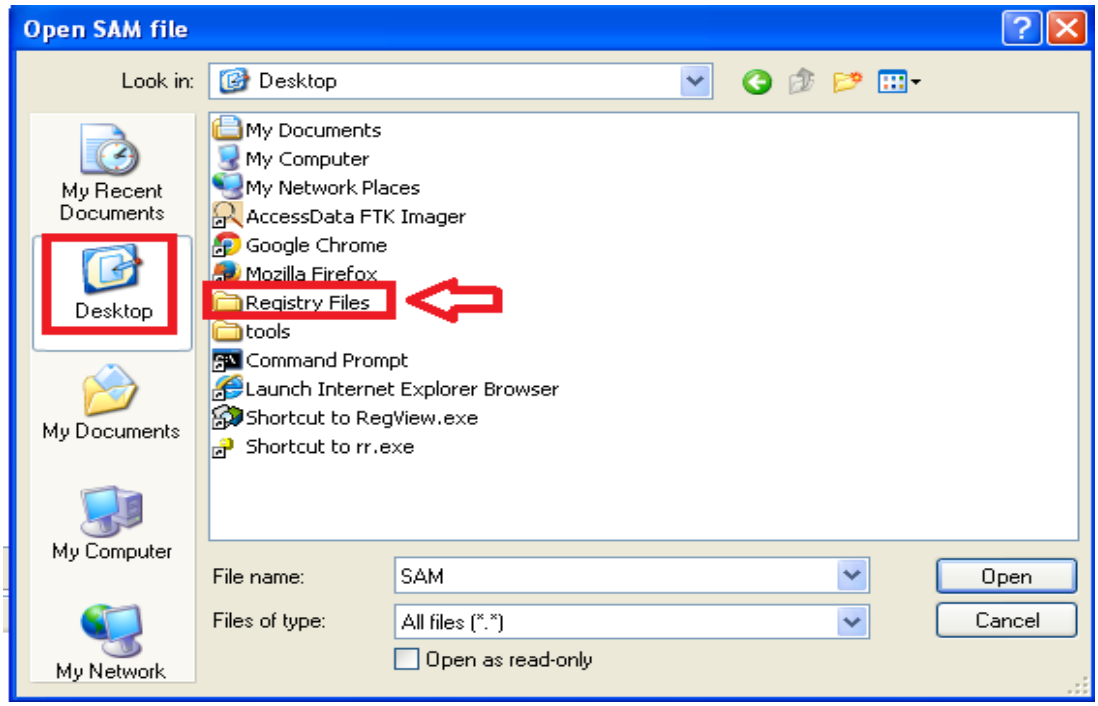
2. To examine a user's profile, select **File > Open registry files.**



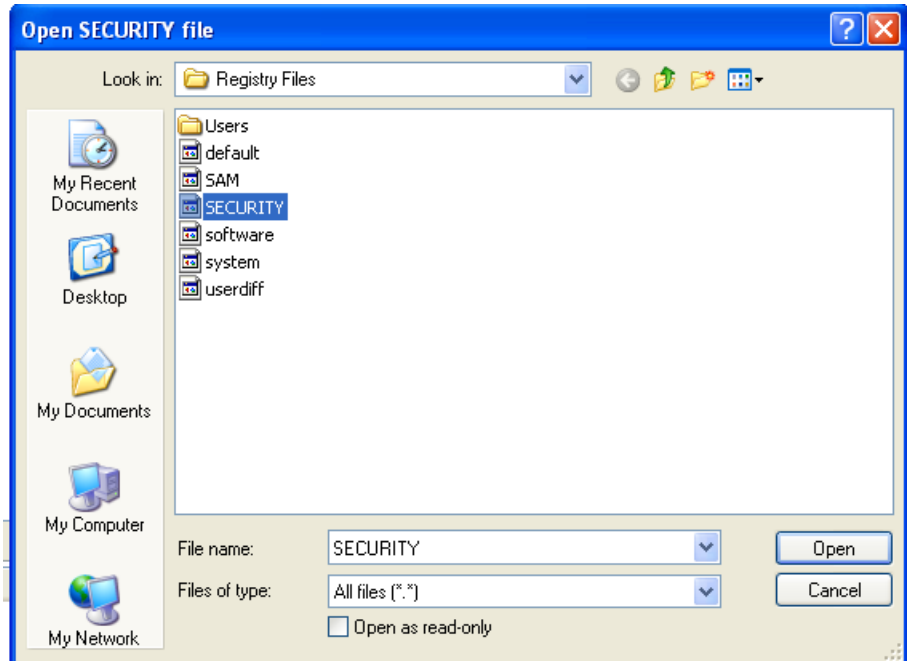
3. In the Open registry files box, click on the browse icon for SECURITY.



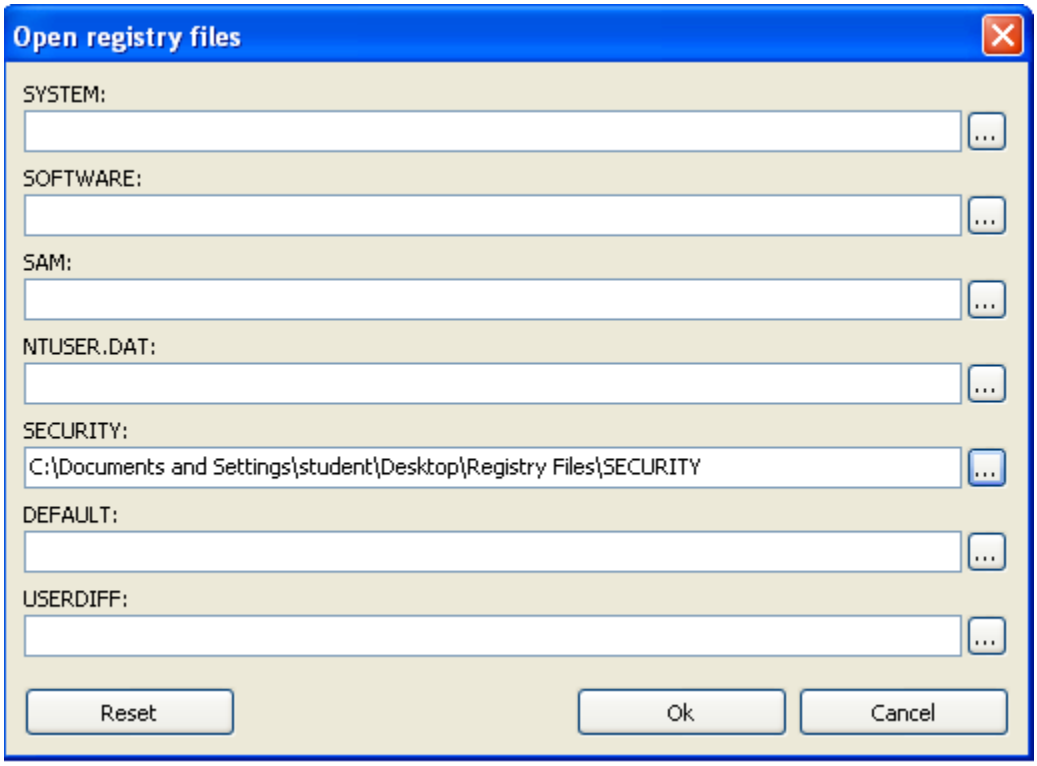
4. Browse to the **Registry Files** folder on the Desktop.



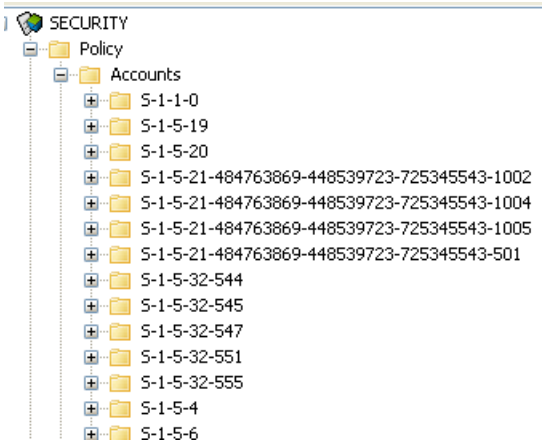
5. Double-click on the **SECURITY** file to open the file in Registry Viewer.



6. Examine the full path to the SECURITY file and click Ok to open the file.



7. Expand Policy, then Accounts. Notice the account ending in 501, which is for the Guest account.

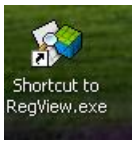


8. Close the RegistryViewer program so the SECURITY Registry file is no longer displayed.

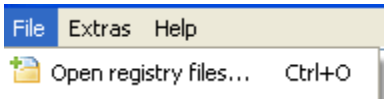
2.6 Exploring the Software Hive

The Software hive stores information about installed software, per-computer settings for each user, file extension associations, and user and operating system information.

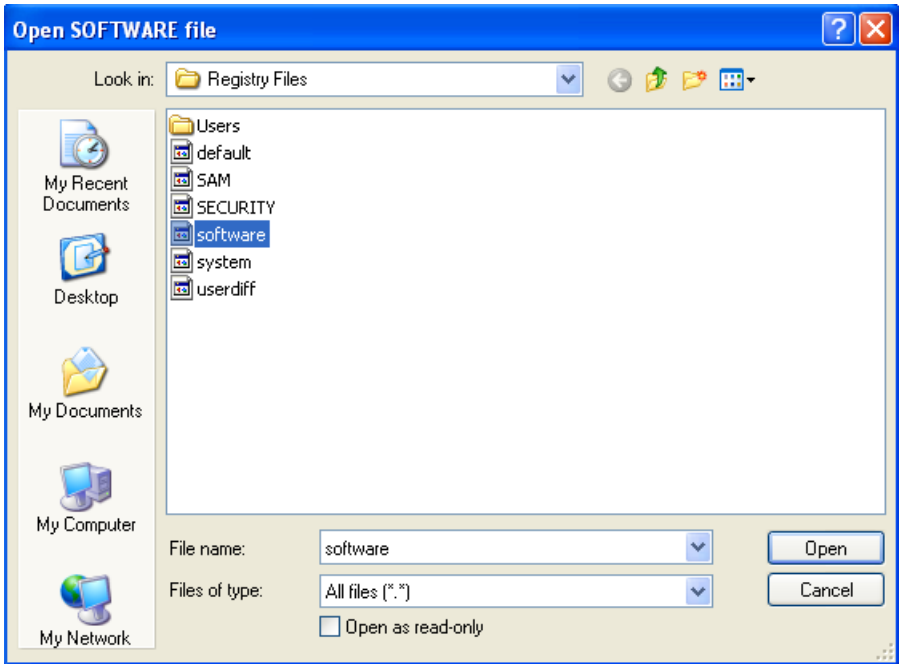
1. Double click the **RegView** shortcut icon on the desktop.



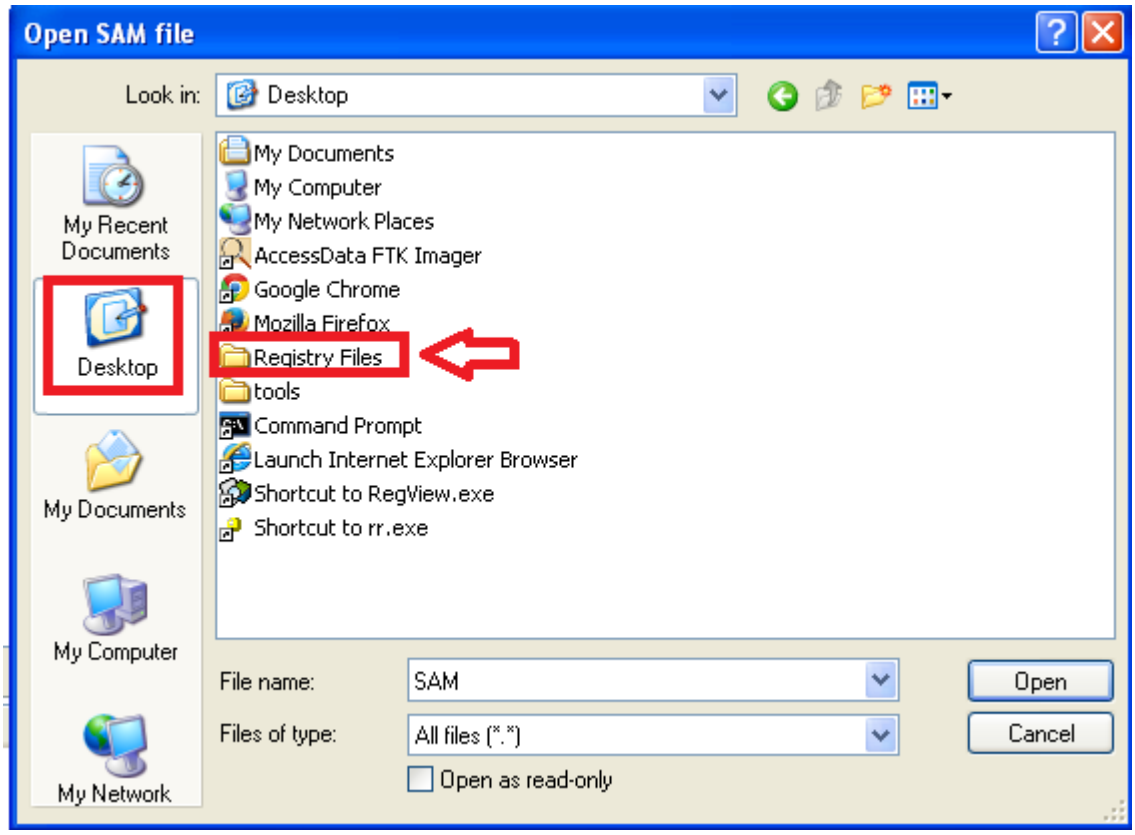
2. To examine a user's profile, select **File > Open registry files.**



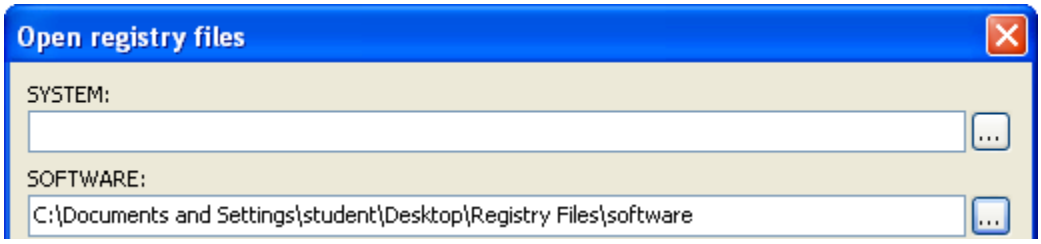
3. In the Open registry files box, click on the browse icon for **software**.



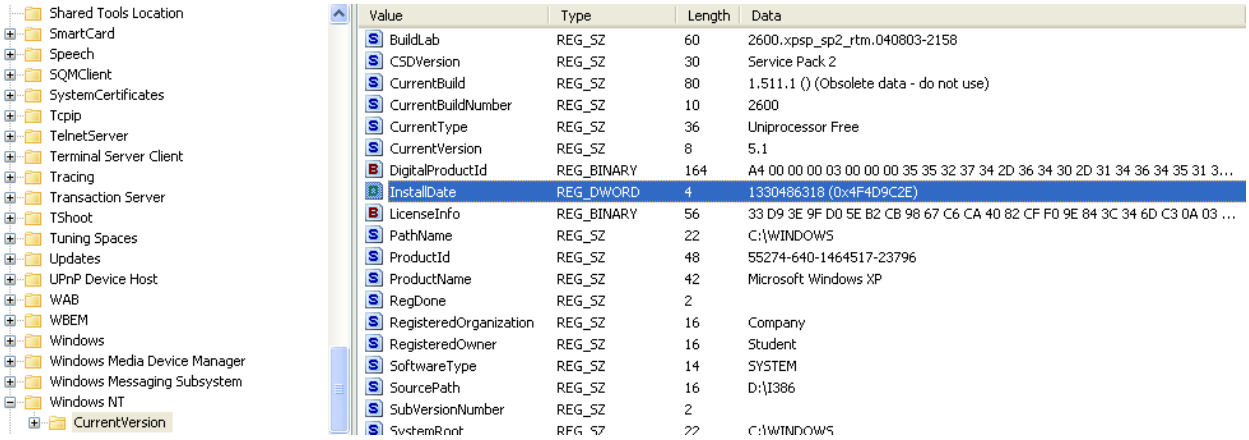
4. Browse to the **Registry Files** folder on the Desktop.



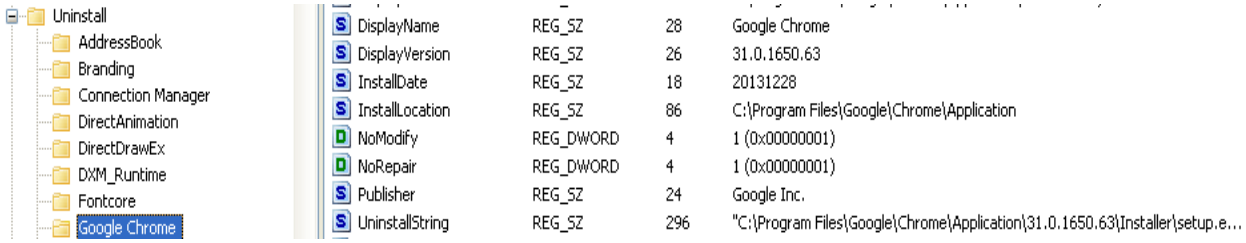
5. Double-click on the **software** file to open the file in Registry Viewer.
6. Examine the full path to the SOFTWARE file and click Ok to open the file.



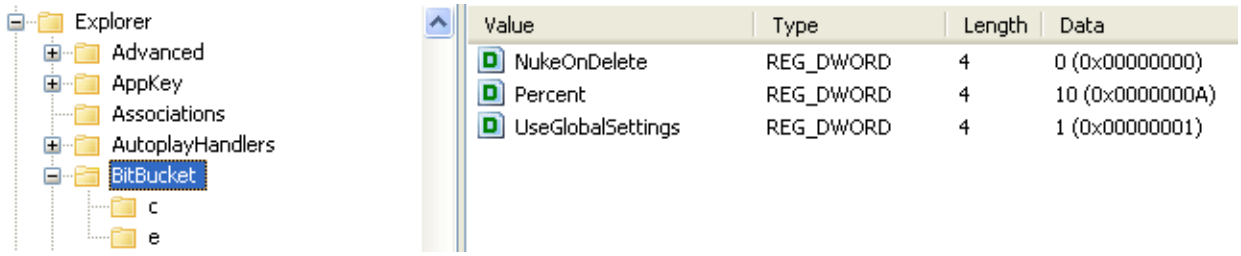
7. To identify the operating system and the time and date of installation, go to **Microsoft > Windows NT > CurrentVersion**. The install date needs to be converted using a dcode program since it is a Windows 64-bit hex code.



8. The Uninstall subkey lists all of the install locations for applications. Expand **Microsoft > Windows (not Windows NT) > CurrentVersion > Uninstall** to view these locations.



9. Each drive letter can be assigned a recycle bin within Windows. We can also verify if a user changed the properties of a recycle bin. For example, users can set files to bypass the recycle bin and just delete an item without recording it in the recycle bin. Drill down through **Microsoft > Windows > CurrentVersion > Explorer > BitBucket > NukeOnDelete**. The key will be set to 1 if the system is bypassing the recycle bin.



2.7 Conclusion

The Windows registry is a database. Each registry key holds information we can explore about the computer. Within each of the users' profiles, there is a file, NTUSER.dat. The NTUSER.dat file provides information about a user. The SAM Registry file holds all of the account information for the users of the computer. The System registry hive holds all of the computer startup parameters, device driver configurations, OS behavior, and hardware configurations. The SECURITY hive stores local security policies including user rights, password policy, user account memberships, a link to the SAM file for updates, and a user interface through User Manager. The Software hive stores information about installed software, per-computer settings for each user, file extension associations, and user and operating system information.

2.8 Discussion Questions

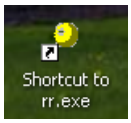
1. What type of information can be located in the SAM registry key?
2. What type of information can be located in the SOFTWARE registry key?
3. What type of information can be located in the NTUSER.DAT registry key?
4. What type of information can be located in the SYSTEM registry key?

3 Analyzing the Registry Hives using RegRipper

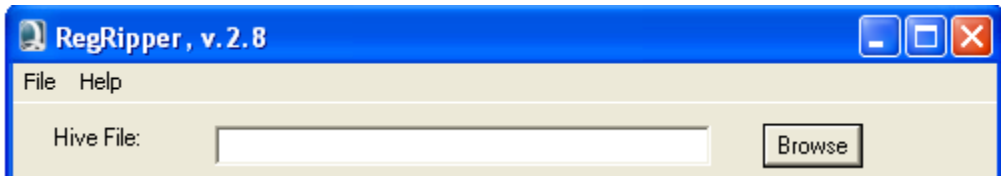
RegRipper is an open source tool that parses each registry file and creates a report detailing values that are found within several subkeys based on plugin modules. In Task 2, we searched the registry manually; Regripper automates the task.

3.1 Using RegRipper

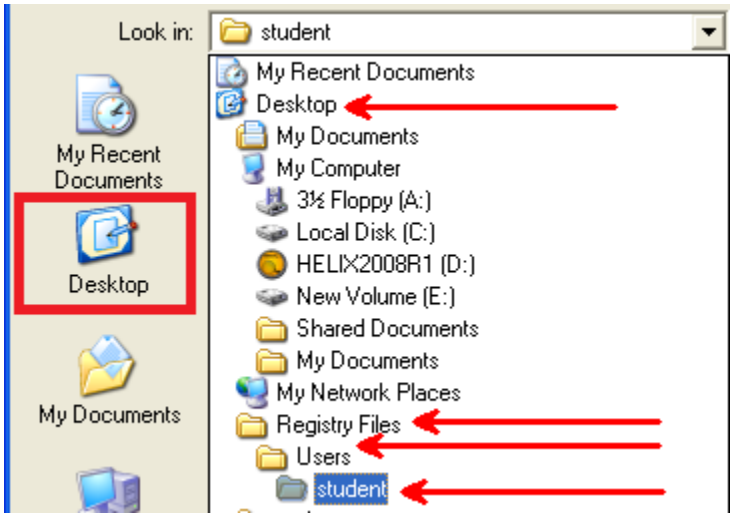
1. On the desktop, double-click the shortcut for rr.exe to open Registry Ripper.



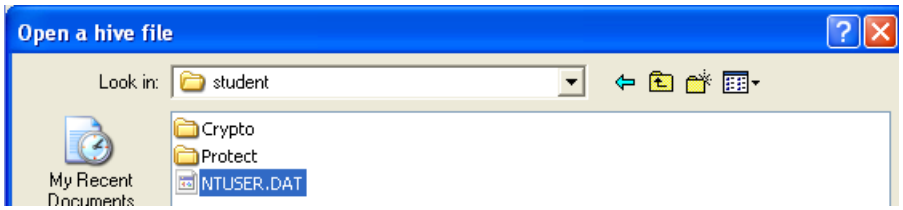
2. Click the Browse button next to Hive File to select the NTUSER.DAT file



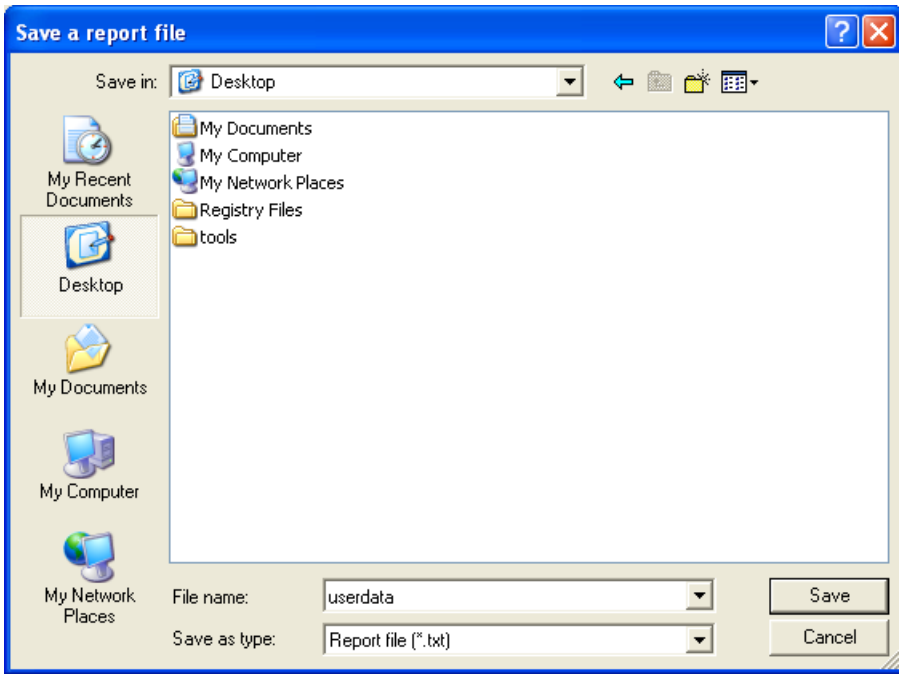
3. In the left pane, click on Desktop. Select **Registry Files folder > users > student**.



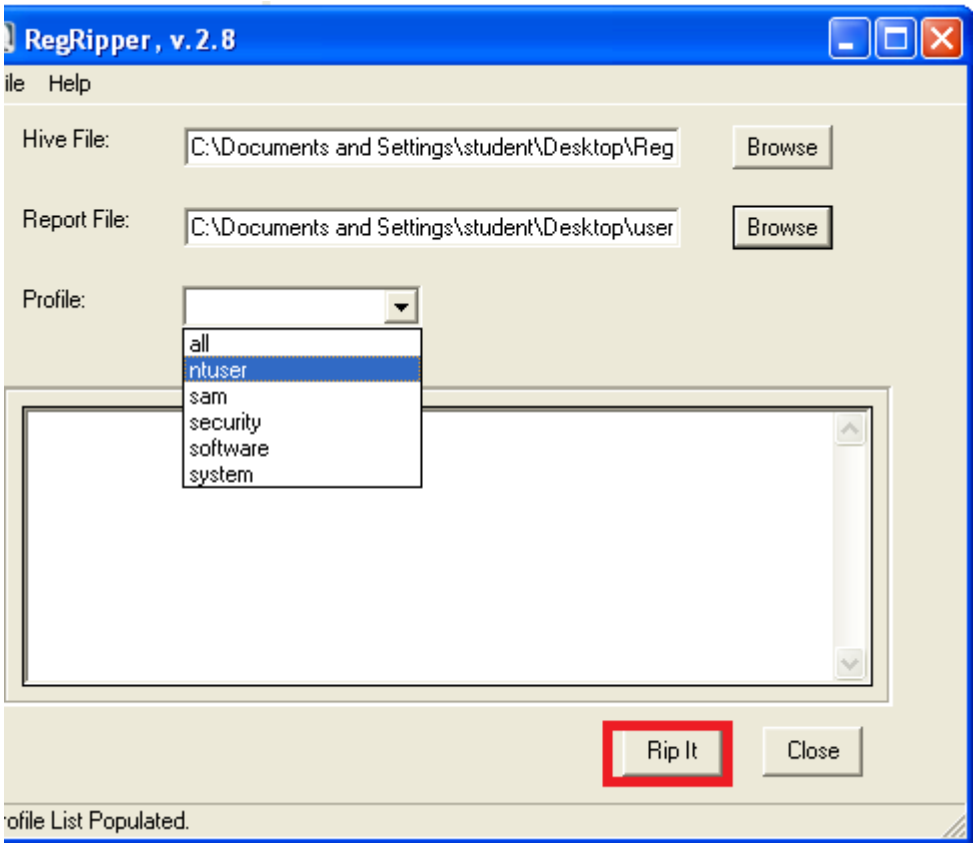
4. Double-click on the **NTUSER.DAT** file and select Open.



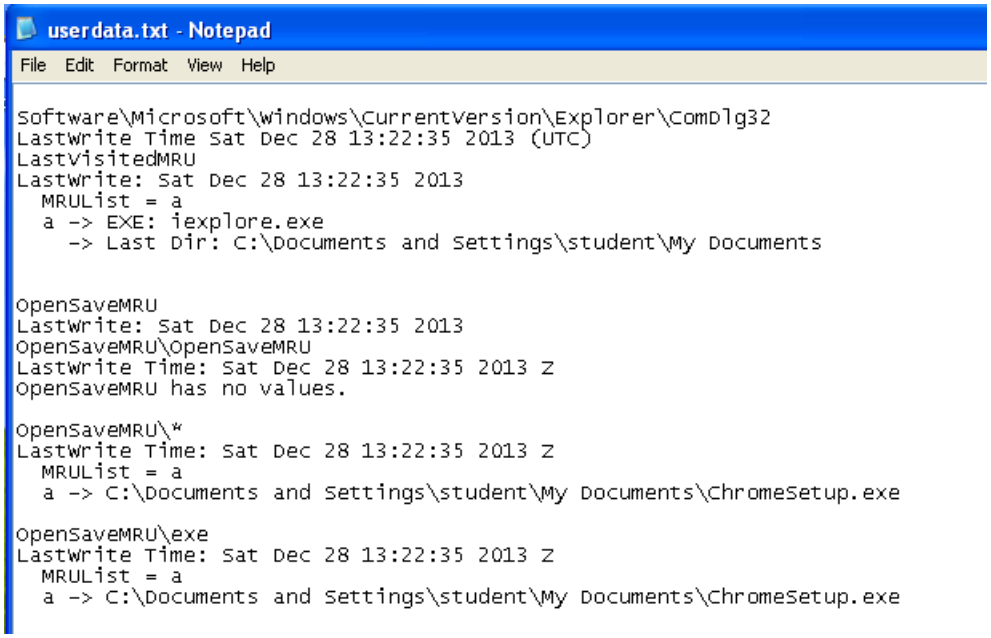
5. Click on the **Browse** button next to Report File to specify the save location and file name for the report file. Browse to the desktop and name the output file **userdata**. Click **Save**.



6. From the **Plugin File** dropdown, select **ntuser** to run the appropriate plugin. Click **Rip It**.



7. A report will be generated on the desktop named Userdata.txt. Open it and compare the information in the file with the data retrieved manually using Registry Viewer.



8. Repeat Steps 2-7 for each registry file name. Name the report file according to the file that you accessed. Select the appropriate Plugin File for each as indicated below.

Hive	Plugin File
Software	software
System	system
Security	security
SAM	sam
Default	ntuser

3.2 Conclusion

RegRipper is an open source tool that parses each registry file and creates a report detailing values that are found within several subkeys based on plugin modules. In Task 2, we searched the registry manually; Regripper automates the task. Both methods are useful and provide information concerning the computer and its users.

3.3 Discussion Questions

1. What Plugin File did you select to view the SAM hive?
2. What indicates if the system bypasses the Recycle Bin when a file is deleted?
3. What is the IP address for the default gateway that this system is using?
4. Which Registry hive can give you information about Most Recently Used items?

References

1. FTK Imager:
   http://www.accessdata.com/

2. RegViewer:
   http://www.gaijin.at/en/dlregview.php

3. RegRipper:
   https://code.google.com/p/regripper/wiki/RegRipper

4. FTK Imager Download:
   http://www.accessdata.com/support/product-downloads#.UcRlmFYo6Ul

5. Windows Registry:
   http://support.microsoft.com/kb/256986

