6.0 LAB MANUAL – WINDOWS REGISTRY

6.1 Learning About Registry

This set of exercises is designed for students with little or no experience with Windows Registry. By performing these exercises the student will:

1. See how Windows uses Registry to store user, application and system settings
2. Learn about the structure of Registry and the top level hives
3. Inspect various keys, and learn the relationship between keys and values
4. Gain experience working with RegEdit to find, edit and export keys
5. Learn how to discover which Registry keys are used to store various values using RegEdit, RegSnap and by searching the Internet

If you already have a strong grasp of Registry and feel confident that you can perform the listed tasks then you may want to skip this set of exercises and proceed to section 6.2.

WARNING - Serious problems might occur if you modify the Windows Registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Do NOT make any changes to Registry unless you know exactly what you're doing. Modify the Registry at your own risk.

6.1.1 Using RegEdit to locate Registry Values

This set of exercises provides experience using RegEdit to manually move through Registry and find the values of specific keys. In other words, you're going to practice drilling down to specific keys and then recording their values. This is a very basic process and if you have experience with Registry you can skip it if you want. But if you don't have any experience this is a good place to start.

You will also change some Windows configuration settings and check their effect on Registry.

1. Open the following key which contains information about the TCP/IP connection.

   HKLM\System\CurrentControlSet\Services\Tcpip\Parameters

   Notice that there are several values. In the space below document the data in the Hostname value, which holds the computer name.

   _____

2. Open the following key which contains the path to the default browser.

   HKEY_CLASSES_ROOT\http\shell\open

   Record the data in the command value in the space below:

   _____

   NOTE - To be technically correct this key lists the default program for displaying files using the http protocol. To be totally technically correct Windows looks at a couple of other keys to determine the value of this key. Just changing this key won't change the default browser. For the entire story see: http://newoldthing.wordpress.com/2007/03/23/how-does-your-browsers-know-that-its-not-the-default-browser/

3. Open the following key which contains information about Internet Explorer for the current user.

   HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main

   Notice that there are many values. Document the data in the Start Page value which holds the URL of the default Start Page (Home Page) in Internet Explorer.

   _____

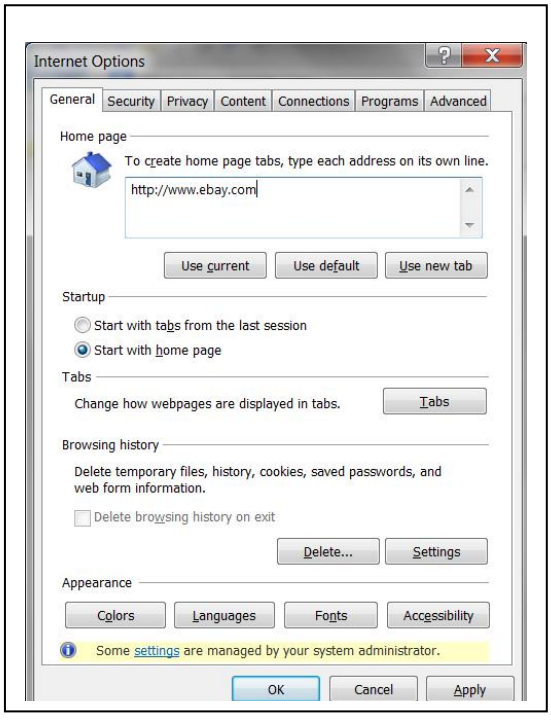
   Next you will change the value of the Start Page in Internet Explorer to see if you have the correct Registry key. If you have the correct key and value in RegEdit, the data will change when you change the Start Page in IE. To change the Start Page do the following:

   A. Start Internet Explorer

   B. Go Tools > Internet Options . If the menus are not displayed right-click in the upper border region of IE and check the Menu Bar box. Or you can click on the Tools icon in the upper right (it looks like a gear) and select Internet Options.

   C. The Internet Options dialog box will be displayed. Ensure that the General tab is selected.

   D. Enter the URL for the new start page in the Home Page section. You can use any URL you wish, just make sure it's different than the current one. Also make sure that you use the full URL including the protocol. In other words, don't just type www.google.com, make sure and use http://www.google.com.



   E. Ensure that the Start with Home Page button is checked.

F. Click Ok to save the changes.

Now return to RegEdit. Click View > Refresh, then check the data in the Start Page value. Has it changed? Document the data in the Start Page value in the space below.

_____

4. Open the following key which contains information about the Desktop display for the current user.

   HKEY_CURRENT_USER\Control Panel\Desktop

   Notice that there are many values. Document the data in the Wallpaper subkey which holds the path to the desktop wallpaper or background.

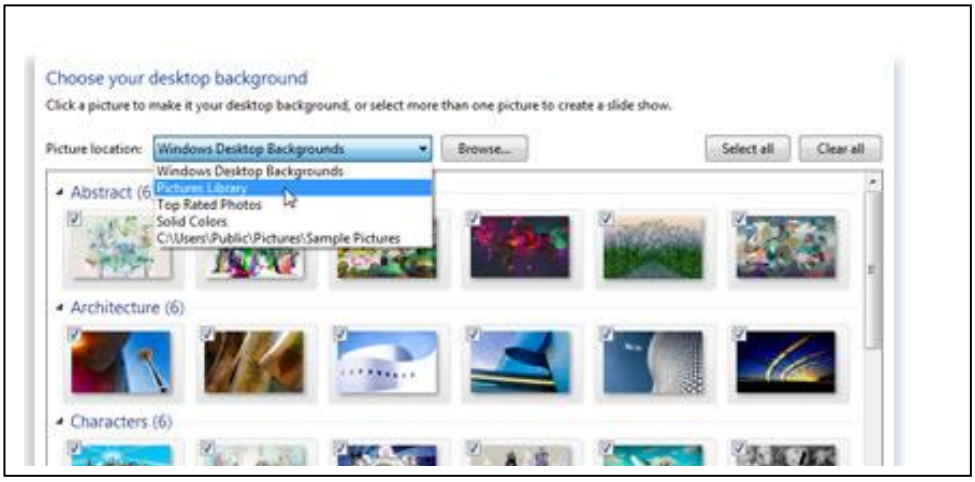
   _____

5. Next you will change the Wallpaper to see if you have the correct Registry key and value. If you have the correct key the data will change when you change the Wallpaper. To change the Start Page from Windows do the following:

   A. The simplest method is to find a picture, right-click and choose Set as Desktop Background

   B. An alternate method is open the Desktop Background by clicking the Start button and clicking Control Panel. In the search box, type desktop background, and then click Change desktop background.

   C. Click the picture or color that you want to use for your desktop background. If the picture you want to use isn't in the list of desktop background pictures, click an item in the Picture location list to see other categories, or click Browse to search for the picture on your computer. When you find the picture that you want, double-click it. It will become your desktop background.



Now return to RegEdit. Click View > Refresh, then check the data in the Wallpaper value. Has it changed? Document the data in the Wallpaper value.

_____

6.1.2 Exporting Registry Values and Copying Registry Key Names

One of the problems in working with Registry is documenting the key and value names and data. The key names or paths can be very long and difficult to write out by hand, and if a key has multiple values it can take a long time to document them all by hand. This set of exercises provides experience automating the process by copying key and value names, and exporting Registry values and data.

1. Document the path to the key and value that contain the computer name using this process:

    A. Open RegEdit and navigate to the key containing the computer name. (See exercise A in the previous for the key).

    B. Write down the path to this key. Yes … write it down by hand using a pen or pencil.

    C. In the right panel of RegEdit, left-click on the value to select it

    D. Go to the **Edit** menu and select **Copy Key Name**, or right-click on the key (not the value) and select **Copy Key Name**

    E. Open Notepad (or any text editor) and select **Edit > Paste**. Notice that you get the Key Name, but you still have to add the Value name if you want it.

    F. Was it easier to write down the path or use Copy Key Name?

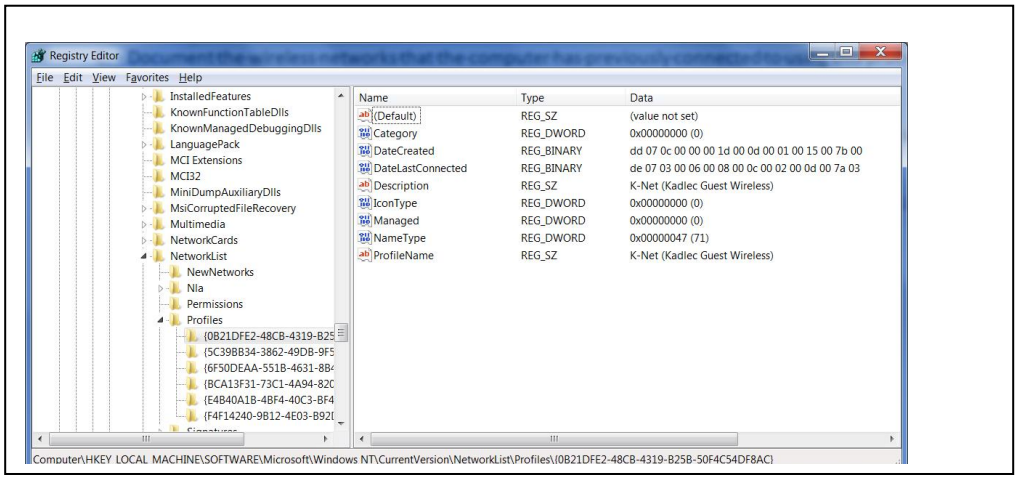
2. Use the process for Copying Key Names from Registry to document the path to the key and value that contains the Internet Explorer Start Page.

3. This exercise demonstrates how to get the data as well as the key and value names. For example, if you want to document the wireless networks that the computer has previously connected to you can either record the information by hand or use the following process:

    A. Open RegEdit and navigate to the following key, which contains a list of wireless networks.

    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

    B. Each of the subkeys contains information about a wireless network that the computer has connected to in the past. In the left panel of RegEdit, left-click on any of the subkeys to display the information for that wireless network.



    C. To document this information you can either write it out manually, or right-click on the subkey and choose **Export**, or an alternate method is to select **File > Export**. Export the file and save it somewhere easy to locate, for example on the Desktop. The file will have an extension of .reg, but it will be a plain text file.

    D. Locate the file you exported and open it with Notepad (or any text editor). Note that since the file is a .reg file Windows wants to use the settings in the file to modify Registry, not open it to edit it. You can either start Notepad and go to File > Open, or rename the file and change the extension from .reg to .txt, or right-click the file and select Open With and then choose Notepad.

    E. Inspect the contents of the file. Notice that it has the path to the Registry key, as well as all of the subkeys and values. If you don't want all of the information in the file you'll have to do some deleting, but this is easier than copying any data by hand.

4. Use the process for Exporting data from Registry to document the list of multimedia drivers used on the computer. This information is stored in the key:

    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\drivers.desc

5. Use the process for Exporting data from Registry to document the list of URLs typed in Internet Explorer by the current user. This information is stored in the key:

   HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

6.1.3 Using RegEdit to change Registry Values (Stupid Registry Tricks)

WARNING - Serious problems might occur if you modify the Registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Do NOT make any changes to Registry unless you know exactly what you're doing. Modify the Registry at your own risk.

As you've seen one of the things that Registry holds is configuration information for Windows. Most of the time you can find a GUI based tool to change the Windows settings, which you should use instead of editing Registry by hand. But there are some settings that don't have a nice tool, which means you have to use RegEdit to change them. This set of exercises provides experience using RegEdit to manually configure Windows. In particular, you will learn how to enable or disable the user's ability to change the desktop theme, screensaver and other desktop properties. Normally you can access these settings by right-clicking the Windows Desktop and selecting **Properties** or **Personalization**.

NOTE – All of the changes you make in this set of exercises will only take effect when the computer is rebooted. If you're working in the CBC Computer Science Labs rebooting the computer will return Registry back to it's frozen state, which means you will never see the effects unless the computer is unfrozen.

1. To disable the user's ability to change Themes in Desktop Properties follow these steps listed below. If you need additional reference the following web sites contain illustrated tutorials, along with instructions for using the Group Policy Editor to change the setting(s):

   http://www.intowindows.com/how-to-prevent-users-from-changing-theme-in-windows-7/
   http://www.tech-recipes.com/rx/7327/windows-7-prevent-users-from-changing-themes/

   A. Start RegEdit

   B. Go to:

      `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies`

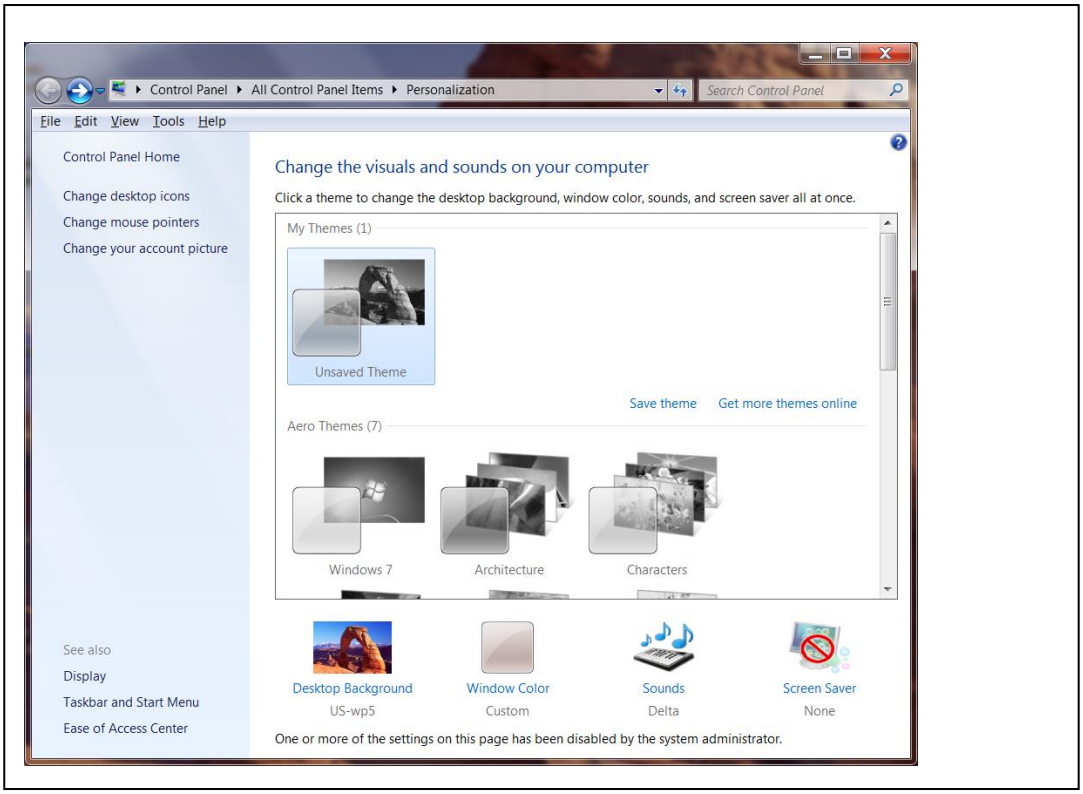
   C. If the `Explorer` key is not present, create it.

   D. Right-click in the right-side panel of RegEdit and select **New > DWORD**

   E. Set the name to **NoThemesTab** and set its value to **1** to disable the ability to change Themes.

   F. Test this by right-clicking on the Desktop and selecting Personalization. Notice that the various Themes will be displayed, but they will be grayed out and you will be unable to change them.

Note – even though the any changes you make in RegEdit should take effect immediately, you may need to restart the computer to see the changes.



G. Make sure and return this setting to it's default value. To re-enable the ability to change Themes, return to RegEdit and set the value of **NoThemesTab** to 0 or delete the key. Remember that you may have to restart the computer to see the changes.

2. To disable the user's ability to change the Desktop Background follow the steps listed below. If you need additional reference the web site:

   http://www.howtogeek.com/howto/16929/prevent-users-from-changing-screen-saver-and-wallpaper-in-windows-7/

   contains an illustrated tutorial, along with instructions for using the Group Policy Editor to change the setting(s).

   A. Start RegEdit

   B. Go to:

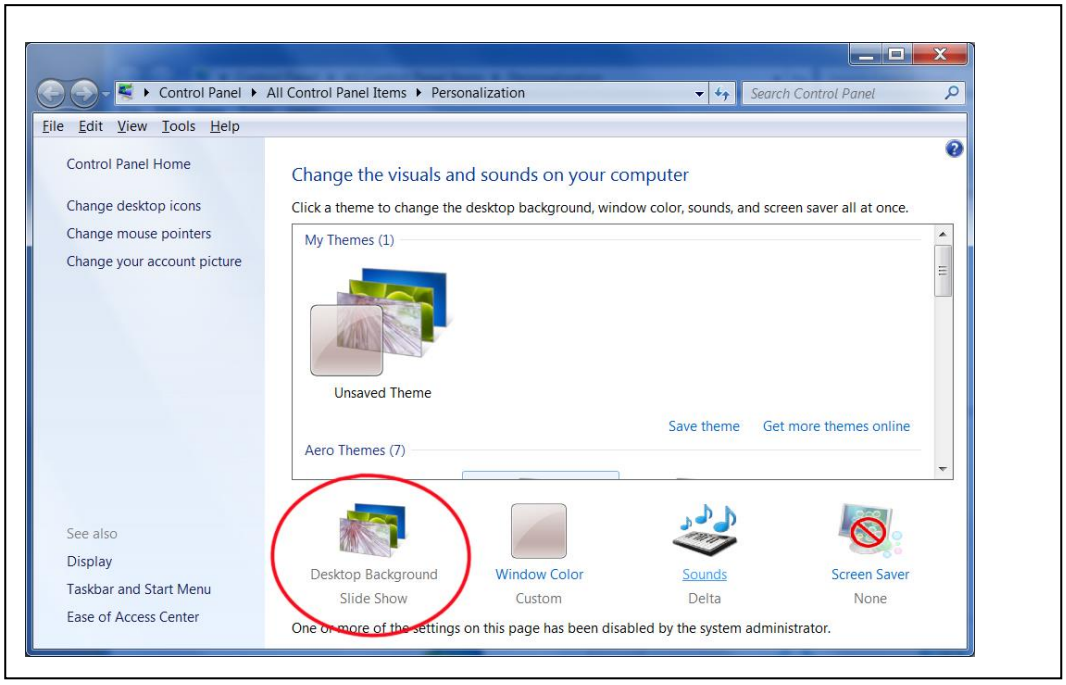
   `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies`

C. If the `ActiveDesktop` key is not present, create it.

D. Right-click in the right-side panel of RegEdit and select **New > DWORD**

E. Set the name to **NoChangingWallpaper** and set its value to **1** to disable the ability to change the WallPaper.

F. Test this by right-clicking on the Desktop and selecting Personalization. Notice that Desktop Background will be grayed out and you will be unable to change it. Note – even though the any changes you make in RegEdit should take effect immediately, you may need to restart the computer to see this change.



G. Make sure and return this setting to it's default value. To re-enable the ability to change the Desktop Background, return to RegEdit and set the value of **NoChangingWallpaper** to 0 or delete the key. Remember that you may have to restart the computer to see the changes.

3. To disable the user's ability to change the Screen Saver use the following information to set the Registry key.

A. The name of the Registry key is:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoDispScrSavPage
```

B. Set the value of this key to **1** to prevent the user from changing the Screen Saver. Set the value of this key to **0**, or delete the key to allow the user from changing the Screen Saver.

C. Make sure and return this setting to it's default value when the exercise is complete.

4. Use the process for editing Registry to disable the user's ability to access the Control Panel use the following information to set the Registry key. If you need additional reference the following web sites contains an illustrated tutorial along with instructions for using the Group Policy Editor to change the setting(s):

   http://www.howtogeek.com/howto/16189/configure-what-items-are-available-in-control-panel-or-completely-disable-it-in-windows-7/

   A. The name of the Registry key is:

      ```
      HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
      ```

   B. Set the value of this key to **1** to prevent the user from accessing the Control Panel. Set the value of this key to **0**, or delete the key to allow access to the Control Panel.

   C. Make sure and return this setting to it's default value when the exercise is complete.

5. Use the process for editing Registry to disable the user's ability to run RegEdit.exe use the following information to set the Registry key. If you need additional reference the following web sites contains an illustrated tutorial along with instructions for using the Group Policy Editor to change the setting(s):

   http://www.computerstepbystep.com/Registry_editor_windows_7.html/

   A. The name of the Registry key is:

      ```
      HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools
      ```

   B. Set the value of this key to **1** to prevent the user from running RegEdit. Set the value of this key to **0**, or delete the key to allow the user to run RegEdit.

   C. Make sure and return this setting to it's default value when the exercise is complete. Since you have locked yourself out of RegEdit, you'll have to use the Group Policy editor to re-enable it.

6.1.4 Searching Registry with RegEdit

One of the ways to discover which Registry holds a specific value is to use the Find function in RegEdit. This only works if you can change something in Windows to a specific string you can serach for, it doesn't work for settings that can simply be turned on and off. The basic process is to use a Windows program to change a setting that uses a specific string, and then use RegEdit to search for that string. For example, if you can change a setting to the string "this is the Registry data I'm searching for", then you can go into RegEdit and search for that string.

This exercise provides experience using the search or **Edit > Find** function in RegEdit to discover which specific key(s) are used to store different pieces of information.

1. Discover the Registry key and value that Internet Explorer uses to hold it's start page (home page) by using the following steps:

   A. Start Internet Explorer and change web browser home page (start page). This is done by selecting **Tools > Internet Options**. Make sure you're on the **General** tab, then change the URL in the **Home Page** section. Make it something distinctive and probably hasn't used somewhere else such as http://www.theonion.com

   B. Start RegEdit, and make sure Computer is selected in the left panel. (RegEdit starts searching from the current location. If one the hives or sub hives is selected it will only search down from that point, it doesn't search back up the Registry. Selecting Computer ensures that RegEdit will search the entire Registry.)

   C. Go to **Edit > Find** or hit **<ctrl-F>**

   D. This opens the Find dialog box. Enter the URL you typed above, and hit the **Find Next** button. RegEdit will display the first match. Look at the key and value name and try and determine whether or not this is the correct key. If the name of the value makes sense, then you've probably found the correct key. And if it's the only key with your test string then this is additional support for this being the correct key. However, if you're not certain you can continue to check Registry and see if there are any other keys that contain the test string. To do this select **Edit > Find Next** or hit **<F3>** to find the next match. If RegEdit finds another key with the test string then you have to decide whether you should test again with a different string, or whether your change caused Windows to update multiple Registry keys. This decision will be easier to make once you gain some experience, but it can be a little confusing when you first being working with Registry.

2. Use the process for searching Registry to discover the Registry key and value that Internet Explorer uses to hold it's list of typed URLs. This is the list of URLs that you can display by clicking the dropdown arrow in IE's Location Dialog Box at the top of the IE window. To begin, start IE and enter the URL for a web site that you have not yet visited. For example, http://www.elvis.com. You can then search Registry for this URL. Hint – the key and value you find should have the characters MRU in them somewhere. Remember MRU stands for Most Recently Used.

3. Use the process for searching Registry to discover the Registry key and value that Microsoft Word uses to hold it's list of Recent files. To begin, start Microsoft Word and save a file with a unique name. You can then search Registry for this name. Hint – the key and value you find should have the characters MRU in them somewhere.

6.1.5 Using RegSnap to locate Registry Keys

Using the RegEdit Find function to discover Registry keys has a couple of big weaknesses. The first is that you have to know what strings you're searching for, and most Registry values don't store strings. For example, say you want to know which key and value are used to store whether or not the Status Line or File Menus are displayed in Internet Explorer. When you turn these on or off in IE you're just checking a box, you're not entering a string, so there's no string to search for.

The second problem is that making a change in Windows or an application can cause multiple changes in Registry. Sometimes a single key and value will change, but usually there will be several changes. For example, installing a program or adding a user will cause many changes to Registry. And finding all of the changes can be a challenge using the RegEdit Find function.

Luckily there's another tool to help discover changes to Registry. This tool is called RegSnap and it can be used to show you all the changes to Registry over a given time period. The basic steps for using RegSnap are as follows:

A. Install and start Regsnap
B. Setup everything you need to make the desired changes. Don't make the changes at this point, but make sure any applications or tools you need are open and ready to use.
C. Return to RegSnap and make an initial snapshot
D. Make the changes. Avoid doing anything else at this time to prevent unnecessary changes to Registry
E. When the changes are complete return to RegSnap and make the second snapshot
F. Use the compare function in RegSnap to compare the initial snapshot and the second snapshot
G. Use the RegSnap report to determine the affected Registry keys and values

1. Use RegSnap to discover the Registry key and value that Windows uses to hold the picture associated with the current user's account. This is the image that's displayed on the login screen. To change the picture go to **Control Panel** and select **User Accounts**. Select **Change Your Picture**.

2. Use RegSnap to discover the Registry key(s) and value(s) that Internet Explorer uses to determine whether or not to display the file menus. This is set by opening IE, right-clicking anywhere in the IE border at the top of the browser and checking the **Menu Bar** box.

3. Use RegSnap to discover the Registry key(s) and value(s) that Internet Explorer uses to determine whether or not to display the Status Line at the bottom of the browser window. This is where the browser tells you the URL associated with any link as you mouse over the link. The Status Line display is set by opening IE, right-clicking anywhere in the IE border at the top of the browser and checking the **Status Line** box.

4. Use RegSnap to discover the Registry key(s) and value(s) that Internet Explorer uses to store the desktop Theme. To change the Theme right-click on the desktop and select **Personalization**, then choose the desired Theme.

6.1.6 Discovering Registry Keys

This set of exercises provides experience figuring out which Registry key(s) are used to store specific information. Use any method desired, a general Internet search, searching inside of RegEdit, or RegSnap, to determine which key(s) are used to store the following information. You answer should include the name of the key(s).

1. A list of users or user accounts
2. The last user to logon to the computer
3. The keys that change when a file is deleted (moved to the recycle bin)
4. The size and position of the Internet Explorer window
5. A user's password
6. Internet Explorer Autocomplete Data for Online Forms

6.2 FTK and Registry– Built-In Reports

Remember that Registry is really a giant database that holds information about Windows, users and software; and there are several database keys that hold information that are of interest in a forensics investigation. Reading the information from Registry requires two things: having a tool which will display the Registry keys and knowing which key(s) to read.

In this set of exercises you will gain experience using FTK to gather information from Registry. You will practice using the default Registry reports in FTK to gather information from a disk image file, read this information in both the Select Registry Reports tool, and in the final FTK Report. Remember that this requires several things:

A. FTK must be installed.

B. The disk image must be loaded in FTK

C. You must have FTK generate the Registry Reports. You can do this while the evidence if being processed as it's loaded in FTK by checking the **Registry Reports** box. Or you can do it later by selecting **Tools > Preliminary Registry Reports**.

D. The default reports can be viewed by selecting either:

   a. **Tools > Select Registry Reports**
   b. **File > Report Wizard** (ensure that you include the Registry Reports on the last dialog box in the wizard.)

6.2.1 REGISTRY INFORMATION FROM MANTOOTH32.E01

Use the default Registry Reports in FTK to inspect the image file **Mantooth32.E01.** Use the information from these reports to answer the following questions:

1. Which of the following files starts automatically when Wes Mantooth logs in?
    A. Spotify
    B. MSNMsgr.exe
    C. Internet Explorer
    D. Myspace

2. When the last time Wes Mantooth ran Internet Explorer?
    A. 3/6/2007
    B. 4/01/2010
    C. 2/12/2008
    D. 6/12/2009

3. Which of the following was NOT typed in the Internet Explorer Location Dialog Box by Wes Mantooth?
    A. www.accessdatarocks.com
    B. http://www.gmail.com/
    C. http://www.comcast.net/
    D. http://www.ebay.com

4. When the last time the user Dracula ran Internet Explorer?
    A. 3/6/2007
    B. 4/01/2010
    C. 2/12/2008
    D. 6/12/2009

5. Which of the following was played from an iPod by Wes Mantooth?
    A. Bill is doomed.avi
    B. wizoz18d.wav
    C. CVJW.mp3
    D. All of the above were played, but none were on an iPod

6. In addition to the Administrator and Guest accounts, how many other user accounts are defined?
    A. 1
    B. 2
    C. 3
    D. 4
    E. 5

7. What is Wes Mantooth's password hint?
    A. groovy man
    B. gravy man
    C. in your face
    D. in your pocket
    E. The password hint is not defined

8. What is Dracula's password hint?
    A. groovy man
    B. gravy man
    C. in your face
    D. in your pocket
    E. The password hint is not defined

9. Which user has an account defined in Registry, but doesn't have a home directory in the Users folder?

10. What is the SID associated with the Wes Mantooth account?
    A. 1000
    B. 100
    C. 27
    D. 127
    E. 503

11. What is the SID associated with the Dracula account?
    A. 1001
    B. 1002
    C. 103
    D. 789
    E. 503

12. What is the Business Name associated with Windows License for the computer associated with this image?
    A. Bram Stoker
    B. Volturi Enterprises
    C. Anchorman Productions
    D. Basic Gloves Inc.
    E. None of the above

13. Which time zone was Windows configured to use? (Don't worry whether it's Standard or Savings, just select the correct base time zone.)
    A. Eastern
    B. Central
    C. Mountain
    D. Pacific
    E. None of the above

6.2.2 REGISTRY INFORMATION FROM WASHER 17.E01

Use the default Registry Reports in FTK to inspect the image file **WASHER 17.E01.** Use the information from these reports to answer the following questions:

1. Which of the following files starts automatically when the Administrator logs in?
    A. Spotify
    B. MSNMsgr.exe
    C. Internet Explorer
    D. aim.exe

2. Which of the following files is in the list of files set to run on startup for all the users?
    A. Spotify
    B. msmsgs.exe
    C. Internet Explorer
    D. Aim.exe

3. What is the Administrator's POP3 username on the mail server mail.comcast.net? (Enter the name in all lower case.)

4. What is the Administrator's POP3 password on the mail server mail.comcast.net?
    A. mrSmee
    B. mail.comcast.net451F6090
    C. password1234
    D. bilbobaggins2
    E. None of the above

5. Which user appears to have used Internet Explorer the most?
    A. Administrator
    B. Billy Bob Brubeck
    C. Captian Hook
    D. The Wolf
    E. Mr Smee

6. Which of the following was viewed by the Administrator?
    A. FamilyGuyEaster.avi
    B. How to steal cars.pdf
    C. Hardbark the Aardvark.jpg
    D. All of the above

7. The Administrator viewed driving directions between which two cities?
    A. Portland Maine and Portland Oregon
    B. Red Feather Lakes Colorado and Artimus Texas
    C. Blue Leg Lakes Colorado and Cut and Shoot Texas
    D. Red Feather Lakes Colorado and Cut and Shoot Texas

8. There is evidence in this image about a certain type of crime. What type of crime does the majority of evidence appear to support?
    A. ID Theft
    B. Child Pornography
    C. Malware
    D. Industrial Espionage
    E. Drugs
    F. None of the above

9. Which of the following strings was entered at the website dogpile.com?
    A. print counterfeit money
    B. How to make meth
    C. hire a hit man
    D. hiding a body
    E. None of the above

10. How many URLs did the Administrator type in Internet Explorer?
    A. 1
    B. 7
    C. 12
    D. 19
    E. 25

11. When was the last time the Administrator typed a URL in Internet Explorer?
    A. 2/15/2005
    B. 2/13/2008
    C. 4/01/2010
    D. 5/13/2011
    E. 7/12/2011

12. How many URLs did Billy Bob Brubeck type in Internet Explorer?
    A. 1
    B. 7
    C. 12
    D. 19
    E. 25

13. What is the SID associated with the Captian Hook account?
    A. 1001
    B. 1006
    C. 106
    D. 789
    E. 503

14. What is the username associated with the account that's used for generating bad debt?
    A. Administrator
    B. Captian Hook
    C. Billy Bob Brubeck
    D. The Wolf
    E. Mr Smee
    F. Artimus

15. What is the Business Name associated with Windows License for the computer associated with this image?
    A. Bram Stoker
    B. Volturi Enterprises
    C. Anchorman Productions
    D. Basic Gloves Inc.
    E. None of the above

16. Which time zone was Windows configured to use? (Don't worry whether it's Standard or Savings, just select the correct base time zone.)
    A. Eastern
    B. Central
    C. Mountain
    D. Pacific
    E. None of the above

6.3 Additional Registry Information with AccessData Registry Viewer

The FTK Registry Reports can be used to display Registry information that someone at AccessData decided was important. This Registry information is very helpful, but there may other information in Registry that you want to examine as part of your investigation. AccessData provides a tool called Registry Viewer that allows you to view any Registry keys you desire. In this set of exercises you will gain experience using AccessData Registry Viewer to read Registry files and find Registry information that is NOT included in the FTK default Registry Reports.

Remember that this requires several things:

A. The AccessData Registry Viewer must be installed. (Make sure that you get this from Canvas. It's an older version that will work with our older version of FTK.)

B. You can run Registry Viewer from within FTK or in standalone mode. If you want to include the Registry information in your FTK case Report you must run Registry Viewer from within FTK, which means the disk image with the Registry files must be loaded in FTK

C. From inside FTK, start the Registry Viewer by selecting **File > Registry Viewer**

D. You must choose the correct Registry file such as SAM, SYSTEM, NTUser.dat, etc. to load into Registry Viewer. Use on the Windows Registry References to decide which Registry file holds the desired piece of information.

6.3.1 ADDITIONAL INFORMATION IN MANTOOTH32.E01

Use the image file **Mantooth32.E01** to answer the following questions:

1. Which of the following is a key in the SAM\Domains\Account\Aliases\Names key?
    A. Day Walkers
    B. Night Walkers
    C. The Brood
    D. Grrrlzz

2. Did Wes Mantooth run FTK? Hint – Look in the NTUser.dat file for Wes Mantooth, then search for FTK or AccessData. If you find a key, try and determine whether it indicates that the program was run or not.
    A. Yes
    B. No

6.4 Exporting Registry Files From an Image

This set of exercises provides experience using Registry Viewer to inspect external Registry files. That is, you will be running Registry Viewer in stand alone mode, outside of FTK. The process is much the same as what you've done before with FTK, however the built-in Registry Reports are missing. So you will have to either know which key(s) you're looking for, or be able search for a string, or manually inspect keys and values.

You will gain experience using FTKImager to open a disk image, locate the Registry files, and export them (save them) so you can later use the AccessData Registry Viewer to locate specific pieces of information. This may seem like an unnecessary step, after all, if you have an image why not just use FTK and Registry Viewer? However, remember that in demo mode FTK has a limit of 5000 files; which means that in many cases the Registry files won't be opened or processed. Exporting the Registry files make it possible to inspect the files Registry Viewer.

The steps for using FTK Imager to export the Registry files from an image are:

A. Install FTK Imager if necessary. Remember that this is AccessData's disk imaging tool, but it can also be used to extract files from an image.

B. Start FTK Imager and open the disk image.

C. Locate the 4 S Registry files, SAM, Security, System and Software. They are in **Windows\System32\Config**

D. Make copies of these files outside of the image by:
    i. Highlighting the files
    ii. Right-Click and choose **Export**
    iii. Create a new folder (some where you can find it like the Desktop). I suggest naming it something like CaseNameEvidence, but you can name it whatever you want.
    iv. Save the files

E. Locate the NTUSER.dat file(s) that contain the User portion of the Registry. They will be in either **Users\Username** or **Documents and Settings\Username** and there will be one for each user.

i. Right-click on the **NTUSER.dat** file and choose **Export**.
ii. If you're going to export this file for more than one user you will have to put each in their own separate folder, because you can't change the file name, it will always be NTUSER.dat and you'll end up overwriting the existing file each time you save a new one if you don't put them in different folders.

Once you have the Registry files outside of the image, you can use AccessData Registry Viewer to inspect them, just like you did in the previous exercises.

6.4.1 Registry Data in **Win2000 NTUSER.Dat**

Use the file **Win2000 NTUSER.Dat** to answer the following questions. This is an NTUser.Dat file which has already been exported from a disk image. You can open it directly in AccessData Registry Viewer.

1. What is the full path to the key named **AccessData HiddenKey**?
   A. 2K.DAT\Control Panel\Appearance\New Schemes
   B. 2K.DAT\Software\AccessData
   C. 2K.DAT\AppEvents\Schemes\Apps\MSMSGS
   D. There is no key with this name

2. What is the name of the only subkey in the key named **AccessData HiddenKey**?
   A. Drac was here
   B. Can't Touch Me!
   C. Top Secret
   D. This key has no name

3. What is the name of the only value in the subkey from the previous question?
   A. Drac was here
   B. Trust me
   C. htcia2003stuff
   D. Check this action !

4. According to the data in Software\Microsoft\Internet Explorer\TypedURLs, which of the following web based mail systems has been used?
   A. http://www.hotmail.com
   B. http://www.gmail.com/
   C. http://www.hushmail.com
   D. http://www.earthlink.net/webmail
   E. None of the above

5. What two Outlook email accounts are associated with this user? (Hint - To answer this question you need to figure out which Registry key holds this data, search the entire Registry.)

6.4.2 Registry Data in **WinXP NTUSER.Dat**

Use the file **WinXP NTUSER.Dat** to answer the following questions. This is an NTUser.Dat file which has already been exported from a disk image. You can open it directly in AccessData Registry Viewer.

1. What is the full path to the key named **AccessData HiddenKey**?
    A. XP.DAT\Control Panel\Appearance\New Schemes
    B. XP.DAT\Software\AccessData
    C. XP.DAT\AppEvents\Schemes\Apps\MSMSGS
    D. There is no key with this name

2. What is the name of the only subkey in the key named **AccessData HiddenKey**?
    A. Drac was here
    B. Can't Touch Me!
    C. Top Secret
    D. This key has no name

3. What is the name of the only value in the subkey from the previous question?
    A. Drac was here
    B. Trust me
    C. htcia2003stuff
    D. Check this action !

4. What is the LDAP Username for the account on the LDAP server ldap.bigfoot.com?
    A. mantooth
    B. htcia2003
    C. htcia2003ldap
    D. htcia bigfoot account

5. What value is stored in the LDAP password for the account on the LDAP server ldap.bigfoot.com?
    A. ldap.bigfoot.comDE452090
    B. htcia2003
    C. password1234
    D. Bigfoot Internet Directory ServiceDE452090
    E. The password is not stored in Registry

6. What is the username for the account on the LDAP server directory.verisign.com?
    A. mantooth
    B. htcia2003
    C. htcia2003verisign
    D. verisignhtcia2003
    E. The username is not stored in Registry

7. According to the data in \Software\Microsoft\Internet Explorer\TypedURLs, which of the following web sites was viewed?
    A. http://www.lasvegas.com
    B. http://www.london.com.uk
    C. http://www.miami.com
    D. http://www.losangeles.com
    E. None of the above

8. Which of the following strings did the user type in the Windows Search box? This is the box that appears when you select **Windows Start Button > Search**. (Hint - To answer this question you need to figure out which Registry key holds this data, search the entire Registry, or search for each of the following strings.)
    A. tangerine
    B. Mp3
    C. flapjacks
    D. lockhart
    E. All of the above
    F. None of the above

6.4.3 Registry Data in **jean-small-reg.E01**

Use the image file **jean-small-reg.E01** to answer the following questions. This is an image file so you will have to extract the Registry files before running AccessData Registry Viewer. Make sure and take note of where the exported files are located, and make sure that you get all of the Registry files including the following:

A. System, SAM, Security and Software
B. The NTUser.dat for each user

1. Has this Windows installation been activated or is it due to expire? To make this determination check the Registry key SECURITY\Policy\Secrets. If there is a subkey that starts with the string L$RTMTIMEBOMB then Windows has not been activated.
    A. Activated
    B. Not Activated

2. How many total user accounts are there? (Include all of the accounts including Administrator, Guest etc. in your answer.)

3. Which of the following is NOT a User Name?
    A. Jean
    B. Hailey
    C. Sacha
    D. Addison

4. Has the Adobe Flash Player been installed, and if so what is the version number? (Look in Software and search for Macromedia)
    A. 7.0
    B. 9.0
    C. 11.0
    D. Not Installed

5. Which of the following websites did Jean visit? (Look at the Software\Microsoft\Internet Explorer\TypedURLs key in NTUSER.DAT for the Jean user.)
    A. eddiebauer.com
    B. gap.com
    C. kohls.com
    D. target.com
    E. landsend.com

6.4.4 Registry Data in **CHARLIE-SMALL-REG.E01**

Use the image file **charlie-small-reg.E01** to answer the following questions. This is an image file so you will have to extract the Registry files before running AccessData Registry Viewer. Make sure and take note of where the exported files are located, and make sure that you get all of the Registry files including the following:

A. System, SAM, Security and Software
B. The NTUser.dat for each user

1. Has this Windows installation been activated or is it due to expire? To make this determination check the Registry key SECURITY\Policy\Secrets. If there is a subkey that starts with the string L$RTMTIMEBOMB then Windows has not been activated.
    A. Activated
    B. Not Activated

2. How many total user accounts are there? (Include all of the accounts including Administrator, Guest etc. in your answer.)

3. Which set of Office tools is being used? (Look in Software and do a search for each of the following.)
    A. Microsoft Office
    B. Open Office
    C. IBM Lotus Symphony
    D. Libre Office

4. Which timezone is Windows configured to use. (Look at the ControlSetXXX\Control\TimeZoneInformation key in SYSTEM. In this case, check both ControlSets to ensure they agree)
    A. Eastern
    B. Central
    C. Mountain
    D. Pacific

5. Which of the following websites did Charlie visit? (Look at the Software\Microsoft\Internet Explorer\TypedURLs key in NTUSER.DAT for the Jean user.)
    A. google.com
    B. ebay.com
    C. amazon.com
    D. msn.com
    E. foxnews.com