GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Advanced Incident Response, Threat Hunting, and Digital Forensics (Forensics
at http://www.giac.org/registration/gcfa

Windows ShellBag Forensics in Depth

GIAC (GCFA) Gold Certification

Author: Vincent Lo, LYLC.SYMPHONICA@GMAIL.COM
Advisor: Tim Proffitt

Accepted:
Mach 24, 2014

Updated:
Nov 19, 2014

Abstract

The problem of identifying when and which folders a user accessed arises often in digital forensics. Forensicators attempt to search for them in the ShellBag information because it may contain registry keys that indicate which folders the user accessed in the past. Their timestamps may demonstrate when the user accessed them. Nevertheless, a lot of activities can update the timestamps. Moreover, the ShellBag structure differs slightly between different Windows operating systems. How to interpret ShellBags correctly has become a challenge. This paper summarizes the details of ShellBag information and discusses various activities across Windows operating systems.

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

1 Introduction

Microsoft Windows records the view preferences of folders and Desktop. Therefore, when the folder/Desktop is visited again, Windows can remember the location of the folder, view and positions of items. Microsoft Windows store the view preferences in the registry keys and values known as "ShellBags".

ShellBag information is crucial when forensicators need to know when and which folder a user accessed. For instance, when a company suspects an employee leaked a confidential document stored on the network, that employee's computer may have the ShellBag information that demonstrates the folder containing that document was accessed shortly before the document was leaked. Furthermore, ShellBags may also show the folders or servers that employee should not access. Those findings are critical to the investigation. Or, when a company suspects an employee maliciously deleted the important files on the network, ShellBag information may demonstrate the employee's computer accessed the folder before the incident happened.

Nevertheless, ShellBags contain many timestamps. The activities that can create or update ShellBag information are complex. In order to interpret it correctly, many factors need to be considered, such as Windows operating systems, folder settings and folder types. The following will explain the details of ShellBag structure and discuss various activities that can create or update the ShellBag information across Windows operating systems.

2 Windows ShellBag Registry Structure

The ShellBag information comprises two main registry keys, BagMRU and Bags. The BagMRU key stores folder names and records folder paths by creating the similar tree structure. The Bags key stores the view preferences such as the window size, location and view mode.

The BagMRU key itself represents the Desktop. Except BagMRU itself, its child keys are not assigned to any specific folders. The key "BagMRU\0" represents the first

© 2014 The SANS Institute Author retains full rights.

folder the ShellBag information is created for. The key "BagMRU\1" represents the second folder and so on.

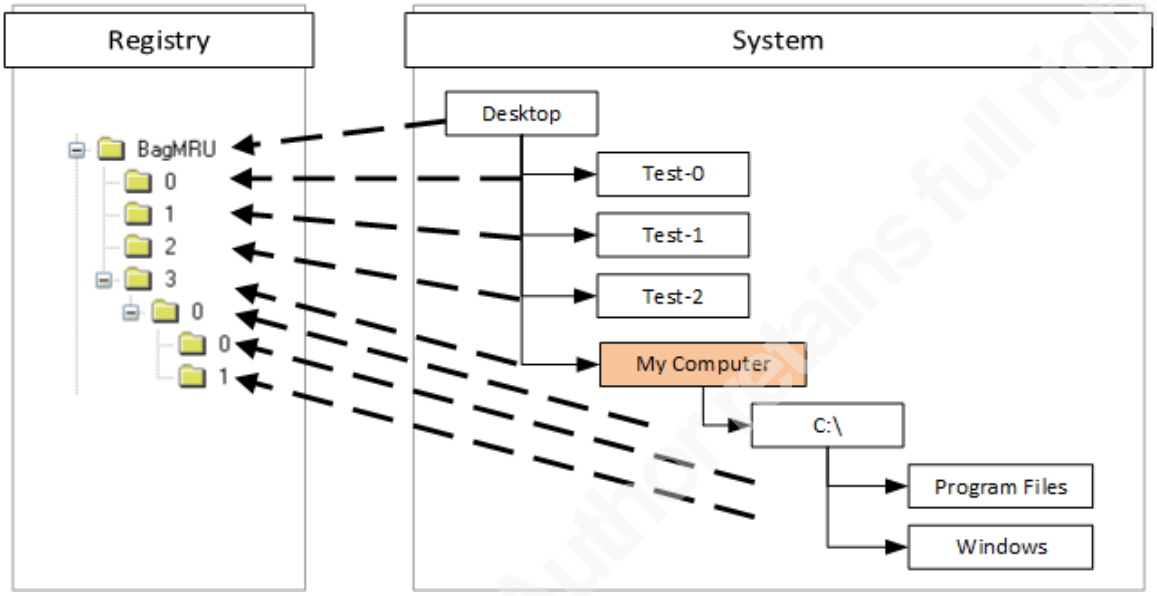


Figure 1 BagMRU Structure

The figure 1 is an example. It shows BagMRU key itself represents the Desktop. Its child key "BagMRU\0" represents "Desktop\Test-0" folder. The key "BagMRU\1" represents "Desktop\Test-1" folder and the key "BagMRU\2" represents the "Desktop\Test-2" folder. For Windows top-level special folders or virtual folders such as "My Documents", "Control Panel" and "My Computer", the registry key of those folders is created right under BagMRU.

As shown in the figure 2, the folder name of child key is stored in the registry value under the parent key. For instance, the folder name of the key "BagMRU\2" is stored in a binary registry value "2" under BagMRU key. It shows the key "2" represents the "Test-2" folder on the Desktop.

© 2014 The SANS Institute Author retains full rights.

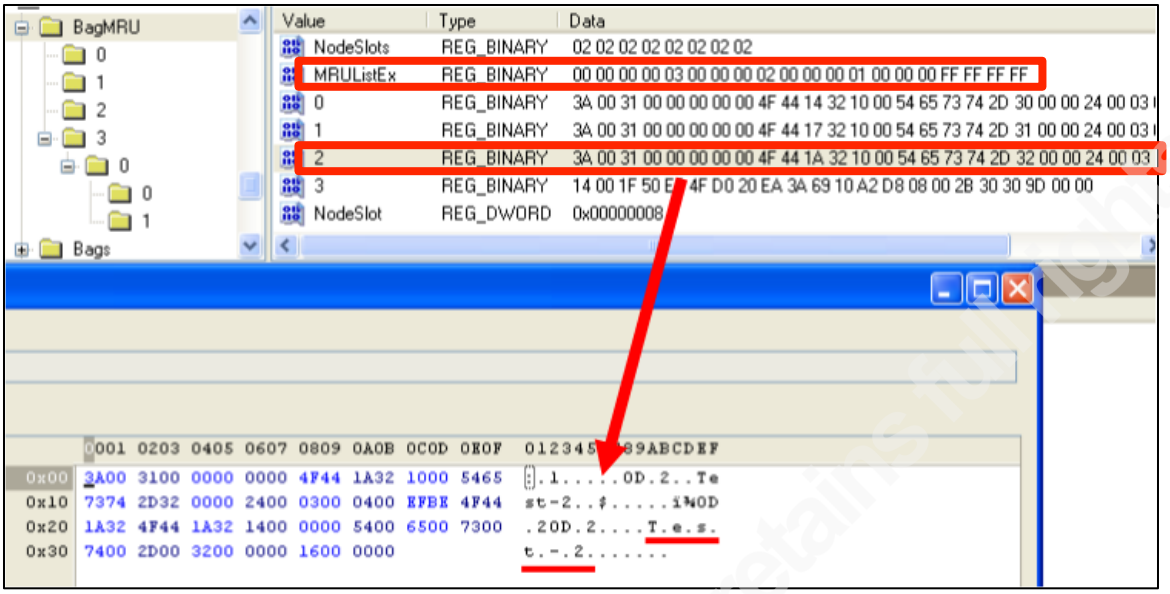


Figure 2 BagMRU Registry Values

Including BagMRU, every registry key under BagMRU has a MRUListEx binary registry value. It records the order of the recent accessed child folders. For instance, the figure above shows the MRUListEx value is "0, 3, 2, 1". It means the order of the most recent accessed folders on the Desktop is "Desktop\Test-0", "Desktop\Test-2" and "Desktop\Test-1". If the order is changed, BagMRU\MRUListEx will be updated accordingly and the last written time of BagMRU will be modified.

Besides MRUListEx, most of keys under BagMRU also contain a DWORD value named NodeSlot. NodeSlot contains a slot number that points to the registry key under Bags, which contains the view preferences. For instance, in the figure 2, BagMRU contains NodeSlot registry value 8. It indicates the view preferences of the Desktop are stored under the "Bags\8" registry key. As shown in the figure 3, "Bags\8\Shell" registry key stores view preferences of the Desktop.

© 2014 The SANS Institute Author retains full rights.

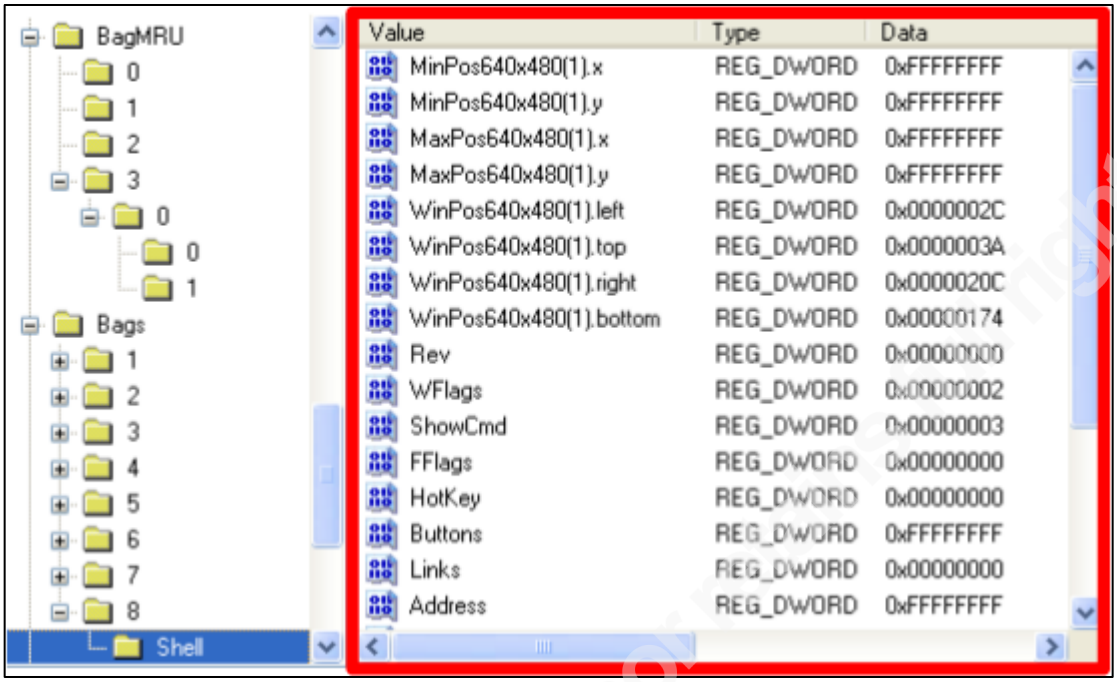


Figure 3 Bags Registry Values

Nevertheless, ShellBag structure differs slightly between Windows operating systems.

2.1 ShellBag Registry Structure in Windows XP

ShellBag registry keys and values in Windows XP can be found in the file below.

Windows Operating System	File containing ShellBag information
Windows XP (32 bit & 64 bit)	%UserProfile%\NTUSER.dat

The registry values can be found in the following registry keys.

Windows Operating System	ShellBag Registry Keys
Windows XP (32 bit & 64 bit)	NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\BagMRU NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\Bags

© 2014 The SANS Institute Author retains full rights.

2.1.1 Shell & ShellNoRoam

The experiments show that the Shell stores the ShellBag information for the Desktop, Windows network folders, remote machines and remote folders. The ShelNoRoam stores the ShellBag information for the Desktop, ZIP files, remote folders, local folders, Windows special folders and virtual folders.

2.2 ShellBag Registry Structure in Windows Vista

ShellBag registry keys and values in Windows Vista can be found in files below.

Windows Operating Systems	File containing ShellBag information
Windows Vista (32 bit & 64 bit)	%UserProfile%\NTUSER.DAT %UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat

The registry values can be found in the following registry keys.

Windows Operating System	ShellBag Registry Keys
Windows Vista (32 bit)	NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\BagMRU UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\Bags
Windows Vista (64 bit)	NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\BagMRU UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\Bags UsrClass.dat\Wow6432Node\Local Settings\Software\Microsoft\Windows\Shell\BagMRU UsrClass.dat\Wow6432Node\Local Settings\Software\Microsoft\Windows\Shell\Bags

© 2014 The SANS Institute Author retains full rights.

According to Microsoft (2012), the following keys may exist. However, they have not been found in my experiments.

NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\BagMRU
NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\Bags

2.2.1 Shell & ShellNoRoam

In Windows XP, ShellBag information is stored under Shell and ShellNoRoam keys. In Windows Vista, ShellNoRoam key is found in NTUSER.DAT only. However, it only stores a DWORD value called "BagMRU Size". It appears, besides "BagMRU Size", the rest of ShellBags information is stored under Shell keys.

2.2.2 NTUSER.DAT & UsrClass.dat

The experiments show that the NTUSER.DAT stores the ShellBag information for the Desktop, Windows network folders, remote machines and remote folders. The UsrClass.dat stores the ShellBag information for the Desktop, ZIP files, remote folders, local folders, Windows special folders and virtual folders.

2.3 ShellBag Registry Structure in Windows 7, 8 and 8.1

ShellBag registry keys and values in Windows 7, 8 and 8.1 can be found in files below.

Windows Operating Systems	File containing ShellBag information
Windows 7, 8 & 8.1 (32 bit & 64 bit)	%UserProfile%\NTUSER.dat %UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat.

The registry values can be found in the keys below.

Windows Operating Systems	ShellBag Registry Keys
Windows 7, 8 & 8.1 (32 bit & 64 bit)	NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\BagMRU UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\Bags

© 2014 The SANS Institute Author retains full rights.

2.3.1 Shell

In Windows XP, Shell and ShellNoRoam keys are used to store ShellBag information. Starting from Windows 7, ShellNoRoam is no longer used. The ShellBag information is stored under Shell keys only.

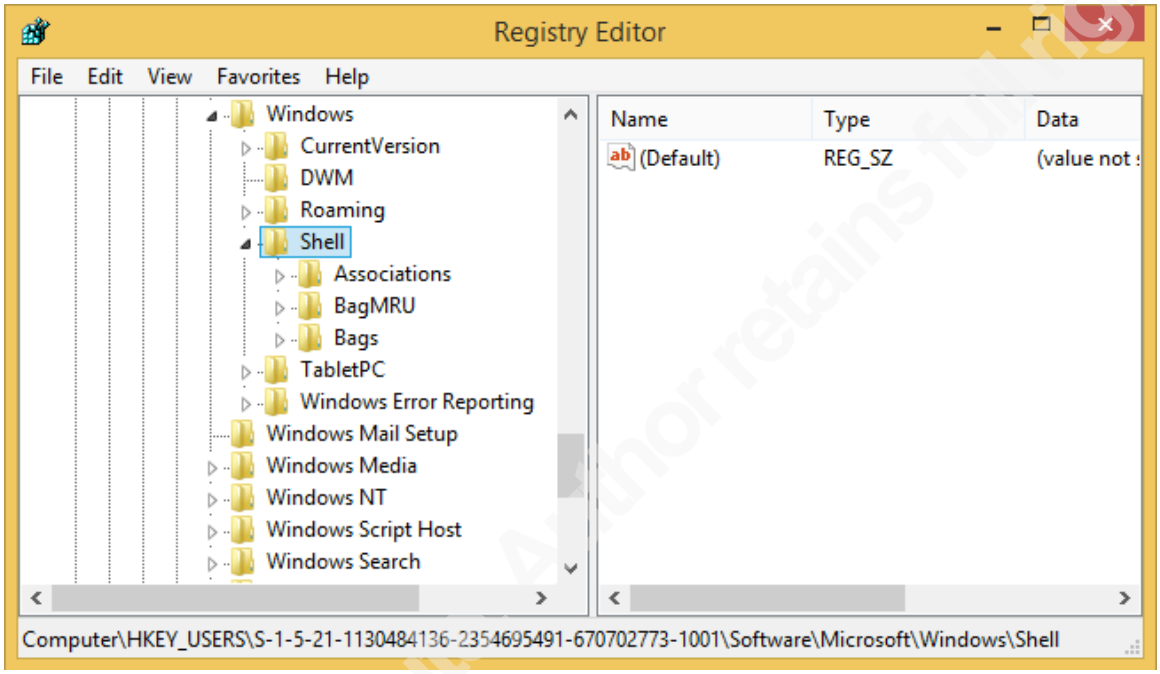


Figure 4 ShellBags structure in Windows 8.1

2.3.2 NTUSER.DAT & UsrClass.dat

The experiments show that the NTUSER.DAT stores the ShellBag information for the Desktop, Windows network folders, remote machines and remote folders. The UsrClass.dat stores the ShellBag information for the Desktop, ZIP files, remote folders, local folders, Windows special folders and virtual folders.

3 Activities

SANS FOR508 course material (2011) indicates ShellBag information is only written when a folder is opened and has default settings adjusted. According to Zhu, Gladyshev and James (2009), ShellBag information is available only for folders that have been opened and closed in Windows Explorer at least once. Nevertheless, the

© 2014 The SANS Institute Author retains full rights.

experiments show ShellBag information can be created under different situations between Windows operating systems.

3.1 Windows XP

3.1.1 Creation

In Windows XP, the experiments show that ShellBag information will be created by various activities. The following will discuss the details.

3.1.1.1 Windows Explorer & Desktop

In the Windows Explorer and on the Desktop, the experiments revealed that when folders are opened, the creation of ShellBag information depends on whether a folder has any child items. The child item can be a file or subfolder. If a folder has the child item(s), once the folder is opened in Windows Explorer, ShellBag registry keys and values will be created for the folder. The last written time of the correspondent BagMRU and Bags registry keys will be created once the folder is opened.

If the folder is empty, the ShellBag keys won't be created when the folder is opened. The ShellBag information will be created when the folder is closed or another folder is opened in the same window. The last written time of those keys will be written once the keys are created.

If a child item is created in the opened empty folder, ShellBag registry keys and values won't be created immediately after the child item is created. The ShellBag information will be created after the folder is closed or another folder is opened in the same window.

However, if a folder has the hidden item(s) and Windows Explorer is configured not to show them, the ShellBag information won't be created when the folder is opened. It will be created when the folder is closed or another folder is opened in the same window. If a folder has the hidden item(s) and Windows Explorer is configured to show them, ShellBag information will be created once the folder is opened.

The experiments also show that without opening the folders, the ShellBag information will be available by the following steps.

© 2014 The SANS Institute Author retains full rights.

- Right click on folders and choose “Properties”. Choose “Customize”. Then, click “OK”.

3.1.1.2 Compressed Files (ZIP Files)

Windows Explorer will not only create the ShellBag information for the folders, but also ZIP files. It will be created by the following steps.

- Open a ZIP file in Windows Explorer and close it or open a folder in the same window.

The ShellBag information will contain the created date, modified date and accessed date of the ZIP file.

3.1.1.3 Search Window

The view preferences of the Search window will be recorded in the ShellBags by the following steps.

- Open Windows Explorer. Click Search icon. Choose the search scope and click Search. Then, close the window or open a folder in the same window.

In the ShellBag information, the folder name is recorded as “Search Result”. However, the view preferences of the Search window can also be recorded in the ShellBags by one of the following steps.

- Open the Search window from Start menu. Then, close the window or open a folder in the same window.
- Open the Search window. Then, choose the search scope and click Search.

By these approaches, the folder name in the ShellBags is recorded as {CCE6191F-13B2-44FA-8D14-324728BEEF2C} instead.

3.1.1.4 Remote Machines & Remote Folders

In Windows XP, when the remote machine is opened and closed in Windows Explorer, its ShellBag information will be written. If those remote machines have any shared folders containing the child item(s), their ShellBag information of shared folders

© 2014 The SANS Institute Author retains full rights.

will be created when they are opened in Windows Explorer. However, if they are empty, their ShellBag information will not be created after they are opened. They will be created after they are closed or another folder is opened in the same window.

3.1.1.5 Windows Special Folders & Virtual Folders

Windows XP contain many special folders, such as "My Documents", "My Music" and "My Pictures". Windows XP also contain virtual folders, such as "My Computer" and "Control Panel" which are the roots of hierarchical trees that contain other virtual folders.

Some folders have more than one folder type. For instance, Desktop can be a special folder, virtual folder or actual file system folder. "My Documents" can be a file system folder, virtual folder or library.

The activities that cause the creation of their ShellBag information depend on the folder type and situation. It can be quite complex. If any special folders or virtual folders are important to the investigation, it is necessary to conduct the experiments to confirm the details with the environment close to the case as much as possible.

3.1.1.6 Removable Devices

Windows XP does not appear to create the ShellBags for folders on removable devices.

3.1.2 Modification

Many user and system activities can change the registry values under ShellBag keys. Once a value is added or changed, the last written time of the ShellBag registry keys will be updated. The following will discuss those registry keys.

3.1.2.1 NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU

This key represents Desktop. When the MRUListEx or NodeSlots is modified, the last written time of this key will be updated.

3.1.2.2 NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU\[node number]

Each [node number] child key under BagMRU represents a remote machine, remote folder or Windows network special folder. When a new key or a new value is

© 2014 The SANS Institute Author retains full rights.

created under the key, the last written time will be updated. When the MRUListEx is modified, it will also update the last written time.

3.1.2.3 NTUSER.DAT\Software\Microsoft\Windows\Shell\Bag\[slot number]

This key only contains a Shell key. The last written time of this key is rarely updated by the user activities.

3.1.2.4 NTUSER.DAT\Software\Microsoft\Windows\Shell\Bag\[slot number]\Shell

This key contains view preferences. When the view preferences are adjusted, the last written of this key will be updated.

3.1.2.5 NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags\1\Desktop

The experiment shows this key appears to be reserved for Desktop, shown as below, to store Desktop's view preferences.



Figure 5 Desktop in Windows XP

© 2014 The SANS Institute Author retains full rights.

However, the view preferences of "Desktop folder", as below, are stored under NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\Bag\[slot number]\Shell.

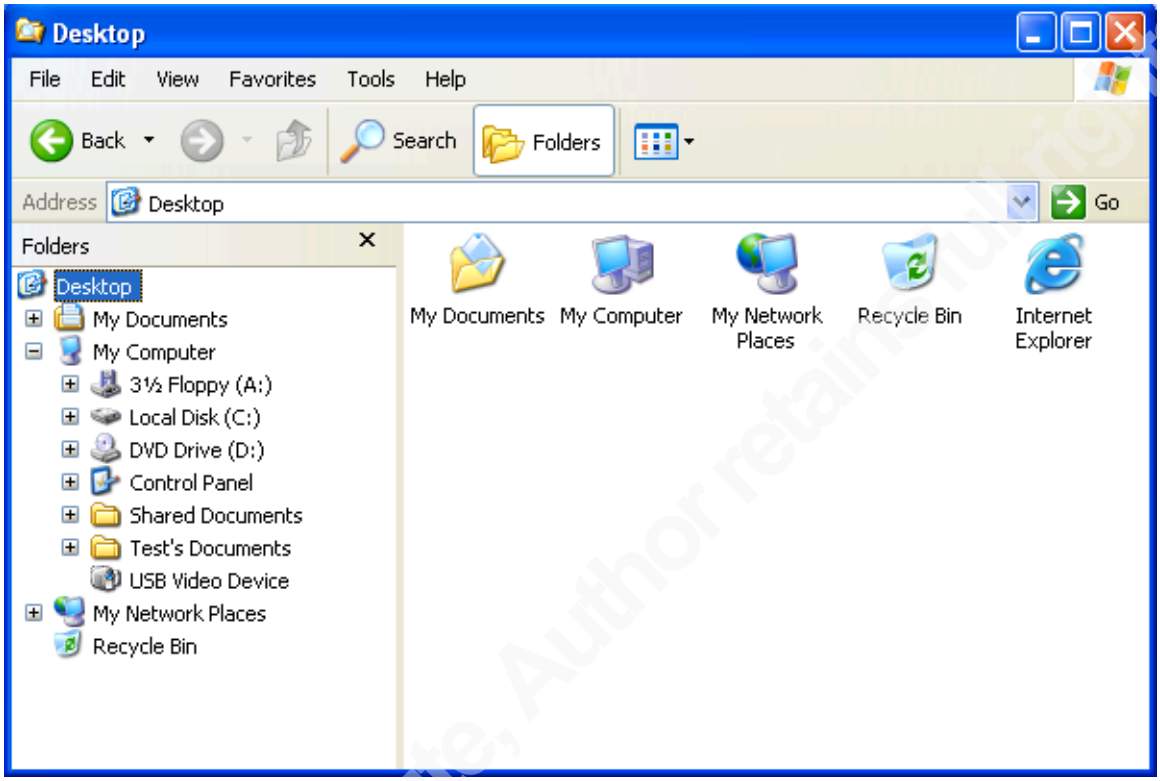


Figure 6 Desktop folder in Windows XP

3.1.2.6 NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\BagMRU

This key represents Desktop. If the ShellBags information is created for any file system folders/ZIP files on Desktop, Windows top-level special folders or virtual folders, it will be created under this key and the last written time will also be updated. When MRUListEx and NodeSlots need to be updated, the last written time will be updated as well.

3.1.2.7 NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\BagMRU\[node number]

Each [node number] child key represents a zip file, file system folder, Windows special folder or virtual folder. It contains the slot number that points to the view preferences and node numbers of the child folders. If a new node number is created or the MRUListEx needs to be updated, the last written time of the BagMRU key will be updated.

© 2014 The SANS Institute Author retains full rights.

In Windows XP, Windows Explorer has six view modes, which are Icons, List, Details, Thumbnails, Tiles and Filmstrip. The experiment shows MRUListEx behaves differently in Thumbnails view. In this view, Windows Explorer shows a folder icon for each folder. Windows Explorer stores a folder icon in the Thumbs.db file. The Thumbs.db file is a hidden database of graphic files for the folder. It stores the filename, modification date and thumbnail of the graphic files. When Windows creates a folder icon, Windows uses {A42CD7B6-E9B9-4D02-B7A6-288B71AD28BA} as its filename in the Thumbs.db. Hence, when the Thumbnail view is set to view the content of the folder, Windows Explorer will search for Thumbs.db in each child folder to look for the folder icon for each child folder.

If the icon cannot be found, Windows Explorer will try to create it. The whole process is quite complicated. It may impact the MRUListEX of child folders and child's child folders. Consequently, it may affect their ShellBags timestamps. The following is the summary of the activities that occur when a folder is opened in the Thumbnail view. More information is provided in Appendix A.

1. Search for Thumbs.db in each child folder in folder name order.
2. If Thumbs.db is found in the child folder, search for the folder icon. If it can be found, it will be shown in Windows Explorer.
3. If Thumbs.db is not found in the child folder, search for folder.jpg and then folder.gif in each child folder. When Windows Explorer searches for them in each child folder, the experiment shows if the child folder's ShellBags information has been created, parent folder's MRUListEx will be updated when it is required. If the child folder's ShellBags information hasn't been created, Windows won't modify the MRUListEx. If MRUListEx is updated, the last written time will also be updated.
4. If folder.jpg or folder.gif is found in the child folder, Windows Explorer will create and display the folder icon. The icon will be stored in the Thumbs.db file in the child folder.

© 2014 The SANS Institute Author retains full rights.

5. If folder.jpg and folder.gif are not found in the child folder, Windows will check whether any graphic files are stored in the child folder. If graphic files are found, Windows will use up to four graphic files to create the icon. The icon will be stored in the Thumbs.db file in the child folder.
6. If no graphic files can be found, Windows Explorer will use the similar steps to search for the folder icon of child's child folder in each child's child folder.
7. If folder icons of child's child folders cannot be found, Windows Explorer will display the default folder icon  for the child folder.

In Thumbnails view, when the Windows Explorer searches for folder.jpg or folder.gif in each child folder or child's child folder in the Thumbnail view, MRUListEx registry value will be updated when it is required. For instance, the folder A contains three child folders, A-0, A-1 and A-2s. Their correspondent BagMRU keys are as below.

Folder Name	BagMRU Key
A	BagMRU\0\0
A-0	BagMRU\0\0\0
A-1	BagMRU\0\0\1
A-2	BagMRU\0\0\2

When the folder A is opened in Windows Explorer in Thumbnail view, if A-0, A-1 and A-2 don't have any folder icons. Every time when the folder A is opened, Windows Explorer will search for folder.jpg and folder.gif in A-0, A-1 and A-2. During the search process, MRUListEx will be updated accordingly. As a consequence, every time when the folder A is opened, BagMRU\0\0\MRUListEx will always be changed to "2 1 0" and the last written time of BagMRU\0\0 will be updated. Therefore, in Thumbnails view, folder's MRUListEx doesn't always reflect user's activities. It may reflect Windows Explorer's activities instead.

© 2014 The SANS Institute Author retains full rights.

3.1.2.8 NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\Bag\[slot number]

This key only contains a Shell key. The last written time of this key is rarely updated by the user activities.

3.1.2.9 NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\Bag\[slot number]\Shell

This key contains view preferences. When the view preferences are adjusted, the last written of this key will be updated.

3.1.3 Deletion

When a folder is deleted, the correspondent ShellBag registry keys and values will not be removed. However, several tools have been developed to remove the ShellBag information from the registry.

3.1.4 ShellBag Inheritance

When a folder or ZIP file is deleted, its ShellBag information won't be deleted. If a folder or ZIP file is deleted and a new one is created with the same name, the new one will inherit the old one's ShellBag information.

3.2 Windows Vista, 7, 8 and 8.1

3.2.1 Creation

In Windows Vista, 7, 8 and 8.1, the experiments show that ShellBag information will be created by various activities in different situations. The following will discuss the details.

3.2.1.1 Windows Explorer

In Windows Explorer, no matter a folder is empty or not, ShellBag information folder will be created when any of the following activities is performed in Windows Explorer.

- Create a folder
- Click a folder to select it
- Right-click a folder

© 2014 The SANS Institute Author retains full rights.

- Click a folder to select it and press an arrow key to move the bar to select other folders (The ShellBag information for those folders will be created.)

As the result, any of the following activities in Windows Explorer will create the ShellBag information for a folder.

- Open a folder (Double-click a folder)
- Rename folder name (Right-click a folder and select "Rename" or select the folder and press "F2". Change the folder name and press enter. The ShellBag information of original and renamed folder names will be created.)
- Delete a folder
- Copy a folder (If both folders are on the local hard drives, the ShellBag information of source folder and destination folder will be created.)

3.2.1.2 Desktop

On the Desktop, no matter a folder is empty or not, the experiments reveal that the ShellBag information for a folder will be created when any of the following activities is performed on Desktop.

- Open a folder
- Right-click a folder
- Cut a folder (Ctrl+x)
- Copy a folder (Ctrl+c)
- Rename a folder (In Windows 7, 8 and 8.1, select the folder and press "F2".)
- Delete a folder (Select the folder and press "Delete")

As the result, the following activities on Desktop will create the ShellBag information.

© 2014 The SANS Institute Author retains full rights.

- Change the folder name (Right-click and choose "Rename". Or, in Windows 7, 8 and 8.1, select the folder and press "F2". Change the folder name and press Enter. The ShellBag information of original folder name will be created.)
- Delete a folder (Right-click and select "Delete" or click the folder and press "Delete")
- Copy a folder (In Windows 7, 8 and 8.1, the ShellBag information of source folder will be created. However, in Vista, if the destination folder is on the Desktop, the ShellBag information of source and destination folders will be created.)

3.2.1.3 Compressed Files (ZIP Files)

Windows Explorer will not only create the ShellBag information for the folders, but also ZIP files. The following steps will create it.

- Open a ZIP file in Windows Explorer and close it or open another folder/ZIP file in the same window.

The ZIP file's created date, modified date and accessed date will be recorded in the ShellBag information.

3.2.1.4 Search Result

The view preferences of the "Search Result" window will be recorded in the ShellBags by the following steps.

- Type the query in the Start menu's "Start Search" column or in Windows Explorer's Search column and execute it. Close the search result or open another folder/ZIP file in the same window.

In Windows Vista and 7, if the query is run in the Start menu's "Start Search" column and the search window appears, the query will be recorded. For instance, if a user types in "ab" in the Start Search and press the enter button, after the search window appears, "query=ab" will be recorded in ShellBags. Windows 8 and 8.1 use different Start

© 2014 The SANS Institute Author retains full rights.

screen design. The search run through Start screen doesn't seem to be recorded in ShellBags.

3.2.1.5 desktop.ini

The desktop.ini file is a hidden file in a folder. It can be used to customize the folder icon and folder type. The experiments show that if the folder type or CLSID is specified in the desktop.ini, Windows Explorer will create the ShellBag information only after the folder is opened.

3.2.1.6 Command Prompt

In Windows Vista, the experiments show that in the Command Prompt, if the folders are created in the %UserProfile%\Desktop folder via "mkdir" command, the ShellBag information of those folders will be created.

3.2.1.7 Removable Devices

ShellBags will be created when folders on removable devices are opened and closed.

3.2.1.8 Remote Machines & Remote Folders

In Windows Vista, the ShellBag information of remote machines will be created after those machines are opened and closed in Windows Explorer or opened and another folder/ZIP file is opened in the same window. If the remote machines have any shared folders, their ShellBag information will be created after they are opened. If the shared folders have any child folders, the ShellBag information of the child folders will be available after the child folders are opened.

In Windows 7, 8 and 8.1, the ShellBag information of remote machines will be created after those machines are opened and closed or opened and another folder/ZIP file is opened in the same window. If the remote machines have any shared folders, their ShellBag information will be created after they are opened. However, if those shared folders contain any child folders, the ShellBag information of the child folders can be available without being opened. The activities mentioned in the "Windows Explorer" section can cause their ShellBag information to be created.

© 2014 The SANS Institute Author retains full rights.

3.2.1.9 Windows Special Folders, Virtual Folders & Libraries

Windows Vista, 7, 8 and 8.1 contain many special folders, such as "Documents", "Music", "Pictures" and "Videos". In Windows 7, 8 and 8.1, those folders are also named "My Documents", "My Music", "My Pictures" and "My Videos". They map to actual file system folders. For instance, the "My Documents" folder maps to "%UserProfile%\Documents" folder and "My Music" folder maps to "%UserProfile%\Music" folder. Windows Vista, 7, 8 and 8.1 also contain virtual folders, such as "Computer" and "Control Panel" which are the roots of hierarchical trees which contain other virtual folders.

Starting from Windows 7, Libraries feature is included in Windows Explorer. A library can gather files or folders from different locations and display them as a single location. By default, Windows Explorer has the "Documents" library, "Music" library, "Pictures" and "Videos" library.

Some folders have more than one folder type. For instance, Desktop can be a special folder, virtual folder or actual file system folder. The profile folder can be a virtual folder or actual file system folders. "Documents" can be a file system folder, virtual folder or library.

The activities that can cause the creation of their ShellBag information depend on the folder type and situation. It can be quite complex. If any special folders or virtual folders are important to the investigation, it is necessary to conduct the experiments to confirm the details with the environment close to the case as much as possible.

3.2.2 Modification

Many user and system activities can change the registry values under ShellBag keys. Once the values are changed, the last written time of the ShellBag registry keys is also updated.

3.2.2.1 NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU

This key represents Desktop. When the MRUListEx or NodeSlots needs to be updated, the last written time of this key will be updated. When a new key is created under this key, the last written time will also be updated.

© 2014 The SANS Institute Author retains full rights.

3.2.2.2 NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU\[node number]

Each [node number] child key under BagMRU represents a Windows network folder, remote machine or remote folder. The experiments show that in order to create this key, the remote folder has to be opened and closed or opened and then another folder/ZIP file is opened in the same window.

3.2.2.3 NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags\1\Desktop

The experiment shows Windows Explorer stores the view preferences of "Desktop" and "Desktop folder" under different registry keys. This key appears to be reserved to store Desktop's view preferences.

3.2.2.4 NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags\1\ComDlg

This key appears to store Desktop's view preference in the dialog box, shown as below.

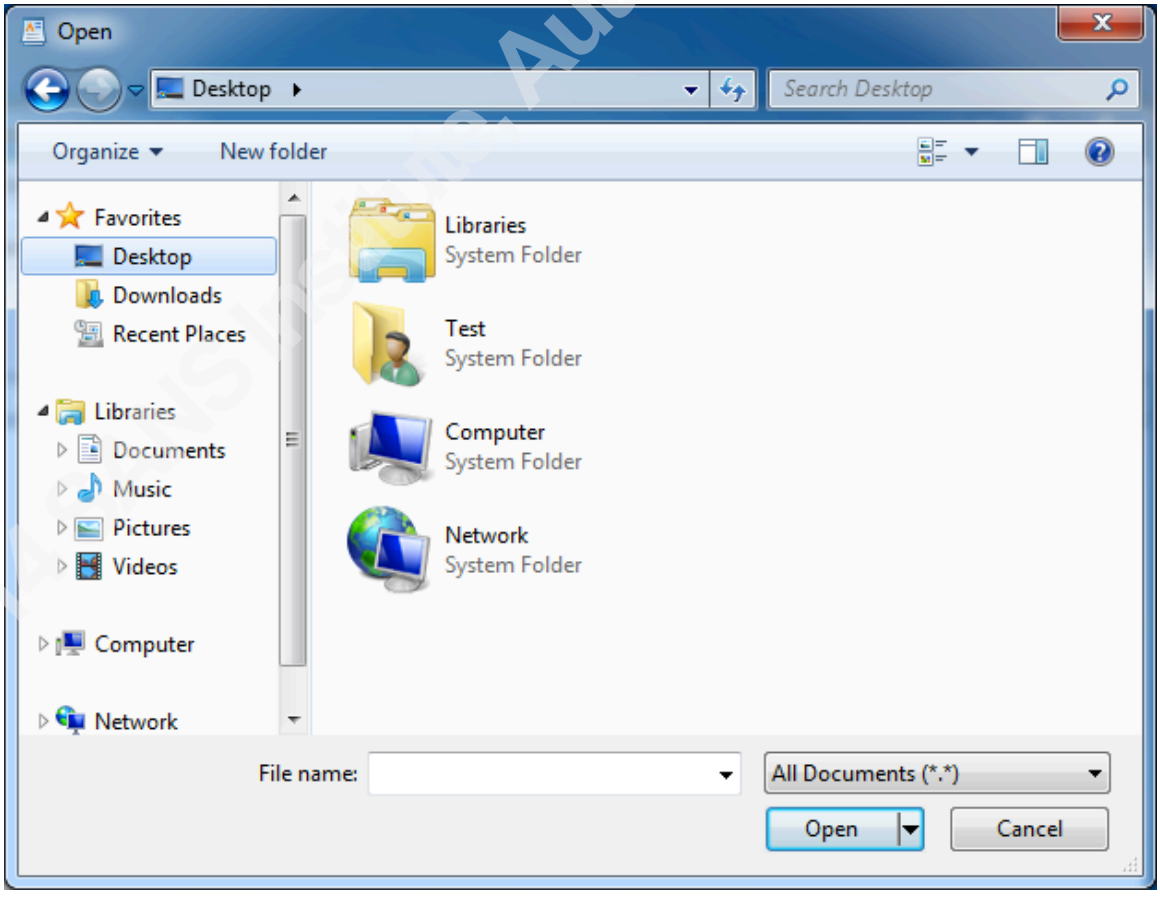


Figure 7 Dialog box in Windows 7

© 2014 The SANS Institute Author retains full rights.

3.2.2.5 NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags\1\ComDlgLegacy

This key appears to store Desktop's view preference in the legacy dialog box.

3.2.2.6 NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags\[slot number]

Each [slot number] stores view preferences for the Windows network folder, remote machine or remote folder.

3.2.2.7 UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

This key represents Desktop. If the ShellBag information is created for any file system folders/ZIP files on Desktop, Windows top-level special folders or virtual folders, they will be created under this key and the last written time will also be updated. Because this key contains MRUListEx and NodeSlots, if Windows Explorer changes them, it will update the last written time as well.

3.2.2.8 UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\[node number]

Each [node number] child key can represents a zip file, file system folder, library, Windows special folder or Windows virtual folder. It contains NodeSlot, MRUListEx and node numbers of the child folders. If the MRUListEx is updated or a new node number is created, it will update the last written time.

Windows Vista, 7, 8 and 8.1 do not appear to have the Thumbnails view. Moreover, they do not use Thumbs.db in each folder to store the icons. They use central thumbnail databases in the %UserProfile%\AppData\Local\Microsoft\Windows\Explorer folder. Windows Explorer doesn't need to scan folder.jpg or folder.gif in each folder any more. Hence, the Thumbnail view issue described in the section 3.1.2.7 doesn't appear in those Windows operating systems.

3.2.2.9 UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\Bags\[slot number]

The last written time of this key is rarely updated. It will be updated when a key, such as Shell, ComDlg or ComDlgLegacy, is created.

© 2014 The SANS Institute Author retains full rights.

3.2.2.10 UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\Bags\[slot number]\ComDlg

Not every [slot number] key contains this key. The folder needs to be opened and closed in the dialog box or opened and another folder is opened in the same dialog box to create this key. This key contains the [folder type GUID] key.

3.2.2.11 UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\Bags\[slot number]\ComDlg\[folder type GUID]

This key contains the folder preferences for a folder in the dialog box.

3.2.2.12 UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\Bags\[slot number]\ComDlgLegacy

Not every [slot number] key contains this key. The folder needs to be opened and closed in the legacy dialog box or opened and another folder is opened in the same legacy dialog box to create this key. This key contains the [folder type GUID] key.

3.2.2.13 UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\Bags\[slot number]\ComDlgLegacy\[folder type GUID]

This key contains the folder preferences for a folder in the legacy dialog box.

3.2.2.14 UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\Bags\[slot number]\Shell

Not every [slot number] key contains this key. This key is created for the folder preferences in Windows Explorer. Depending on the folder types, some of them don't have any registry values. However, some of them store the following registry values.

- KnownFolderDerivedFolderType
- SniffedFolderType

SniffedFolderType shows the type of the folder. For instance, if the folder contains graphic files, this registry value will show Pictures. If the folder contains documents, this registry value will show Documents.

© 2014 The SANS Institute Author retains full rights.

3.2.2.15 UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\Bags\[slot number]\Shell\[folder type GUID]

Windows Explorer stores the view preference in this key. When Windows Explorer creates this key for a folder, it will check the folder type and create the GUID accordingly. For instance, if the folder type is generic, Windows Explorer will create UsrClass.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags\[slot number]\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}. If the folder contains a graphic file, Windows Explorer will create UsrClass.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags\[slot number]\Shell\{B3690E58-E961-423B-B687-386EBFD83239}. If the folder contains a document, it will create UsrClass.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags\[slot number]\Shell\{7d49d726-3c21-4f05-99aa-fdc2c9474656}. The Appendix B has the full list of folder type and GUID by Joachim Metz.

Certain folders may have more than one GUID. SniffedFolderType shows which GUID stores the current view settings. Therefore, if the view preference is modified, the last written time of that GUID will be updated.

3.2.3 Deletion

When a folder is deleted, the correspondent ShellBag registry keys and values will not be removed. However, several tools have been developed to remove the ShellBag information from the registry.

3.2.4 ShellBags Inheritance

When a folder or ZIP file is deleted, its ShellBag information won't be deleted. If a folder or ZIP file is deleted and a new one is created with the same name, the new one will inherit the old one's ShellBag information.

4 Conclusion

ShellBags contain the folder structure and view preferences. It may help forensicators identify when and which folders a user accessed. Furthermore, it may demonstrate when and which remote machines/servers a user accessed via Windows Explorer. However, ShellBag structure differs slightly between Windows versions. A lot

© 2014 The SANS Institute Author retains full rights.

of activities can affect its timestamps. Consequently, many factors need to be considered in order interpret it correctly. The sections above summarize the ShellBag structure in different Windows operating systems. They also shed light on how various activities impact the ShellBag timestamps across Windows versions. Those sections can help forensicators have the better understanding of ShellBag information. Nevertheless, they also demonstrate its complexity. Further work is required to explore more details. If the investigation requires the ShellBag information, further experiments need to be conducted with the environment close to the case as much as possible.

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

5 References

SANS Institute (2011). SANS Forensics 508. n.p.: Author

Zhu, Y., Gladyshev, P., & James, J. (2009). Using shellbag information to reconstruct user activities, Digital Investigation. Retrieved from http://www.dfrws.org/2009/proceedings/p69-zhu.pdf

McFedries, P., Winslow, G., Andersen, S., & Wilson, A. (2003). Insider Power Techniques for Microsoft® Windows® XP. Microsoft Press

Microsoft. (2013, May 22). How to modify your folder view settings or to customize a folder. Retrieved Aug 15, 2013, from http://support.microsoft.com/kb/812003

Microsoft. (2012, June 28). Changes to the size, view, icon or position of a folder are lost. Retrieved Aug 6, 2013, from http://support.microsoft.com/kb/813711

Tilbury, C. (2011, July 5). Computer Forensic Artifacts: Windows 7 Shellbags [Web log post]. Retrieved from http://digital-forensics.sans.org/blog/2011/07/05/shellbags

TzWorks. (2011, July 5). Windows ShellBag Parser (sbag). Retrieved from https://www.tzworks.net/prototype_page.php?proto_id=14

Microsoft. (n.d.). Registry Value Types. Retrieved from http://msdn.microsoft.com/en-us/library/ms724884%28VS.85%29.aspx

Microsoft. (n.d.). folderType Element (Library Schema). Retrieved from http://msdn.microsoft.com/en-us/library/windows/desktop/dd798386%28v=vs.85%29.aspx

Carvey, H. (2009). Registry Analysis SANS Forensic Summit 2009. Retrieved from http://computer-forensics.sans.org/summit-archives/2009/8-harlan-carvey-registry-analysis.pdf

Metz, J., (2013, June 23). Folder Type identifiers. Retrieved from http://code.google.com/p/libfwsi/wiki/FolderTypeIdentifiers

Microsoft. (2013, November 16). Registry Keys Affected by WOW64. Retrieved from http://msdn.microsoft.com/en-us/library/windows/desktop/aa384253%28v=vs.85%29.aspx

Microsoft. (n.d.). CSIDL. Retrieved from http://msdn.microsoft.com/en-us/library/windows/desktop/bb762494%28v=vs.85%29.aspx

© 2014 The SANS Institute Author retains full rights.

Microsoft. (n.d.). KNOWNFOLDERID. Retrieved from http://msdn.microsoft.com/en-us/library/windows/desktop/dd378457%28v=vs.85%29.aspx

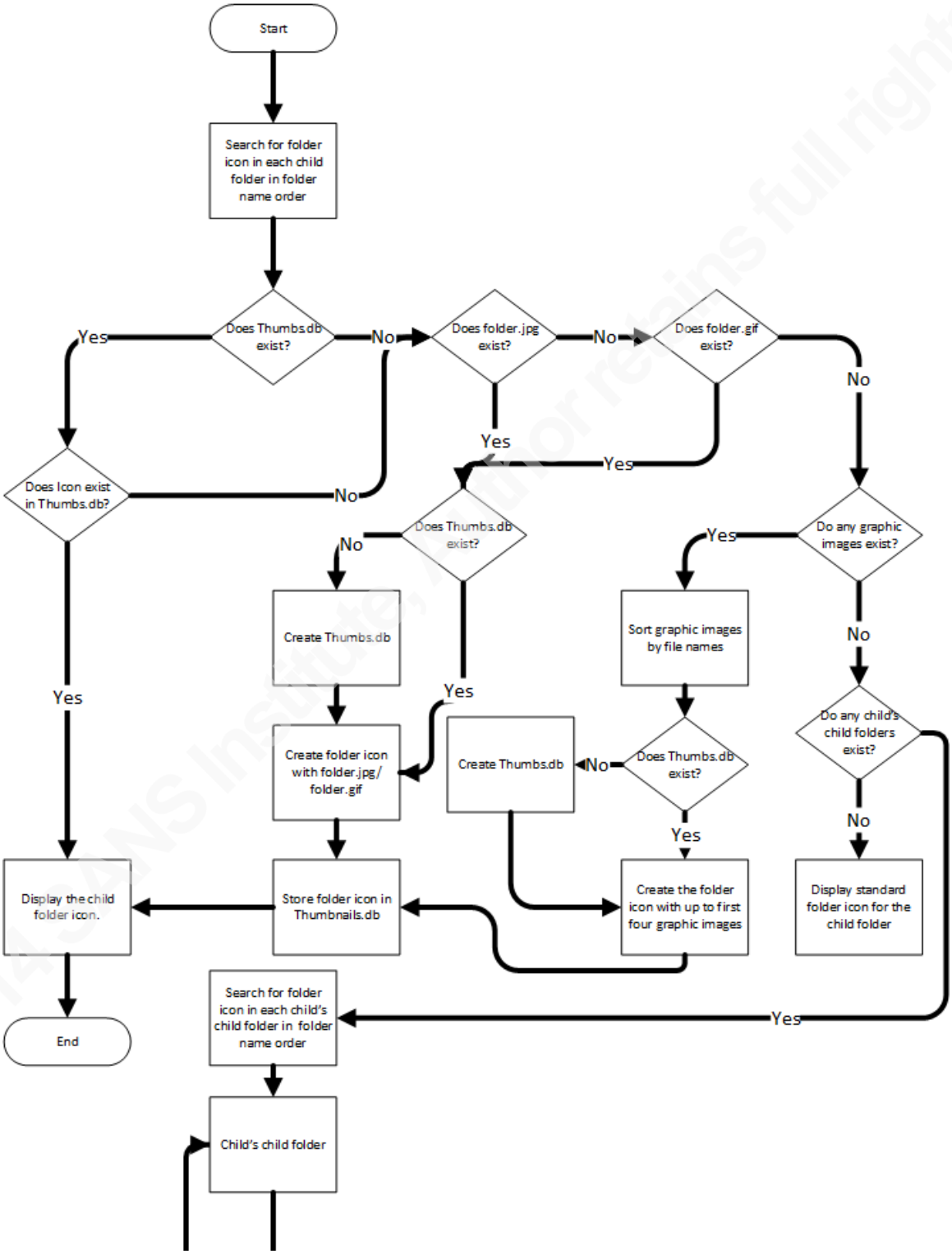
Microsoft. (n.d.). Working with libraries. Retrieved from http://windows.microsoft.com/en-au/windows7/working-with-libraries

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

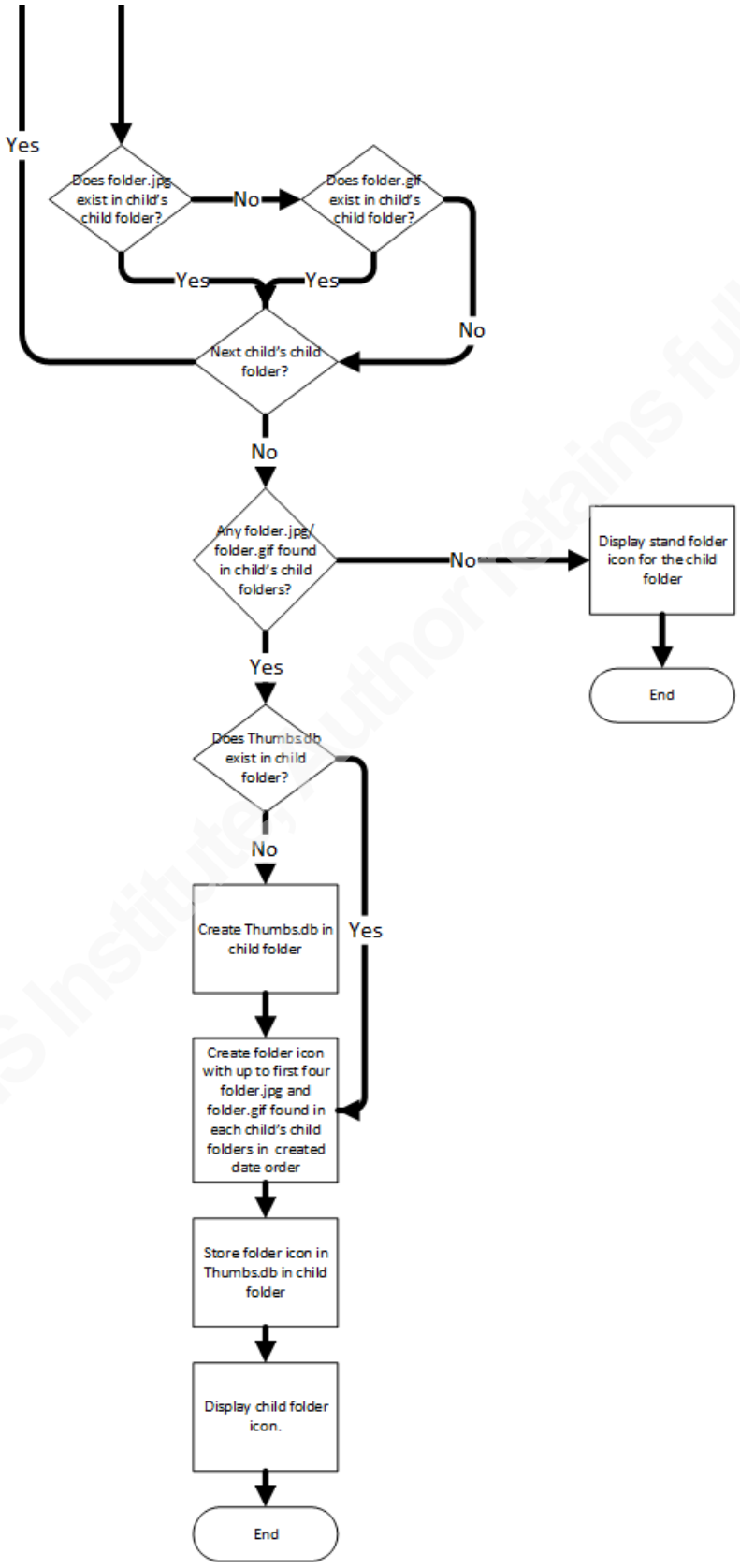
Appendix A

Thumbnail view activity in Windows XP.



Vincent Lo, LYLC.SYMPHONICA@GMAIL.COM

© 2014 The SANS Institute Author retains full rights.



Vincent Lo, LYLC.SYMPHONICA@GMAIL.COM

© 2014 The SANS Institute Author retains full rights.

Appendix B

Folder Type Listed by Joachim Metz (2013).

GUID	Description
{0b0ba2e3-405f-415e-a6ee-cad625207853}	Searches
{0b2baaeb-0042-4dca-aa4d-3ee8648d03e5}	Pictures.Library
{0c3794f3-b545-43aa-a329-c37430c58d2a}	ControlPanelAllItems
{20338b7b-531c-4aad-8011-f5b3db2123ec}	Contacts.SearchResults
{292108be-88ab-4f33-9a26-7748e62e37ad}	Videos.LibraryFolder
{2c7bbec6-c844-4a0a-91fa-cef6f59cfda1}	Printers
{36011842-dccc-40fe-aa3d-6177ea401788}	Documents.SearchResults
{3d1d4ea2-1d8c-418a-bff8-f18370157b55}	OtherUsers.SearchResults
{3f2a72a7-99fa-4ddb-a5a8-c604edf61d6b}	Music.Library
{3f98a740-839c-4af7-8c36-5badfb33d5fd}	Documents.LibraryFolder
{4dcafe13-e6a7-4c28-be02-ca8c2126280d}	Pictures.SearchResults
{503a4e73-1734-441a-8eab-01b3f3861156}	Communications.SearchResults
{524ddb2b-2a4f-43b8-b8fe-e91ef9d8ba69}	Contacts.Library
{549461d3-eb58-4c80-ba29-f1204c4502c3}	Internet
{59bd6dd1-5cec-4d7e-9ad2-ecc64154418d}	UsersLibraries.SearchResults
{5c4f28b5-f869-4e84-8e60-f11db97c5cc7}	Generic
{5f4eab9a-6833-4f61-899d-31cf46979d49}	Generic.Library
{5fa96407-7e77-483c-ac93-691d05850de8}	Videos
{631958a6-ad0f-4035-a745-28ac066dc6ed}	Videos.Library
{654a1b99-8a4b-4e7b-a4e1-46378ad77a61}	Contacts.LibraryFolder
{6d9969ff-612f-48ef-9b90-853fd82e6ec2}	Sync
{6ef8b050-8a6a-4d79-8344-9dfb5cf391fb}	RestrictedNonIndexed
{71689ac1-cc88-45d0-8a22-2943c3e7dfb3}	Music.SearchResults
{7d49d726-3c21-4f05-99aa-fdc2c9474656}	Documents
{7f2f5b96-ff74-41da-afd8-1c78a5f3aea2}	PublishedItems
{7fde1a1e-8b31-49a5-93b8-6be14cfa4943}	Generic.SearchResults
{80213e82-bcfd-4c4f-8817-bb27601267a9}	CompressedFolder
{834d8a44-0974-4ed6-866e-f203d80b3810}	SearchHome
{8faf9629-1980-46ff-8023-9dceab9c3ee3}	OpenSearch
{91475fe5-586b-4eba-8d75-d17434b8cdf6}	Communications
{921c636d-9fc8-40d7-899e-0845dcd03010}	PublishedItems.SearchResults
{94d6ddcc-4a68-4175-a374-bd584a510b78}	Music
{978e0ed7-92d6-4cec-9b59-3135b9c49ccf}	Music.LibraryFolder
{982725ee-6f47-479e-b447-812bfa7d2e8f}	SearchConnector
{b337fd00-9dd5-4635-a6d4-da33fd102b7a}	OtherUsers
{b3690e58-e961-423b-b687-386ebfd83239}	Pictures
{b372207c-0011-438f-9151-098b2e36b887}	FileItemAPIs

Vincent Lo, LYLC.SYMPHONICA@GMAIL.COM

© 2014 The SANS Institute Author retains full rights.

{b689b0d0-76d3-4cbb-87f7-585d0e0ce070}	Games
{c1f8339f-f312-4c97-b1c6-ecdf5910c5c0}	Pictures.LibraryFolder
{c4d98f09-6124-4fe0-9942-826416082da9}	UsersLibraries
{cd0fc69b-71e2-46e5-9690-5bcd9f57aab3}	UserFiles
{d674391b-52d9-4e07-834e-67c98610f39d}	Programs
{da3f6866-35fe-4229-821a-26553a67fc18}	Generic.LibraryFolder
{db2a5d8f-06e6-4007-aba6-af877d526ea6}	AccountPictures
{de2b70ec-9bf7-4a93-bd3d-243f7881d492}	Contacts
{de4f0660-fa10-4b8f-a494-068b20b22307}	ControlPanelCategory
{e053a11a-dced-4515-8c4e-d51ba917517b}	UserFiles.SearchResults
{ea25fbd7-3bf7-409e-b97f-3352240903f4}	Videos.SearchResults
{ef87b4cb-f2ce-4785-8658-4ca6c63e38c6}	StartMenu
{fbb3477e-c9e4-4b3b-a2ba-d3f5d3cd46f9}	Documents.Library

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.