WINDOWS SHELLBAGS FORENSICS IN DEPTH

SANS Digital Forensics Incident Response Summit 2014

Vincent Lo

Klein & co.
investigate / discover / respond
WHO AM I?

Vincent Lo
CISSP, GCFA Gold, GCIH, GREM, CCE

Blog: lylcdigitalforensics.blogspot.com
Twitter: @_VincentLo_
CONTENT
What is ShellBag?
ShellBag Structure
ShellBag Activities
Case Study
WHAT IS SHELLBAG?
Windows behavior
SHELLBAG STRUCTURE
SHELLBAG STRUCTURE

DESKTOP
SHELLBAG STRUCTURE
SHELLBAG STRUCTURE
**SHELLBAG STRUCTURE**

<table>
<thead>
<tr>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeSlot</td>
<td>REG_DWORD</td>
<td>0x00000003</td>
</tr>
<tr>
<td>MRUListEx</td>
<td>REG_BINARY</td>
<td>FF FF FF FF</td>
</tr>
</tbody>
</table>
QUESTION

So...what can ShellBags do for digital forensic investigators?

- It may prove a user accessed certain folders which he/she shouldn't.
- It may show the directories on external devices.
- It may contain what files existed on the Desktop at the time. (itempos)
WHEN WILL THE SHELLBAGS BE CREATED?

Myth 1:  
When the folder is opened and closed in Windows Explorer at least once. (2009)

The experiment says...

Myth 2:  
When a folder is opened and has default settings adjusted. (2011)

The experiment says...
SHELLBAG CREATION

The activities that could create ShellBags are not always the same.
WINDOWS XP
SHELLBAG CREATION

- Windows Explorer & Desktop
- Compressed Files (ZIP files)
- Search Window
- Remote Machines & Folders
- Windows Special Folders & Virtual Folders
- Removable Devices
- Exception
WINDOWS XP
SHELLBAG CREATION

- Windows Explorer & Desktop
  Windows Explorer
  Desktop
**Windows XP SHELLBAG CREATION**

- **Windows Explorer & Desktop**
  - Does the folder contain any **visible child items (files or subfolders)**?
    - If the folder contains visible child item(s), ShellBags will be created when the folder is **opened**.
    - If the folder contains does **NOT** contain any visible child items, ShellBags will be created when the folder is **opened and closed**.

**Closed**: The Windows Explorer is closed or another folder is opened in the same window.
• Windows Explorer & Desktop
  ■ What if the folder doesn't contain any visible child items but only hidden child item(s) (files or subfolders)?
    o If Windows Explorer is configured to show them, ShellBags will be created when the folder is opened.
    o If Windows Explorer is configured NOT to show them, ShellBags will be created when the folder is opened and closed.
Compressed Files (ZIP files)

- ShellBags will be created, when a ZIP file is opened and closed in Windows Explorer.

The ShellBags information will include the created date, modified date and accessed date of the ZIP file.
WINDOWS XP
SHELLBAG CREATION

- Search Window
Search Window

- Search Results folder
  - 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.

- {CCE6191F-13B2-44FA-8D14-324728BEEF2C} folder
  - Open the Search window from Start menu. Then, close the window or open a folder in the same window.
  - Open the Search window from Start menu. Then, choose the search scope and click Search.
WINDOWS XP
SHELLBAG CREATION
Remote Machines & Remote Folders
Remote Machines & Remote Folders

- Remote Machines
  - ShellBags will be created when the remote machine is opened and closed.

- Remote Folders
  - If the folder contains visible child item(s), ShellBags will be created when the folder is opened.
  - If the folder contains does NOT contain any visible child items, ShellBags will be created when the folder is opened and closed.
Windows Special Folders & Virtual Folders
(It is very complicated.)

- **Special Folders**
  - Examples: My Documents, My Music and My Pictures

- **Virtual Folders**
  - Examples: My Computer and Control Panel

- **Multiple Identities**
  - Example: Desktop can be a special folder, virtual folder or actual file system folder.
  - Example: My Documents can be a file system folder or virtual folder.
WINDOWS XP

SHELLBAG CREATION

- Windows Special Folders & Virtual Folders
  (It is very complicated.)

The activities that cause the creation of their ShellBags depend on the folder type and situation.
Removable Devices
- Windows XP does NOT create the ShellBags for folders on removable devices.
WINDOWS XP
SHELLBAG CREATION

• Exception
  - Right click on the folder and choose Properties → Customize. Then, click "OK".
WINDOWS VISTA, 7, 8 AND 8.1
SHELLBAG CREATION
WINDOWS VISTA, 7, 8 AND 8.1
SHELLBAG CREATION

- Windows Explorer
- Desktop
- Removable Devices
- Remote Machines & Folders
- Compressed Files (ZIP files)
- Search Result
- desktop.ini
- Command Prompt
- Windows Special Folders, Virtual Folders & Libraries
WINDOWS VISTA, 7, 8 AND 8.1
SHELLBAG CREATION

- Windows Explorer
  - It doesn't matter whether a folder is empty or not.
    - Create a folder
    - Click a folder to select it
    - Click a folder to select it and press an arrow key to move the bar to select other folders (The ShellBags information for those folders will be created.)
    - Right click a folder
  - The folder doesn't have to be opened.
Windows Vista, 7, 8 and 8.1

Shellbag Creation

- Windows Explorer
  - As the result, the following activities in Windows Explorer will create the ShellBags information.
    - Open a folder (Double-click a folder)
    - Rename a folder (Right-click a folder and select "Rename" or select the folder and press "F2". Change the folder name and press enter. The ShellBags of original and renamed folder names will be created.)
    - Delete a folder
    - Copy a folder to local drives (ShellBags of the source folder and destination folder will be created.)
WINDOWS VISTA, 7, 8 AND 8.1
SHELLBAG CREATION

• Desktop
  - The activities that could create the ShellBags are **NOT** exactly the same as Windows Explorer.
    - Open a folder
    - Right-click a folder
    - Cut a folder (Ctrl+x)
    - Copy a folder (Ctrl+c)
    - Rename a folder (select the folder and press "F2") – Only 7, 8 and 8.1
    - Delete a folder (Select the folder and press "Delete")
Windows Vista, 7, 8 and 8.1
ShellBag Creation

- Desktop
  - As the result, the following activities will create the ShellBags information for a folder.
    1. Rename a folder (Right-click a folder and select "Rename" or select the folder and press "F2" (The later one doesn't create the ShellBags in Vista). Change the folder name and press enter. The ShellBags of original folder name will be created.)
    2. Delete a folder (Right-click and select "Delete" or click the folder and press "Delete")
    3. Copy a folder (ShellBags of the source folder will be created.) In Vista, the source and destination folders will be created if the destination folder is on the Desktop.
SHELLBAG CREATION

- Removable Devices
  - ShellBags will be created when folders on removable devices are opened and closed.
Remote Machines & Remote Folders
- Remote Machines
  - ShellBags will be created when the remote machine is opened and closed.
- Remote Folders
  - ShellBags will be created when the folder is opened.
- Remote Folders ➔ Child Folders
  - ShellBags will be created when the child folder is opened.
Remote Machines & Remote Folders
- Remote Machines
  - ShellBags will be created when the remote machine is opened and closed.
- Remote Folders
  - ShellBags will be created when the folder is opened.
- Remote Folders ➔ Child Folders
  - ShellBags can be created without being opened. The activities mentioned in the "Windows Explorer" section can cause their ShellBags information to be created.
WINDOWS VISTA, 7, 8 AND 8.1
SHELLBAG CREATION

• Compressed Files (ZIP files)
  o ShellBags will be created, when a ZIP file is opened and closed in Windows Explorer.

The ShellBags information will include the created date, modified date and accessed date of the ZIP file.
WINDOWS VISTA AND 7
SHELLBAG CREATION

• Search Result
  o Type the query in the Smart menu's "Start Search" or in Windows Explorer’s Search column and execute it.

In Windows Vista and 7, if the query is run in the Start menu’s “Start Search” column, when the search window appears, the query will be recorded.

Windows 8 and 8.1 use different Start screen design. The search run through Start screen doesn’t seem to be recorded in ShellBags.
WINDOWS VISTA, 7, 8 AND 8.1
SHELLBAG CREATION

• desktop.ini
  o If the folder type or CLSID is specified in the desktop.ini, Windows Explorer will create the ShellBags information only after the folder is opened.
Command Prompt

This occurs on Vista only.

- In the Command Prompt, if the folders are created in the `%UserProfile%\Desktop` folder via "mkdir" command, the ShellBags information of those folders will be created.
WINDOWS VISTA, 7, 8 AND 8.1
SHELLBAG CREATION

• Windows Special Folders, Virtual Folders & Libraries
  (It is very complicated.)
  ▪ Special Folders
    □ Examples: Documents, Music, Picture and Videos
  ▪ Virtual Folders
    □ Examples: My Computer and Control Panel
  ▪ Libraries (7, 8 and 8.1)
    □ Examples: Documents, Music, Picture and Videos
The activities that cause the creation of their ShellBags depend on the folder type and situation.
"The truth is in the details." - Stephen King
**SCENARIO**

Data Leak

- The *Autobots* smartphone company is going to announce their new smartphone on **Monday 6 October 2014**.
- This cutting edge product is called **UPhone 7 Minus**.
- Autobots spent 12 months on building a new solid smartphone.
- It uses the latest high-technology material so it is.......
SCENARIO

Data Leak

- However, *Autobots* found their new product information has been leaked on an anonymous blog on *Sunday 5 October morning*.
- The confidential testing photo was also disclosed......
SCENARIO

Data Leak

- *Autobots* immediately performed the internal investigation this morning.
- They identified that the leaked photo and confidential product information was stored in a remote shared folder named *Optimus Prime* which is the codename of the project.
- Through Windows Event logs, *Autobots* noticed their employee *Laserbeak* logged into the network yesterday around 3am.
- *Laserbeak* has no reason to access *Optimus Prime* folder.
- How can we prove *Laserbeak* leaked the information to the internet?
**SCENARIO**

Data Leak

- Laserbeak’s computer has *Windows 7 Profession with SP1* installed.
- The `\Cybertron\Projects\Optimus Prime` folder info was found in ShellBags. It was created around 3:12am.
- The `E:\Optimus Prime` folder info was also found in ShellBags which was created around 3:14am.
- The USB device information shows E drive is a removable device.

What can we do with the information above?
Laserbeak's computer has Windows 7 Profession with SP1 installed.

The `\Cybertron\Projects\Optimus Prime` folder info was found in ShellBags. It was created around 3:12am.

The `E:\Optimus Prime folder` info was also found in ShellBags which was created around 3:14am.

The USB device information shows E drive is a removable device.

Did Laserbeak open the folder?
<table>
<thead>
<tr>
<th>Operating System</th>
<th>Files containing ShellBags information</th>
</tr>
</thead>
</table>
| 7, 8 and 8.1 (32 bit & 64 bit) | `%UserProfile%\NTUSER.DAT
%UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat` |
## Windows 7, 8 and 8.1

<table>
<thead>
<tr>
<th>Operating System</th>
<th>ShellBags Registry Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>7, 8 and 8.1 (32 bit &amp; 64 bit)</td>
<td><strong>NTUSER.DAT\Software\Microsoft\Windows*<em>Shell*</em>BagMRU</strong></td>
</tr>
<tr>
<td></td>
<td><strong>NTUSER.DAT\Software\Microsoft\Windows*<em>Shell*</em>Bags</strong></td>
</tr>
<tr>
<td></td>
<td><strong>UsrClass.dat\Local Settings\Software*<em>Microsoft\Windows*</em>Shell**BagMRU</strong></td>
</tr>
<tr>
<td></td>
<td><strong>UsrClass.dat\Local Settings\Software*<em>Microsoft\Windows*</em>Shell**Bags</strong></td>
</tr>
</tbody>
</table>
## WINDOWS 7, 8 AND 8.1

<table>
<thead>
<tr>
<th>Operating System</th>
<th>ShellBags Registry Keys</th>
</tr>
</thead>
</table>
| 7, 8 and 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                                                                                    |
THANK YOU!

SANS360: SHELLBAG ANALYSIS TOOLS

Email: LYLC.SYMPHONICA@gmail.com
Blog: lylcdigitalforensics.blogspot.com
Twitter: @_VincentLo_