

WINDOWS SHELLBAGS FORENSICS IN DEPTH

KEEP
CALM
AND
UNDERSTAND
SHELLBAGS

RUXCON 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_](https://twitter.com/_VincentLo_)



KEEP
CALM
AND
UNDERSTAND
SHELLBAGS

CONTENT

What is ShellBag?
ShellBag Structure
ShellBag Activities
Case Study

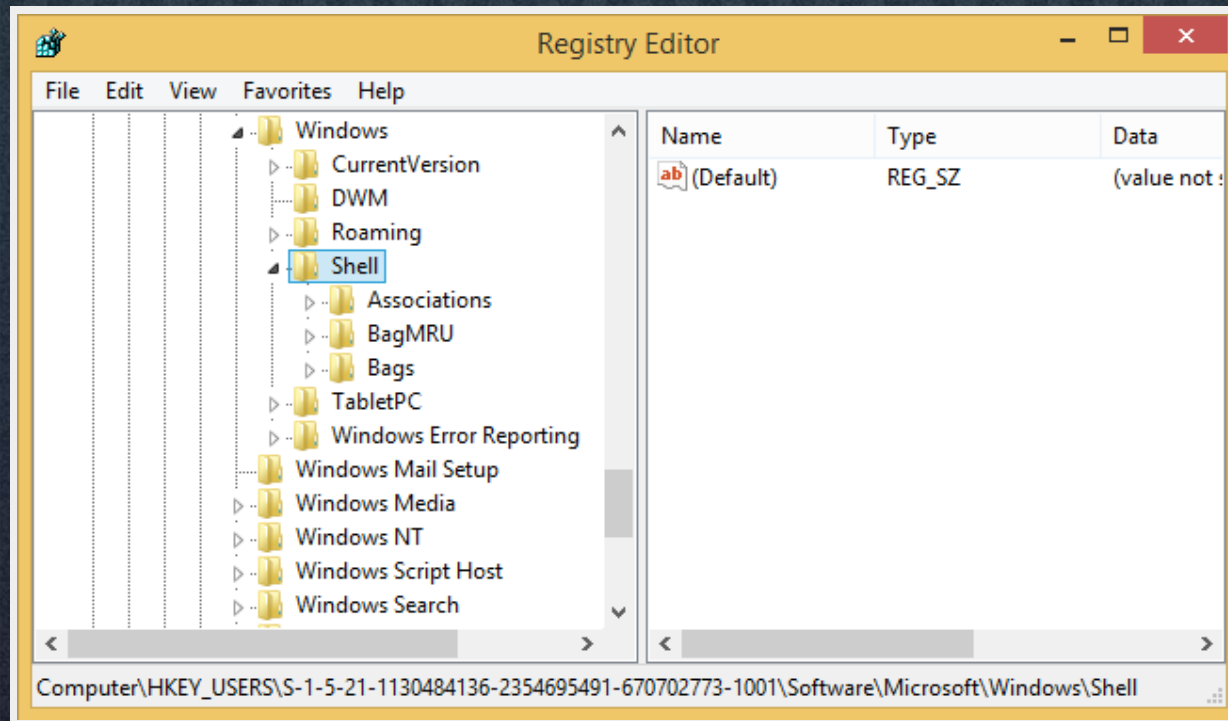
WHAT IS SHELLBAG?

Windows behavior



SHELLBAG STRUCTURE

KEEP
CALM
AND
UNDERSTAND
SHELLBAGS



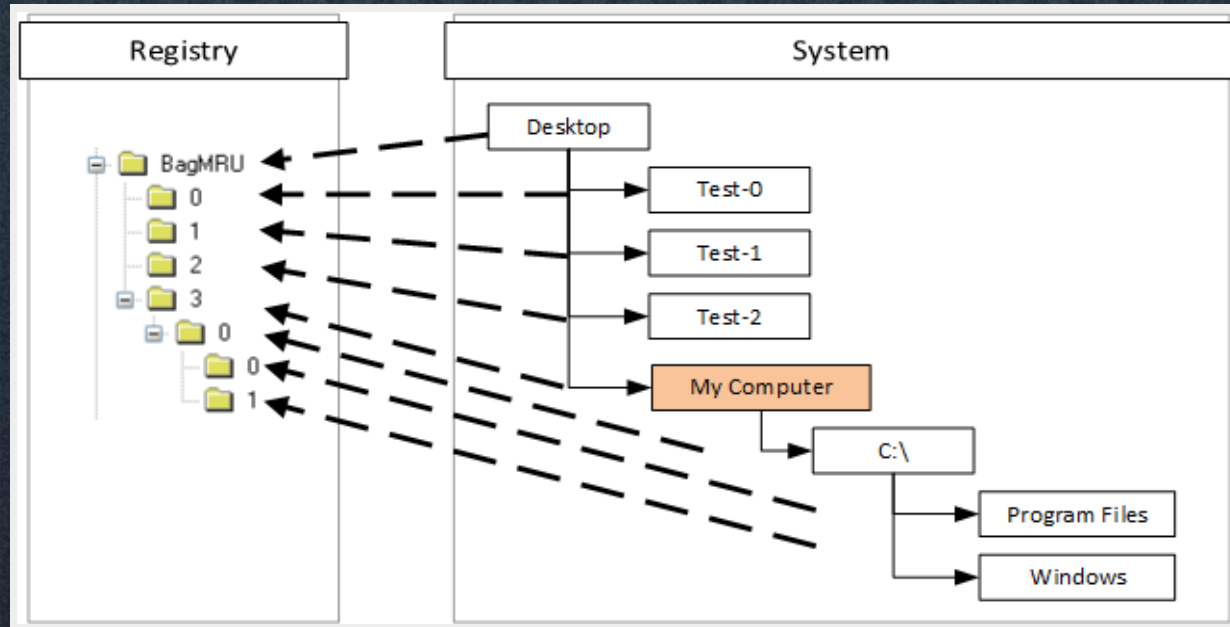
SHELLBAG STRUCTURE

DESKTOP

KEEP
CALM
AND
UNDERSTAND
SHELLBAGS



SHELLBAG STRUCTURE



SHELLBAG STRUCTURE

The screenshot shows the Windows Registry Editor with the following table of values:

Value	Type	Data
NodeSlots	REG_BINARY	02 02 02 02 02 02 02 02
MRUListEx	REG_BINARY	00 00 00 00 03 00 00 00 02 00 00 00 01 00 00 00 FF FF FF FF
0	REG_BINARY	3A 00 31 00 00 00 00 00 4F 44 14 32 10 00 54 65 73 74 2D 30 00 00 24 00 03
1	REG_BINARY	3A 00 31 00 00 00 00 00 4F 44 17 32 10 00 54 65 73 74 2D 31 00 00 24 00 03
2	REG_BINARY	3A 00 31 00 00 00 00 00 4F 44 1A 32 10 00 54 65 73 74 2D 32 00 00 24 00 03
3	REG_BINARY	14 00 1F 50 E 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 00 00
NodeSlot	REG_DWORD	0x00000008

Below the table is a hex dump of the data for the '2' entry:

```
0001 0203 0405 0607 0809 0A0B 0C0D 0E0F 012345 6789ABCDEF
0x00 3A00 3100 0000 0000 4F44 1A32 1000 5465 0123456789ABCDEF
0x10 7374 2D32 0000 2400 0300 0400 4FBF 4F44 st-2...f.....iWOD
0x20 1A32 4F44 1A32 1400 0000 5400 6500 7300 .20D.2....T.e.s.
0x30 7400 2D00 3200 0000 1600 0000 t.-.2.....
```


SHELLBAG STRUCTURE

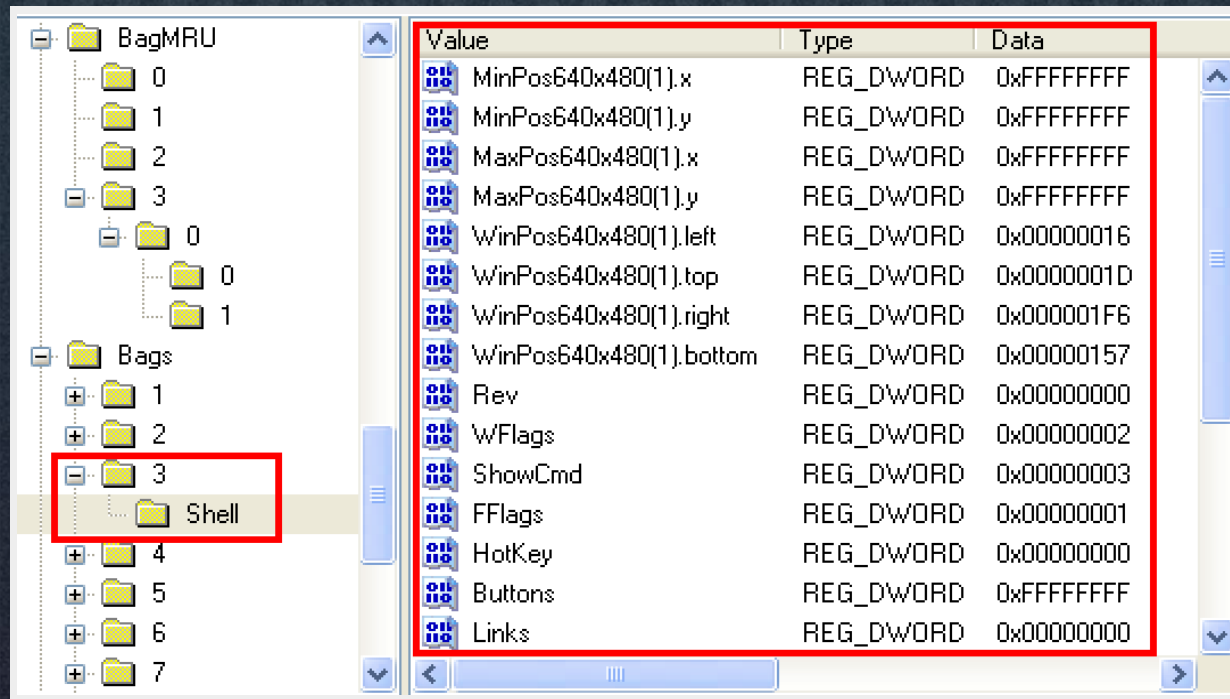
The screenshot displays the Windows Registry Editor. The left pane shows a tree view of the registry structure. The right pane shows a table of registry values. Red boxes and arrows highlight the mapping between folders and registry values.

Value	Type	Data
NodeSlot	REG_DWORD	0x00000003
MRUListEx	REG_BINARY	FF FF FF FF

The tree view shows the following structure:

- BagMRU
 - 0
 - 1
 - 2
 - 3
 - 0
 - 1
- Bags
 - 1
 - 2
 - 3
 - 4
 - 5
 - 6

SHELLBAG STRUCTURE



Value	Type	Data
MinPos640x480(1).x	REG_DWORD	0xFFFFFFFF
MinPos640x480(1).y	REG_DWORD	0xFFFFFFFF
MaxPos640x480(1).x	REG_DWORD	0xFFFFFFFF
MaxPos640x480(1).y	REG_DWORD	0xFFFFFFFF
WinPos640x480(1).left	REG_DWORD	0x00000016
WinPos640x480(1).top	REG_DWORD	0x0000001D
WinPos640x480(1).right	REG_DWORD	0x000001F6
WinPos640x480(1).bottom	REG_DWORD	0x00000157
Rev	REG_DWORD	0x00000000
WFlags	REG_DWORD	0x00000002
ShowCmd	REG_DWORD	0x00000003
FFlags	REG_DWORD	0x00000001
HotKey	REG_DWORD	0x00000000
Buttons	REG_DWORD	0xFFFFFFFF
Links	REG_DWORD	0x00000000

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

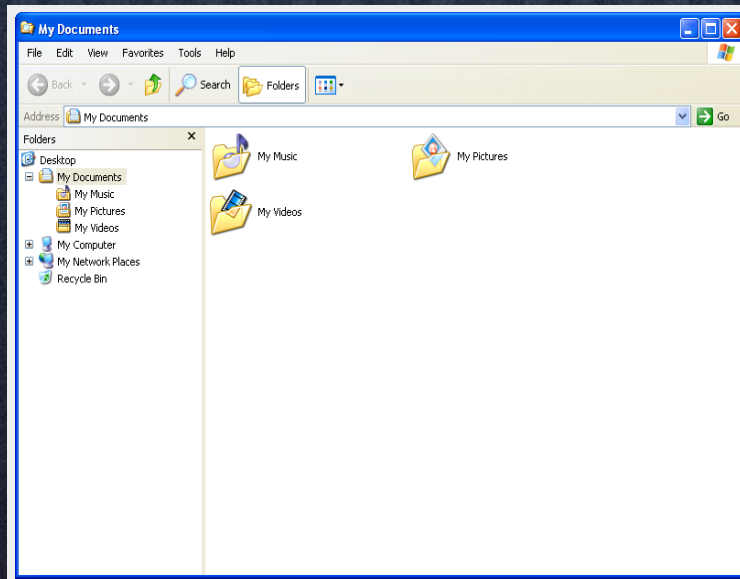
- Windows Explorer & Desktop
- Compressed Files (ZIP files)
- Search Window
- Remote Machines & Folders
- Windows Special Folders & Virtual Folders
- Removable Devices
- Exception

WINDOWS XP SHELLBAG CREATION

KEEP
CALM
AND
UNDERSTAND
SHELLBAGS

- 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 XP

SHELLBAG CREATION

- Windows Explorer & Desktop
 - *What if the folder doesn't contain any visible child items but only hidden child item(s) (files or subfolders)?*
 - If Windows Explorer is configured to show them, ShellBags will be created when the folder is **opened**.
 - If Windows Explorer is configured **NOT** to show them, ShellBags will be created when the folder is **opened and closed**.

WINDOWS XP

SHELLBAG CREATION

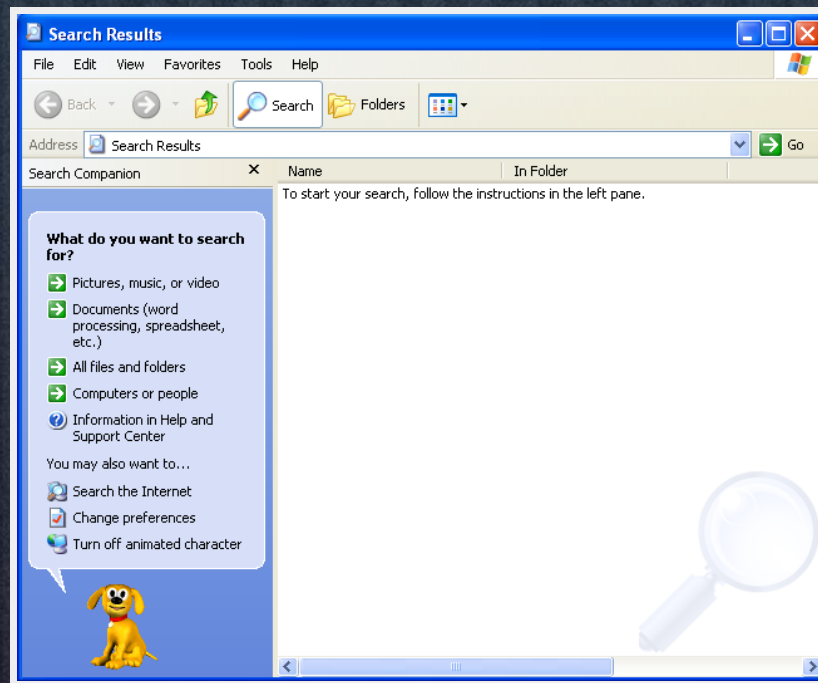


- Compressed Files (ZIP files)
 - ShellBags will be created, when a ZIP file is **opened and closed** in Windows Explorer.

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

WINDOWS XP SHELLBAG CREATION

- Search Window



WINDOWS XP

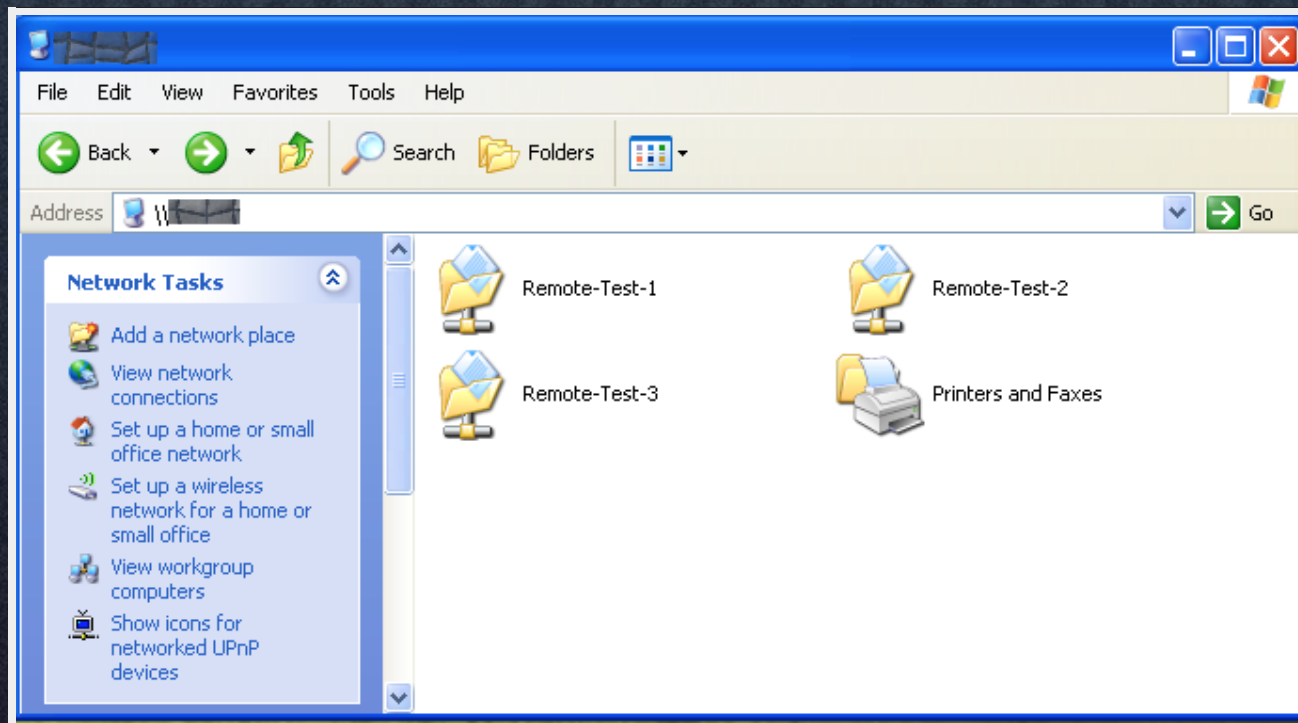
SHELLBAG CREATION

- 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

KEEP
CALM
AND
UNDERSTAND
SHELLBAGS



WINDOWS XP

SHELLBAG CREATION

- 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 XP

SHELLBAG CREATION



- 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.

WINDOWS XP

SHELLBAG CREATION

- 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



KEEP
CALM
AND
UNDERSTAND
SHELLBAGS

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.
 - 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.)
 - Delete a folder (Right-click and select "Delete" or click the folder and press "Delete")
 - 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.

WINDOWS VISTA, 7, 8 AND 8.1

SHELLBAG CREATION



- Removable Devices
 - ShellBags will be created when folders on removable devices are **opened and closed**.

WINDOWS VISTA

SHELLBAG CREATION



- 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**.

WINDOWS 7, 8 AND 8.1

SHELLBAG CREATION

- 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)
 - 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

- Type the query in the Start 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
 - 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.

WINDOWS VISTA

SHELLBAG CREATION

- 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*

WINDOWS VISTA, 7, 8 AND 8.1

SHELLBAG CREATION



- Windows Special Folders, Virtual Folders & Libraries (It is very complicated.)
 - Multiple Identities
 - **Example:** *Desktop* can be a special folder, virtual folder or actual file system folder.
 - **Example:** *Documents* can be a file system folder, virtual folder or a library.

The activities that cause the creation of their ShellBags depend on the folder type and situation.

CASE STUDY



"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?

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.

Did Laserbeak open the folder?

WINDOWS 7, 8 AND 8.1



Operating System	Files containing ShellBags information
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

Operating System	ShellBags Registry Keys
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

WINDOWS 7, 8 AND 8.1

KEEP
CALM
AND
UNDERSTAND
SHELLBAGS

Operating System	ShellBags Registry Keys
7, 8 and 8.1 (32 bit & 64 bit)	<code>NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU</code> <code>NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags</code> <code>UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\BagMRU</code> <code>UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\Bags</code>

THANK YOU!

Email: LYLC.SYMPHONICA@gmail.com

Blog: lylcdigitalforensics.blogspot.com

Twitter: [@_VincentLo_](https://twitter.com/_VincentLo_)



KEEP
CALM
AND
UNDERSTAND
SHELLBAGS