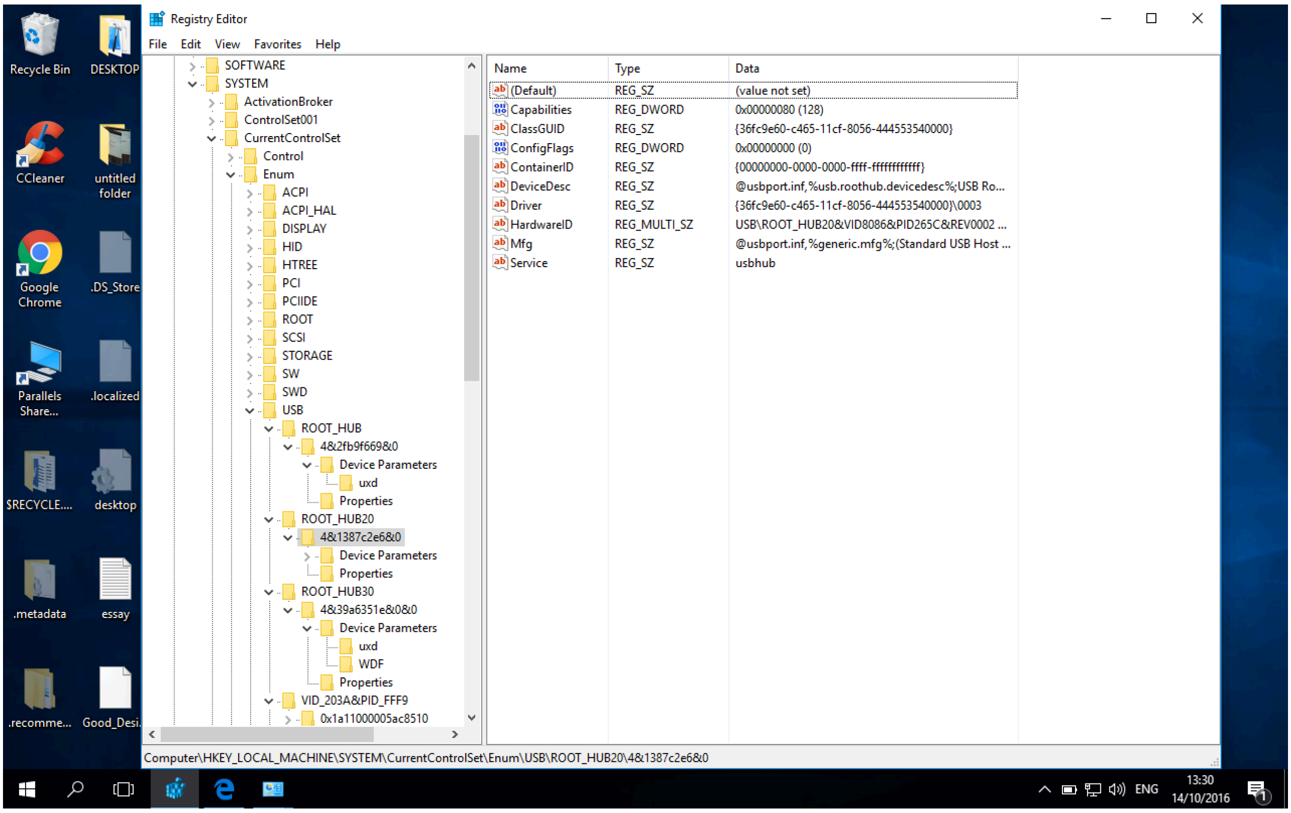
Part 1.

In order to view the information about the USB devices sorted on the system, I had to view the registry. The path to the registry was “HKEY_LOCAL_MACHINE/SYSTEM/CURRENTCONTROLSET/ENUM/USB/. At the end of this path, there is numerous folders that contain information about different USB’s that have been used on this machine. Information such as product ID. Also information such as when the last time the USB was plugged in.

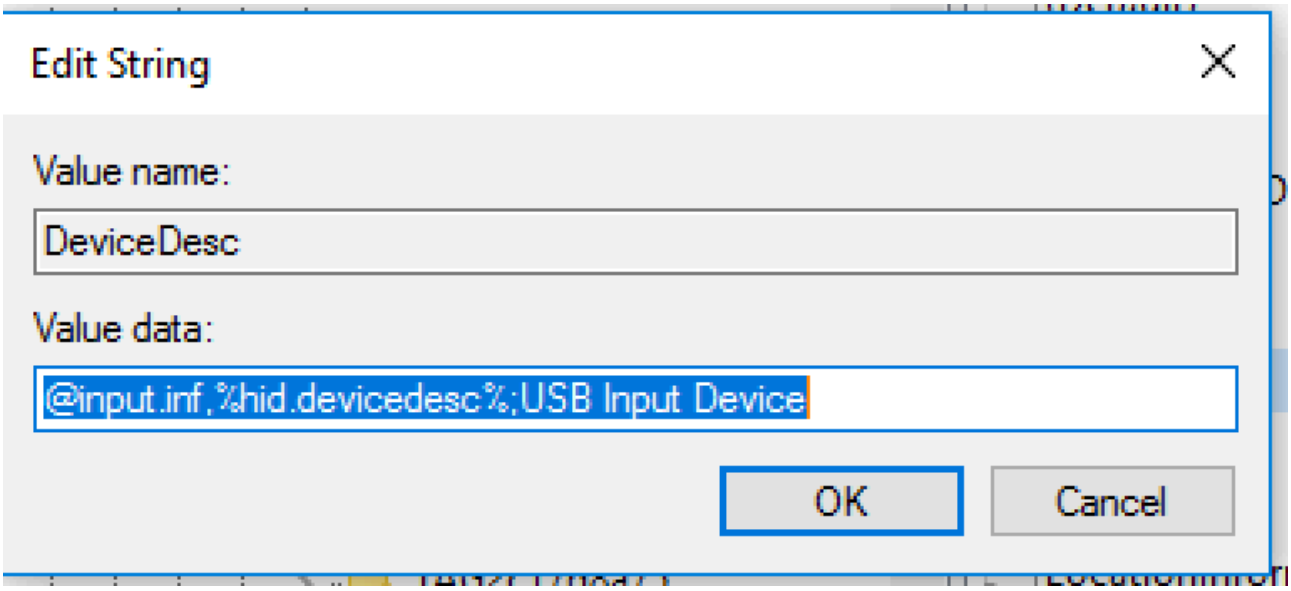
The following screenshot shows the path listed above.



| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| Capabilities | REG_DWORD | 0x00000080 (128) |
| ClassGUID | REG_SZ | {36fc9e60-c465-11cf-8056-444553540000} |
| ConfigFlags | REG_DWORD | 0x00000000 (0) |
| ContainerID | REG_SZ | {00000000-0000-0000-ffff-ffffffffffff} |
| DeviceDesc | REG_SZ | @usbport.inf,%usb.roothub.devicedesc%;USB Ro... |
| Driver | REG_SZ | {36fc9e60-c465-11cf-8056-444553540000}\0003 |
| HardwareID | REG_MULTI_SZ | USB\ROOT_HUB20&VID8086&PID265C&REV0002 ... |
| Mfg | REG_SZ | @usbport.inf,%generic.mfg%;(Standard USB Host ... |
| Service | REG_SZ | usbhub |

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\ROOT_HUB20\4&1387c2e6&0

When a user selects on a row, a box will pop up with the value name and the data. In the following example, when I selected DeviceDesc, the following appeared in the screen shot below. As we can see, the device description has value data of USB input device.



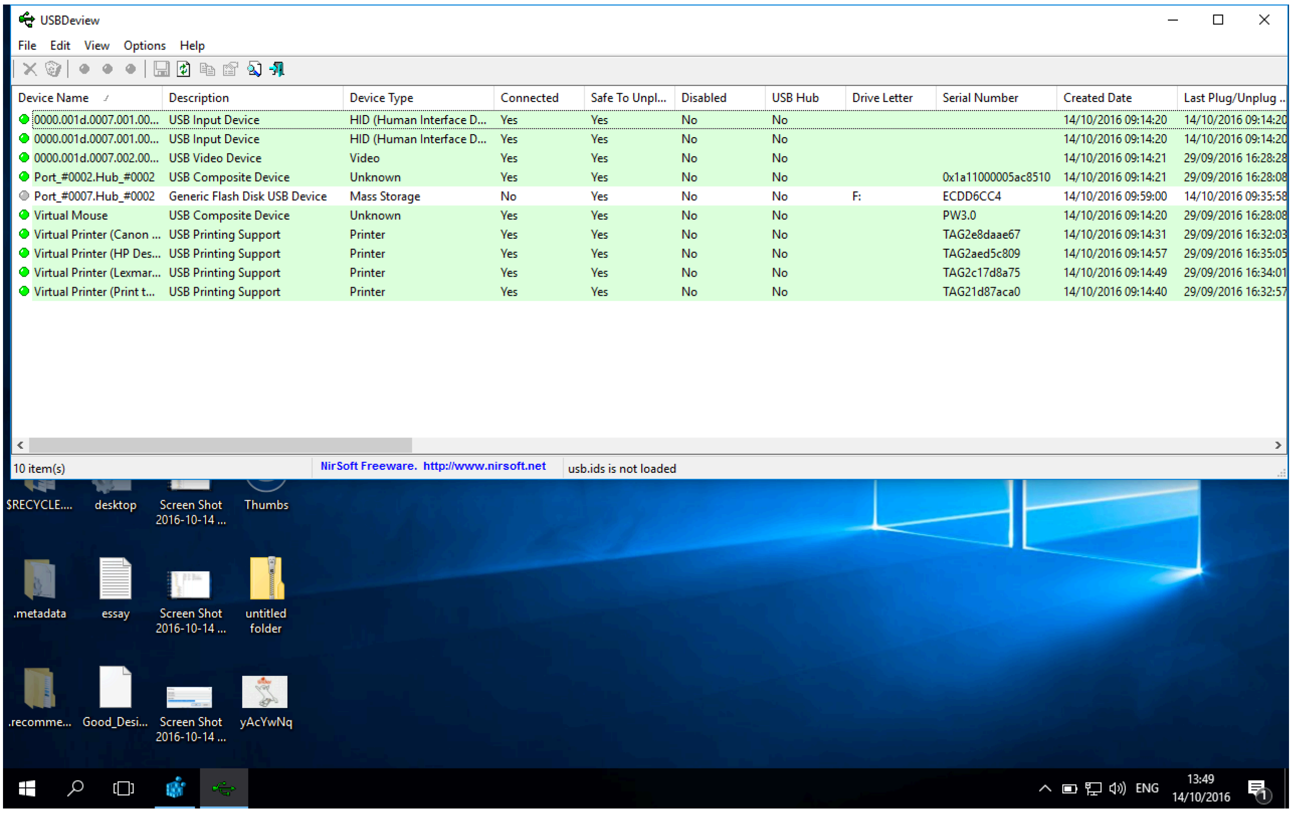
Value name:

DeviceDesc

Value data:

@input.inf,%hid.devicedesc%;USB Input Device

In order to retrieve  more information about USB stored in the registry, I downloaded a tool that will display the information in a better format and easier to read view. The tool I downloaded was USBdeview.



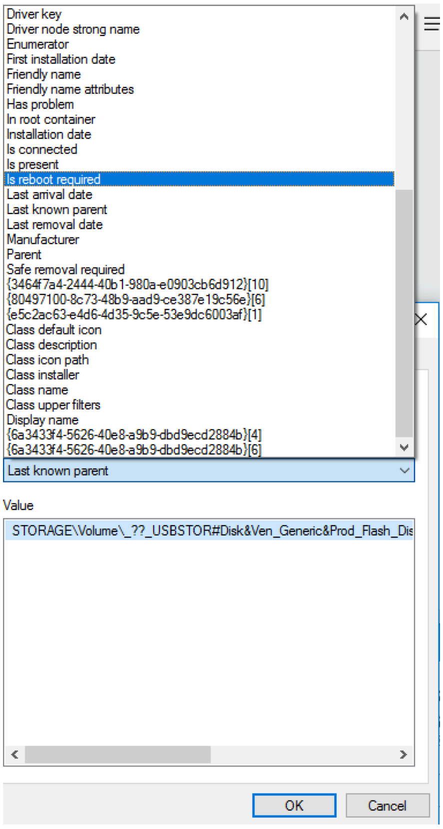
| Device Name | Description | Device Type | Connected | Safe To Unpl... | Disabled | USB Hub | Drive Letter | Serial Number | Created Date | Last Plug/Unplug .. |
|---|---|---|---|---|---|---|---|---|---|---|
| ● 0000.001d.0007.001.00... | USB Input Device | HID (Human Interface D... | Yes | Yes | No | No | | | 14/10/2016 09:14:20 | 14/10/2016 09:14:20 |
| ● 0000.001d.0007.001.00... | USB Input Device | HID (Human Interface D... | Yes | Yes | No | No | | | 14/10/2016 09:14:20 | 14/10/2016 09:14:20 |
| ● 0000.001d.0007.002.00... | USB Video Device | Video | Yes | Yes | No | No | | | 14/10/2016 09:14:21 | 29/09/2016 16:28:28 |
| ● Port_#0002.Hub_#0002 | USB Composite Device | Unknown | Yes | Yes | No | No | | 0x1a11000005ac8510 | 14/10/2016 09:14:21 | 29/09/2016 16:28:08 |
| ○ Port_#0007.Hub_#0002 | Generic Flash Disk USB Device | Mass Storage | No | Yes | No | No | F: | ECDD6CC4 | 14/10/2016 09:59:00 | 14/10/2016 09:35:58 |
| ● Virtual Mouse | USB Composite Device | Unknown | Yes | Yes | No | No | | PW3.0 | 14/10/2016 09:14:20 | 29/09/2016 16:28:08 |
| ● Virtual Printer (Canon ... | USB Printing Support | Printer | Yes | Yes | No | No | | TAG2e8daae67 | 14/10/2016 09:14:31 | 29/09/2016 16:32:03 |
| ● Virtual Printer (HP Des... | USB Printing Support | Printer | Yes | Yes | No | No | | TAG2aed5c809 | 14/10/2016 09:14:57 | 29/09/2016 16:35:05 |
| ● Virtual Printer (Lexmar... | USB Printing Support | Printer | Yes | Yes | No | No | | TAG2c17d8a75 | 14/10/2016 09:14:49 | 29/09/2016 16:34:01 |
| ● Virtual Printer (Print t... | USB Printing Support | Printer | Yes | Yes | No | No | | TAG21d87aca0 | 14/10/2016 09:14:40 | 29/09/2016 16:32:57 |

10 item(s) NirSoft Freeware. http://www.nirsoft.net usb.ids is not loaded

As i was running a VM of microsoft, the  above screenshot displays information such as the device name, device type, serial number, last plugged in, the creation date.

The Windows registry can be very useful to find information about devices that have been connected to the divide. A lot of information is stored which can help investigators to identify what devices have been plugged into a system.

Another way in which a user can retrieve information from a USB that is plugged into the system is to right click on the device and select the properties. Information such as device name, device description, last time it was plugged in, last arrival date, manufacturer and last known parent can be found.



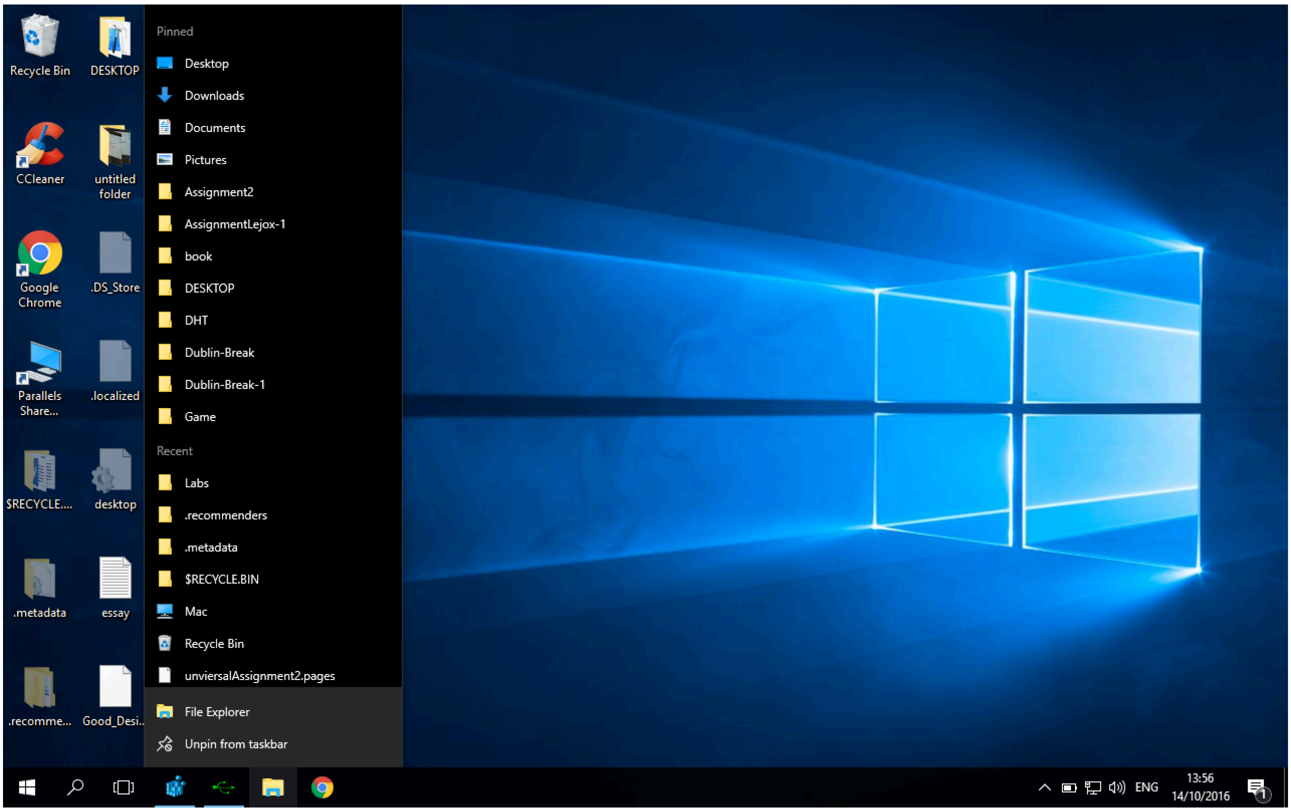
Last known parent

Value

STORAGE\Volume_??_USBSTOR#Disk&Ven_Generic&Prod_Flash_Dis

Part 2.

A jump list is feature that provides a graphical interface to a user that allows them to view files that have been recently accessed on an application. The following image shows a jump list for my file explorer.

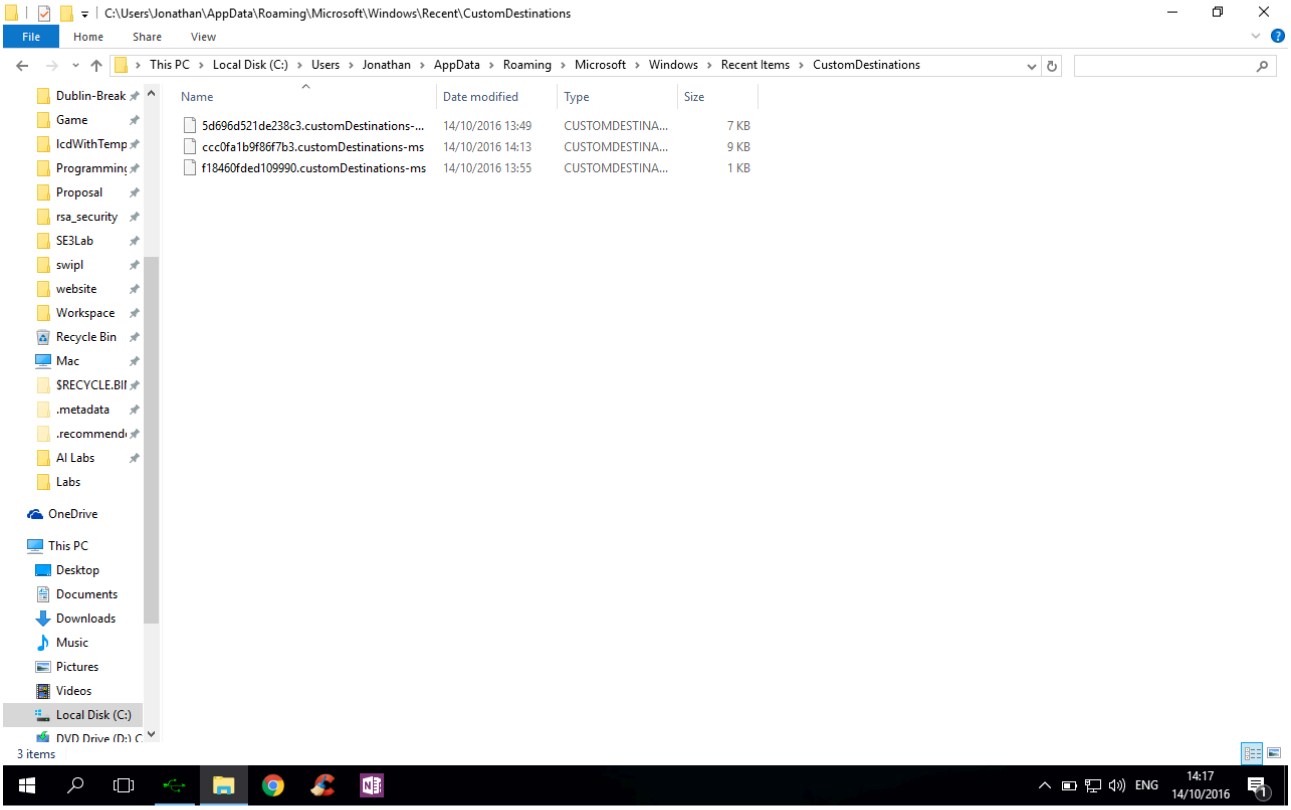


When a user pins a application onto their task bar, two files are created depending on the application. The first path where a file is created is in C:\Users\Jonathan\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

or the second path depending on the application is in C:\Users\Jonathan\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

Information such as the AppID, date modified, this includes the date and time and the size of the file are created.

Here is a screenshot of the the customDestinations path.

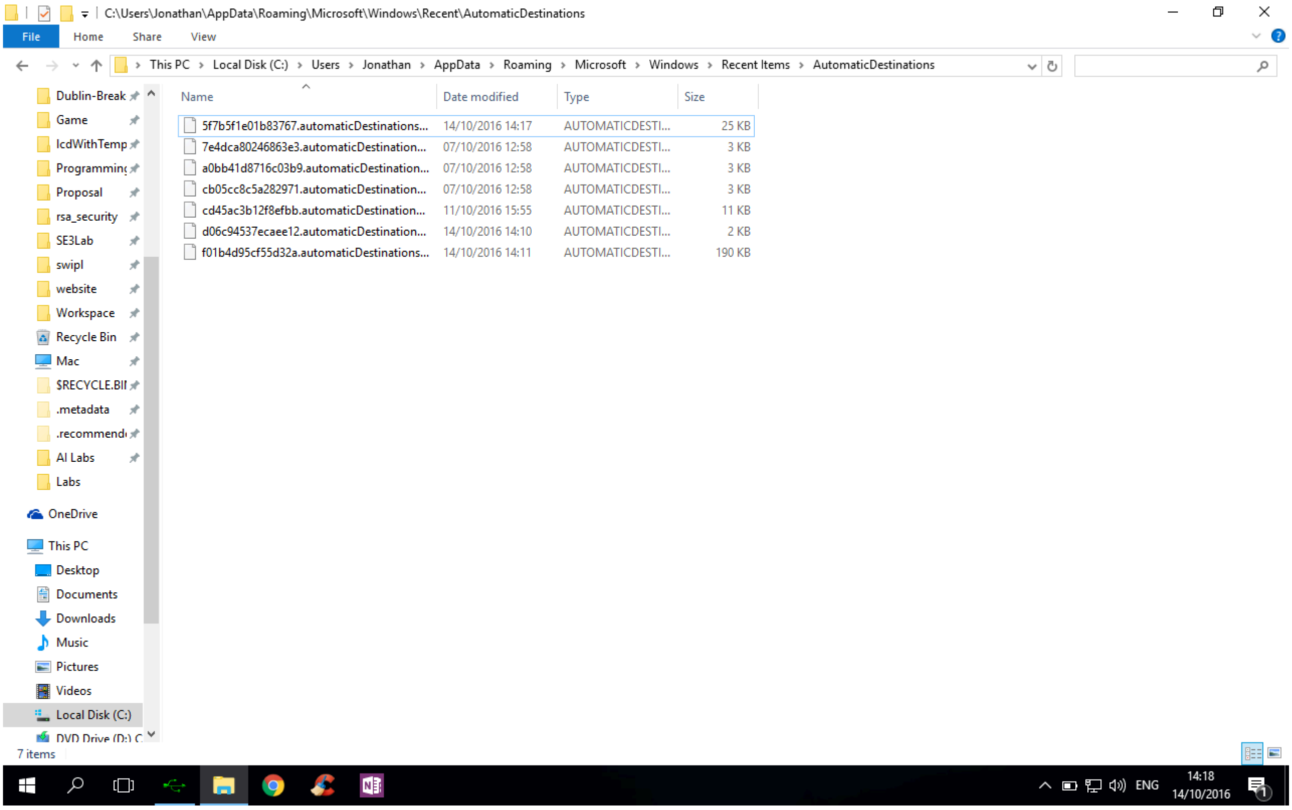


C:\Users\Jonathan\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

This PC › Local Disk (C:) › Users › Jonathan › AppData › Roaming › Microsoft › Windows › Recent Items › CustomDestinations

| Name | Date modified | Type | Size |
|---|---|---|---|
| 5d696d521de238c3.customDestinations-... | 14/10/2016 13:49 | CUSTOMDESTINA... | 7 KB |
| ccc0fa1b9f86f7b3.customDestinations-ms | 14/10/2016 14:13 | CUSTOMDESTINA... | 9 KB |
| f18460fded109990.customDestinations-ms | 14/10/2016 13:55 | CUSTOMDESTINA... | 1 KB |

The following screenshot displays the automaticDestinations.

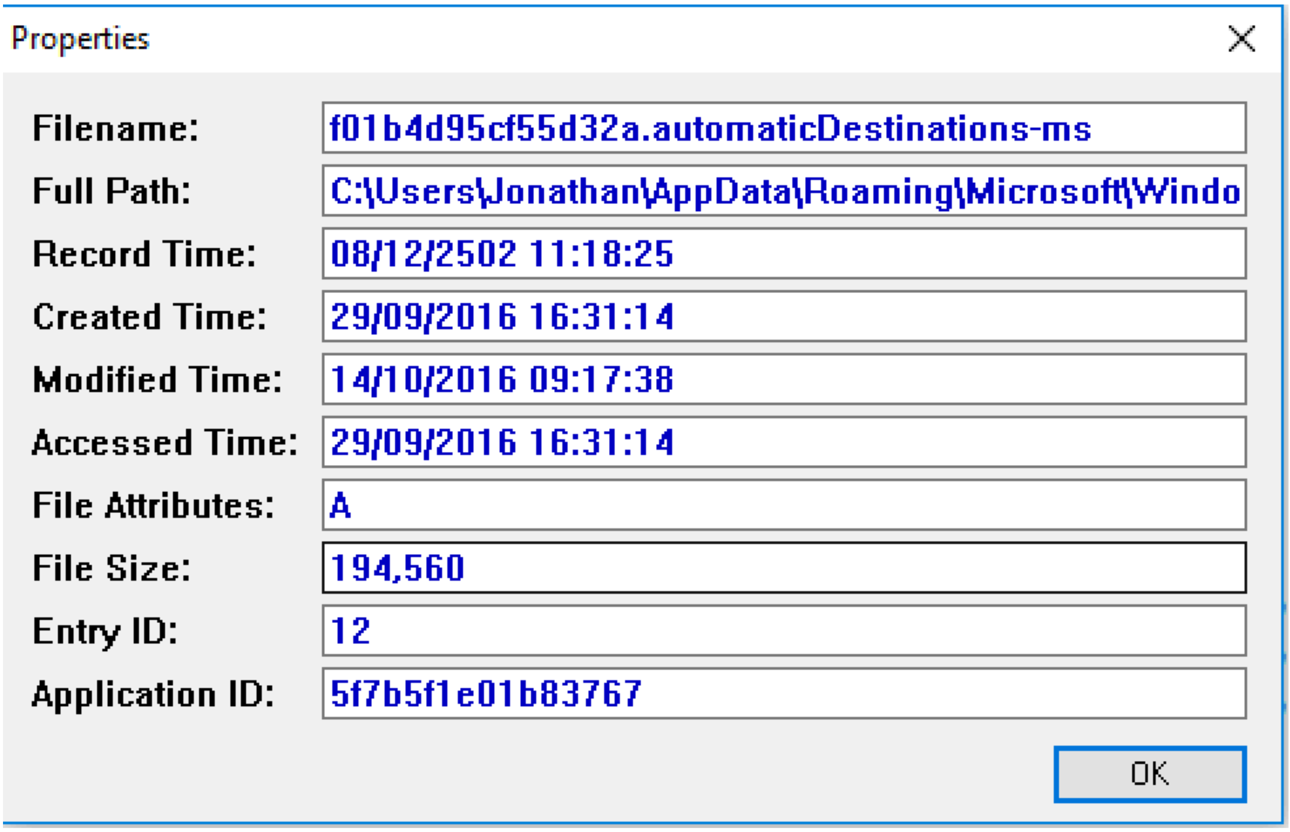


C:\Users\Jonathan\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

This PC › Local Disk (C:) › Users › Jonathan › AppData › Roaming › Microsoft › Windows › Recent Items › AutomaticDestinations

| Name | Date modified | Type | Size |
|---|---|---|---|
| 5f7b5f1e01b83767.automaticDestinations... | 14/10/2016 14:17 | AUTOMATICDESTI... | 25 KB |
| 7e4dca80246863e3.automaticDestination... | 07/10/2016 12:58 | AUTOMATICDESTI... | 3 KB |
| a0bb41d8716c03b9.automaticDestination... | 07/10/2016 12:58 | AUTOMATICDESTI... | 3 KB |
| cb05cc8c5a282971.automaticDestination... | 07/10/2016 12:58 | AUTOMATICDESTI... | 3 KB |
| cd45ac3b12f8efbb.automaticDestination... | 11/10/2016 15:55 | AUTOMATICDESTI... | 11 KB |
| d06c94537ecaee12.automaticDestination... | 14/10/2016 14:10 | AUTOMATICDESTI... | 2 KB |
| f01b4d95cf55d32a.automaticDestinations... | 14/10/2016 14:11 | AUTOMATICDESTI... | 190 KB |

I downloaded tool called jumpiest view, this allows me to view the .automaticDestinations-ms and the .customDestinations-ms. Information such filename, path, record time, created time, accessed time and application ID cane retrieved. This information can be beneficial to investigators because even the original file for which the jump list was created for was deleted, the jump list files aren't deleted so information such as the data from the screenshot below can be still viewed.



Properties

| | |
|---|---|
| Filename: | f01b4d95cf55d32a.automaticDestinations-ms |
| Full Path: | C:\Users\Jonathan\AppData\Roaming\Microsoft\Windo |
| Record Time: | 08/12/2502 11:18:25 |
| Created Time: | 29/09/2016 16:31:14 |
| Modified Time: | 14/10/2016 09:17:38 |
| Accessed Time: | 29/09/2016 16:31:14 |
| File Attributes: | A |
| File Size: | 194,560 |
| Entry ID: | 12 |
| Application ID: | 5f7b5f1e01b83767 |

Reference:
http://www.nirsoft.net/utils/usb_devices_view.html

https://www.magnetforensics.com/computer-forensics/how-to-analyze-usb-device-history-in-windows/

http://forensicartifacts.com/tag/jump-lists/
http://www.nirsoft.net/utils/jump_lists_view.html