




































## 1-. ¿Qué información contienen los perfiles?

| Nombre  | Tipo       | Datos   |
|---|------------|---|
|  (Predeterminado)  | REG_SZ     | (valor no establecido)                          |
|  Category          | REG_DWORD  | 0x00000000 (0)                                  |
|  DateCreated       | REG_BINARY | e5 07 05 00 01 00 11 00 09 00 36 00 16 00 37 03 |
|  DateLastConnec... | REG_BINARY | e5 07 0b 00 02 00 02 00 0c 00 04 00 38 00 57 01 |
|  Description       | REG_SZ     | Red   |
|  Managed           | REG_DWORD  | 0x00000000 (0)                                  |
|  NameType          | REG_DWORD  | 0x00000006 (6)                                  |
|  ProfileName       | REG_SZ     | Red   |

R= Información sobre el usuario.

## 2-. ¿Qué información contienen los registros en RecentDocs?

| Nombre   | Tipo       | Datos   |
|--|------------|---|
|  (Predeterminado) | REG_SZ     | (valor no establecido)                                    |
|  0                | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  1                | REG_BINARY | 49 00 6e 00 74 00 65 00 72 00 6e 00 65 00 74 00 00 00...  |
|  10               | REG_BINARY | 30 00 33 00 5f 00 54 00 65 00 73 00 74 00 4d 00 61 00...  |
|  100              | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  101             | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  102            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  103            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  104            | REG_BINARY | 49 00 4d 00 47 00 5f 00 35 00 30 00 30 00 35 00 2e 00...  |
|  105            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  106            | REG_BINARY | 49 00 4d 00 47 00 5f 00 33 00 30 00 32 00 38 00 2e 00...  |
|  107            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  108            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  109            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  11             | REG_BINARY | 49 00 4d 00 47 00 5f 00 37 00 38 00 34 00 37 00 2e 00...  |
|  110            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  111            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  112            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  113            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  114            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  115            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  116            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  117            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  118            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  119            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  12             | REG_BINARY | 46 00 6f 00 74 00 6f 00 73 00 00 00 5c 00 32 00 00 00 ... |
|  120            | REG_BINARY | 49 00 4d 00 47 00 5f 00 31 00 33 00 38 00 35 00 2e 00...  |
|  121            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  122            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  123            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |
|  124            | REG_BINARY | 3f 00 54 00 69 00 74 00 6c 00 65 00 49 00 64 00 3d 00...  |

R= Los registros de los documentos recientes

Podemos identificar los archivos pdf que se accedieron?

R= No

3-. ¿Qué información encuentro en ese registro?

| Nombre   | Tipo   | Datos   |
|--|--------|---|
|  (Predeterminado) | REG_SZ | (valor no establecido)  |
|  url1             | REG_SZ | <a href="http://go.microsoft.com/fwlink/p/?LinkId=255141">http://go.microsoft.com/fwlink/p/?LinkId=255141</a> |

4-. ¿Es importante la información que se encuentra en la ruta?

R= No pude llegar a esa ruta, no encontré la carpeta de services

5-. ¿Qué indicios nos da la información que se almacena en esa ruta?

R= Que son programas que están en nuestro equipo que pueden controlar diferentes aspectos, en mi caso me aparece una aplicación que es un anti-cheat de un juego y un controlador.

6-. ¿Qué indicios nos da la información que se almacena en los subregistros “Services”?

R= Creo que tiene que ver con algunas aplicaciones que tenemos en nuestro ordenador, pero me inclino más por que son drivers







7-. ¿Qué información guardan los subregistros de ésta ruta?

{ControlSet001\Enum\USBSTOR\Disk&Ven\_&Prod\_USB\_DISK\_2.0&Rev\_PMAP

| Nombre   | Tipo   | Datos                  |
|--|--------|------------------------|
|  (Predeterminado) | REG_SZ | (valor no establecido) |

R= La verdad no se que sea la información que se guarda ahí.

8-. ¿Qué información podemos determinar de los registros ubicados en esa ruta?

| Nombre  | Tipo       | Datos   |
|---|------------|---|
|  (Predeterminado)  | REG_SZ     | (valor no establecido)                                    |
|  \??\Volume{6ec... | REG_BINARY | 5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ... |
|  \??\Volume{a77... | REG_BINARY | 5c 00 3f 00 3f 00 5c 00 53 00 43 00 53 00 49 00 23 00 ... |
|  \DosDevices\C:    | REG_BINARY | 44 4d 49 4f 3a 49 44 3a cb c1 d9 6d f7 9d 58 41 b5 7f...  |
|  \DosDevices\D:    | REG_BINARY | 44 4d 49 4f 3a 49 44 3a cc 29 3e ca b6 0d a4 4b b6 1...   |
|  \DosDevices\E:    | REG_BINARY | 5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ... |

R= Si no me equivoco, por los nombres creo que se refiere a los discos duros que tenemos.