



Curso de Ciberseguridad

Análisis Forense en Windows

Análisis Forense Informático



Registro de Windows.....	4
Recuperación de Claves-Valor.....	6
Last Write Time.....	7
SAM.....	13
Identificando Usuarios y Grupos.....	13
Passwords en blanco.....	14
Principales Artefactos del registro de Windows.....	15
Identificar la versión del sistema.....	15
Nombre de la máquina.....	16
Zona horaria.....	17
Fecha de último acceso	18
Interfaces de Red.....	18
Histórico de Redes	20
Cuando se conectó a una Red.....	22
Carpetas Compartidas.....	23
AutoStart Programs.....	25
Información de Apagado	25
Búsqueda en Win7.....	26
Búsqueda en Win 8 /10	27
Typed Paths Windows 10.....	27
Recent Docs.....	28
Office Recent Docs.....	29
Office Reading Locations.....	29
Autoguardado de Ficheros Office.....	30
LastVisited MRU.....	32
OpenSaveMRU.....	33
Últimos Comandos Ejecutados	33
User AssistKey.....	35
FeatureUsage.....	37
Windows RecentAPPs.....	39
Shell Items.....	39
Recent Documents (LNK).....	40
Jumplists.....	44
Shellbags.....	47



Dispositivos USB.....	49
Mass Storage Device.....	49
Picture Transfer Protocol.....	50
Media Transfer Protocol.....	50
Identificar evidencias de uso dispositivos USB.....	51
USBStor.....	51
Identificación de VID/PID	52
Obtener el nombre del volumen.....	53
Obtener la última unidad asignada.....	53
Localizar el usuario que ha utilizado el USB.....	56
Volumen Serial Number.....	56
Timestamps.....	57



REGISTRO DE WINDOWS

El registro de Windows es uno de los artefactos más importante para un investigador, ya que dispone de mucha información acerca del sistema y de la actividad del usuario. Veremos cuatro secciones relacionadas con el registro de Windows:

- ◆ Registro de Windows: veremos todo lo necesario para leer el registro
- ◆ Usuario / Grupo: analizaremos la información relacionada permitiendo obtener el último login y los usuarios que tienen acceso al sistema. En el SAM.
- ◆ Configuración del sistema: obtener la última dirección IP, identificar los puntos de acceso a los que se ha conectado. SYSTEM o SOFTWARE
- ◆ Actividad del usuario: la parte más útil en cuento al registro. Monitorizar la actividad gracias a los documentos abiertos, aplicaciones ejecutadas, etc. NTUSER.DAT

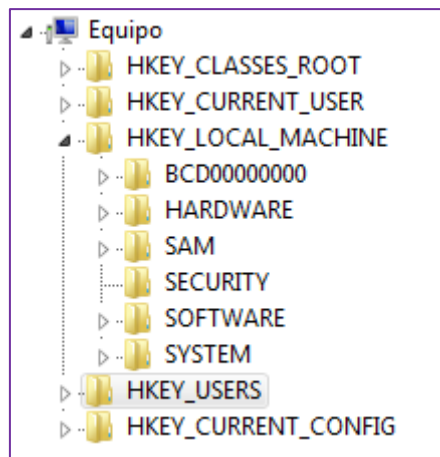
Donde se encuentran los ficheros de registro en un sistema Windows: en **%Windir%\System32\Config:**

- ◆ SAM -> **HKEY_LOCAL_MACHINE**
- ◆ SECURITY -> **HKEY_LOCAL_MACHINE**
- ◆ SYSTEM -> **HKEY_LOCAL_MACHINE**
- ◆ SOFTWARE -> **HKEY_LOCAL_MACHINE**
- ◆ DEFAULT -> **HKEY_LOCAL_MACHINE**

Existen también otro registro, relacionado con el usuario en **\%UserProfile%\{user}\:**

- ◆ NTUSER.DAT -> **HKEY_CURRENT_USER**

Si abrimos nuestro Sistema y ejecutamos regedit.exe, veremos que la raíz del registro es la siguiente:



Los sistemas Windows disponen de una copia de seguridad del registro localizado en
%Windir%\System32\Config\RegBack:

- ◆ SAM -> HKEY_LOCAL_MACHINE
- ◆ SECURITY -> HKEY_LOCAL_MACHINE
- ◆ SYSTEM -> HKEY_LOCAL_MACHINE
- ◆ SOFTWARE -> HKEY_LOCAL_MACHINE
- ◆ DEFAULT -> HKEY_LOCAL_MACHINE

Esta copia de seguridad solo está disponible de Windows Vista en adelante y de Windows 2008 Server en adelante. Otro lugar donde podíamos encontrar una copia del registro sería en las Shadow Copies.

¿Qué registros hay asociados al usuario?

1. NTUSER.DAT

- ◆ C:\Users\{username}\NTUSER.DAT -> WinVista-Win10
- ◆ C:\Documents and Settings\{username}\NTUSER.dat -> XP



2. USRCLASS.DAT

- ◆ C:\Users\{username}\AppData\Local\Microsoft\Windows\USRCLASS.DAT -> Solo disponible a partir de Win7/Win8/Win10

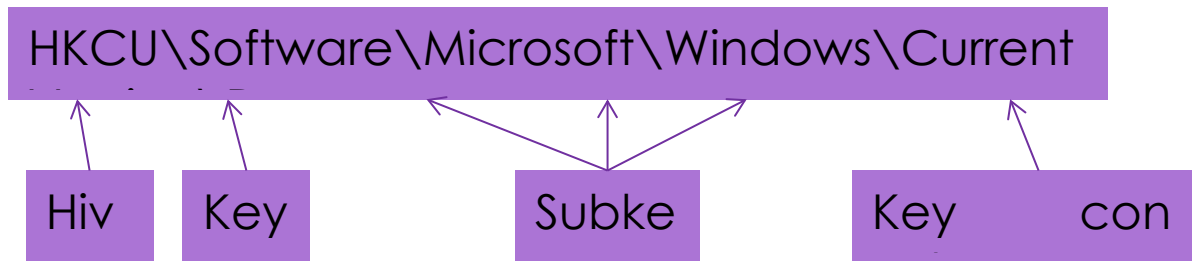
USRCLASS.DAT es muy importante porque contiene información en cuanto la ejecución de programas indicando que directorios y han sido abiertos o cerrados.

- ◆ El propósito principal del UsrClass.DAT es ayudar a la UAC.

Estos registros de usuario son únicos para usuario del sistema, por lo que siempre habrá uno para cada usuario.

RECUPERACIÓN DE CLAVES-VALOR

¿Qué hay dentro del registro de Windows? La información está organizada de la siguiente manera:



Key : similar a los directorios (keys) y subdirectorios (subkeys)

- ◆ Produce una jerarquía de directorios

Values: información almacenada dentro de una key

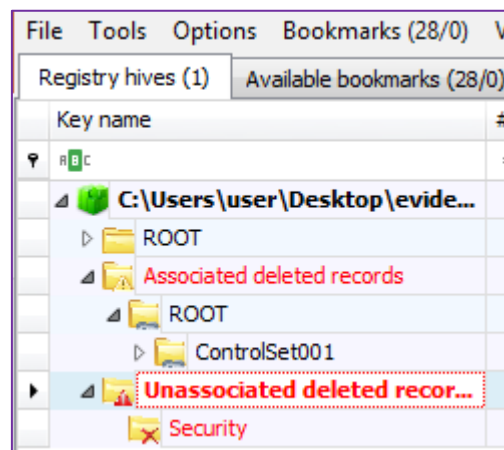
- ◆ Contiene información en forma de: strings, integers, lists.

Los Hives del registro de Windows tiene espacio libre similar al sistema de archivos, por lo que se podrán recuperar keys borradas. Una clave borrada es marcada, pero no es deslocalizada, por lo que permite la recuperación de:

- ◆ Keys
- ◆ Values
- ◆ TimeStamps

El registro de Windows, dispone de espacio libre o unallocated, similar a los sistemas de archivos que vimos anteriormente. Este hecho permite recuperar:

- ◆ Keys
- ◆ Values
- ◆ TimeStamps



Hoy en día no hay herramientas anti forenses que limpien completamente el espacio libre del registro.

Se puede identificar el funcionamiento de este espacio libre en el siguiente enlace:

<http://sentinelchicken.com/data/JolantaThomassenDISSERTATION.pdf>

En la imagen anterior vemos la herramienta **Registry Explorer** donde aparece en rojo las claves-valor que han sido borradas. Más adelante veremos cómo funciona esta herramienta.

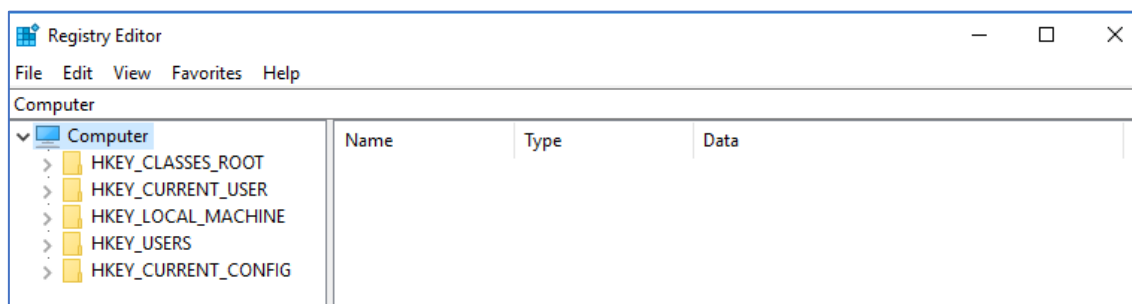
LAST WRITE TIME

Dentro del registro también hay timestamps y se le llama “**Last Write Time**”. Como bien dice su nombre, es la última vez que se modificó la key-value del registro. Para poder interpretar este campo como una fecha real, es necesario realizar pruebas con la aplicación que escriba en el registro y poder contextualizar la información.

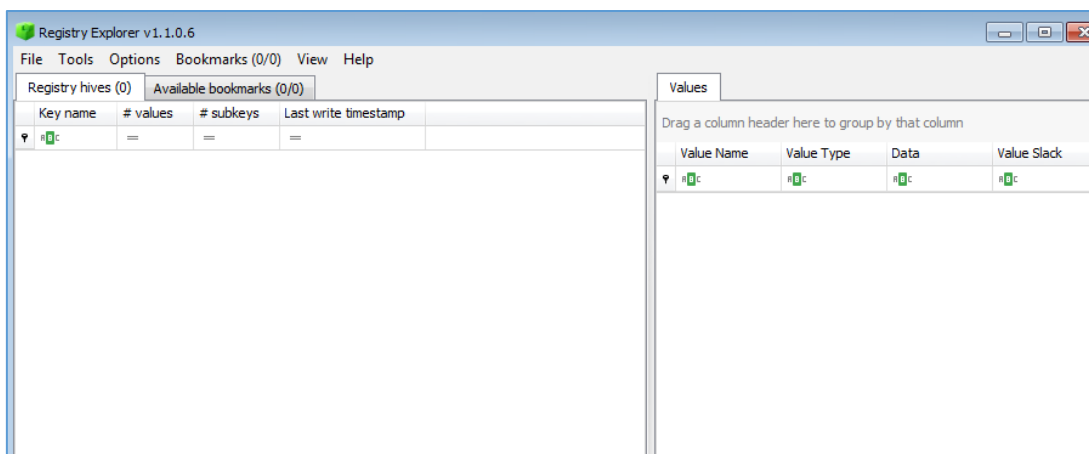
Otro elemento que indica un orden temporal es el **MRU**, que es el acrónimo de Most Recently Used.

- ◆ Existen varios MRU que son responsables del drop-down sobre un menú que aparece o cuando tecleas algo en Internet Explorer.
- ◆ En el registro, los MRULists son una Key-Value que son responsables de mantener registrado las adiciones al registro. Por lo tanto, se puede determinar en qué orden se añadió.
- ◆ La MRUList pueden variar en función del sistema operativo.
- ◆ El Last write de la key será la fecha del primer MRUList que ocurrió

Herramientas para Analizar el Registro de manera online:



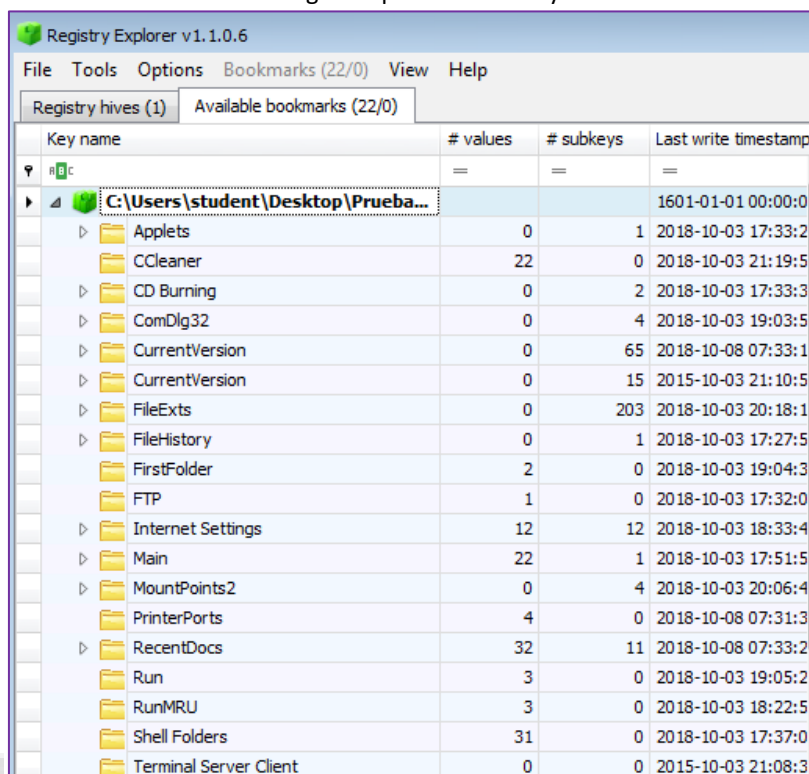
Herramientas para Analizar el Registro de manera offline: Registry Explorer



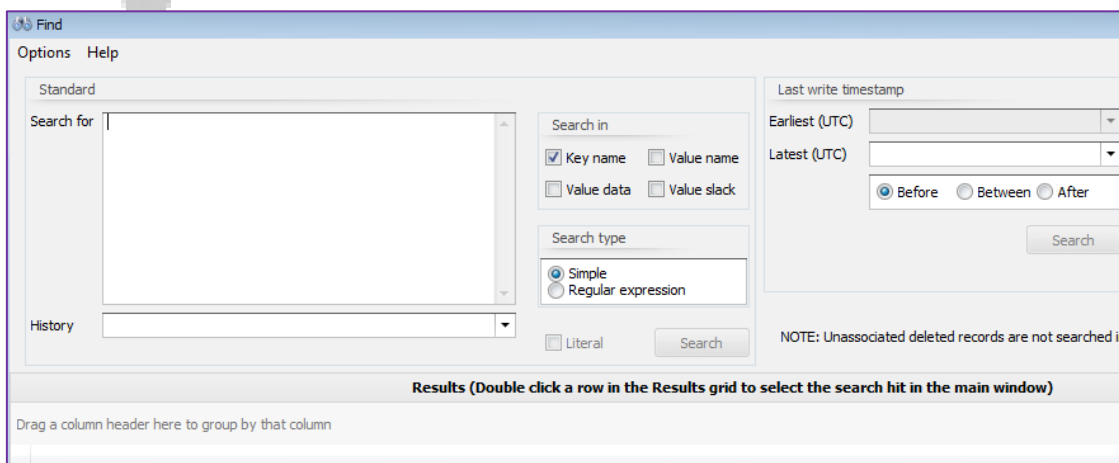
QUANTIKA¹⁴

Registry Explorer dispone de:

1. **Bookmarks:** en función del registry hive cargado (NTUSER.DAT,SYSTEM,etc), carga unos bookmarks u otros. Son claves del registro que se conocen y contienen información útil



2. **Find:** permite buscar por el string o regex, filtrando por tiempo, valores mínimos.



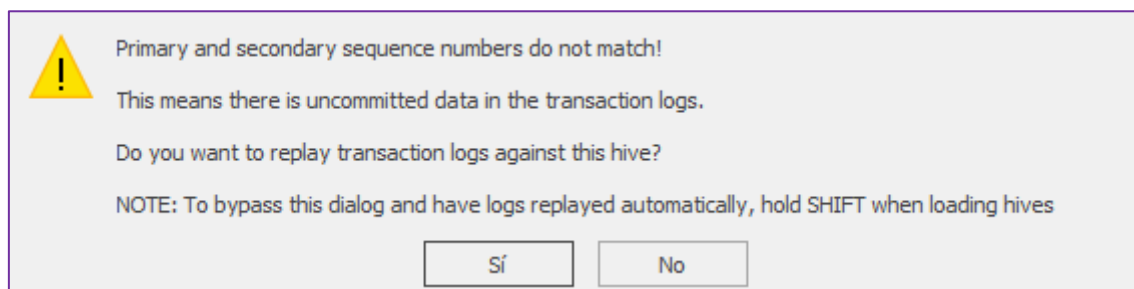
**Ver video: 001/MÓD. 3 - Registry Explorer*

Otro factor a tener en cuenta de esta herramienta es que es capaz de identificar cuando un registro está sucio, es decir que hay información pendiente de ser grabada.

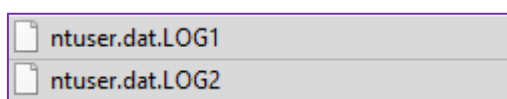
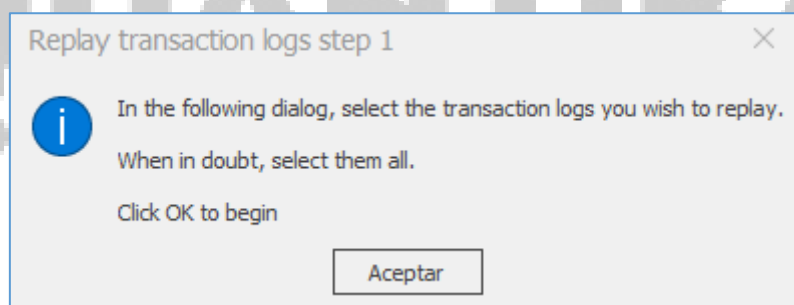
¿Dónde está esa información? Pues está en la misma carpeta donde encontremos el registro, pero con la extensión .LOG, por ejemplo:

- Ntuser.dat
- Ntuser.dat.LOG1
- Ntuser.dat.LOG2

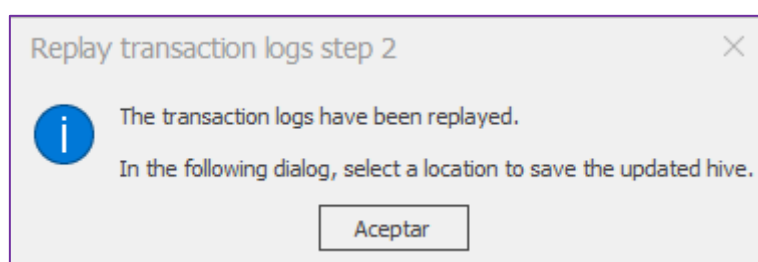
Cuando detecta un registro sucio, aparece el siguiente mensaje:



Este hecho es muy importante, ya que, si hay información pendiente, dicha información puede ser vital para la investigación. A la pregunta anterior deberemos indicarle que sí y a continuación nos pedirá seleccionar los *.LOG



Y por último nos pedirá la localización del nuevo registro o hive a guardar con los cambios que han sido introducidos:



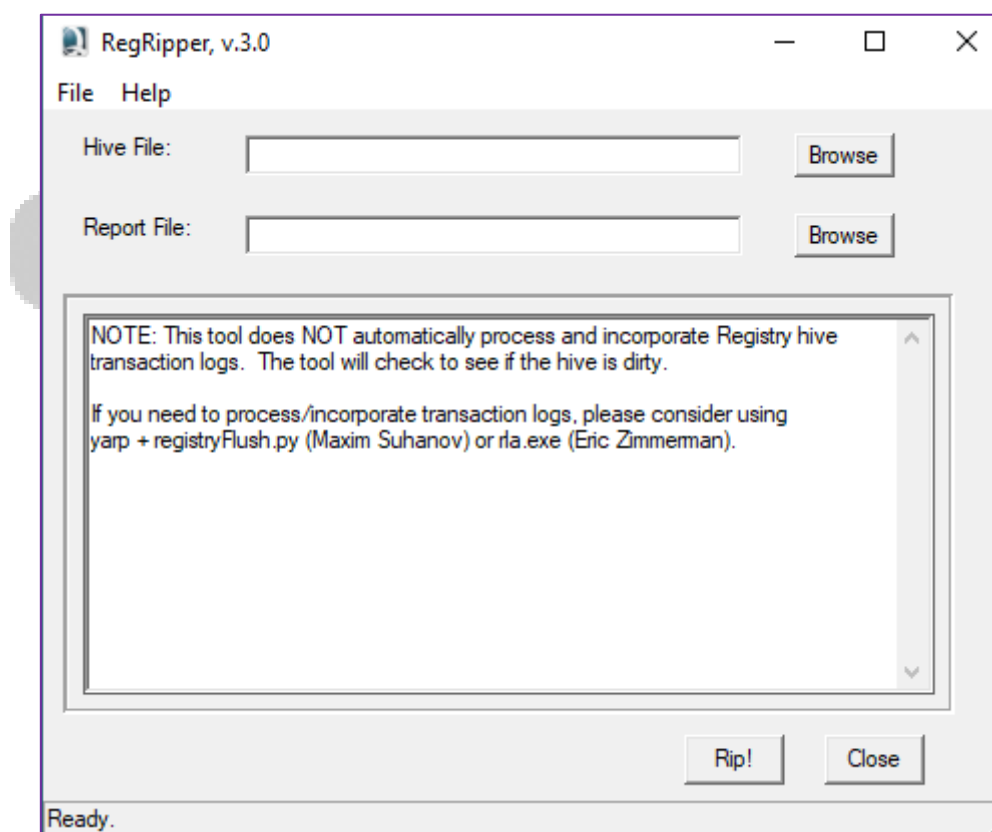
Este tipo de funcionamiento respecto al registro empezó a aplicarse a partir de Windows 8, se puede obtener más información en el siguiente enlace:

<https://github.com/msuhanov/regf-samples/blob/master/8.1-unreconciled/Flush%20strategies%20in%20the%20Windows%20registry.md>

RegRipper es otra herramienta escrita en Perl que se encarga de analizar los hives del registro. El análisis no es tan user friendly como lo que presenta Registry Explorer, pero también dispone de unos bookmarks o plugins de localizaciones de key-value del Registro con información relevante:

<https://github.com/keydet89/RegRipper3.0/tree/master/plugins>

A diferencia de Registry Explorer, en RegRipper se le debe indicar mediante el campo de Profile cuál es el tipo de hive que va a analizar. De esta manera cargará los plugins acordemente.

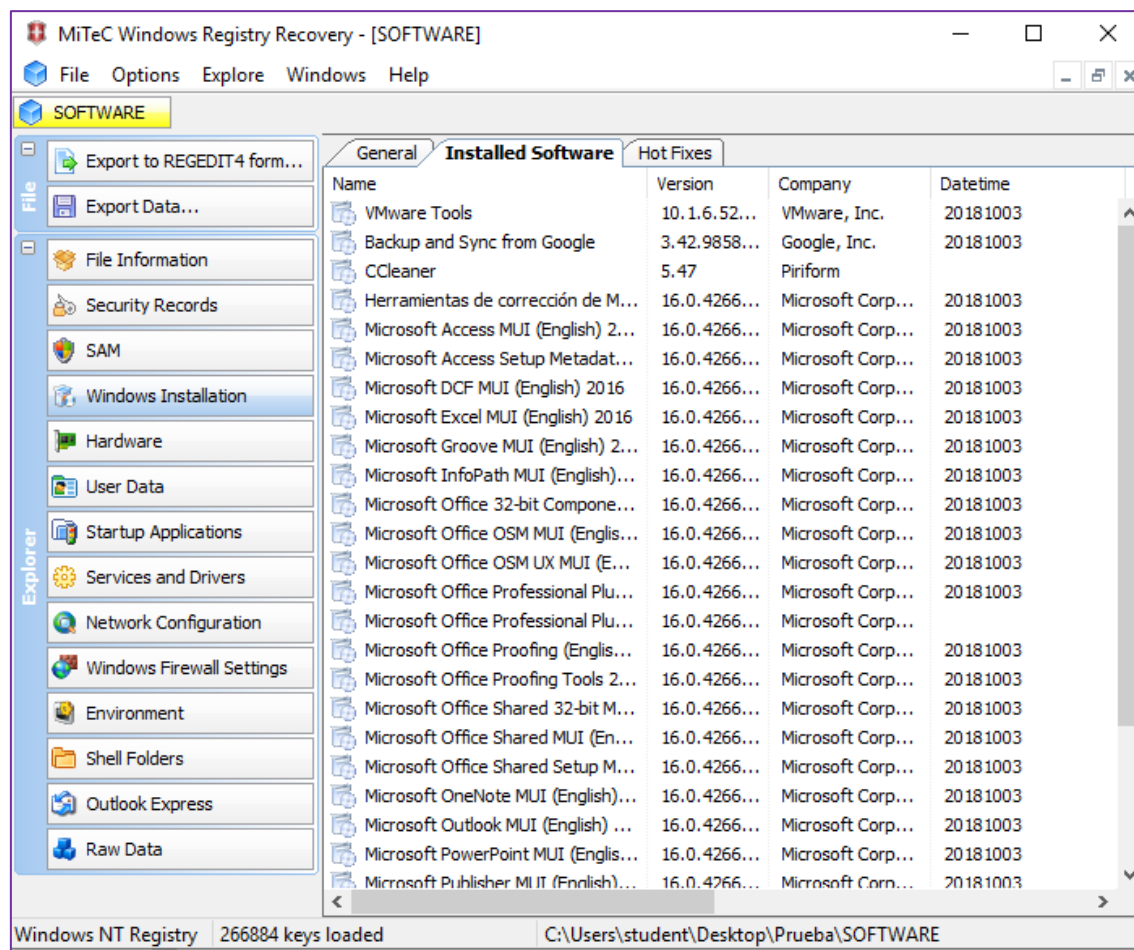


El reporte de RegRipper es un fichero de texto que puede ser abierto con Notepad++.

**Ver video: 002/MÓD. 3 - RegRipper*



Windows Registry Recovery es otro software que permite analizar el registro de Windows, de manera visual. Es muy útil para obtener que aplicaciones han sido instaladas, como podemos apreciar en la imagen inferior.



En función del Hive seleccionado, las opciones de la izquierda dispondrán de información.

**Ver Video:003/MÓD. 3 - WRR*

SAM

El fichero SAM o hive SAM, contiene todos los usuarios y grupos que hay nivel local en el sistema Windows. También dispone de los hashes pertinentes que son validados cuando un usuario hace login.

IDENTIFICANDO USUARIOS Y GRUPOS

Del fichero SAM podemos obtener a que grupo está asignado el usuario como, por ejemplo:

- ◆ Administradores
- ◆ Usuarios
- ◆ Usuarios del escritorio Remoto

¿Qué información podemos obtener del registro SAM del usuario?

La información se encuentra en SAM\Domains\Account\Users y contiene:

- ◆ El usuario y el RID asociado a él.
- ◆ Variedad de información asociado al usuario
- ◆ Último login (vacío si se utiliza una cuenta Microsoft para hacer login)
- ◆ Último login fallido
- ◆ Contador de login
- ◆ Política de passwords
- ◆ Cuando se creó la cuenta.

Use...	Invalid Login Count	Total Login Count	Created On	Last Login Time	Last Password ...	Last Incorrect ...	Expires On	User Name	Full Name	Passwor...	Groups
1001	0	0	2018-10-03 17:27:49		2018-10-03 17:...			ismis	Ismael Serrano		Administrators, Users
1002	0	4	2018-10-08 07:35:54	2018-10-08 08:19:49	2018-10-08 07:...	2018-10-08 07:...		pedro			Users
504	0	0	2018-10-03 17:21:03		2018-10-03 17:...			WDAGUtilityAccount			

En la imagen anterior se ve el detalle que el usuario "ismis" utiliza una cuenta Microsoft para hacer login, debido a que el campo "Last Logon Time" está vacío.

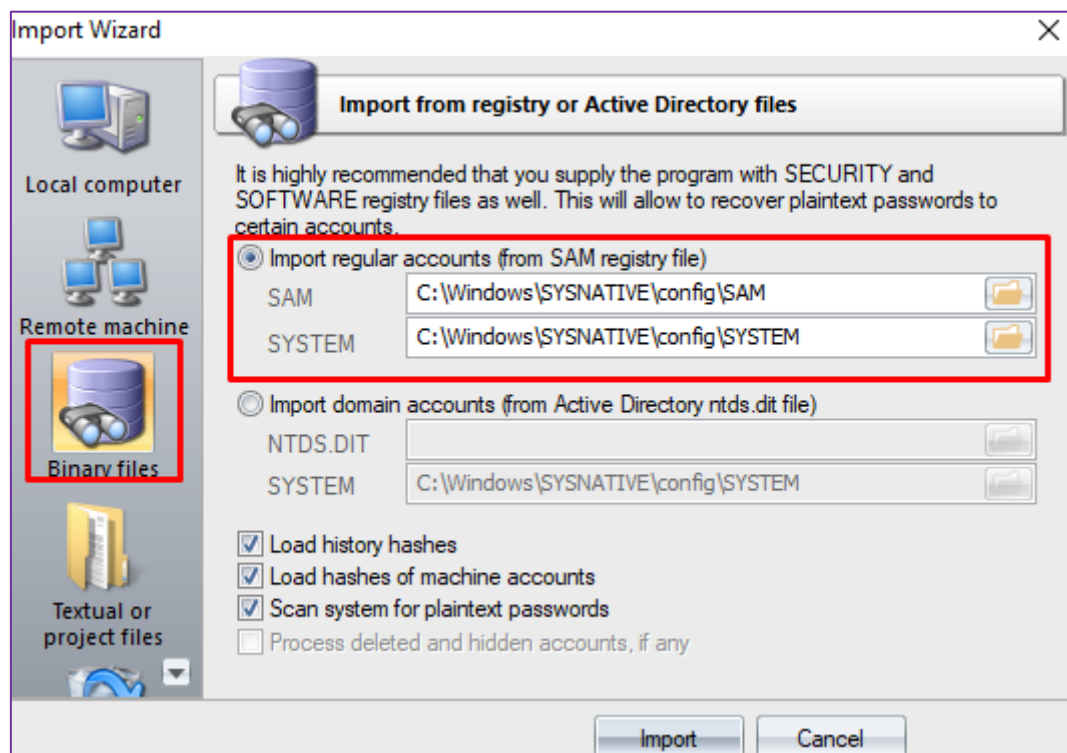
Con la herramienta WRR se puede identificar correctamente:

General Groups and Users	
Users	Property Value
Administrator	SID S-1-5-21-3562354317-1246539426-1872400879-1001
Guest	Full name Ismael Serrano
DefaultAccount	Last password set 10/3/2018 5:27:51 PM
WDAGUtilityAccount	Account expiration 12/30/1899 2:48:05 AM
ismis	
pedro	

PASSWORDS EN BLANCO

Windows 10 implementa un cifrado de hashes, que puede inducir a error, si no es analizado correctamente. Si la herramienta no es capaz de interpretar este nuevo cifrado aparecerá que el NTLM-HASH es un blanco: 31d6cfe0d16ae931b73c59d7e0c089c0

Para poder ver los hashes es necesario tener el SAM y el SYSTEM del sistema. Gracias a la herramienta **Windows Password Recovery** de Passcape podríamos verificar su hash:



Windows Password Recovery si puede leer el nuevo cifrado AES 128 de Windows, [mimikatz](#) también.

User name	RID	LM password	NT password	LM h...	NT hash	Description
<input type="checkbox"/> Administrator	500	<Empty>	<Empty>			Built-in account for administering the com...
<input type="checkbox"/> Guest	501	<Empty>	<Empty>			Built-in account for guest access to the co...
<input type="checkbox"/> DefaultAccount	503	<Empty>	<Empty>			A user account managed by the system.
<input checked="" type="checkbox"/> WDAGUtilityAccount	504	<Empty>			42BA2EDF254B6342F1370B680FC3737C	A user account managed and used by the s...
<input checked="" type="checkbox"/> ismiserrani2345@gmail.com	1001	<Empty>			08FA17EF16A707A63E8607E7478DAA28	
<input checked="" type="checkbox"/> pedro	1002	<Empty>			94000977A697D50F077BAFB019829C59	

Si no lo leyese bien, aparecería un hash blanco: 31d6cfe0d16ae931b73c59d7e0c089c0



PRINCIPALES ARTEFACTOS DEL REGISTRO DE WINDOWS

A continuación, vamos a identificar las principales claves-valor del registro que pueden ser susceptibles de ser usadas en caso de realizar una investigación.

Antes de comenzar el análisis, se debe tener en cuenta que Windows respecto a que configuración carga en su sistema operativo utiliza el registro SYSTEM.

Dentro de SYSTEM, esta una Clave-Valor que indica que configuración es la que aplica:

- ◆ ControlSet001: configuración que es cargada cuando arranca el sistema operativo
- ◆ ControlSet002: ultima configuración buena conocida.

Como veremos más adelante, cuando hagamos una referencia a SYSTEM, siempre trabajaremos con ControlSet001.

IDENTIFICAR LA VERSIÓN DEL SISTEMA

Este artefacto forense, como bien el título, nos va a permitir identificar en el registro la versión del sistema.

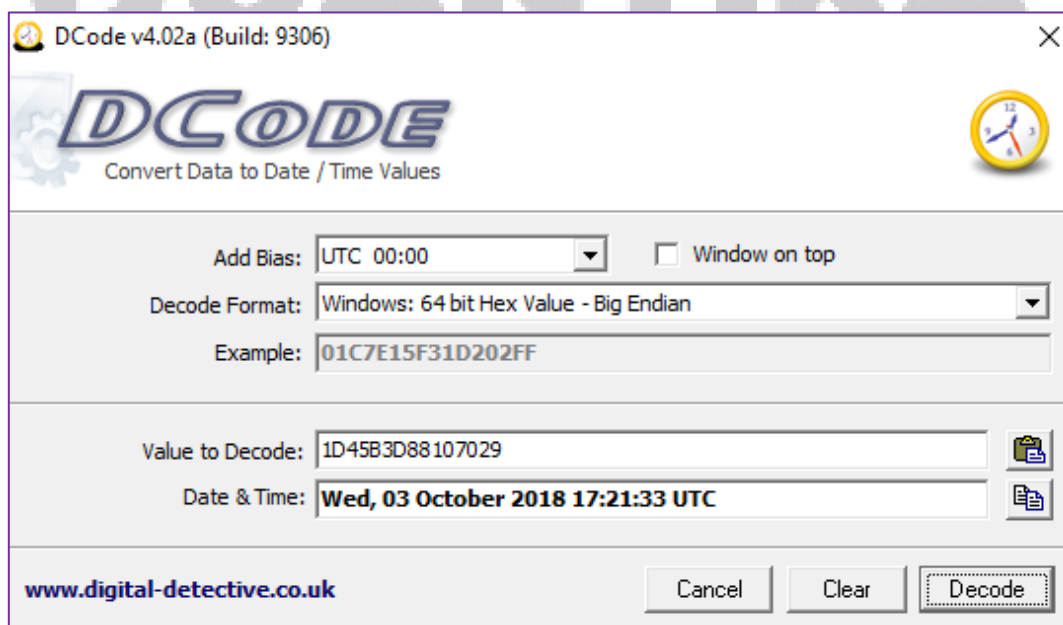
Ruta: **Software\Microsoft\Windows NT\CurrentVersion**

Determina:

- ◆ La versión de Windows
- ◆ Service Pack instalador
- ◆ Fecha de instalación en formato Epoch Time (número de segundos desde el 1/1/1970)
- ◆ En Windows tiene el campo Install Time que sigue el formato de Windows 64 bit, respecto al tiempo

SystemRoot	RegSz	C:\Windows	00-00-00-00-00-00
BuildBranch	RegSz	rs5_release	00-00-00-00
BuildGUID	RegSz	ffffffff-ffff-ffff-ffffffff	00-00
BuildLab	RegSz	17763.rs5_release.180914-1434	
BuildLabEx	RegSz	17763.1.amd64fre.rs5_release.180914-1434	00-00
CompositionEditionID	RegSz	Enterprise	00-00-00-00-00-05
CurrentBuild	RegSz	17763	
CurrentBuildNumber	RegSz	17763	
CurrentMajorVersionNumber	RegDword	10	
CurrentMinorVersionNumber	RegDword	0	
CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00-00-00-00-00-00
CurrentVersion	RegSz	6.3	00-00-00-00
EditionID	RegSz	Professional	00-00
EditionSubManufacturer	RegSz		
EditionSubstring	RegSz		
EditionSubVersion	RegSz		
InstallationType	RegSz	Client	00-00-00-00-00-00
InstallDate	RegDword	1538587293	
ProductName	RegSz	Windows 10 Pro	72-00-70-00-72-00-69-00-73-00-6
ReleaseId	RegSz	1809	00-00
SoftwareType	RegSz	System	00-00-00-00-00-00
UBR	RegDword	1	
PathName	RegSz	C:\Windows	00-00-00-00-00-00
ProductId	RegSz	00330-80000-00000-AA502	76-6B-63-00
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-30-33-30-2...	
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-35-00-35-00-30-00...	5C-00-5C-00
RegisteredOwner	RegSz	ismiserrani2345@gmail.com	
RegisteredOrganization	RegSz		
InstallTime	RegQword	131830608934498345	00-00-00-00

En el registro encontraremos la fecha (Install Time) en decimal, la convertimos a hexadecimal y la pasamos por la herramienta Dcode (Windows: 64 Bit Hex Value Big Endian)



DCode: <https://www.digital-detective.net/dcode/>

NOMBRE DE LA MÁQUINA



Es útil ya que el nombre de la maquina aparece en otras localizaciones, pero generalmente se usa para asegurar que estamos trabajando con el equipo correcto.

Ruta: **System\ControlSet001\Control\ComputerName\ComputerName**

RBC	RBC	RBC	RBC
(default)	RegSz	mnmsrvc	DC-00-00-00
ComputerName	RegSz	DESKTOP-9D0L8DV	70-00-69-00

ZONA HORARIA

Es útil para correlacionar correctamente la actividad en la evidencia:

- ◆ Logs internos del sistema y timestamps estarán basadas en esta información
- ◆ Antes habíamos visto los timestamps del registro están en UTC.
- ◆ FAT está asociada a la hora local del sistema y por lo tanto a este parámetro. NTFS esta en UTC.

Ruta: **System\ControlSet001\Control\TimeZoneInformation**

QUANTIKA¹⁴



Drag a column header here to group by that column

Value Name	Value Data
Root	Root
Bias	-60
DaylightBias	-60
DaylightName	@tzres.dll,-301
DaylightStart	Month 3, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
StandardBias	0
StandardName	@tzres.dll,-302
StandardStart	Month 10, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 3:0:0:0
TimeZoneKeyName	Romance Standard Time
ActiveTimeBias	-120

Romance Standard Time = Central European TIME:

https://en.wikipedia.org/wiki/Central_European_Time

FECHA DE ÚLTIMO ACCESO

Por defecto Windows no actualiza la fecha de último acceso. Es una propiedad que se encuentra en el registro:

Ruta: **System\ControlSet001\Control\FileSystem**

- Hay que verificar si esta activado buscando NtfsDisableLastAccessUpdate = 0
- Por defecto viene activada esta opción lo que impide saber cuándo se accedió (Win7-Win10)

NtfsDisableEncryption	RegDword	0
NtfsDisableLastAccessUpdate	RegDword	1
NtfsDisableLfsDowngrade	RegDword	0
NtfsDisableVolumeHints	RegDword	0

Comando para activarlo: **fsutil behavior set disablelastaccess 0**

INTERFACES DE RED

¿Por qué es útil?

- Determinar los interfaces de red de la maquina
- Determinar si el sistema tuvo una IP Estática o por DHCP

Obtener GUID de la interface para hacer correlaciones

Ruta: **System\ControlSet001\Services\Tcpip\Parameters\Interfaces\{GUID_INTERFACE}**

storgosft		RegDword	1
StorSvc			
storufs			
storsvc			
svsvc			
swenum			
swprv			
Synth3dVsc			
SysMain			
SystemEventsBroker			
TabletInputService			
TapiSrv			
Tcpip			
Linkage			
Parameters			
Adapters			
DNSRegisteredAdapters			
Interfaces			
{3f08ac97-e552-42ba-859c-72ed6d806619}			
{65449752-c738-11e8-adcf-806e6f6e963}			
{b6d0b397-506c-4681-b245-d5da39691a20}			
{d82acf49-790b-4c47-a095-336f124270bb}			
{e64f4909-33bd-4b94-ab36-72e47b94149e}			
NsiObjectSecurity			

EnableDHCP	RegDword	1
Domain	RegSz	
NameServer	RegSz	
DhcpIPAddress	RegSz	192.168.192.133
DhcpSubnetMask	RegSz	255.255.255.0
DhcpServer	RegSz	192.168.192.254
Lease	RegDword	1800
LeaseObtainedTime	RegDword	20
T1	RegDword	920
T2	RegDword	1595
LeaseTerminatesTime	RegDword	1820
AddressType	RegDword	0
IsServerNapAware	RegDword	0
DhcpConnForceBroadcastFlag	RegDword	0
DhcpDomain	RegSz	localdomain
DhcpNameServer	RegSz	192.168.192.2
DhcpDefaultGateway	RegMultiSz	192.168.192.2
DhcpSubnetMaskOpt	RegMultiSz	255.255.255.0
DhcpInterfaceOptions	RegBinary	FC-00-00-00-00-00-00-00-00-00-00-00-00...
DhcpGatewayHardware	RegBinary	C0-A8-C0-02-06-00-00-00-00-50-56-EB-4...
DhcpGatewayHardwareCount	RegDword	1

Esta información aparece mucho mejor representada en el WRR:

SOFTWARE	NTUSER.DAT	SAM	SYSTEM
File	Components	TCP/IP	
Export to REGEDIT4 form...	Wi-Fi	Adapter	ZyDAS ZD1211 802.11 b+g Wireless LAN
Export Data...	Enabled DHCP	Enabled DHCP	1
File Information	Ethernet (Kernel Debugger)	Adapter	Microsoft Kernel Debug Network Adapter
Security Records	Enabled DHCP	Enabled DHCP	1
SAM	Ethernet0	Adapter	Intel(R) 82574L Gigabit Network Connection
Windows Installation	Enabled DHCP	Enabled DHCP	1
Hardware	DhcpIPAddress	DhcpIPAddress	192.168.192.133
User Data	DhcpSubnetMask	DhcpSubnetMask	255.255.255.0
Startup Applications	DhcpServer	DhcpServer	192.168.192.254
Services and Drivers	Lease	Lease	708
Network Configuration	LeaseObtainedTime	LeaseObtainedTime	14
Windows Firewall Settings	T1	T1	398
Environment	T2	T2	638
Shell Folders	LeaseTerminatesTime	LeaseTerminatesTime	71C
Outlook Express	AddressType	AddressType	0
Raw Data	IsServerNapAware	IsServerNapAware	0
	DhcpConnForceBroadcastFlag	DhcpConnForceBroadcastFlag	0
	DhcpDomain	DhcpDomain	localdomain
	DhcpNameServer	DhcpNameServer	192.168.192.2
	DhcpDefaultGateway	DhcpDefaultGateway	192.168.192.2
	DhcpSubnetMaskOpt	DhcpSubnetMaskOpt	255.255.255.0
	DhcpInterfaceOptions	DhcpInterfaceOptions	FC 00 00 00 00 00 00 00 00 00 00 00 00
	DhcpGatewayHardware	DhcpGatewayHardware	C0 A8 C0 02 06 00 00 00 00 50 56 EB 4C 33
	DhcpGatewayHardwareCount	DhcpGatewayHardwareCount	1
	Bluetooth Network Connection	Adapter	Bluetooth Device (Personal Area Network)
	Enabled DHCP	Enabled DHCP	1

HISTÓRICO DE REDES

¿Qué podemos encontrar?

- ◆ Identificar redes a la que el equipo se conecto
- ◆ Identificar si las redes eran cableadas o inalámbricas
- ◆ Identificar el nombre dominio
- ◆ Identificar el SSID
- ◆ Identificar la MAC Address del gateway

Ruta:

- ◆ **Software\Microsoft\Windows NT\CurrentVersion\NetworkList**
- ◆ **Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache**

¿Por qué es útil?

- ◆ Primera y última vez que se produjo la conexión a la red
- ◆ Listar conexiones que han sido conectadas a través de VPN

Drag a column header here to group by that column

Network Name	Name Type	First Connect LOCAL	Last Connected LOCAL	Managed	DNS Suffix	Gateway Mac Address	Profile GUID
Network	Wired	2018-10-03 19:21:00	2018-10-08 10:19:27		<none>	00-50-56-EB-4C-33	{54ADAF4F-0492-458F-96EA-652ED5ABD35C}

La anterior imagen corresponde con la evidencia de prácticas, sin embargo, podemos encontrar también las WiFi a las que el equipo estuvo conectado y en especial la MAC del SSID:

Network Name	Name Type	Gateway Mac Address	First Connect LOCAL
Hotel Eurostars Gran Valencia	Wireless	6C-3B-6B-DD-8F-16	2019-11-25 17:56:08
WIFI_GUEST	Wireless	00-1C-7F-7D-29-EF	2019-06-03 13:10:22
MOVISTAR_1010	Wireless	00-4A-77-E2-57-31	2018-12-19 19:38:38
mitm	Wireless	B4-86-55-47-7D-FD	2019-09-26 18:41:21
Melia	Wireless	00-0B-86-6E-FC-44	2019-03-13 17:34:04
IHGConnect	Wireless	CC-03-D9-22-0D-10	2020-01-14 09:23:52
CODIGO1_25FE50	Wireless	06-D6-AA-72-B7-07	2019-09-05 10:40:01
DIRECT-dv-FireTV_6bb6	Wireless		2020-01-15 00:33:51

Existe un servicio en Internet, llamado [Wigle](http://wigle.net) que tiene una base de datos de las MAC de los SSID de las WiFi

The screenshot shows the Wigle.net website interface. At the top, there's a navigation bar with icons for View, Uploads, Info, Stats, and Tools. Below this, a banner reads "All the networks. Found by Everyone." followed by statistics: STUMBLERS (285,144), WIFI NETWORKS (674,076,399), WIFI OBSERVATIONS (9,581,400,567), and WIFI TODAY (47,360). The main content area is divided into two columns. The left column contains three announcement boxes: "File processing is back!" (dated Fri, 26 Jun 2020 17:10:02 GMT), "File Processing Paused" (dated Tue, 23 Jun 2020 20:55:20 GMT), and "Reminder about group registration" (dated Mon, 15 Jun 2020 20:02:09 GMT). The right column features a map of San Francisco with a search bar at the top that says "Buscar dirección o lugar". The map shows various streets and landmarks like the University of San Francisco and Kezar Stadium.

El servicio de Wigle, es alimentado por los propios usuarios que instalan una aplicación en el celular o teléfono móvil de tal manera que van posicionando las WiFi que hay alrededor.

Para acceder a Wigle es necesario registrarse.

CUANDO SE CONECTÓ A UNA RED

Propósito:

- ◆ Identificar el tipo de red a la que se conectó
- ◆ Identificar el SSID de la red inalámbrica
- ◆ El timestamp de este artefacto esta local time.

Ruta:

- ◆ **Software\Microsoft\WZCSVC\Parameters\Interfaces\{GUID} -> XP**
- ◆ **Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles -> Win7-Win10**

Si la maquina es Win7-Win10 el tipo de red (NameType) viene definido de la siguiente manera:

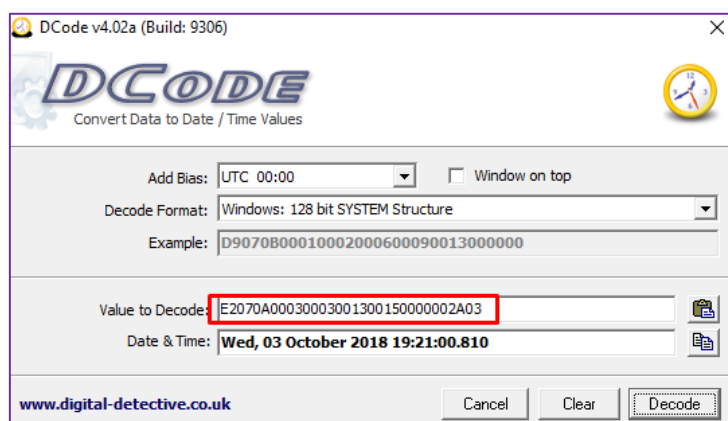
- ◆ 0x47 -> Wireless
- ◆ 0x06 -> Cableada
- ◆ 0x17 -> 3G

Categoría:

- ◆ Public -> 0
- ◆ Private / Home -> 1
- ◆ Domain /Work 2

ProfileName	RegSz	Network	0B-F1-7B-60
Description	RegSz	Network	00-00-00-00
Managed	RegDword	0	
Category	RegDword	0	
DateCreated	RegBinary	E2-07-0A-00-03-00-03-00-13-00-15-0...	73-FC-7B-10
NameType	RegDword	6	
DateLastConnected	RegBinary	E2-07-0A-00-01-00-08-00-0A-00-13-...	00-00-00-00

Podemos identificar también DateCreated y DateLastConnected. Usando Windows 128 bit time y esta almacenado en local time.



Con el ProfileGUID {54ADAF4F-0492-458F-96EA-652ED5ABD35C} podemos mapear información histórica.

CARPETAS COMPARTIDAS




¿Qué podemos identificar?

- ◆ Carpetas compartidas a nivel local
- ◆ Configuración de dichas carpetas compartidas

Ruta: **System\ControlSet001\Services\lanmanserver\Shares**

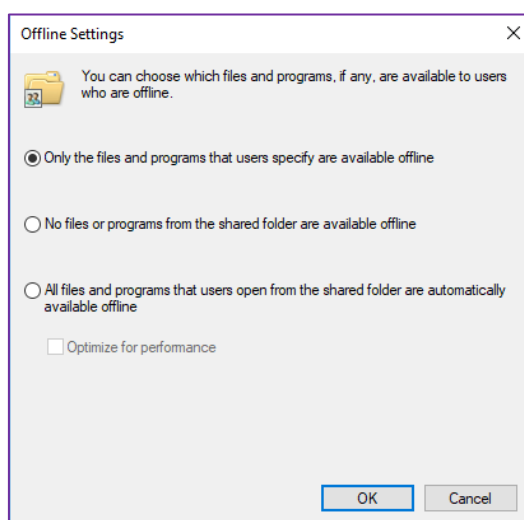
Flags:

- ◆ CSCFlags: Caching Setting
- ◆ MaxUses: Usuarios máximos
- ◆ Permissions: Permisos de la carpeta
- ◆ Remark: Comentarios del usuario añadidos
- ◆ Type: Tipo de compartición

Value Name	Value Type	Data
 c	 c	 c
Tools	RegMultiSz	CATimeout=0 CSCFlags=32 MaxUses=4294967295 Path=C:\Users\smis\OneDrive\Escritorio\Tools Permissions=0 Remark=Carpeta Compartida ShareName=Tools Type=0

Client Side Caching

Esta opción aparece dentro del CSCFLAGS: Si se comparte la carpeta con el Client Side Caching, si el cliente está desconectado de la red, dispondrá de una copia del fichero en su sistema.





La copia de estos ficheros se guarda tanto en el cliente como en el servidor en la ruta C:\Windows\CSC:

- ◆ CSCFlag=0 -> Opción por defecto, donde el usuario debe indicar que ficheros quiere cachear
- ◆ CSCFlag=16 -> Cacheo de documentos automáticos. "All files and programs that users open from the shared folder are automatically available offline" with the "optimize for performance."
- ◆ CSCFlag=32 Igual que la opción anterior, pero con la opción de "Optimizado para rendimiento"
- ◆ CSCFlag=48 Cache deshabilitada.
- ◆ CSCFlag=2048: Opción por defecto en Win7-Win10 hasta que el usuario deshabilita "Simple File Sharing" o utiliza las opciones avanzadas de compartición. Por defecto también el "Homegroup"

Maxuses: número total de conexiones a una compartición simple. Es un dato para limitar las conexiones. Por defecto 4294967295 para 32 bits.

Path: directorio local.

Permissions: aparentemente, este valor puede ayudar a determinar cómo se compartió una carpeta. 0 es para cuando el valor ha sido creado mediante GUI o Powershell.

- ◆ Para Windows 7-Windows10, el valor es 9 si fue creado con el advanced file sharing y 63 si fue mediante línea de comandos.

Type: tipo de dispositivo o recurso accedido

- ◆ 0 = Disk Drive/ Folder
- ◆ 1 = Impresora
- ◆ 3 = IPC
- ◆ 2147483 = Admin (Disk,Printer, Device o IPC)



AUTOSTART PROGRAMS

¿Qué obtenemos?

- ◆ Determinar que programas se ejecutan automáticamente
- ◆ Útil para localizar malware
- ◆ Determinar la última fecha de cuando se actualizó (generalmente ultimo arranque del sistema)

Ruta:

- ◆ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run
- ◆ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce
- ◆ Software\Microsoft\Windows\CurrentVersion\Runonce
- ◆ Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- ◆ Software\Microsoft\Windows\CurrentVersion\Run

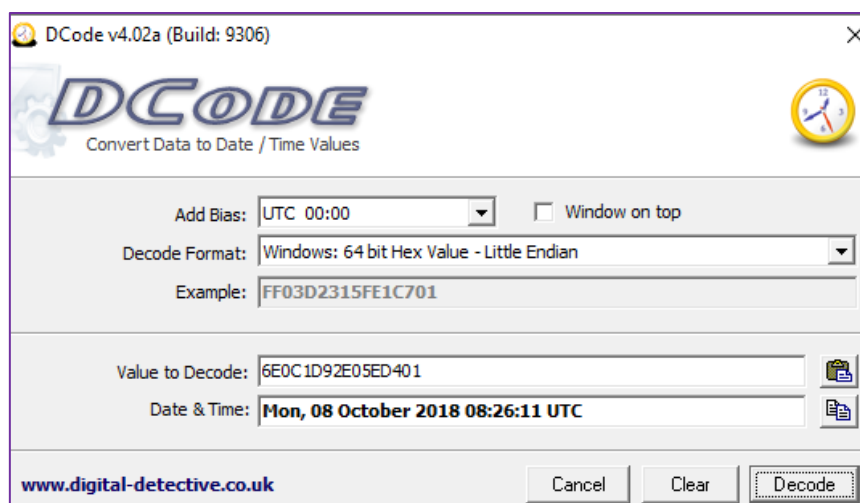
INFORMACIÓN DE APAGADO

Ruta:

- ◆ System\ControlSet001\Control\Windows (Hora de apagado)
- ◆ System\ControlSet001\Control\Watchdog\Display (Shutdown count) – solo XP

Las fechas están en HEX en formato Windows 64 Little Endian

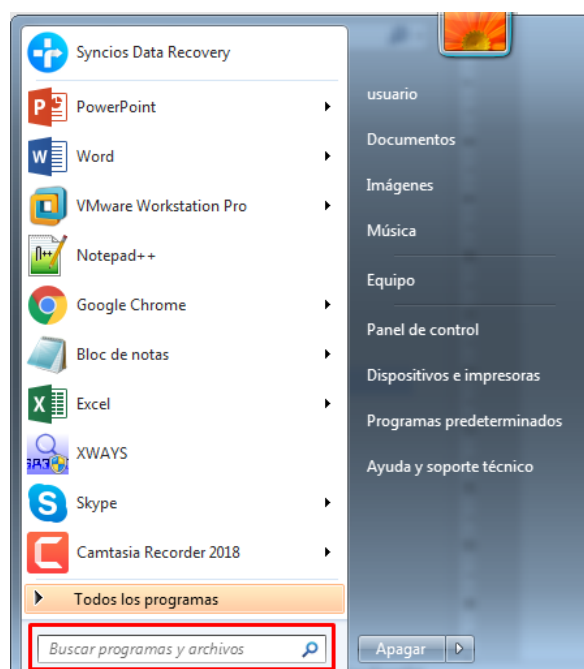
Value Name	Value Type	Data
#	#	#
ComponentizedBuild	RegDword	1
CSDBuildNumber	RegDword	1
CSDReleaseType	RegDword	0
CSDVersion	RegDword	0
Directory	RegExpandSz	%SystemRoot%
ErrorMode	RegDword	0
FullProcessInformationSID	RegBinary	01-06-00-00-00-00-05-50-00-00-00-5E-F3-0F-B1-81-64-AE-04-B1-4C-A2-29-14-B1-4C-21-A6-56-86-56
NoInteractiveServices	RegDword	1
ShellErrorMode	RegDword	1
SystemDirectory	RegExpandSz	%SystemRoot%\system32
ShutdownTime	RegBinary	6E-0C-1D-92-E0-5E-D4-01



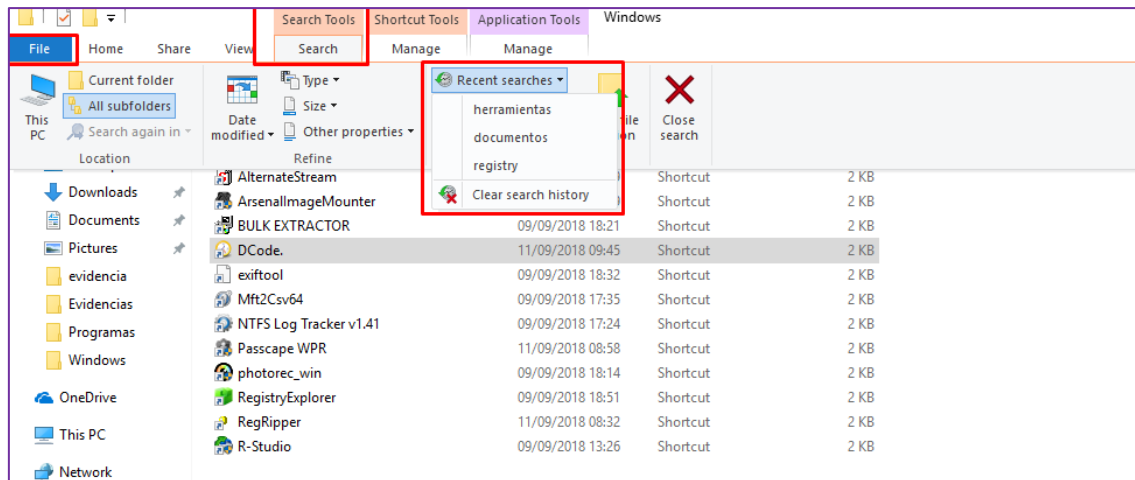
BÚSQUEDA EN WIN7

Ruta: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordwheelQuery

Aunque **Windows vista no tiene** almacenados los valores de búsqueda en el registro, Windows 7/8/10 sí.



BÚSQUEDA EN WIN 8 /10



Ruta: **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery**

- ◆ Como Windows 8/10 pierde el botón de Inicio, las búsquedas quedan limitadas a la barra de búsqueda del Explorer.
- ◆ Las búsquedas son almacenadas en orden temporal.
- ◆ MRU = 0 es la última búsqueda

Search Term	Mru Position	Key Name
RBC	=	RBC
docx	0	WordWheelQuery
doc	1	WordWheelQuery
ppt	2	WordWheelQuery
.pptx	3	WordWheelQuery
.ppt	4	WordWheelQuery

TYPED PATHS WINDOWS 10

Muestra como se ha escrito una ruta en el menú de inicio o en la barra del Explorer. Es útil para demostrar que el usuario, conocía con antelación la ruta exacta.

Ruta: **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths**

Values		
Drag a column header here to group by that column		
Value Name	Value Type	Data
nc	nc	nc
url1	RegSz	search-ms:displayname=Search%20Results%20in%20Quick%20access&crumb=fileextension%3A~<
url2	RegSz	E:\Files



RECENT DOCS

Documentos recientes que han sido abiertos por el usuario desde Windows XP a Win10

Ruta: **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**

Extension	Value Name	Target Name	Lnk Name
RecentDocs	30	User Accounts	User Accounts (2).lnk
RecentDocs	29	::{60632754-C523-4B62-B45C-4172DA012619}	User Accounts.lnk
RecentDocs	23	System and Security	System and Security.lnk
RecentDocs	2	::{BB06C0E4-D293-4F75-8A90-CB05B6477EEE}	System.lnk
RecentDocs	27	The Internet	The Internet (2).lnk
RecentDocs	26	network	ms-settingsnetwork.lnk
RecentDocs	28	network-ethernet	ms-settingsnetwork-ethernet.lnk
RecentDocs	25	history?fsi=1&FORM=WNSHIS	https--www.bing.com-profile-historyfsi=1&FORM=WNSHIS.lnk
RecentDocs	24	Tools	Tools (2).lnk
RecentDocs	21	secret.txt	secret.txt.lnk
RecentDocs	0	::{60632754-C523-4B62-B45C-4172DA012619}	User Accounts.lnk
RecentDocs	22	know-your-file-types.jpg	know-your-file-types.lnk
RecentDocs	10	Files	Files.lnk
RecentDocs	20	presentacion.pptx	presentacion.lnk
RecentDocs	13	didier.de.saint.pierre.es.ppt	didier.de.saint.pierre.es.lnk
RecentDocs	19	microsoft.com&form=B00032&ocid=SettingsHAQ-BingIA&mkt=en-US	https--www.bing.com-searchq=activate%20windows%2010%20sitemicrosoft.com&form=B00032&ocid=SettingsHAQ-BingIA&mkt=en-US.lnk
RecentDocs	18	emailandaccounts	ms-settingsemailandaccounts.lnk
RecentDocs	17	PPT	PPT.lnk
RecentDocs	16	E:\	DATA (E).lnk
RecentDocs	15	New folder	New folder.lnk
RecentDocs	14	Downloads	Downloads.lnk
RecentDocs	9	asasasasas.docx	asasasasas.lnk
RecentDocs	12	Google_searching.pdf	Google_searching.lnk
RecentDocs	11	supported.pdf	supported.lnk
RecentDocs	8	Database11.accdb	Database11.lnk

MRU = 0 sería el más actual

OFFICE RECENT DOCS

Este artefacto forense muestra los documentos ofimáticos recientes, abiertos por el usuario:

Ruta: **NTUSER.DAT\Software\Microsoft\Office\{Version}\{Excel|Word}\FileMRU**

- ◆ 14.0 Office 2010
- ◆ 12.0 Office 2007
- ◆ 11.0 Office 2003
- ◆ 10.0 Office XP

NTUSER.DAT\Software\Microsoft\Office\{Version}\{Excel|Word}\ UserMRU\LiveID_###\FileMRU -> Office 365

- ◆ 15.0 office 2013
- ◆ 16.0 Office 2016

La clave **FileMRU** tendrá una lista de los ficheros más recientes de office ordenados del 1-50.

Value Name	Last Opened	Last Closed	File Name
Item 1	2018-10-03 21:06:42	2018-10-03 20:08:31	C:\Users\jsmis\OneDrive\Documents\asasasasas.docx
Item 2	2018-10-03 20:52:29	2018-10-03 20:08:31	C:\Users\jsmis\OneDrive\Documents\Word Document.docx

Dentro de este artefacto lo interesante es que viene la ruta completa si es comparada con el directorio "Recent Docs" que veremos más adelante.

En la misma localización dentro de los Office 365 aparece una key llamada PlaceMRU, el cual muestra la localización del path previamente abierto en ese directorio.

Los 8 bytes que hay a continuación de la letra T es un timestamp en formato Windows 64 Big Endian.

Value Name	Value Type	Data
Item 1	RegSz	[F00000000 [T01D45B4C387375C2] 000000000]*C:\Users\jsmis\OneDrive\Documents\

OFFICE READING LOCATIONS

Otro artefacto forense que podemos encontrar dentro del registro de Windows, es la posición de lectura sobre el ultimo documento que teníamos abierto.

Este mensaje sale al abrir el documento tal y como se puede apreciar en la siguiente imagen:

Bienvenido de nuevo

Continúa desde donde lo dejaste:

ISO27037: Fase de Preservación
Ayer

La ruta donde Podemos encontrar el último documento es la siguiente:

- **NTUSER.DAT\Software\Microsoft\Office\<version>\Word\Reading Locations\Document X.**

Un ejemplo de cómo se encontraría, tal hallazgo en el registro es el siguiente:

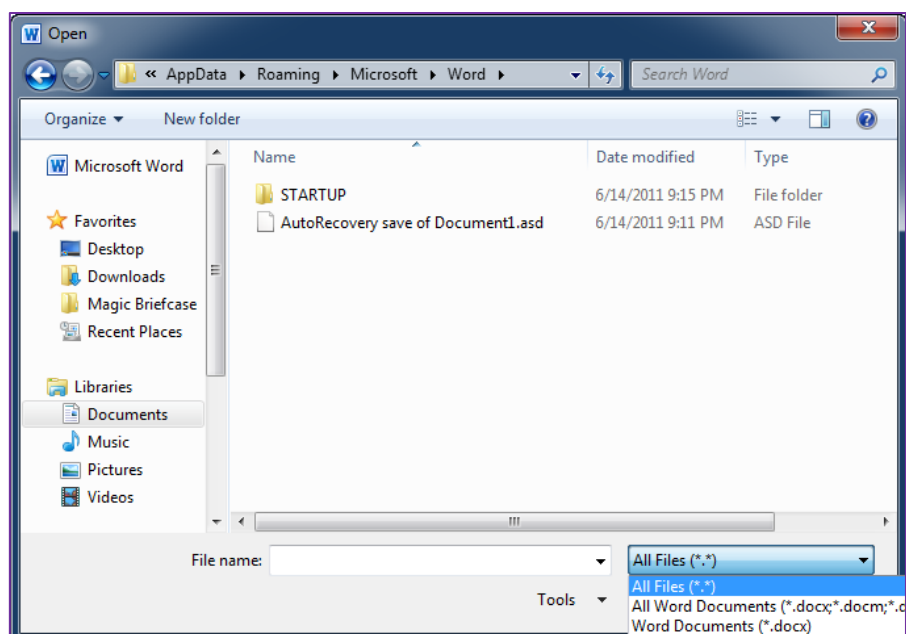
Values		
Drag a column header here to group by that column		
Value Name	Value Type	Data
ABC	ABC	ABC
File Path	RegSz	C:\Users\Donald\Documents\Mini Patisserie Business Plan2.docx
Datetime	RegSz	2013-10-21T15:40
Position	RegSz	273713180 0

AUTOGUARDADO DE FICHEROS OFFICE

Los ficheros de autoguardado están en la carpeta:

Ruta: **C:\Usuarios\<usuario>\AppData\Roaming\Microsoft\{Excel|Word|Powerpoint}**

- ◆ Ficheros con extensión .asd



El fichero se renombraría y ya podría ser abierto.

QUANTIKA¹⁴

LASTVISITED MRU

Windows tiene cajas de diálogo que todos los programas usan. Es decir, las aplicaciones utilizan estas cajas de dialogo para abrir o guardar fichero, insertar un directorio.

- ◆ Tenemos dos tipos:
 - LastVisitedMRU
 - OpenSaveMRU

LastVisitedMRU:

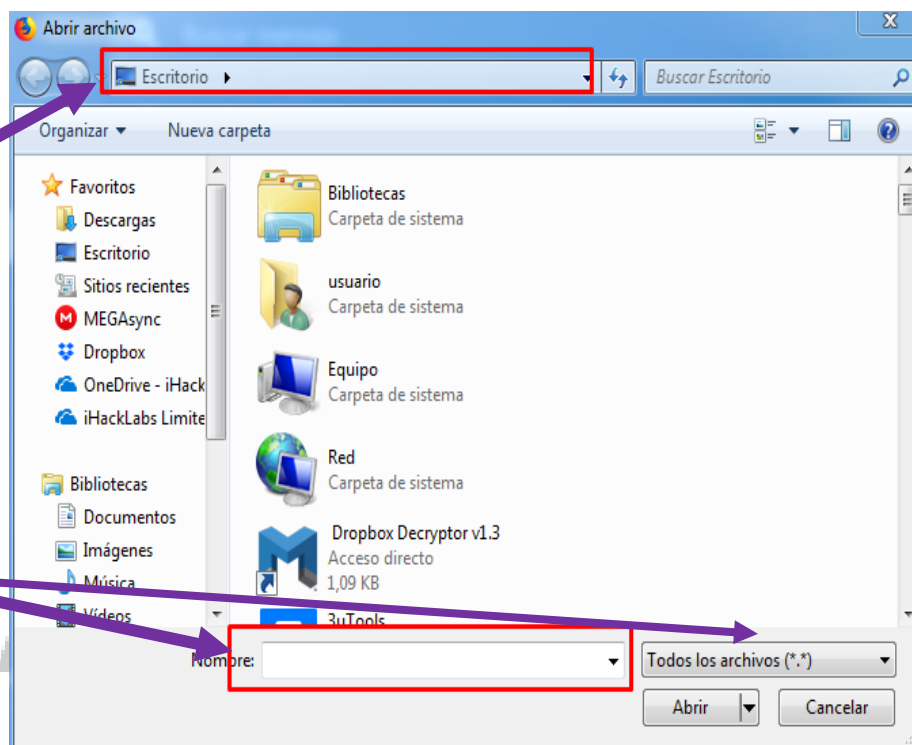
Ultimo directorio del
archivo abierto

Ejecutable usado

OpensaveMRU:

Para guardar o abrir
ficheros

Contiene los últimos
ficheros



LastVisitedMRU, este artefacto **monitoriza que aplicación** abre o guarda el fichero que hemos visto en el OpenSaveMRU. Te indica la ruta donde abrió el fichero y el ejecutable

Ruta:

- ◆ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisited MRU -> WinXP
- ◆ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisited MRU LasVisitedPidIMRU -> (Win7-Win10)



Value Name	Mrp Posi...	Executable	Absolute Path	Opened On
My Computer	=	My Computer	My Computer	=
3	0	chrome.exe	My Computer\Desktop\Files	2018-10-03 20:44:16
5	1	firefox.exe	My Computer\Desktop\Tools	
4	2	{058E840E-CF15-4490-AE30-C895CE27AE13}	My Computer\C:\Users\jsmis\OneDrive\Escritorio\Files	
2	3	{B56D0A9E-4BAA-4A93-88FD-916806851025}	My Computer\Documents	
1	4	{BEAC0269-B1E9-4F0D-B26F-123746CAF4E6}	My Computer\Documents	
0	5	{C8199FDB-BCD3-484D-972D-F8A592F269AC}	My Computer\C:\Users\jsmis\OneDrive\Documents	

OPENSAREMRU

Este artefacto monitoriza los ficheros que han sido abierto o guardados dentro de una ventana de Windows. Esto no solamente ocurre con los navegadores sino con la mayoría de las aplicaciones.

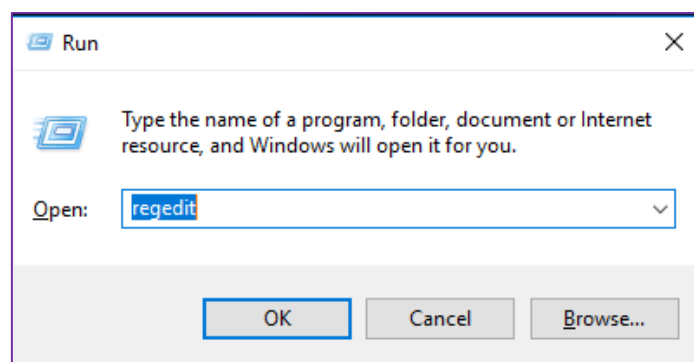
Ruta:

- ◆ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU -> Win XP
- ◆ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU -> (Win7-Win10)

Extension	Value Name	Mrp Position	Absolute Path	Opened On
My Computer	My Computer	=	My Computer	=
*	8	0	My Computer\Desktop\Tools\know-your-file-types.jpg	2018-10-03 20:44:16
accdb	0	0	My Computer\Documents\Database11.accdb	2018-10-03 18:56:47
docx	1	0	My Computer\C:\Users\jsmis\OneDrive\Documents\asasasasas.docx	2018-10-03 19:02:31
exe	0	0	My Computer\Desktop\ccsetup547.exe	2018-10-03 19:04:43
jpg	0	0	My Computer\Desktop\Tools\know-your-file-types.jpg	2018-10-03 20:44:16
pdf	1	0	My Computer\Desktop\Files\Google_searching.pdf	2018-10-03 19:05:45
pptx	0	0	My Computer\C:\Users\jsmis\OneDrive\Escritorio\Files\presentacion.pptx	2018-10-03 20:16:39
xlsx	0	0	My Computer\Documents\Book1.xlsx	2018-10-03 18:55:24
*	7	1	My Computer\C:\Users\jsmis\OneDrive\Escritorio\Files\presentacion.pptx	
docx	0	1	My Computer\Documents\Word Document.docx	
pdf	0	1	My Computer\Desktop\Files\supported.pdf	
*	6	2	My Computer\Desktop\Files\Google_searching.pdf	
*	5	3	My Computer\Desktop\ccsetup547.exe	
*	4	4	My Computer\Desktop\Files\supported.pdf	
*	3	5	My Computer\C:\Users\jsmis\OneDrive\Documents\asasasasas.docx	
*	2	6	My Computer\Documents\Database11.accdb	
*	1	7	My Computer\Documents\Book1.xlsx	
*	0	8	My Computer\Documents\Word Document.docx	

ÚLTIMOS COMANDOS EJECUTADOS

Este artefacto, muestra los últimos comandos ejecutados desde el menú de ejecutar (RunBox):



QUANTIKA¹⁴

Ruta:

- ◆ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- ◆ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Policies\RunMRU

Value Name	Mru Position	Executable	Opened On
ABC	=	ABC	=
b	0	cmd	2018-10-03 18:22:58
a	1	services.msc	

USER ASSISTKEY

Todos los programas con interfaz grafico que son ejecutados desde el escritorio son monitorizados por el launcher de Windows.

Ruta: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count

El GUID es el identificador de la aplicación que se utiliza.

Datos que podemos obtener:

- ◆ Last Run Time (UTC)
- ◆ Run Count: número de veces que se ha ejecutado
- ◆ Nombre de la aplicación GUI
- ◆ Focus Time: tiempo total que la aplicación ha tenido el foco.
- ◆ Focus Count: número total de veces que la aplicación salió y entro del foco.

El valor del nombre también tiene un significado en los User Assist Keys. El nombre de la clave siempre empezara por UEME_ e ira seguido por:

- ◆ RUNPATH: path absoluto del ejecutable. Un usuario normalmente ha clicado a través de la interface de Windows Explorer.
- ◆ RUNCPL: para lanzar el panel de control.
- ◆ RUNPIDL: puntero al fichero actual como un fichero LNK.
- ◆ UIQCUT: cuenta las veces que ha sido lanzado a través del QUICKLaunch
- ◆ UISCUT: Cuenta las veces que ha sido lanzado a través de un acceso directo en el escritorio.
- ◆ UITOOLBAT: mantiene información sobre los clicks de Windows Explorer ToolBar

drag a column header here to group by that column

Value Name	Program Name	Run ...	Focus Co...	Focus Time	Last Executed
HRZR_PGYPHPbhaq:pgbe	UEME_CTLCUACount:ctor	0	0	0d, 0h, 00m, 00s	
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SS08}\Npprffbevrf\Convag.yax	{Programs}\Accessories\Snipping Tool.Ink	9	0	0d, 0h, 00m, 00s	2018-10-03 17:30:25
HRZR_PGYPFFVBA	UEME_CTLSESSION	66	0	0d, 0h, 00m, 00s	
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SS08}\Npprffbevrf\Convag.yax	{Programs}\Accessories\Paint.Ink	7	0	0d, 0h, 00m, 00s	2018-10-03 17:30:25
{N77S5Q77-2R2O-44P3-N6N2-NON601054N51}\Npprffbevrf\Abgrcnq.yax	{Programs}\Accessories\Notepad.Ink	6	0	0d, 0h, 00m, 00s	2018-10-03 17:30:25
{9R399SNO-1S9P-4S13-O827-48O24O6P7174}\GnfxOne\Svyr Rkcybere.yax	{User Pinned}\TaskBar\File Explorer.Ink	18	0	0d, 0h, 00m, 00s	2018-10-08 07:33:03
P:\Hfref\Choyvp\Qrfxgbc\Tbtyr Puebzy.yax	C:\Users\Public\Desktop\Google Chrome.Ink	7	0	0d, 0h, 00m, 00s	2018-10-03 19:02:43
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SS08}\Onpxhc naq Flap sebz Tbtyr\Onpxhc naq Flap sebz Tbtyr.yax	{Programs}\Backup and Sync from Google\Backup and Sync from Google.Ink	1	0	0d, 0h, 00m, 00s	2018-10-03 18:14:30
P:\Hfref\Choyvp\Qrfxgbc\Tbtyr Qbpf.yax	C:\Users\Public\Desktop\Google Docs.Ink	2	0	0d, 0h, 00m, 00s	2018-10-03 20:15:43
P:\Hfref\Choyvp\Qrfxgbc\Sversbk.yax	C:\Users\Public\Desktop\Firefox.Ink	5	0	0d, 0h, 00m, 00s	2018-10-03 20:52:14
{N77S5Q77-2R2O-44P3-N6N2-NON601054N51}\Fifgrz Gbbyf\Pbznaq Cebzcg.yax	{Programs}\System Tools\Command Prompt.Ink	2	0	0d, 0h, 00m, 00s	2018-10-03 20:54:46
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SS08}\Qebcobk\Qebcobk.yax	{Programs}\Dropbox\Dropbox.Ink	1	0	0d, 0h, 00m, 00s	2018-10-03 18:23:14
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SS08}\Bhgybbx 2016.yax	{Programs}\Outlook 2016.Ink	2	0	0d, 0h, 00m, 00s	2018-10-03 19:01:19
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SS08}\Ubeq 2016.yax	{Programs}\Word 2016.Ink	2	0	0d, 0h, 00m, 00s	2018-10-03 19:02:13
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SS08}\Rkpzy 2016.yax	{Programs}\Excel 2016.Ink	1	0	0d, 0h, 00m, 00s	2018-10-03 18:54:40
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SS08}\Npprff 2016.yax	{Programs}\Access 2016.Ink	1	0	0d, 0h, 00m, 00s	2018-10-03 18:56:08
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SS08}\Npebong Emraq QP.yax	{Programs}\Acrobat Reader DC.Ink	2	0	0d, 0h, 00m, 00s	2018-10-03 20:11:00

Registry Explorer interpreta directamente los valores en la columna Program Name.

En el caso de no conocer la ruta en el registro, podemos ayudarnos del siguiente enlace:

<https://www.dfir.training/resources/downloads/windows-registry>

Description	XP	Vista	Win7	Win8	Win10	key
\$MFT Zone Definition	XP		7	8	10	SYSTEM\ControlSet###\Control\FileSystem\NtfsMftZoneReservation
64 BitShim Cache			7			HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatCache\AppCompatCache
AccessData FTK Time Zone Cache						NTUSER.DAT\Software\AccessData\Products\Forensi Toolkit\Settings\TimeZoneCache
AccessData Registry Viewer Recent File List						NTUSER.DAT\Software\Accessdata\Registry Viewer\Recent File List
Acro Software CutePDF						NTUSER.DAT\Software\Acro Software Inc\CPW
Adobe						NTUSER.DAT\Software\Adobe\
Adobe Acrobat						NTUSER.DAT\Software\Adobe\Acrobat Reader\AVGer\cRecentFiles\c#
Adobe Photoshop Last Folder						NTUSER.DAT\Software\Adobe\Photoshop\VisitedDir
Adobe Photoshop MRUs						NTUSER.DAT\Software\Adobe\MediaBrowser\MRU\Photoshop\FileList

Como vemos en la imagen anterior, nos indica si aplica a los distintos sistemas operativos, así como la ruta de donde se debe buscar

FEATUREUSAGE

Este artefacto, solo aplica para Windows 10 y hace un seguimiento de los eventos asociados con la Barra de Tareas, por ejemplo, cuando un usuario ejecuta una aplicación fijada en ella. Los artefactos de FeatureUsage se encuentran en el archivo de registro NTUSER.DAT bajo la siguiente ruta:

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage

Podemos encontrar unas pocas subclaves de abajo de FeatureUsage:

FeatureUsage	1	5	2019-09-28 08:25:51
AppBadgeUpdated	10	0	2020-04-23 06:25:11
AppLaunch	8	0	2020-04-23 09:56:43
AppSwitched	221	0	2020-04-23 10:07:21
ShowJumpView	29	0	2020-04-22 09:23:22
TrayButtonClicked	4	0	2020-04-23 07:06:04

AppBadgeUpdated: esta subclave lleva un registro de las actualizaciones de las etiquetas de las aplicaciones de la barra de tareas. Por ejemplo, si usas Telegram y recibes un mensaje nuevo, puedes ver un icono rojo en la insignia de la aplicación con el número de mensajes nuevos. Así que aquí podemos encontrar la ruta de la aplicación y el número de actualizaciones de la insignia:

Type viewer	Binary viewer
Value name	C:\Users\0136\AppData\Roaming\Telegram Desktop\Telegram.exe
Value type	RegDword
Value	4097

AppLaunch: esta subclave registra los lanzamientos de aplicaciones, que se fijan en la barra de tareas. Por supuesto, no todos los usuarios pinchan aplicaciones, pero si lo hacen, tendrás una buena cantidad de pruebas digitales:

Type viewer	Binary viewer
Value name	MSEdge
Value type	RegDword
Value	3

AppSwitched. Esta subclave registra los clics izquierdos en las aplicaciones de la barra de tareas cuando un usuario quiere cambiar de una a otra. Esta subclave es muy interesante desde una perspectiva forense ya que puede contener un gran número de registros, que pueden ser la fuente de pruebas de ejecución:

Type viewer	Binary viewer
Value name	D:\mimikatz_trunk\x64\mimikatz.exe
Value type	RegDword
Value	3

ShowJumpView. Esta subclave rastrea los clics del botón derecho del ratón en las aplicaciones de la barra de tareas. Un usuario puede hacerlo, por ejemplo, para comprobar o abrir archivos recientes. Esto puede ser un artefacto adicional que apunta a las aplicaciones usadas más frecuentemente:

Type viewer	Binary viewer
Value name	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Office 16\WINWORD.EXE
Value type	RegDword
Value	6

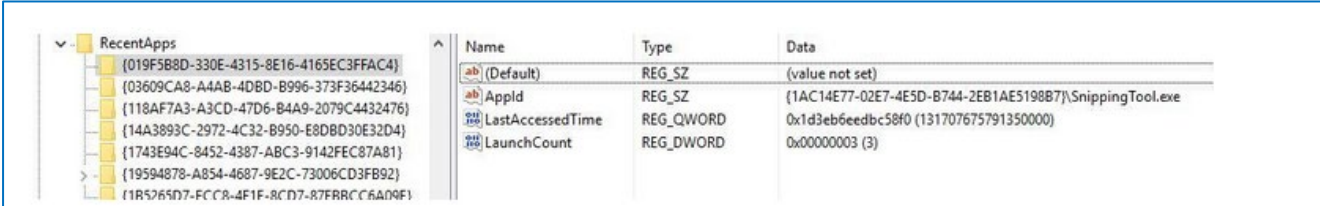
TrayButtonClick. Esta subclave rastrea los clics izquierdos en los siguientes elementos de la barra de tareas: Botón del reloj, botón de inicio, botón del Centro de Notificación y cuadro de búsqueda. Como en los ejemplos anteriores, puedes ver el número de clics en cada elemento:

Value Name	Value Type	Data
RB C	RB C	RB C
StartButton	RegDword	179
SearchBox	RegDword	590
ClockButton	RegDword	32
NotificationCenterButton	RegDword	60

WINDOWS RECENTAPPS

Windows RecentApps, es un nuevo artefacto forense de Windows 10 que nos puede indicar la ejecución de aplicaciones, las RecentApps. En este caso se encuentra dentro del registro del usuario NTUSER.DAT

Ruta: **Software\Microsoft\Windows\Current Version\Search\RecentApps**



Name	Type	Data
(Default)	REG_SZ	(value not set)
AppId	REG_SZ	{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe
LastAccessedTime	REG_QWORD	0x1d3eb6eedbc58f0 (131707675791350000)
LaunchCount	REG_DWORD	0x00000003 (3)

- ◆ AppID: nombre de la aplicación
- ◆ LastAccessTime= última ejecución en UTC en formato epoc
- ◆ LaunchCount= Número de veces que ha sido ejecutado

SHELL ITEMS

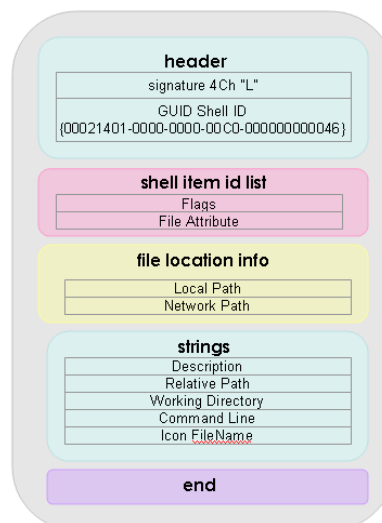
¿Qué es un shell item? Información o fichero que tiene información para acceder a otro fichero

Atributos:

- ◆ Tipo del target donde está el fichero: fijo, extraíble, red
- ◆ Path del fichero target: unidad, etiqueta del volumen
- ◆ Metadatos: MAC timestamps, tamaño, registro MFT, Número de secuencia

Tipos:

- ◆ Accesos directos (LNK)
- ◆ Jumplists
- ◆ Shellbags



Header de LNK

Al tener una firma específica se podría realizar carving para recuperar los que se hayan borrado.

RECENT DOCUMENTS (LNK)

Windows crea este shortcut cuando un usuario abre o utiliza un fichero.

Ruta:

- ◆ Win7-Win10: C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent
- ◆ Office: C:\Users\<user>\AppData\Roaming\Microsoft\Office\Recent
- ◆ Máximo 149 ficheros y directorios

Tipos

- ◆ 1- Fichero Target
- ◆ 2- Directorio padre del fichero target

Información:

- ◆ MAC Times del target File
- ◆ Información del volumen donde está el target file
- ◆ Directorio del target file

Los archivos podrían haber sido borrados o eliminados, almacenados en un recurso compartido de red o USB, por lo que, aunque el archivo podría ya no estar allí, seguirá existiendo los archivos LNK asociados con el archivo original. Las fechas del sistema de archivos indicaran:

- ◆ **Fecha de creación-> la primera vez que se abrió**
- ◆ **Fecha de modificación -> La última vez que se abrió.**

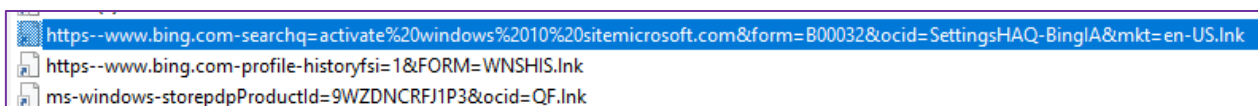
AppData > Roaming > Microsoft > Windows > Recent Items		
Name	Date created	Date modified
actual	11/09/2018 10:43	11/09/2018 11:23
Binarios	09/09/2018 13:28	09/09/2018 13:27
borrado	11/09/2018 09:20	11/09/2018 09:22
DESKTOP-CAOKCFK.wpr	11/09/2018 09:05	11/09/2018 09:05
evidencia	09/09/2018 18:54	11/09/2018 11:21
Evidencias	09/09/2018 13:50	11/09/2018 09:21
U.D. 1 - 55	11/09/2018 09:43	11/09/2018 09:43

QUANTIKA¹⁴

Nuevo funcionamiento de Recent Documents en Windows 10

- ◆ Cuando un fichero es creado, también se crea su LNK en el RECENT (anteriormente solo cuando se abría). Se mantiene las fechas del sistema de archivo.
- ◆ Cuando una carpeta es creada en un directorio, la carpeta, la carpeta padre y la carpeta abuelo son creados como LNK en el RECENT.
- ◆ El mayor cambio es que ahora en los ficheros LNK se incluye la extensión y antes no.

Nuevos tipos de LNK con URLs en Windows 8/10



¿Como se generó este tipo de LNK?

1. Run Dialog
2. Windows Search Charm
3. A través de un fichero LNK
4. A través de un link de una aplicación

Herramientas para analizar ficheros LNK: **LINKPARSER**

FileModifiedDate	FileAccessDate	FileCreationDate	FileLink.FileName	FileLink.FilePath
10/3/2018 6:54 PM	10/16/2018 7:28 PM	10/3/2018 6:54 PM	All.lnk	C:\Users\student\Des...
10/3/2018 7:06 PM	10/16/2018 7:28 PM	10/3/2018 7:02 PM	asasasasasas.lnk	C:\Users\student\Des...
10/3/2018 6:55 PM	10/16/2018 7:28 PM	10/3/2018 6:55 PM	Book 1.lnk	C:\Users\student\Des...
10/3/2018 8:07 PM	10/16/2018 7:28 PM	10/3/2018 8:07 PM	DATA (E).lnk	C:\Users\student\Des...
10/3/2018 6:56 PM	10/16/2018 7:28 PM	10/3/2018 6:56 PM	Database 1.lnk	C:\Users\student\Des...
10/3/2018 6:56 PM	10/16/2018 7:28 PM	10/3/2018 6:56 PM	Database 11.lnk	C:\Users\student\Des...
10/3/2018 6:54 PM	10/16/2018 7:28 PM	10/3/2018 6:54 PM	david_berard.lnk	C:\Users\student\Des...
10/3/2018 8:15 PM	10/16/2018 7:28 PM	10/3/2018 8:07 PM	didier.de.saint.pierre.es.lnk	C:\Users\student\Des...
10/3/2018 8:07 PM	10/16/2018 7:28 PM	10/3/2018 8:07 PM	Downloads.lnk	C:\Users\student\Des...
10/3/2018 8:16 PM	10/16/2018 7:28 PM	10/3/2018 7:03 PM	Files.lnk	C:\Users\student\Des...
10/3/2018 7:05 PM	10/16/2018 7:28 PM	10/3/2018 7:05 PM	Google_searching.lnk	C:\Users\student\Des...
10/3/2018 9:02 PM	10/16/2018 7:28 PM	10/3/2018 9:02 PM	https--www.bing.com-profile-historyfsi=1&FOR...	C:\Users\student\Des...
10/3/2018 8:13 PM	10/16/2018 7:28 PM	10/3/2018 8:13 PM	https--www.bing.com-searchq=activate%20wi...	C:\Users\student\Des...
10/3/2018 8:44 PM	10/16/2018 7:28 PM	10/3/2018 8:44 PM	know-your-file-types.lnk	C:\Users\student\Des...
10/3/2018 8:13 PM	10/16/2018 7:28 PM	10/3/2018 8:13 PM	ms-settingsemailandaccounts.lnk	C:\Users\student\Des...
10/3/2018 9:23 PM	10/16/2018 7:28 PM	10/3/2018 9:23 PM	ms-settingsnetwork-ethernet.lnk	C:\Users\student\Des...
10/3/2018 9:23 PM	10/16/2018 7:28 PM	10/3/2018 9:20 PM	ms-settingsnetwork.lnk	C:\Users\student\Des...
10/3/2018 5:35 PM	10/16/2018 7:28 PM	10/3/2018 5:35 PM	ms-windows-storepdpProductId=9WZDNCRF...	C:\Users\student\Des...



Campos:

- ◆ Link: son las fechas del destino UTC, es decir, las fechas del sistema de archivos del fichero en si
- ◆ File: son las fechas propias del LNK del UTC
- ◆ El hash MD5 es el del propio LNK, nunca del fichero en sí.
- ◆ MAC Address del equipo donde está el fichero original.
- ◆ Volume Label: Etiqueta del volumen
- ◆ DriveType: tipo de medio -> muy útil para dispositivos USB

**Ver Video:004/MÓD. 3 - LinkParser*

LeCMD: otra herramienta para analizar LNK

```
Command Prompt
LECmd version 1.1.0.1
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

Command line: -d C:\Users\student\Desktop\LNKS --csv C:\Users\student\Desktop\Output -q

Warning: Administrator privileges not found!

Looking for lnk files in 'C:\Users\student\Desktop\LNKS'

Found 32 files

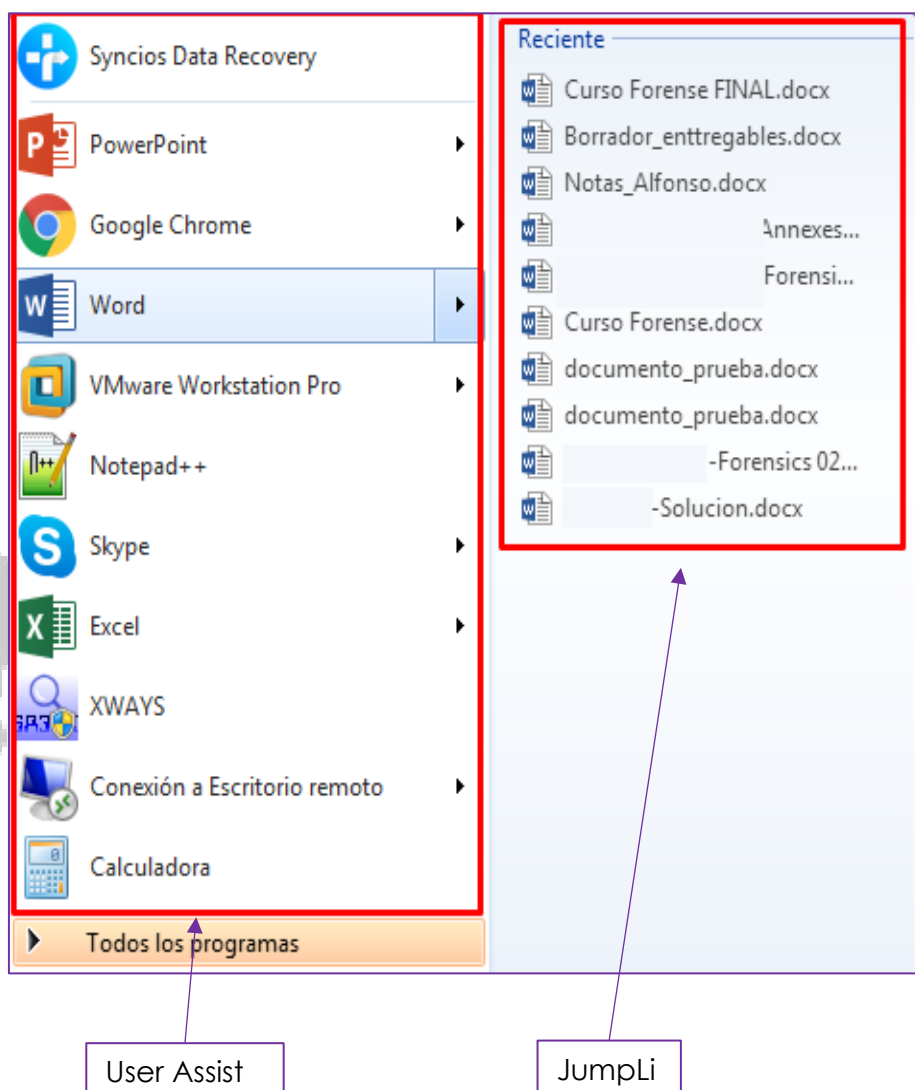
----- Processed 'C:\Users\student\Desktop\LNKS\All.lnk' in 0.06985830 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\asasasasas.lnk' in 0.00482400 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\Book1.lnk' in 0.00148330 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\DATA (E).lnk' in 0.00072540 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\Database1.lnk' in 0.00041600 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\Database11.lnk' in 0.00095840 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\david_berard.lnk' in 0.00987870 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\didier.de.saint.pierre.es.lnk' in 0.00075740 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\Downloads.lnk' in 0.00106140 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\Files.lnk' in 0.00050900 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\Google_searching.lnk' in 0.00126230 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\https--www.bing.com-profile-historyfsi=1&FORM=WNSHIS.lnk' in 0.0014
390 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\https--www.bing.com-searchq=activate%20windows%2010%20itemicrosoft
com&form=B00032&ocid=SettingsHAQ-BingIA&mkt=en-US.lnk' in 0.00031530 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\know-your-file-types.lnk' in 0.00080490 seconds -----
----- Processed 'C:\Users\student\Desktop\LNKS\ms-settingsemailandaccounts.lnk' in 0.00065840 seconds -----
```

**Ver Video: 005/MÓD. 3 - LECMD*

JUMPLISTS

Los usuarios pueden “saltar” a los archivos recientemente abiertos. Para las investigaciones forenses proporciona otra ubicación donde verificar la creación de ficheros no ejecutables.

Esto debe coincidir con el registro de RecentDocs, Recent Docs *ext, Office Recent Docs y los ficheros LNK en el Recent Folder.



Hay dos tipos de Jumplists:

- ◆ **automáticos** que son creados por cada aplicación de Windows
- ◆ **custom** que son creados con el desarrollo específico de la aplicación.

Los dos se pueden encontrar en el Recent Folder.

Dentro cada fichero JUMPLIST puede haber fechas propias: creación de la entrada, modificación de la entrada y último acceso a la entrada. En la imagen superior, para el fichero documento_prueba.docx podría tener estas fechas.

Automatic destinations está en el siguiente directorio:

- ◆ **C:\Users\<profile>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations.**

Contiene una lista de aplicaciones ordenadas por AppID. Los nombres están en el formato XXXXXXXX.autmaticDestinations-ms

- ◆ **Creation Time:** Primera fecha de ejecución (a nivel el sistema de archivos)
- ◆ **Modificación time:** última fecha de ejecución de la aplicación (a nivel el sistema de archivos)

Name	Date created	Date modified
5d696d521de238c3.automaticDestinations-ms	10/3/2018 9:04 PM	10/3/2018 9:05 PM
5f7b5f1e01b83767.automaticDestinations-ms	10/3/2018 7:32 PM	10/3/2018 10:57 PM
7e4dca80246863e3.automaticDestinations-ms	10/3/2018 7:35 PM	10/8/2018 9:33 AM
9a165f62edbf161.automaticDestinations-ms	10/3/2018 7:35 PM	10/3/2018 7:35 PM
9b9cdc69c1c24e2b.automaticDestinations-ms	10/3/2018 10:44 PM	10/3/2018 10:44 PM
9d1f905ce5044aee.automaticDestinations-ms	10/3/2018 7:32 PM	10/3/2018 11:02 PM
4293e440ad719476.automaticDestinations-ms	10/3/2018 8:52 PM	10/3/2018 9:06 PM
6824f4a902c78fbd.automaticDestinations-ms	10/3/2018 7:45 PM	10/3/2018 7:45 PM
7821f5bf3954ed50.automaticDestinations-ms	10/3/2018 10:08 PM	10/3/2018 10:16 PM
beb8bc0ef1324736.automaticDestinations-ms	10/3/2018 8:55 PM	10/3/2018 8:55 PM
c343543d4ee31de7.automaticDestinations-ms	10/3/2018 8:56 PM	10/3/2018 8:56 PM
de48a32edcbe79e4.automaticDestinations-ms	10/3/2018 8:54 PM	10/3/2018 8:54 PM
f01b4d95cf55d32a.automaticDestinations-ms	10/3/2018 7:32 PM	10/3/2018 10:57 PM
f18460fded109990.automaticDestinations-ms	10/3/2018 10:13 PM	10/3/2018 11:23 PM

La información almacenada en el directorio de Automatic Destinations tiene que tener un único archivo con el AppID.

Custom Destinations está en el siguiente directorio:

- ◆ **C:\Users\<profile>\AppData\Roaming\Microsoft\Windows\Recent\CustomDestination**

Son creados por cada aplicación y por lo tanto "custom"

Un Jumplist customizado está destinado a presentar el contenido que la aplicación ha establecido como importante basado en el uso previo o a través de una acción que ha sido indicada por el usuario como importante, tal como añadir el ítem a favoritos o anclar la aplicación a la barra de inicio. También tienen una APPID.

- ◆ **Creation Time** (a nivel el sistema de archivos): primera vez de ejecución.
- ◆ **Modificación time:** última vez que la aplicación fue añadida al fichero en concreto (a nivel el sistema de archivos)

Name	Date created	Date modified
5d696d521de238c3.customDestinations-...	10/3/2018 8:03 PM	10/3/2018 8:03 PM
7e4dca80246863e3.customDestinations-ms	10/3/2018 7:32 PM	10/3/2018 7:32 PM
9d1f905ce5044aee.customDestinations-ms	10/3/2018 7:32 PM	10/3/2018 10:25 PM
590aee7bdd69b59b.customDestinations-...	10/8/2018 10:21 AM	10/8/2018 10:21 AM
6824f4a902c78fbd.customDestinations-ms	10/3/2018 7:47 PM	10/3/2018 11:00 PM
9149d0f5ebf7f710.customDestinations-ms	10/3/2018 8:33 PM	10/3/2018 8:33 PM
ccc0fa1b9f86f7b3.customDestinations-ms	10/3/2018 9:05 PM	10/3/2018 11:19 PM
f01b4d95cf55d32a.customDestinations-ms	10/3/2018 7:32 PM	10/3/2018 7:32 PM
f18460fded109990.customDestinations-ms	10/3/2018 7:35 PM	10/8/2018 9:33 AM

Los Jumplist evidencian que una aplicación específica existió y se ejecutó.

Cada Jumplist, sea automático o custom, tiene su AppID. Este tipo de identificador está asociado a un programa en concreto como vemos en la imagen siguiente:

Application IDs			
AppID	Application Description	Date Added	Source
65009083bfa6a094	(app launched via XPMode)	8/22/2011	Win4n6 List Serv ↗
469e4a7982cea4d4	? (.job)	8/22/2011	Win4n6 List Serv ↗
b0459de4674aab56	(.vmcx)	8/22/2011	Win4n6 List Serv ↗
89b0d939f117f75c	Adobe Acrobat 9 Pro Extended (32-bit)	8/22/2011	Microsoft Windows 7 Forum ↗
26717493b25aa6e1	Adobe Dreamweaver CS5 (32-bit)	8/22/2011	Microsoft Windows 7 Forum ↗
e2a593822e01aed3	Adobe Flash CS5 (32-bit)	8/22/2011	Microsoft Windows 7 Forum ↗
c765823d986857ba	Adobe Illustrator CS5 (32-bit)	8/22/2011	Microsoft Windows 7 Forum ↗
84f066768a22cc4f	Adobe Photoshop CS5 (64-bit)	8/22/2011	Microsoft Windows 7 Forum ↗
44a398496acc926d	Adobe Premiere Pro CS5 (64-bit)	8/22/2011	Microsoft Windows 7 Forum ↗
23646679aaccfae0	Adobe Reader 9.	8/22/2011	Microsoft Windows 7 Forum ↗
23646679aaccfae0	Adobe Reader 9 x64	8/22/2011	Win4n6 List Serv ↗
45e994e9d5f739	Adobe Reader 9.5 (64-bit)	6/22/2011	Microsoft Windows 7 Forum ↗

Listado de Jumlist: <https://gist.github.com/atilaromero/2146441>



Herramienta para analizar Jumplist: **JumpList Explorer**

JumpList Explorer v0.7.0.1

File Tools Help

Drag a column header here to group by that column

Source File Name	Jump List Type	App ID	App ID Description	Lnk File Count	File Size
C:\Users\student\Desktop\pruebajum\A...	Automatic	5d696d521de238c3	Google Chrome 9.0.597.84 /...	2	4,608
C:\Users\student\Desktop\pruebajum\A...	Automatic	5f7b5f1e01b83767	HAMBONE	11	16,896
C:\Users\student\Desktop\pruebajum\A...	Automatic	7e4dca80246863e3	Control Panel (?)	2	3,584
C:\Users\student\Desktop\pruebajum\A...	Automatic	9a165f62eddfa161	Unknown AppId	1	3,072
C:\Users\student\Desktop\pruebajum\A...	Automatic	9b9cdc69c1c24e2b	Notepad 64-bit	1	3,584
C:\Users\student\Desktop\pruebajum\A...	Automatic	9d1f905ce5044aee	Edge Browser	4	9,216
C:\Users\student\Desktop\pruebajum\A...	Automatic	4293e440ad719476	Unknown AppId	2	4,608
C:\Users\student\Desktop\pruebajum\A...	Automatic	6824f4e902c78fbd	Unknown AppId	0	2,560
C:\Users\student\Desktop\pruebajum\A...	Automatic	7821f5bf3954ed50	Unknown AppId	3	6,656
C:\Users\student\Desktop\pruebajum\A...	Automatic	beb8bc0ef1324736	Unknown AppId	1	3,072
C:\Users\student\Desktop\pruebajum\A...	Automatic	c343543d4ee31de7	Unknown AppId	2	4,608
C:\Users\student\Desktop\pruebajum\A...	Automatic	de48a32edcbe79e4	Adobe Acrobat Reader DC 2...	1	4,096
C:\Users\student\Desktop\pruebajum\A...	Automatic	f01b4d95cf55d32a	Windows Explorer Windows ...	19	23,040
C:\Users\student\Desktop\pruebajum\A...	Automatic	f18460fde109990	Unknown AppId	3	4,096

**Ver Video: 006/MÓD. 3 - JumplistExplorer*

SHELLBAGS

Los sistemas Windows almacenan las opciones de visualización de Windows Explorer mediante entradas de registro y son conocidas como ShellBags.

- ◆ Esto nos permite saber que directorio han sido accedidos a nivel local, de red o dispositivos extraíbles.
- ◆ Evidencia la existencia de directorios previos.

Localización de las Shellbags:

Explorer Access:

- ◆ **USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags**
- ◆ **USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU**



Desktop Access:

- ◆ **NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU**
- ◆ **NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags**

Los documentos de Microsoft tienen Shellbags adicionales y están presentes en los sistemas Win7-Win10

La existencia de dicha entrada en el registro prueba que usuario especificó visitó al menos una vez ese directorio.

Para analizar los shellbags, vamos a utilizar Shelbag Explorer:

Drag a column header here to group by that column										
Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Miscellaneous	
PPT		Directory	0	20:07:30 03-10-2018	20:07:30 03-10-2018	20:07:30 03-10-2018	20:07:58 03-10-2018	20:07:58 03-10-2018		NTFS file system
Summary Details Hex										
Registry last write time: 2018-10-03 20:07:25.822										

Respecto a los timestamps:

- En azul corresponde con los MAC times del sistema de archivos de la carpeta PPT
- En rojo es la información propia de shellbag, donde indica la última interacción con la carpeta PPT y cuál fue la primera.
- También indica el sistema de archivos sobre el que estaba la carpeta.

**Ver Video:007/MÓD. 3 - ShellbagExplorer*

Hasta ahora hemos dicho:

- ◆ Evidenciar que se ha ejecutado mediante el análisis del UserAssist
- ◆ Evidenciar que se ha “tocado” realizando un timeline del sistema de archivos o del registro.
- ◆ Evidenciar que directorios has abierto mediante el análisis de Shellbags.



DISPOSITIVOS USB

Los dispositivos de almacenamiento USB son muchas veces objeto de investigación, debido a que son utilizados para copiar ficheros/carpetas. ¿Qué información podemos obtener siempre de un dispositivo USB?

- ◆ Vendor/Make/Version
- ◆ Número de serie único

¿Qué información podemos obtener relacionada con un dispositivo de almacenamiento USB?

- ◆ Determinar la unidad asignada y el nombre del volumen
- ◆ Encontrar el usuario que utilizó ese dispositivo USB
- ◆ Descubrir la primera vez que el dispositivo USB fue conectado
- ◆ Determinar la última vez que el dispositivo USB fue conectado
- ◆ Determinar cuando el dispositivo fue quitado del sistema

¿Cuáles son los artefactos forenses que podemos utilizar para identificar la copia de un fichero a un dispositivo de almacenamiento USB?

1. Windows Registry Hives:

- ◆ System
- ◆ Software
- ◆ Ntuser.dat

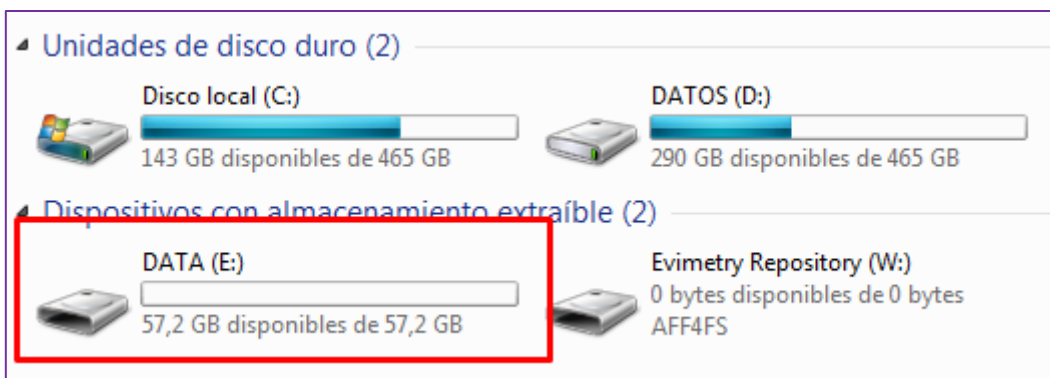
2. Setupapi.dev.log

3. Shell Items

- ◆ Jumplists
- ◆ LNK Files
- ◆ ShellBags

MASS STORAGE DEVICE

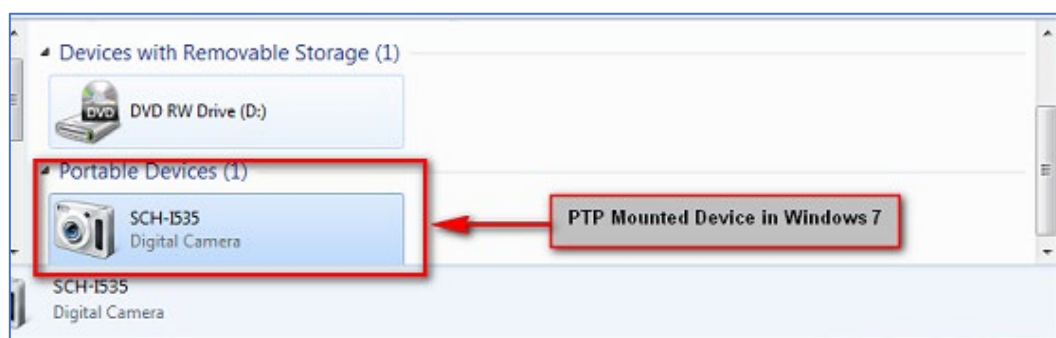
También conocidos como dispositivos de almacenamiento (USB Mass Storage). En Windows son montados automáticamente siempre que el sistema de archivos sea compatible con Windows.



PICTURE TRANSFER PROTOCOL

Desarrollado por el International Imaging Industry Association. Un dispositivo PTP en Windows:

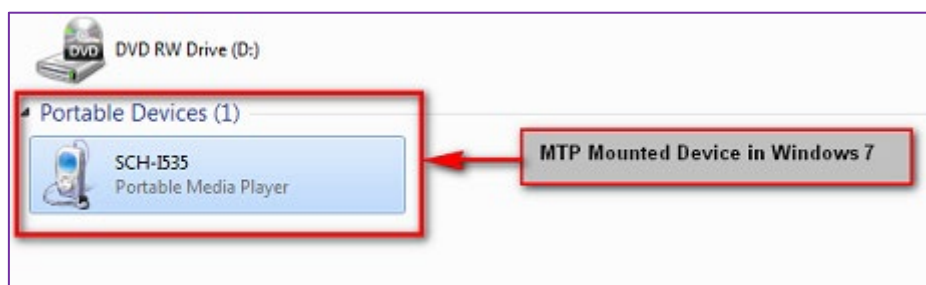
- ◆ No tiene acceso al sistema de archivos
- ◆ Solo tiene acceso a imágenes y archivos de video
- ◆ Dispone Exploración limitada y lógica del contenido



MEDIA TRANSFER PROTOCOL

¿Qué características tiene el MTP?

- ◆ Mejora y extensión del PTP.
- ◆ No tiene acceso al sistema de archivos.
- ◆ Acceso a la tarjeta interna y SD.
- ◆ Dentro de Windows es montado como un dispositivo portable



IDENTIFICAR EVIDENCIAS DE USO DISPOSITIVOS USB

MSC USB

Creación de ficheros LNK para todos los ficheros que hayan sido abiertos

- ◆ Windows Recent Folder
- ◆ Microsoft Office Recent Folder
- ◆ Jumplist: Automatic Destinations

MTP USB

Windows puede o no puede crear ficheros LNK. Depende de la aplicación y del tipo de archivo.

Algunos MTP LNK no apuntan a la fuente MTP pero apunta al WPDNSE folder:

C:\users\<username>\Appdata\Local\Temp\WPDNSE\{GUID}

Computer\SCH-I535\Phone\Phone_Test Folder 2\Phone_Folder2-TestDOC.doc
LNK to File Created
C:\Users\Win7SP1\AppData\Roaming\Microsoft\Office\Recent\Phone_Folder2-TestDOC.doc.LNK
Target File Path
{CLSID_MyComputer}\C:\Users\Win7SP1\AppData\Local\Temp\WPDNSE\{021B0157-01D4-0193-8701-A70164014D01}\Phone_Folder2-TestDOC.doc
LNK to Folder Created
C:\Users\Win7SP1\AppData\Roaming\Microsoft\Office\Recent\{021B0157-01D4-0193-8701-A70164014D01}.LNK
Target Folder Path
{CLSID_MyComputer}\C:\Users\Win7SP1\AppData\Local\Temp\WPDNSE\{021B0157-01D4-0193-8701-A70164014D01}

Los ficheros DOC No apuntan a la fuente original sino a un directorio temporal. Solo ocurre con los documentos office.

- ◆ Los ficheros JPG si dejan un LNK verdadero a la fuente original.
- ◆ Los Ficheros PDF, TXT y XLS no producen ningún fichero LNK.

¿Qué contiene el directorio temporal WPDNSE?

- ◆ Mantiene una copia del fichero
- ◆ El directorio es temporal y no sobrevive a un reinicio
- ◆ El GUID se saca de una Shellbag

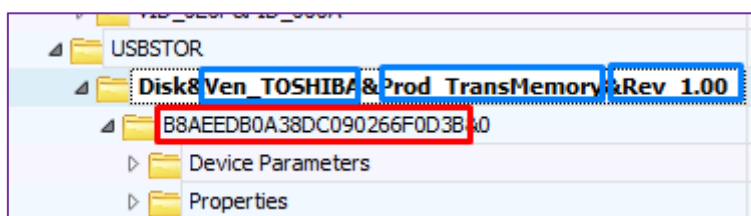
USBSTOR

El registro USBstor, se encarga de monitorizar cualquier dispositivo USB que haya sido conectado a la máquina:

Ruta: **SYSTEM\ControlSet001\Enum\USBSTOR**

¿Por qué es útil?

- ◆ Se puede identificar al fabricante, el producto y la versión de un dispositivo MSC que está conectado a la máquina.
- ◆ Identificar un único dispositivo USB que ha sido conectado a la máquina.
- ◆ Determinar el tiempo por el cual el dispositivo estuvo conectado a la máquina
- ◆ Identificar el número de serie físico del dispositivo USB.

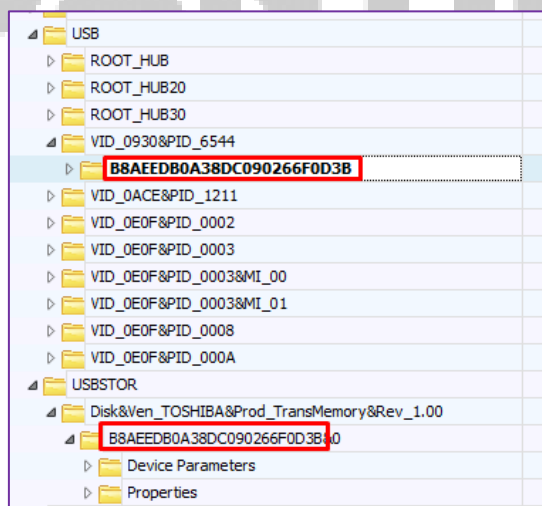


En rojo el número de serie del dispositivo. En azul el Device Class ID.

IDENTIFICACIÓN DE VID/PID

Para localizar estos valores debemos de recurrir a **SYSTEM\ControlSet001\Enum\USB:**

- ◆ VID: Vendor ID
- ◆ PID: Product ID



VID:0930 y PID:6544

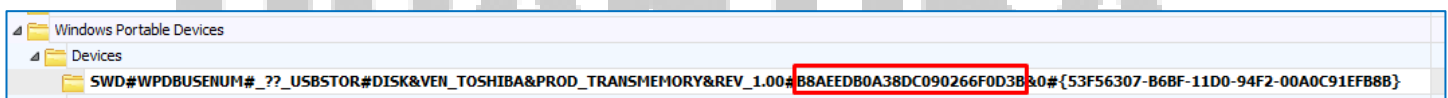
DeviceDesc	RegSz	@usbstor.inf,%genericbulkonly.deviceDesc%;USB Mass Storage Device
LocationInformation	RegSz	Port_#0001.Hub_#0005
Capabilities	RegDword	148
Address	RegDword	1
ContainerID	RegSz	{37c7bd8b-2c93-5380-b51f-68b1b99121a2}
HardwareID	RegMultiSz	USB\VID_0930&PID_6544&REV_0100 USB\VID_0930&PID_6544
CompatibleIDs	RegMultiSz	USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08
ClassGUID	RegSz	{36fc9e60-c465-11cf-8056-444553540000}
Service	RegSz	USBSTOR
Driver	RegSz	{36fc9e60-c465-11cf-8056-444553540000}\0009
Mfg	RegSz	@usbstor.inf,%generic.mfg%;Compatible USB storage device
ConfigFlags	RegDword	0

OBTENER EL NOMBRE DEL VOLUMEN

Ruta: **SOFTWARE\Microsoft\Windows Portable Devices\Devices**

Aplica para MSC, MTP y PTP

- ◆ Se relaciona el dispositivo USB Físico, que dispone de un número de serie con un nombre de Volumen.
- ◆ El nombre del volumen puede ser mapeado a una unidad mediante los ficheros LNK



Drag a column header here to group by that column		
Value Name	Value Type	Data
Value Name	Value Type	Data
FriendlyName	RegSz	DATA

Para las capturas de imagen anteriores, el nombre del volumen es DATA.

OBTENER LA ÚLTIMA UNIDAD ASIGNADA

Solo MSC que sean **discos de almacenamiento externos** aplica la siguiente casuística para la ruta del registro: **System\MountedDevices**

Los dispositivos particionados con MBR dejan una firma de 4 bytes, en el registro, la clave **MountedDevices**. Para el particionado en GPT deja el GUID del tipo de partición. **89**

La firma del MBR se encuentra el primer sector en el offset 0X1B8 o 440 del disco



D:	D:	D:	D:
\??\Volume{38139932-cb02-11e8-8c57-34238779763e}	RegBinary	5F-00-3F-00-3F-00-5F-00-55-00-53-00-...	00-00-00-00-00-00
\??\Volume{78520c8e-cd6d-11e8-8c5b-34238779763e}	RegBinary	5F-00-3F-00-3F-00-5F-00-55-00-53-00-...	00-00-00-00
\??\Volume{a02d288c-cc75-11e8-8c59-34238779763e}	RegBinary	5F-00-3F-00-3F-00-5F-00-53-00-43-00-...	
\??\Volume{a02d288d-cc75-11e8-8c59-34238779763e}	RegBinary	7B-00-33-00-38-00-31-00-33-00-39-00-...	00-00-00-00-00-00
\??\Volume{e0f95a2f-cae1-11e8-8c50-806e6f6e6963}	RegBinary	5C-00-3F-00-3F-00-5C-00-53-00-43-00-...	00-00-00-00
\DosDevices\C:	RegBinary	AC-09-B3-3F-00-00-60-22-00-00-00-00	
\DosDevices\D:	RegBinary	5C-00-3F-00-3F-00-5C-00-53-00-43-00-...	00-00-00-00
\DosDevices\E:	RegBinary	DE-90-F2-1C-00-00-10-00-00-00-00-00	42-00-53-00-54-00-4F-00-52-00-23-00-44-...
\DosDevices\F:	RegBinary	D1-5A-1B-C6-00-40-00-00-00-00-00-00	53-00-49-00-23-00-44-00-69-00-73-00-68-...
\DosDevices\G:	RegBinary	23-84-AC-B8-00-00-60-22-00-00-00-00	61-00-31-00-63-00-2D-00-63-00-62-00-30-...

QUANTIKA¹⁴

QUANTIKA¹⁴

tem\MountedDevices:

Volume{2e1ce865-c747-11e8-add4-34238779763e}	Re...	5F-00-3F-00-3F-00-5F-00-55-00-53...	00-00-00-00
DeviceID{...}	Re...	5F-00-3F-00-3F-00-5F-00-55-00-53...	00-00-00-00

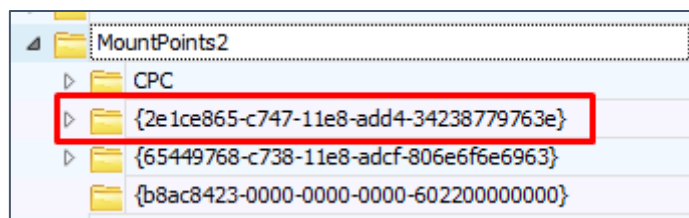
LOCALIZAR EL USUARIO QUE HA UTILIZADO EL USB

1. El primer paso es localizar el GUID del Volumen en **SYSTEM\mountedDevices**. Localizando el número de serie dentro del mismo.

`\??\Volume{2e1ce865-c747-11e8-add4-34238779763e}`

2. Y luego este GUID asociarlo al NTUSER.DAT del usuario:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Mountpoints2



Ha sido encontrado dentro del NTUSER.DAT del usuario ismis.

VOLUMEN SERIAL NUMBER

El volumen serial number, es el número de serie del volumen lógico del sistema de archivos:

- ◆ No confundir con el número de serie físico del dispositivo.
- ◆ Solo dispositivos MSC

Ruta: **Software\Microsoft\Windows NT\CurrentVersion\EMDMgmt**

```
Command Prompt
Microsoft Windows [Version 10.0.17763.55]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\student>vol
Volume in drive C has no label.
Volume Serial Number is C0A1-3738

C:\Users\student>
```

¿Por qué es útil?

Sabiendo el nombre del volumen y el serial number del volumen puedes correlacionar la información con los ficheros LNK y la clave de registro RecentDocs

Este artefacto dependerá de si el servicio ReadyBoost este habilitado o no.

¿Qué información hay en EMDMgmt Key?

- ◆ Fabricante

- ◆ ID
- ◆ Serial number
- ◆ Volume Name del sistema de archivos, muy útil para relacionar con los LNK.

¿Qué pasaría si el dispositivo USB es reformateado? Un formateo solo escribe los datos necesarios para tener de nuevo un sistema de archivos “limpio”. No realiza ningún borrado.

- ◆ **Tendríamos un nombre de volumen nuevo**
- ◆ **Tendríamos un nuevo volumen serial number**
- ◆ **Pero se mantiene el serial number físico del dispositivo.**

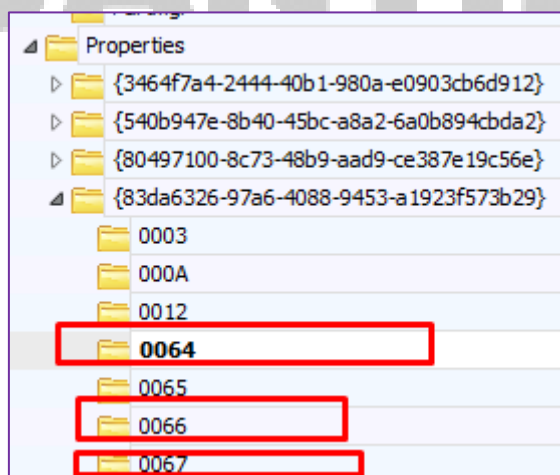
TIMESTAMPS

Primera y última vez que se conectó al dispositivo

Ruta:

System\ControlSet001\Enum\USBSTOR\{VEN_PROD_VERSION}\{USB serial}\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\

- ◆ Win7 y Win8 -> **Primera conexión** -> 0064
- ◆ Win8 en adelante -> **Ultima conexión** -> 0066
- ◆ Win8 en adelante -> **Fecha de desconexión con independencia de si es quitado con seguridad o sin ella.** -> 0067



Timestamps 64 bits Hex Windows Time Little Endian pero Registry Explorer los interpreta:

- ◆ 0064: 10/3/2018 8:06:48 PM +00:00
- ◆ 0066: 10/3/2018 8:24:46 PM +00:00
- ◆ 0067: 10/3/2015 9:17:12 PM +00:00

También podemos analizar el fichero **SetupApi.dev.log** para obtener timestamps de cuando se produjo la conexión USB:

Ruta:

- ◆ XP -> C:\Windows\setupapi.log
- ◆ Win7-Win10 -> C:\Windows\inf\setupapi.dev.log

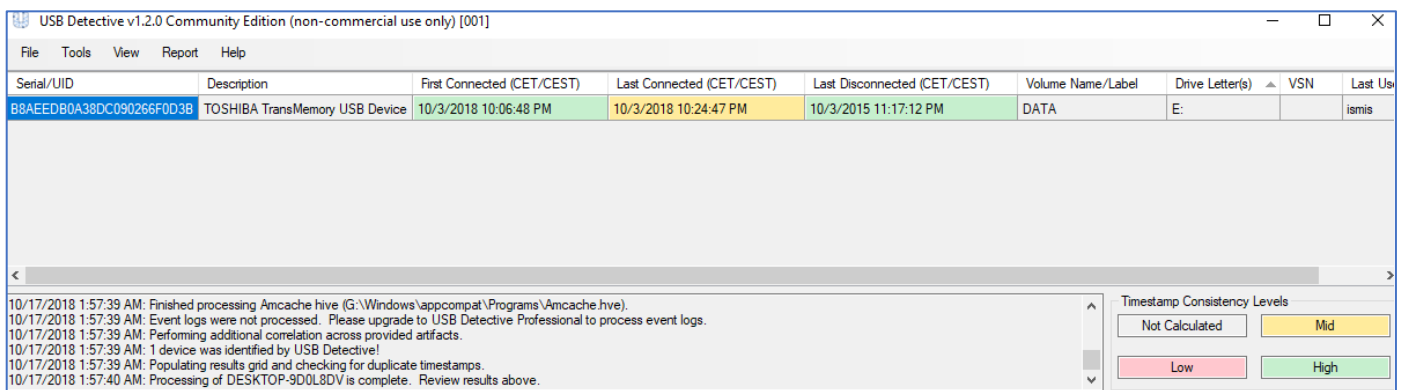
Los timestamps están local time.

```
[Device Install (Hardware initiated) - SWD\WPDBUSENUM\??_USBSTOR#DisksVen_TOSHIBA&Prod_TransMemory&Rev_1.00#B8AEEDB0A38DC090266F0D3B&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
Section_start 2018/10/03 22:06:48.881
dvi: {Build Driver List} 22:06:48.881
dvi: Searching for compatible ID(s):
dvi: wpdbusenum\fs
dvi: swd\generic
dvi: Created Driver Node:
dvi: HardwareID - wpdbusenum\fs
dvi: InfName - C:\Windows\System32\DriverStore\FileRepository\wpdfs.inf_amd64_10bfelc48f153b03\wpdfs.inf
dvi: DevDesc - WPD FileSystem Volume Driver
dvi: Section - Basic Install
```

También podemos utilizar los eventos del sistema para localizar los timestamps, a partir de Windows 7 / 8 / 10. Lo veremos en el próximo modulo

Herramientas para realizar todos estos pasos de manera automática:

USB Detective



**Ver Video:008/MÓD. 3 - USB Detective*



Los datos concuerdan con lo que hemos analizado anteriormente. Incluso el VSN o volumen serial number no ha sido capaz de encontrarlo como nosotros.

QUANTIKA¹⁴