

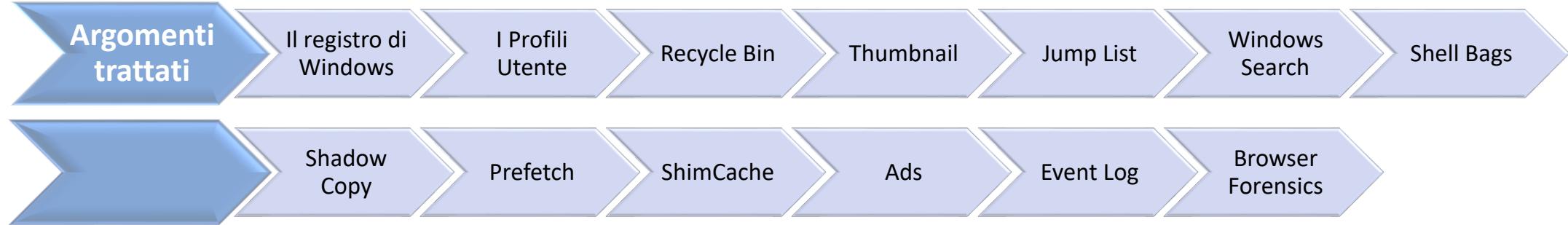


*Fondazione ITS Roberto Rossellini – Esperto in Cybersecurity*



## **Master Cyber Security Windows Forensics**

*A.C.C. Francesco Bernardi – francesco.bernardi@poliziadistato.it*



# I file di Registro

Quali sono i file di registro più importanti dove ricavare informazioni nell'analisi forense?

I registri di configurazione del sistema operativo si trovano nel seguente percorso :  
%SystemRoot%\System32\Config\:

Sam – HKEY\_LOCAL\_MACHINE\SAM

Security – HKEY\_LOCAL\_MACHINE\SECURITY

Software – HKEY\_LOCAL\_MACHINE\SOFTWARE

System – HKEY\_LOCAL\_MACHINE\SYSTEM

Default – HKEY\_USERS\.DEFAULT

Userdiff – Non associato a nessuna Hive, utilizzato solo nell'upgrade del sistema operativo.

# I file di Registro

Nella directory %SystemRoot%\System32\Config\RegBack sono presenti le copie delle seguenti chiavi di registro create ogni 10 giorni dal programma RegIdleBackup.

- Sam
- Security
- Software
- System
- Default

Il backup è attivo solo su Windows Vista, Win7, Win8, Win10 fino alla versione 1709, Server 2008, e Server 2016.

Da Win10 1803 compreso Win11 il Sistema non esegue il backup in automatico ma deve essere abilitato dall'utente, tramite il registro.

In questi registri possiamo trovare delle chiavi eventualmente non più disponibili nel sistema.

Il backup non viene effettuato sulle chiavi del profilo utente. (Ntuser.dat e Usrclass.dat)

# I file di Registro

**I file di registro del profilo utente li troviamo nel percorso:**

**Ntuser.dat (Win7)**

C:\Users\ <username>\

**Usrclass.dat (Win7-10-11)**

C:\Users\ <username>\ AppData\ Local\ Microsoft\ Windows\USRCLASS.DAT

Questa file è molto importante perché contiene alcune informazioni per quanto riguarda l'esecuzione dei programmi ed è disponibile per ogni utente.

Negli altri sistemi Windows Xp/2000 il registro Ntuser.dat si trova nel percorso:

%UserProfile% = C:\Documents and Settings\<utente>\

# I file di Registro

Alcuni dei dati più interessanti per le attività di analisi provengono dai registri utenti.

Da *Ntuser.dat* e *Usrclass.dat* è possibile estrarre informazioni quali:

- Keyword ricercate nel PC (WordWheelQuery)
- Path digitate dall'utente (TypedPaths)
- Documenti aperti recentemente (tracciati sia dal S.O. che da Office) (RecentDocs, FileMRU, PlaceMRU, LNK files, cartella Recent)
- Documenti aperti/salvati recentemente e path recenti (tramite dialog box)(LastVisitedMRU, OpenSaveMRU, OpenSavePidlMRU)
- Documenti recenti o più frequenti (JumpList: cartelle Recent\AutomaticDestinations e Recent\CustomDestinations)
- Comandi eseguiti (tramite Start/Run) (RunMRU)
- Programmi eseguiti (incluso il numero di esecuzioni e il tempo per cui ciascun programma è stato attivo) (UserAssist)
- Cartelle aperte (in alcuni casi con il loro contenuto) (ShellBags)

# I file di Registro

- HKEY\_USERS contiene tutti i profili utenti caricati nel sistema
- HKEY\_CURRENT\_USER profilo dell'utente correntemente collegato al sistema
- HKEY\_LOCAL\_MACHINE contiene una vasta gamma di configurazioni e Informazioni per il sistema tra cui le impostazioni hardware e software
- HKEY\_CURRENT\_CONFIG contiene le informazioni di profilo hardware utilizzato durante l'avvio
- HKEY\_CLASSES\_ROOT contiene informazioni di configurazione relative alle applicazioni usate per aprire i vari file sul sistema

# I file di Registro

Quando un utente effettua il login, queste sono le chiavi di registro che vengono utilizzate per eseguire applicazioni in automatico:

- **HKEY\_LOCAL\_MACHINE\ Software\Microsoft\Windows\CurrentVersion\Runonce**
- **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run**
- **HKEY\_LOCAL\_MACHINE \ Software\Microsoft\Windows\CurrentVersion\Run**
- **HKEY\_CURRENT\_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows\Run**
- **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run**
- **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce**

Importante: se il sistema parte in “safe mode”, queste chiavi vengono ignorate.

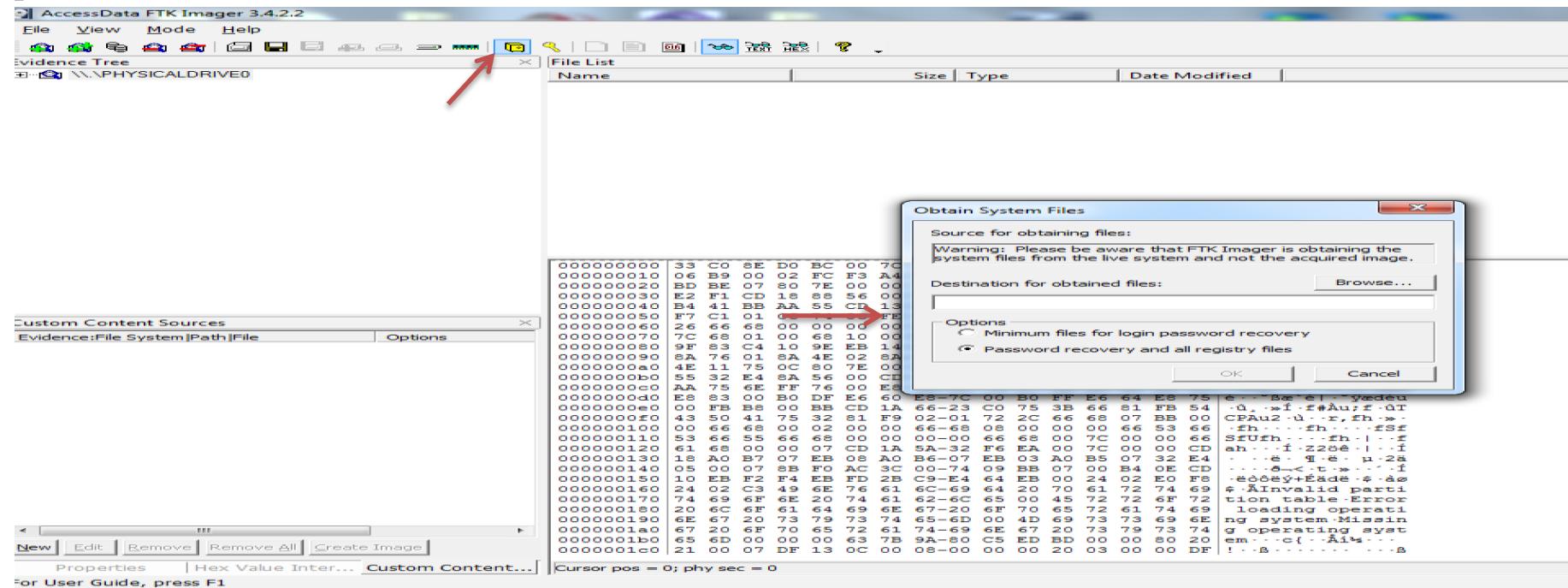
# I file di Registro

Queste due voci di registro vengono lette quando un utente esegue qualsiasi programma e possono essere sfruttate da eventuali malware o ransomware per immettere codice da eseguire:

- **HKEY\_LOCAL\_MACHINE\Software\Classes\Exefile\Shell\Open\command**
- **HKEY\_CLASSES\_ROOT\Exefile\Shell\Open\Command**

# I file di Registro

Con Ftk Imager in un'analisi live è possibile esportare tutti i registri di Windows, compresi quelli di ogni singolo utente cliccando sul tasto “Obtain System Files” e nella finestra spuntare



“Password recovery and all registry files”.

L'unico file che non viene salvato è Usrclass.dat che deve essere esportato a “mano”

# I file di Registro

Per il parsing del registro di Windows è possibile utilizzare

- RegRipper scaricabile gratuitamente da <https://github.com/keydet89/RegRipper3.0>
- Cafae della TzWorks, tools a pagamento scaricabile da [https://tzworks.com/prototype\\_page.php?proto\\_id=19](https://tzworks.com/prototype_page.php?proto_id=19)
- Kape scaricabile previa registrazione da <https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape>  
La documentazione ufficiale la troviamo qui <https://github.com/EricZimmerman/KapeFiles>

# I file di Registro SAM

## HKEY\_LOCAL\_MACHINE\SAM e HKEY\_LOCAL\_MACHINE\Security

Nelle macchine non connesse ad un dominio, questi file contengono le informazioni relative alla gestione degli accessi.

Normalmente, anche con privilegi di amministratore, non è possibile visualizzare il contenuto di queste chiavi. L'accesso è consentito solo all'utente system.

Il primo posto in cui cercheremo informazioni è il SAM. Il file SAM ci aiuterà a enumerare tutti gli utenti che hanno un profilo sulla macchina. Se la macchina è parte di un dominio, il file SAM contenente l'utente e i profili saranno collocati nel Domain Controller.

Nel Sam troviamo:

- Associazione di un nome utente a un SID (Security Identifier): Ci sono molti artefatti su una macchina Windows che fanno riferimento al SID dell'utente e non al nome utente.
- Possiamo vedere la data di ultimo login e quante volte si è loggato alla macchina.

## IMPORTANTE

Tutti i tempi memorizzati nel Registro di sistema saranno in **UTC**, quindi dovranno essere necessarie conversioni di fuso orario.

# I file di Registro SAM

Parsing con RegRipper del file di registro SAM

*samparse v.20160203*

*(SAM) Parse SAM file for user & group mbrshp info*

*User Information*

*Username : xxx [1000]*



**Nome Utente**

*Full Name :*

*User Comment :*

*Account Type : Default Admin User*

*Account Created : Thu Dec 15 09:07:11 2016 Z*



**Data creazione Account**

*Name :*

*Password Hint : Ricordami*



**Hint della password impostata dall'utente**

*Last Login Date : Wed Jun 28 12:30:19 2017 Z*

*Pwd Reset Date : Thu Dec 15 09:07:11 2016 Z*

*Pwd Fail Date : Thu May 11 06:14:52 2017 Z*

*Login Count : 132*

*--> Password does not expire*

*--> Password not required*

*--> Normal user account*

**Ultimo Login e quanto volte è stato effettuato l'accesso. Se l'utente accede tramite account Microsoft Live ID il campo "Count" non viene incrementato.**

# I file di Registro SAM

## *Group Membership Information*

---

*Group Name : Guests [1]*

*LastWrite : Thu Dec 15 09:06:48 2016 Z*

*Group Comment : Gli utenti del gruppo Guests dispongono dello stesso tipo di accesso di cui dispongono i membri del gruppo Users, ad eccezione dell'account Guest che contiene ulteriori restrizioni*

*Users :*

**S-1-5-21-3415635297-2310919608-2875765266-501** ← **Sid Guest**

*Group Name : Administrators [2]*

*LastWrite : Thu Dec 15 09:07:11 2016 Z*

*Group Comment : Gli amministratori hanno privilegi di accesso completo e senza limitazioni al computer/dominio*

*Users :*

**S-1-5-21-3415635297-2310919608-2875765266-500** ← **Sid**

**Amministratore**

**S-1-5-21-3415635297-2310919608-2875765266-1000** ← **Sid Utente**

# I file di Registro SOFTWARE

Nella chiave di registro:

- SOFTWARE \ Microsoft\ Windows NT\ CurrentVersion possiamo individuare la versione di Microsoft Windows installata, il relativo service pack ( se installato) la data di installazione, ultima scrittura sul disco e il nome a cui è registrato il Sistema Operativo.

La data di installazione è una di quelle poche date che non segue lo standard di Windows ma è in Epoch Time e segue lo standard 12:00am 1/1/1970.

 **InstallDate**      REG\_DWORD      0x58525d41 (1481792833)

Basta convertire il valore 1481792833 con un convertire online per esempio <https://www.epochconverter.com/> e avremmo la data di installazione del S.O. , nel nostro caso

GMT: Thursday, 15 December 2016 09:07:13

Your time zone: giovedì, 15 dicembre 2016 10:07:13 GMT+01:00

# I file di Registro SOFTWARE

Parsing con RegRipper del file di registro SOFTWARE

*WinNT\_CV*

*Microsoft\Windows NT\CurrentVersion*

*LastWrite Time Wed Jun 14 10:07:21 2017 (UTC)*

← **Ultima scrittura su disco**

*RegisteredOrganization :*

*RegisteredOwner : xxx*

← **Nome a cui è registrato il S.O.**

*EditionID : Ultimate*

*SystemRoot : C:\Windows*

*PathName : C:\Windows*

*CSDVersion : Service Pack 1*

*ProductName : Windows 7 Ultimate*

*CurrentType : Multiprocessor Free*

*ProductId : 00426-OEM-8992662-00015*

*BuildLab : 7601.win7sp1\_ldr.170512-0600*

*ProductName = Windows 7 Ultimate*

← **Sistema Operativo**

**Installato**

*CSDVersion = Service Pack 1*

*InstallDate = Thu Dec 15 09:07:13 2016*

← **Data Installazione S.O.**

# I file di Registro SYSTEM

Nel file di registro SYSTEM possiamo trovare tantissime informazioni utili per l'analisi forense:

- ControlSet “*HKEY\_LOCAL\_MACHINE\SYSTEM\Select*”
- Computer Name “*SYSTEM\CurrentControlSet\Control\ComputerName \ComputerName*”
- TimeZone “*SYSTEM\CurrentControlSet\Control\TimeZoninformation*”
- Last Access Time “*SYSTEM\CurrentControlSet\Control\FileSystem*”
- Network Interface “*SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces*”
- Shutdown “*SYSTEM\CurrentControlSet\Control\Windows*”
- Usb Device “*SYSTEM\CurrentControlSet\Enum\USBSTOR*”

# I file di Registro SYSTEM

- Che cos'è un ControlSet?

Il ControlSet contiene le impostazioni di configurazione del sistema necessarie per controllare l'avvio del sistema ed informazioni sui driver e i servizi.

- Perché ci sono due ControlSet (ControlSet001 e ControlSet002)?

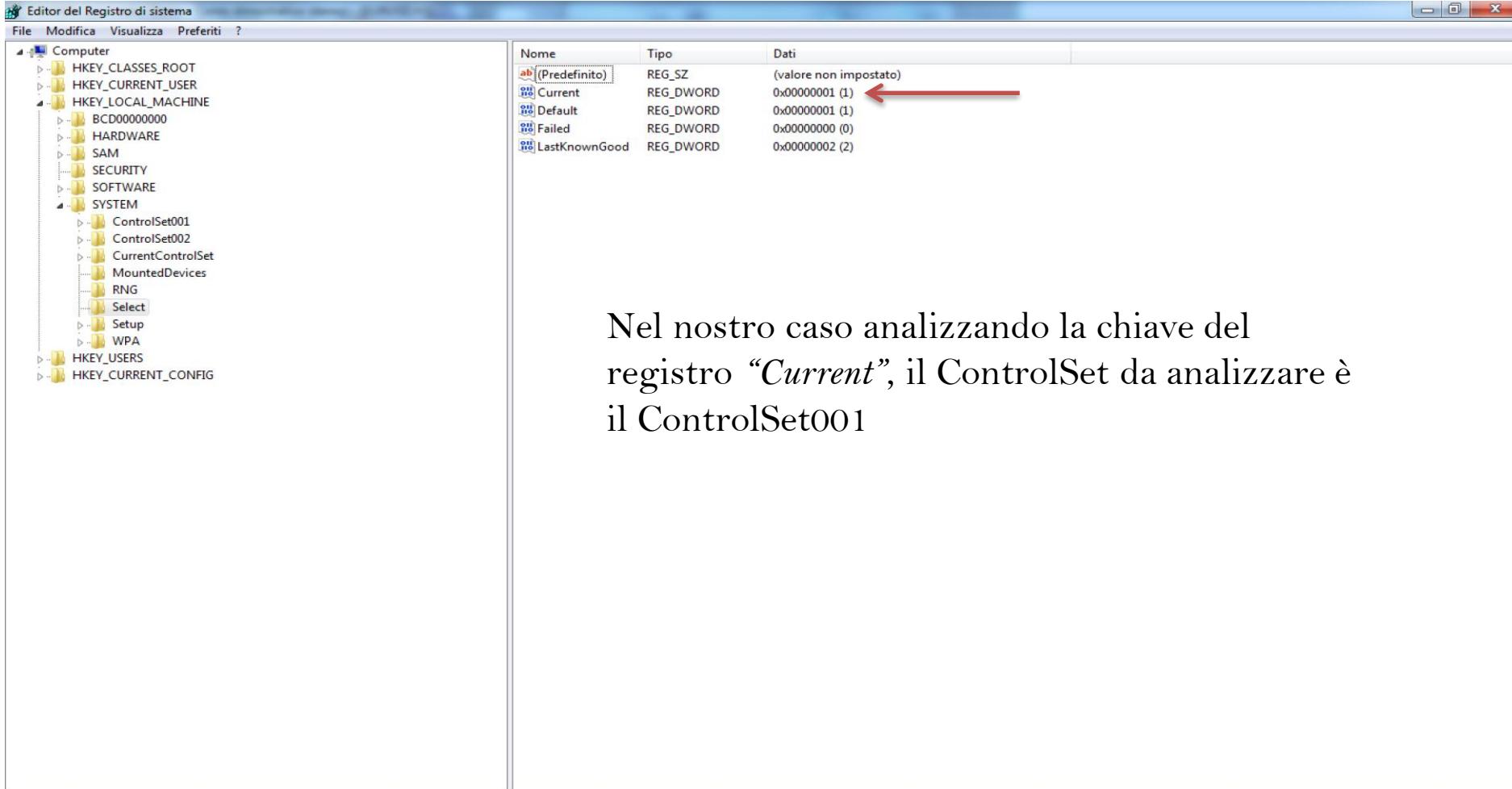
ControlSet001 è tipicamente il ControlSet che ha avviato il computer è di solito contiene la versione più aggiornata del ControlSet.

ControlSet002 è la versione "Last Known Good". E' uno snapshot del registro di sistema effettuato durante l'ultimo boot ed è considerato l'ultimo affidabile e privo di errori.

Possiamo vedere il giusto ControlSet dalla voce di registro

HKEY\_LOCAL\_MACHINE\SYSTEM\Select

# I file di Registro SYSTEM



The screenshot shows the Windows Registry Editor window. The left pane displays a tree view of registry keys under 'Computer'. The 'Select' key under 'SYSTEM' is selected. The right pane shows a table of values for this key:

Nome	Tipo	Dati
(Predefinito)	REG_SZ	(valore non impostato)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000002 (2)

A red arrow points to the 'Current' value entry.

Nel nostro caso analizzando la chiave del registro “*Current*”, il ControlSet da analizzare è il ControlSet001

Computer\HKEY\_LOCAL\_MACHINE\SYSTEM>Select

14:50 30/06/2017



# I file di Registro SYSTEM

*Parsing con RegRipper del file di registro SYSTEM (Computer Name)*

---

*compname v.20090727*

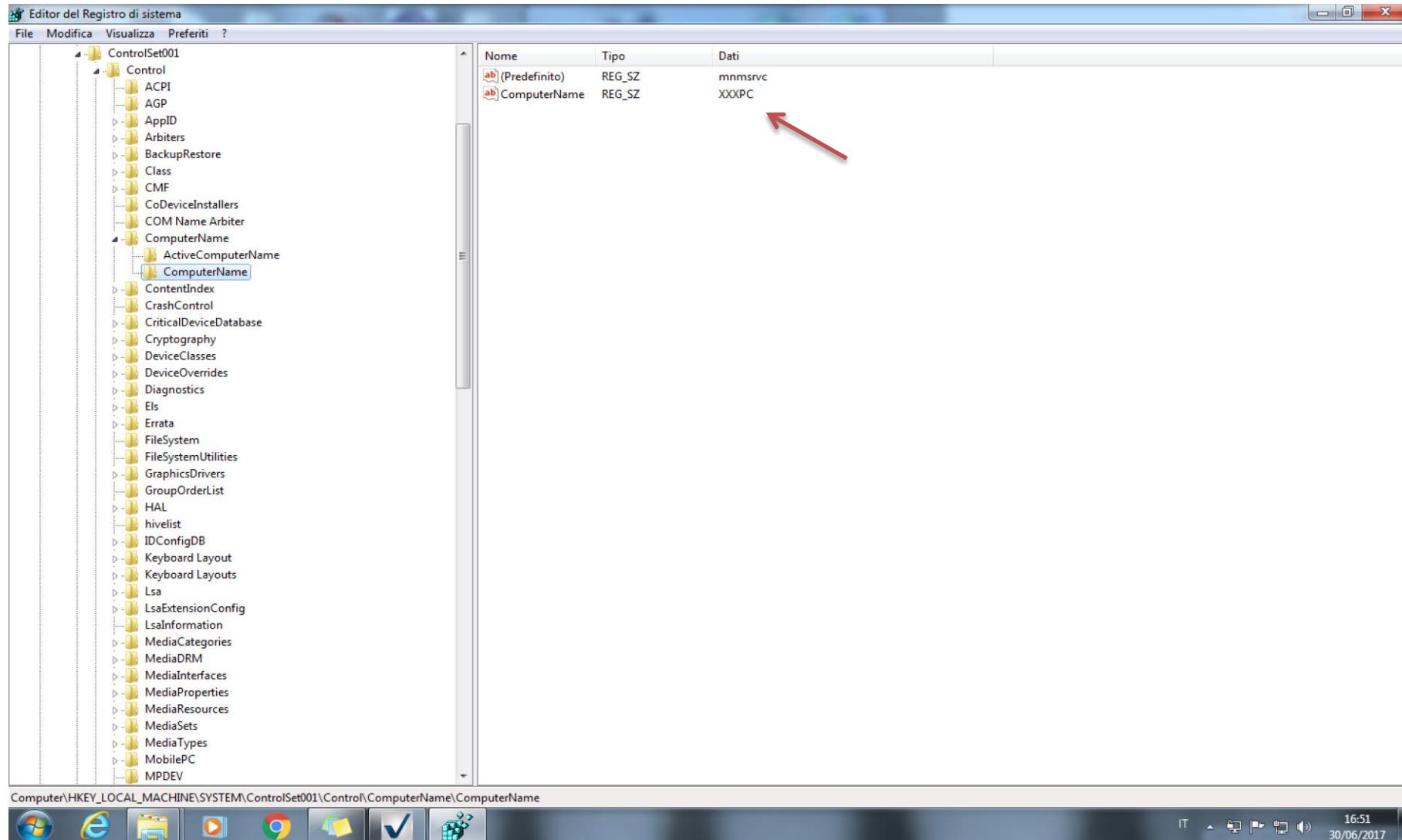
*(System) Gets ComputerName and Hostname values from System hive*

*ComputerName = XXXPC*

*TCP/IP Hostname = xxxpc*

---

# I file di Registro SYSTEM



The screenshot shows the Windows Registry Editor window. The left pane displays a tree view of registry keys under `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName`. The right pane is a table with columns **Nome**, **Tipo**, and **Dati**, showing two entries:

Nome	Tipo	Dati
(Predefinito)	REG_SZ	mnmssrvc
ComputerName	REG_SZ	XXXPC

A red arrow points to the `ComputerName` entry in the table.

Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ComputerName

16:51 30/06/2017

# I file di Registro SYSTEM

Parsing con RegRipper del file di registro SYSTEM (TimeZone)

---

*timezone v.20160318*

*(System) Get TimeZoneInformation key contents*

*TimeZoneInformation key*

*ControlSet001\Control\TimeZoneInformation*

*LastWrite Time Tue Mar 28 05:21:11 2017 (UTC)*

*DaylightName -> @tzres.dll,-321*

*StandardName -> @tzres.dll,-322* ←

W. Europe Standard Time

*Bias -> -60 (-1 hours)*

*ActiveTimeBias -> -120 (-2 hours)*

*TimeZoneKeyName-> W. Europe Standard Time*

---

Il numero **-321/-322** dopo la stringa `@tzres.dll` è un codice che identifica il Timezone, nel nostro caso W. Europe Standard Time. Sul sito [https://www.win7dll.info/tzres\\_dll.html](https://www.win7dll.info/tzres_dll.html) sono disponibili tutti i codici.

# I file di Registro SYSTEM

**Editor del Registro di sistema**

File Modifica Visualizza Preferiti ?

Nome	Tipo	Dati
ab(Predefinito)	REG_SZ	(valore non impostato)
ActiveTimeBias	REG_DWORD	0xfffffff88 (4294967176)
Bias	REG_DWORD	0xfffffc4 (4294967236)
DaylightBias	REG_DWORD	0xfffffc4 (4294967236)
abDaylightName	REG_SZ	@tzres.dll,-321
DaylightStart	REG_BINARY	00 00 03 00 05 00 02 00 00 00 00 00 00 00 00 00
DynamicDayligh...	REG_DWORD	0x00000000 (0)
StandardBias	REG_DWORD	0x00000000 (0)
abStandardName	REG_SZ	@tzres.dll,-322
StandardStart	REG_BINARY	00 00 0a 00 05 00 03 00 00 00 00 00 00 00 00 00
abTimeZoneKeyN...	REG_SZ	W. Europe Standard Time

Nome della chiavi: Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation

Icone della barra dei taskbar: Start, Internet Explorer, File Explorer, File Manager, Task View, Checkmark, File History.

Informazioni sullo schermo: 17:32, 30/06/2017.

# I file di Registro SYSTEM

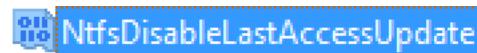
Nel file di registro alla voce “*SYSTEM\CurrentControlSet\Control\FileSystem*” c’è una voce **NtfsDisableLastAccessUpdate** che consente di attivare o disattivare il timestamp di accesso all’ultimo file. Se disattivato, l’ultimo accesso al file non viene registrato dal sistema.

Nei sistemi operativi fino a Windows Xp era attivo.

Dalle versioni di Windows Vista, Win7, Win8 e Win10 è disattivato di default, dalla versione 20H di Windows 10 il sistema viene aggiornato ed è attivo di default.

Senza il last access, potrebbe essere più difficile specificare quando i programmi sono stati aperti l’ultima volta dall’utente e questo rende più difficile fare un’analisi accurata dei file.

Se il valore è impostato a 1 il Last Access Update è disattivato, sotto una foto del valore del registro di Windows 7



REG\_DWORD

0x00000001 (1)

Da Windows 10 possiamo vedere se il last access è attivo con il comando:

***fsutil behavior query disablelastaccess***

Il Last Access può essere "Gestito dall’utente" e "Gestito dal Sistema", se è gestito dal sistema il Last Access è abilitato per i volumi NTFS quando la dimensione del volume di sistema (che di solito è montata come unità "C:") è pari o inferiore a 128 GB. Se il volume di sistema è maggiore, il Last access è disabilitato.

Possiamo cambiare i valori con in comando

***fsutil behavior set disablelastaccess***



# I file di Registro SYSTEM

Dentro il registro System un'altra chiave importante è  
*SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces*

Questo chiave contiene molte informazioni sulle schede di rete configurate nel sistema

- Nome rete
- Indirizzi IP
- Gateway
- DHCP
- GUID Interface ( Globally Unique Identifier)



# I file di Registro SYSTEM

Parsing con RegRipper del file di registro SYSTEM (Network Interfaces)

*network v.20080324*

*(System) Gets info from System\Control\Network GUIDs*

*Network key*

*Interface {865D9AD8-FFEE-4A4B-9048-B66E6A90ACB8}*

*LastWrite time Thu May 11 06:25:51 2017 (UTC)*

*Name = Connessione alla rete locale (LAN) 2*

*PnpInstanceID = ROOT\NET\0000*

*MediaSubType =*

*Interface {FD40DC46-A887-4585-ADC9-B7070B806DE1}*

*LastWrite time Thu Dec 15 09:15:01 2016 (UTC)*

*Name = Connessione alla rete locale (LAN)*

*PnpInstanceID = PCI\VEN\_8086&DEV\_100F&SUBSYS\_075015AD&REV\_01\4&3AD87E0A&0&0888*

*MediaSubType =*

*nic v.20100401*

*(System) Gets NIC info from System hive*

*Adapter: {865D9AD8-FFEE-4A4B-9048-B66E6A90ACB8}*

*LastWrite Time: Thu May 11 06:25:50 2017 Z*

*EnableDHCP 1*

*Adapter: {FD40DC46-A887-4585-ADC9-B7070B806DE1}*

*LastWrite Time: Thu Dec 15 08:51:16 2016 Z*

*EnableDHCP 1*

---



# I file di Registro SYSTEM

*nic2 v.20150812*

*(System) Gets NIC info from System hive*

*ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.*

*Adapter: {865D9AD8-FFEE-4A4B-9048-B66E6A90ACB8}*

*LastWrite Time: Mon May 29 09:04:58 2017 Z*

*UseZeroBroadcast 0*

*EnableDeadGWDetect 1*

*EnableDHCP 1*

*NameServer*

*Domain*

*RegistrationEnabled 1*

*RegisterAdapterName 0*

*DhcpIPAddress 192.168.0.6*

*DhcpSubnetMask 255.255.255.252*

*DhcpServer 192.168.0.5*

*Lease 31536000*

*LeaseObtainedTime Mon May 29 08:58:25 2017 Z*

*T1 Mon Nov 27 20:58:25 2017 Z*

*T2 Fri Apr 13 17:58:25 2018 Z*

*LeaseTerminatesTime Tue May 29 08:58:25 2018 Z*

*AddressType 0*

*IsServerNapAware 0*

*DhcpConnForceBroadcastFlag 0*

*DhcpSubnetMaskOpt 255.255.255.252*



# I file di Registro SYSTEM

*ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.*

*Adapter: {FD40DC46-A887-4585-ADC9-B7070B806DE1}*

*LastWrite Time: Wed Jun 28 15:44:31 2017 Z*

*UseZeroBroadcast       0*

*EnableDeadGWDetect    1*

*EnableDHCP            1*

*NameServer*

*Domain*

*RegistrationEnabled    1*

*RegisterAdapterName   0*

*DhcpIPAddress         192.168.93.130*

*DhcpSubnetMask        255.255.255.0*

*DhcpServer            192.168.93.254*

*Lease                1800*

*LeaseObtainedTime     Wed Jun 28 15:44:31 2017 Z*

*T1                    Wed Jun 28 15:59:31 2017 Z*

*T2                    Wed Jun 28 16:10:46 2017 Z*

*LeaseTerminatesTime   Wed Jun 28 16:14:31 2017 Z*

*AddressType          0*

*IsServerNapAware     0*

*DhcpConnForceBroadcastFlag  0*

*DhcpGatewayHardwareCount   1*

*DhcpNameServer          192.168.93.2*

*DhcpDefaultGateway     192.168.93.2*

*DhcpDomain             localdomain*

*DhcpSubnetMaskOpt     255.255.255.0*

*ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.*

---



# I file di Registro SYSTEM

*nic\_mst2 v.20080324*

*(System) Gets NICs from System hive; looks for MediaType = 2*

*Interface {FD40DC46-A887-4585-ADC9-B7070B806DE1}*

*Name: Connessione alla rete locale (LAN)*

*Control\Network key LastWrite time Thu Dec 15 09:15:01 2016 (UTC)*

*Services\Tcpip key LastWrite time Wed Jun 28 15:44:31 2017 (UTC)*

*DhcpDomain = localdomain*

*DhcpIPAddress = 192.168.93.130*

*DhcpSubnetMask = 255.255.255.0*

*DhcpNameServer = 192.168.93.2*

*DhcpServer = 192.168.93.254*

*Interface {865D9AD8-FFEE-4A4B-9048-B66E6A90ACB8}*

*Name: Connessione alla rete locale (LAN) 2*

*Control\Network key LastWrite time Thu May 11 06:25:51 2017 (UTC)*

*Services\Tcpip key LastWrite time Mon May 29 09:04:58 2017 (UTC)*

*DhcpDomain =*

*DhcpIPAddress = 192.168.0.6*

*DhcpSubnetMask = 255.255.255.252*

*DhcpNameServer =*

*DhcpServer = 192.168.0.5*

---



# I file di Registro SYSTEM

# I file di Registro SYSTEM

**Editor del Registro di sistema**

File Modifica Visualizza Preferiti ?

Nome	Tipo	Dati
(Predefinito)	REG_SZ	(valore non impostato)
AddressType	REG_DWORD	0x00000000 (0)
DhcpConnForceBroadcastFlag	REG_DWORD	0x00000000 (0)
DhcpDefaultGateway	REG_MULTI_SZ	192.168.93.2
DhcpDomain	REG_SZ	localdomain
DhcpGatewayHardware	REG_BINARY	c0 a8 5d 02 06 00 00 00 50 56 f6 fa 35
DhcpGatewayHardwareCount	REG_DWORD	0x00000001 (1)
DhcpInterfaceOptions	REG_BINARY	2c 00 00 00 00 00 04 00 00 00 00 00 00 b6 8...
DhcpIpAddress	REG_SZ	192.168.93.130
DhcpNameServer	REG_SZ	192.168.93.2
DhcpServer	REG_SZ	192.168.93.254
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpSubnetMaskOpt	REG_MULTI_SZ	255.255.255.0
Domain	REG_SZ	
EnabledDeadGWDetect	REG_DWORD	0x00000001 (1)
EnableDHCP	REG_DWORD	0x00000001 (1)
IsServerNapAware	REG_DWORD	0x00000000 (0)
Lease	REG_DWORD	0x00000708 (1800)
LeaseObtainedTime	REG_DWORD	0x595680ae (1498841262)
LeaseTerminatesTime	REG_DWORD	0x595687b6 (1498843062)
NameServer	REG_SZ	
RegisterAdapterName	REG_DWORD	0x00000000 (0)
RegistrationEnabled	REG_DWORD	0x00000001 (1)
T1	REG_DWORD	0x59568432 (1498841262)
T2	REG_DWORD	0x595686d5 (1498842837)
UseZeroBroadcast	REG_DWORD	0x00000000 (0)

**Indirizzo IP Gateway**

**Indirizzo IP, Subnet**

**GUID**

Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{FD40DC46-A887-4585-ADC9-B7070B806DE1}

18:50 30/06/2017

# I file di Registro

Altri importanti chiavi di registro per l'identificazione della Network sono:

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged  
SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed  
SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache

In queste chiavi possiamo identificare le reti connesse in passato al computer:

- Identificare tipologia di rete
- Identificare Nome dominio/intranet
- Identificare SSID
- Identificare l'indirizzo MAC Address
- Identificare le reti connesse tramite una VPN

# I file di Registro

Possiamo trovare altre informazioni sul tipo di connessione nelle seguenti chiavi

SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\{GUID} ( In Windows XP)

SOFTWARE \Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles (Vista/Win7-10)

In questa chiave sono presenti i GUID che contengono il nome, il tipo di rete, la data di creazione e l'ultima data di connessione (in binario).

Il nome della rete lo troviamo nel campo Description

Il tipo di rete lo vediamo nel campo Nametype (in esadecimale)

Nametype Value Ox47 Wireless

Nametype Value Ox06 Wired

Nametype Value Ox17 Broadband (3g)

Nei seguenti sistemi Windows 2000, XP, 2003,Vista e 7 è possibile creare le condivisioni di rete tramite il comando “net share” se l’utente ha utilizzato questa procedura da riga di comando e non da GUI possiamo trovare traccia di questa condivisione nella chiave di registro:

- **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\Shares**

# I file di Registro SYSTEM

Nella chiave di registro “*SYSTEM\CurrentControlSet\Control\Windows*” possiamo vedere data e ora dell’ultimo shutdown, il valore è in esadecimale.

Solo su Windows XP nella chiave “*SYSTEM\CurrentControlSet\Control\Watchdog\Display*” possiamo vedere anche quante volte il sistema è stato spento.

Parsing con RegRipper del file di registro SYSTEM (Shutdown)

*shutdown v.20080324*

*(System) Gets ShutdownTime value from System hive*

*ControlSet001\Control\Windows key, ShutdownTime value*

*ControlSet001\Control\Windows*

*LastWrite Time Tue Jun 27 21:12:18 2017 (UTC)*

*ShutdownTime = Tue Jun 27 21:12:18 2017 (UTC)*

---

*shutdowncount v.20080709*

*(System) Retrieves ShutDownCount value*

*ControlSet001\Control\Watchdog\Display not found.*

# I file di Registro SYSTEM

**Editor del Registro di sistema**

File Modifica Visualizza Preferiti ?

Nome	Tipo	Dati
ab (Predefinito)	REG_SZ	(valore non impostato)
ComponentizedBuild	REG_DWORD	0x00000001 (1)
CSDBuildNumber	REG_DWORD	0x0000446a (17514)
CSDReleaseType	REG_DWORD	0x00000000 (0)
CSDVersion	REG_DWORD	0x00000100 (256)
Directory	REG_EXPAND_SZ	%SystemRoot%
ErrorMode	REG_DWORD	0x00000000 (0)
NoInteractiveServices	REG_DWORD	0x00000000 (0)
ShellErrorMode	REG_DWORD	0x00000001 (1)
ShutdownTime	REG_BINARY	e2 b3 f6 0e 8a ef d2 01
SystemDirectory	REG_EXPAND_SZ	%SystemRoot%\system32

Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Windows

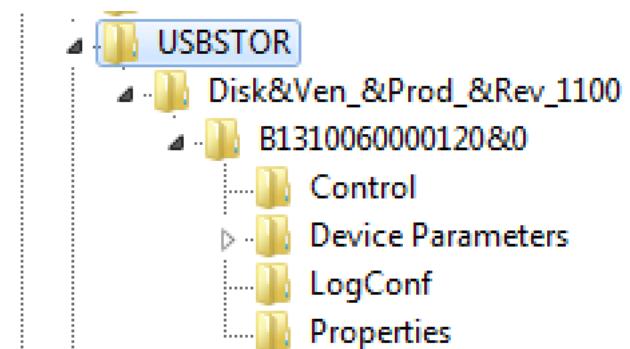
IT 15:01 01/07/2017

# I file di Registro SYSTEM

Ogni volta che viene collegato un nuovo dispositivo USB al sistema, si lasceranno informazioni riguardanti questo dispositivo USB all'interno del registro. Queste informazioni possono identificare in modo univoco ogni periferica USB collegata al sistema. Il Sistema operativo Windows memorizza ID produttore, ID del prodotto, revisione e numero di serie per ogni dispositivo USB collegato. Queste informazioni possono essere trovate nella seguente chiave di registro:

*“SYSTEM\CurrentControlSet\Enum\USBSTOR”*

Quando analizziamo la chiave ci troviamo le diciture come nella foto. La parte Disk&Ven ecc... è il Device Class ID, mentre il codice B13100 ecc.. è l'Unique Serial, il seriale del dispositivo.



# I file di Registro SYSTEM

Aprendo la chiave avremo a disposizione altre informazioni sulla dispositivo.

Nome	Tipo	Dati
(Predefinito)	REG_SZ	(valore non impostato)
Capabilities	REG_DWORD	0x00000010 (16)
Class	REG_SZ	DiskDrive
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{e57f70bd-4ebf-503f-9f9a-390c4d1b3ca5}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Unità disco
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0001
FriendlyName	REG_SZ	USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\Disk_____1100 USBSTOR\Disk_____ USBSTOR\Disk...
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(unità disco standard)
Service	REG_SZ	disk



# I file di Registro SYSTEM

Parsing con RegRipper del file di registro SYSTEM (Usb)

*usb v.20141111*

*(System) Get USB key info*

*USBStor*

*ControlSet001\Enum\USB*

*VID\_090C&PID\_1000 [Sat Jul 1 13:15:39 2017]*

*S/N: B1310060000120 [Sat Jul 1 13:15:41 2017]*

*Device Parameters LastWrite: [Sat Jul 1 13:15:40 2017]*

*LogConf LastWrite : [Sat Jul 1 13:15:39 2017]*

*Properties LastWrite : [Sat Jul 1 13:15:40 2017]*

***InstallDate*** : Sat Jul 1 13:15:41 2017 UTC

***FirstInstallDate***: Sat Jul 1 13:15:41 2017 UTC



# I file di Registro SYSTEM

*usbstor v.20141111*

*(System) Get USBStor key info*

*USBStor*

*ControlSet001\Enum\USBStor*

*Disk&Ven\_&Prod\_&Rev\_1100 [Sat Jul 1 13:15:41 2017]*

*S/N: B1310060000120&0 [Sat Jul 1 13:15:42 2017]*

*Device Parameters LastWrite: [Sat Jul 1 13:15:42 2017]*

*LogConfLastWrite : [Sat Jul 1 13:15:41 2017]*

*Properties LastWrite : [Sat Jul 1 13:15:42 2017]*

*FriendlyName : USB Device*

*InstallDate : Sat Jul 1 13:15:42 2017 UTC*

*FirstInstallDate: Sat Jul 1 13:15:42 2017 UTC*

*wpdbusenum v.20141111*

*(System) Get WpdBusEnumRoot subkey info*

*DISK&VEN\_&PROD\_&REV\_1100 (B1310060000120&0)*

*LastWrite: Sat Jul 1 14:00:00 2017*

*DeviceDesc:*

***Friendly: MIA USB***

*Mfg:*

*Device Parameters LastWrite: [Sat Jul 1 13:15:48 2017]*

*LogConfLastWrite : [Sat Jul 1 13:15:46 2017]*

*Properties LastWrite : [Sat Jul 1 13:15:47 2017]*

*InstallDate : Sat Jul 1 13:15:48 2017 UTC*

*FirstInstallDate: Sat Jul 1 13:15:48 2017 UTC*

# I file di Registro SYSTEM

Il nome del dispositivo Usb lo troviamo nella chiave  
“*SYSTEM\ControlSet001\Enum\WpdBusEnumRoot*” nella sottochiave  
FriendlyName

 FriendlyName

REG\_SZ

MIA USB

Ma anche nella chiave “*SOFTWARE\Microsoft\Windows Portable Devices*”

Un'altra chiave importante è “*SYSTEM\MountedDevices*” contiene un elenco dei dispositivi montati o che sono stati collegati precedentemente al sistema, i loro nomi dei volumi, il GUID, il nome del dispositivo, e il suo seriale.

# I file di Registro SYSTEM

Nome	Tipo
ab (Predefinito)	REG_SZ
\??\Volume{612a80b9-c2a3-11e6-9312-806e6f6e6963}	REG_BINARY
\??\Volume{612a80ba-c2a3-11e6-9312-806e6f6e6963}	REG_BINARY
\??\Volume{612a80bd-c2a3-11e6-9312-806e6f6e6963}	REG_BINARY
\??\Volume{6ba5e161-5bfd-11e7-83ed-14109fe0bbfa}	REG_BINARY
\DosDevices\C:	REG_BINARY
\DosDevices\D:	REG_BINARY
\DosDevices\E:	REG_BINARY

**Modifica valore binario**

Nome valore:  
\\?\Volume{6ba5e161-5bfd-11e7-83ed-14109fe0bbfa}

Dati valore:

0008	55	00	53	00	42	00	53	00	U.S.B.S.
0010	54	00	4F	00	52	00	23	00	T.O.R.#.
0018	44	00	69	00	73	00	6B	00	D.i.s.k.
0020	26	00	56	00	65	00	6E	00	&.V.e.n.
0028	5F	00	26	00	50	00	72	00	_&.P.r.
0030	6F	00	64	00	5F	00	26	00	O.d._&
0038	52	00	65	00	76	00	5F	00	R.e.v.
0040	31	00	31	00	30	00	30	00	1.1.0.0
0048	23	00	42	00	31	00	33	00	#.B.1.3.
0050	31	00	30	00	30	00	36	00	1.0.0.6.
0058	30	00	30	00	30	00	30	00	0.0.0.0.
0060	31	00	32	00	30	00	26	00	1.2.0.&
0068	30	00	23	00	7B	00	35	00	0.#.{.5.
0070	00	00	00	00	00	00	00	00	0.z.p.z.

**OK**      **Annulla**

# I file di Registro SYSTEM

Per determinare la prima volta che un dispositivo è stato connesso a Windows, è importante analizzare il file **setupapi.dev.log** che si trova in *C:\Windows\inf*

Questo file viene modificato durante l'installazione di un dispositivo USB. Il registro setupapi tiene traccia delle installazioni di aggiornamenti, delle installazioni del driver di periferiche e delle installazioni del service pack per scopi di risoluzione dei problemi. L'analisi del file correlata alle informazioni trovate con RegRipper fornisce una visione più dettagliata di come vengono utilizzati i dispositivi USB in un sistema.

Gli orari nel file sono impostati sul fuso orario locale

# File di Log utili per l'indagine

File di log	Descrizione
C:\WINDOWS\PANTHER\setupact.log	Contiene informazioni sulle azioni di installazione durante l'installazione.
C:\WINDOWS\PANTHER\setuperr.log	Contiene informazioni sugli errori di installazione durante l'installazione.
C:\WINDOWS\PANTHER\miglog.xml	Contiene informazioni sulla struttura della directory utente. Queste informazioni includono gli identificatori di sicurezza (SID).
C:\WINDOWS\INF\setupapi.dev.log	Contiene informazioni sui dispositivi Plug and Play e l'installazione del driver.
C:\WINDOWS\INF\setupapi.app.log	Contiene informazioni sull'installazione dell'applicazione.
%WINDIR%\Memory.dmp %WINDIR%\Minidump.dmp	Questi file vengono generati quando si verifica un arresto anomalo del sistema operativo

# I file di Registro

## Permessi e privilegi di accesso al registro

Come il file system NTFS, ogni chiave di registro e sottochiave ha una Access Control List (ACL) associata. Ciascuna ACL comprende un certo numero di voci dette Access Control Entries (ACE).

Una ACE definisce l'utente o il gruppo al quale è consentito l'accesso alla risorsa e quale tipo di accesso (Read, Full Control e Special Access).

Le ACL del registro NON DIPENDONO dal file system in uso quindi sono attive anche se il S.O. è installato su FAT32.

I permessi sono assegnati solo alle chiavi di registro, non si estendono ai valori.

Poiché l'accesso a certe chiavi del registro costituisce un'operazione privilegiata (accesso al SAM, Security, machine policy, user policy), di norma all'utente è impedita la modifica (e in certi casi anche la lettura) delle chiavi più critiche.

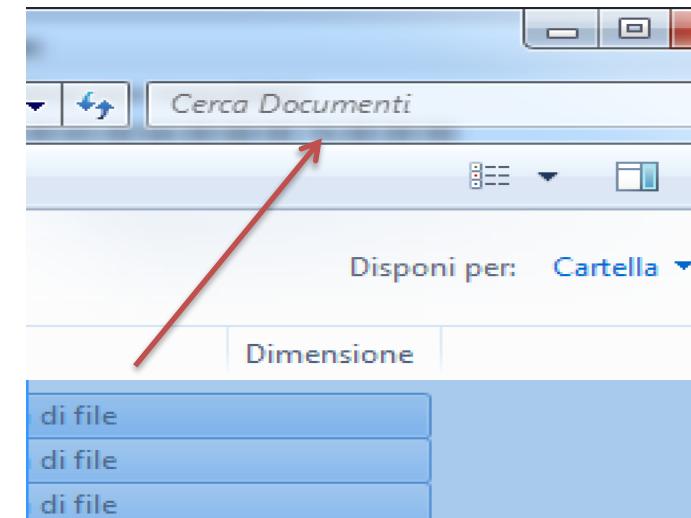
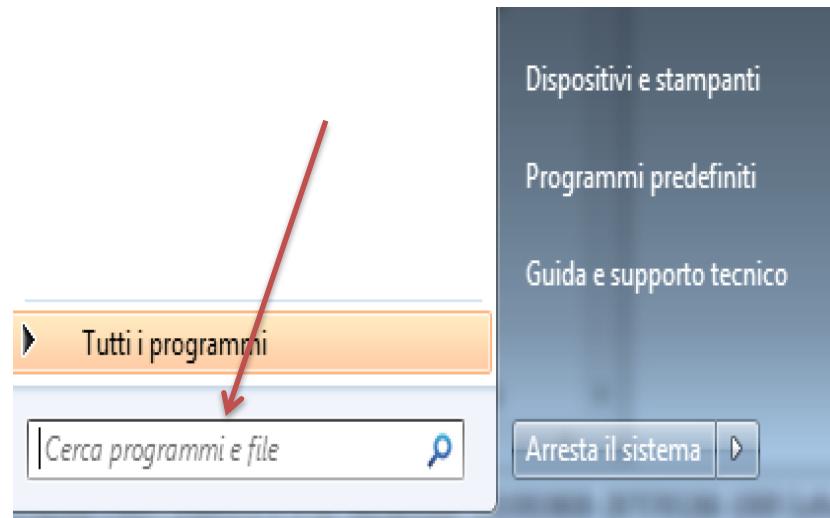
In una installazione domestica l'utente viene automaticamente inserito nel gruppo Administrators.

# Analisi attività Utente NTUSER.DAT

## WordWheelQuery

Anche se Vista non dispone di valori di ricerca registrati nel Registro di sistema, Windows 7 e Windows 8/10 hanno questa funzione.

La chiave del Registro di sistema chiamata "WordWheelQuery" registrerà le ricerche storiche di programmi e file sulla macchina. La chiave registra quello che l'utente digita sia nel menu di avvio o nella barra di ricerca di Explorer.



# Analisi attività Utente NTUSER.DAT



# Analisi attività Utente NTUSER.DAT



Parsing con RegRipper del file di registro NTUSER.DAT (WordWheelQuery)

*wordwheelquery v.20100330*

*(NTUSER.DAT) Gets contents of user's WordWheelQuery key*

*Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery  
LastWrite Time Sat Jul 1 15:37:47 2017 (UTC)*

*Searches listed in MRUListEx order*

*5 ricerca programmi e file*

*4 prova ricerca wordwhel*

*3 ricerca documenti*

*2 prova reg*

*1 regedit*

*0 regedit*

# Analisi attività Utente NTUSER.DAT

Le applicazioni mantengono una lista MRU (Most Recently Used).

La lista dei documenti recenti è individuabile alla seguente chiave di registro:

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

La MRU-list è formata:

- value name: contiene il nome del file aperto
- MRUListEx key: l'ordine con cui sono stati aperti

Altre MRU-list possono essere trovate in:

*NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer RunMRU*

Questa key contiene una lista di tutti i valori scritti nel box "run" presente nel menu Start

Un'altra chiave simile a RunMRU è la chiave TypedURLs:

*NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs*

che mantiene la lista degli URL digitati nella Address bar

Un'altra posizione dove trovare informazioni MRU può essere trovata in:

*NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU*

Questa chiave registra le applicazioni utilizzate di recente e l'ultimo percorso utilizzato per aprire un file.

# Profili Utente (Windows 7 / 10 / 11)

I profili degli utenti sono memorizzati nella cartella C:\Users\<nomeutente>

All'interno di questa cartella si trova la cartella “AppData” che contiene le informazioni più interessanti dal punto di vista forense.

I documenti recenti si trovano nella cartella

C:\Users\<nomeutente>\Appdata\Roaming\Microsoft\Windows\Recent

I file sono memorizzati con estensione LNK (collegamento).

Analizzando le proprietà dei file .lnk la data di creazione si riferisce alla prima volta che il file è stato aperto, mentre la data di ultima modifica è l'ultima apertura del file

# Cartelle Utente

Altre cartelle interessanti nel profilo utente sono:

- Preferiti (**C:\Users\<nomeutente>\Links**)
- Desktop (**C:\Users\<nomeutente>\Desktop**)
- Documenti (**C:\Users\<nomeutente>\Documents**)
- Immagini (**C:\Users\<nomeutente>\Pictures**)
- Video (**C:\Users\<nomeutente>\Video**)
- Menu Avvio (**C:\Users\<nomeutente>\AppData\Roaming\Microsoft\Windows\Start Menu**)
- Invia a (**C:\Users\<nomeutente>\AppData\Roaming\Microsoft\Window\Send to** )
- Modelli  
(**C:\Users\<nomeutente>\AppData\Roaming\Microsoft\Window\Templates**)
- Contatti (**C:\Users\<nomeutente>\Contacts**)

# Cestino

Il cestino di Windows è un elemento molto importante nell'analisi forense, può contenere artefatti che sono considerati una preziosa fonte di prove digitali.

Introdotto in Windows 95 nel tempo il cestino ha cambiato nome e posizione in Windows 95/98/me c'era un singolo file chiamato info2, *C:\RECYCLED\INFO2*, questo file contiene metadati su ciascun file eliminato come il percorso originale, la dimensione del file e la data/ora in cui è stato eliminato.

In Windows NT/2000/XP il file INFO2 era ancora presente, ma è stato spostato in una sottocartella, infatti da questa versione è stato introdotto il SID (Security Identifier) per ogni utente  
*"C:\RECYCLER\SID\*\INFO2"*

Da Windows Vista e versioni successive il percorso del Recycler è stato rinominato in *C:\\$Recycle.Bin\SID\** ed introdotti i file *\$I e \$R*.

Per ogni file cancellato dal sistema ci sono due file nel cestino. Il primo contiene le informazioni su nome del file, cartella e data di cancellazione, mentre il secondo contiene i dati veri e propri.

- **\$I#####** Nome, percorso e data di cancellazione
- **\$R#####** Contenuto del file originale

# Cestino

```
Xxx@DESKTOP-ZZTOP C:\$RECYCLE.BIN
$ dir /a
Il volume nell'unità C è Windows
Numero di serie del volume: D288-73D5

Directory di C:\$RECYCLE.BIN

19/07/2022 14:34 <DIR> .
05/01/2023 13:02 <DIR> ..
19/07/2022 14:34 <DIR> S-1-5-18
19/07/2022 12:20 <DIR> S-1-5-21-3947942548-306631893-856481394-1000
10/01/2023 07:54 <DIR> S-1-5-21-3947942548-306631893-856481394-1001
17/03/2022 18:28 <DIR> S-1-5-21-3947942548-306631893-856481394-500
07/06/2021 20:47 <DIR> S-1-5-21-403872919-2063800802-3952231467-500
    0 File          0 byte
    7 Directory  172.571.467.776 byte disponibili
```

```
Xxx@DESKTOP-ZZTOP C:\$RECYCLE.BIN
$ cd S-1-5-21-3947942548-306631893-856481394-1001
```

```
Xxx@DESKTOP-ZZTOP C:\$RECYCLE.BIN\S-1-5-21-3947942548-306631893-856481394-1001
$ dir /a
Il volume nell'unità C è Windows
Numero di serie del volume: D288-73D5

Directory di C:\$RECYCLE.BIN\S-1-5-21-3947942548-306631893-856481394-1001

10/01/2023 07:54 <DIR> .
19/07/2022 14:34 <DIR> ..
10/01/2023 07:54           23 $R048R20.txt
10/01/2023 07:54           114 $I048R20.txt
10/01/2023 07:54 <DIR> .
    107 File        28.058 byte
    2 Directory  172.551.106.560 byte disponibili
```

```
Xxx@DESKTOP-ZZTOP C:\$RECYCLE.BIN\S-1-5-21-3947942548-306631893-856481394-1001
$
```

```
Xxx@DESKTOP-ZZTOP C:\$RECYCLE.BIN
$ wmic useraccount get name,sid
Name          SID
Administrator  S-1-5-21-3947942548-306631893-856481394-500
DefaultAccount S-1-5-21-3947942548-306631893-856481394-503
Guest          S-1-5-21-3947942548-306631893-856481394-501
WDAGUtilityAccount S-1-5-21-3947942548-306631893-856481394-504
Xxx          S-1-5-21-3947942548-306631893-856481394-1001
```

```
Xxx@DESKTOP-ZZTOP C:\$RECYCLE.BIN\S-1-5-21-3947942548-306631893-856481394-1001
$ type $I048R20.txt
0x1000 L"$@+C:\Users\Xxx\Desktop\Prova Recycle Bin.txt"
Xxx@DESKTOP-ZZTOP C:\$RECYCLE.BIN\S-1-5-21-3947942548-306631893-856481394-1001
$ type $R048R20.txt
Prova Recycle Bin!!!!!!
```

```
Xxx@DESKTOP-ZZTOP C:\Users\Xxx\Desktop\RBCmd
# RBCmd.exe -f C:\Users\Xxx\Desktop\$I048R20.txt
RBCmd version 1.5.0.0
```

Author: Eric Zimmerman (saericzimmerman@gmail.com)  
<https://github.com/EricZimmerman/RBCmd>

Command line: -f C:\Users\Xxx\Desktop\\$I048R20.txt  
Found 1 files. Processing...

Source file: C:\Users\Xxx\Desktop\\$I048R20.txt

Version: 2 (Windows 10/11)  
File size: 23 (23B)  
File name: C:\Users\Xxx\Desktop\Prova Recycle Bin.txt  
Deleted on: 2023-01-10 07:54:12

Processed 1 out of 1 files in 0,0889 seconds

Per il Parser del file \$I utilizziamo il programma RBCmd scaricabile da <https://ericzimmerman.github.io/>

# Thumbnail

Thumbnails è una funzionalità di Windows, che consente di memorizzare in un database le anteprime delle immagini visionate dall'utente.

In Windows XP era presente un file nascosto denominato Thumbs.db per ciascuna cartella del sistema in cui erano presenti delle immagini.

Per ogni immagine erano memorizzati preview dell'immagine (anche se cancellata),data di ultima modifica e nome del file originale.

Da Windows Vista le informazioni sono memorizzate in diversi file denominati Thumbscache, in base alla risoluzione e sono memorizzati nel percorso

***C:\Users\XxX\AppData\Local\Microsoft\Windows\Explorer***

Sono state modificate alcune proprietà, infatti la data e l'ora non viene memorizzata e il percorso dove si trova l'immagine originale non sempre è riportato.

# Thumbnail

In base alla risoluzione memorizzata Windows crea i seguenti file:

- thumbcache\_16.db
- thumbcache\_32.db
- thumbcache\_48.db
- thumbcache\_96.db
- thumbcache\_256.db

Successivamente sono stati aggiunti anche le seguenti risoluzioni:

- thumbcache\_768.db
- thumbcache\_1280.db
- thumbcache\_1920.db
- thumbcache\_2560.db

Da Windows 10 sono stati inseriti, sempre nello stesso percorso, i file database anche per le icone denominati iconcache\_\*\*\*.db

Per visualizzare i database è possibile scaricare il programma gratuito Thumbcacheviewer dal sito <https://thumbcacheviewer.github.io/>

# Jump List

Le Jump List permettono di accedere rapidamente ai file ed alle cartelle che si utilizzano di frequente.

All'interno della cartella *C:\Users\[profilo]\AppData\Roaming\Microsoft\Windows\Recent* si trovano le informazioni relative alle Jump List, analizzando le quali si possono estrarre interessanti informazioni.

Ogni Jump List può contenere operazioni da eseguire, collegamenti a file e documenti di uso recente e collegamenti a documenti preferiti.

La memorizzazione automatica delle informazioni nella Jump List si può disattivare dalla barra delle applicazioni.

Esistono due tipologie di Jump List: le **Automatic Jump List** e le **Custom Jump List**.

In particolare quelle automatiche raggiungibili all'indirizzo:

- *C:\Users\[profilo]\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\* collezionano e memorizzano informazioni sull'utilizzo di programmi e dati da parte dell'utente, mentre quelle personalizzate sono raggiungibili all'indirizzo:
  - *C:\Users\[profilo]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\* forniscono un elenco personalizzato di voci nel menu.

È compito dello specifico applicativo tenere traccia dell'utilizzo e dell'aggiornamento della Jump List. In queste cartelle è presente un file distinto per ogni applicazione, alcune delle quali possono avere un file in entrambe le cartelle.

# Jump List

La cartella di destinazioni automatiche contiene un elenco di applicazioni ordinate da AppID. Sono in un formato XXXXXXXXXXXXXXXXX.automaticDestinations-ms, dove il nome è di circa 16 cifre e l'estensione è automaticDestination-ms

Anche i dati di creazione e modifica in questa cartella sono importanti.

Creation Time: Prima volta dell'esecuzione dell'applicazione, quando il file è stato aperto.

Modification Time: L'ultima volta dell'esecuzione dell'applicazione.

I dati memorizzati nella cartella AutomaticDestinations dispongono ciascuno di un file unico preceduto dall'appID dell'applicazione associata. I dati in questi file vengono memorizzati utilizzando il formato Structured Storage. I dati in questi file possono essere analizzati utilizzando il software Structured Storage Viewer della MiTeC, scaricabile al link

<http://www.mitec.cz/ssv.html>

I dati in questi file possono essere utilizzati per mappare la cronologia dell'applicazione dal suo primo utilizzo.

# Jump List

La Custom Destinations contiene i file creati da ciascuna applicazione ma in questa cartella possiamo trovare i file aggiunti dall'utente per esempio l'utente ha inserito un elemento preferito ai menù o inserito un collegamento alla barra delle applicazioni o di avvio.

La maggior parte delle applicazioni hanno un jumplist personalizzato.

Custom Destination è una cartella con un elenco di Applicazioni ordinate da AppID con l'estensione customDestinations-ms. Anche i tempi di creazione e modifica in questa cartella sono importanti.

Creazione Time = La prima volta che un elemento viene aggiunto al file AppID. In genere, ciò corrisponde alla prima esecuzione dell'applicazione.

Modiftcation Time = L'ultima volta che l'elemento è stato aggiunto al file AppID.

# Jump List



In ciascuna Jump List, sia Automatic che Custom, vengono visualizzati gli ID dell'applicazione. Ogni applicazione ha degli identificatori univoci universali per tutti i sistemi Windows che corrispondono al programma cui fanno riferimento. Ad esempio, l'AppID per Word 2007 è adecfb853d77462a.

Sul sito [https://forensicswiki.xyz/wiki/index.php?title=List\\_of\\_Jump\\_List\\_IDs](https://forensicswiki.xyz/wiki/index.php?title=List_of_Jump_List_IDs) sono disponibili tutti i codici delle JumpList

Nella slide successiva possiamo vedere le Jump List corrispondenti ad alcuni programmi principali.

# Jump List

23646679aaccfae0	Adobe Reader 9.***
9839aec31243a928	Excel 2010
b8c29862d9f95832	InfoPath 2010
5da8f997fd5f9428	Internet Explorer
28c8b86deab549a1	Internet Explorer 8
b91050d8b077a4e8	Media Center
918e0ecb43d17e23	Notepad
9b9cdc69c1c24e2b	Notepad
3094cdb43bf5e9c2	OneNote 2010
be71009ff8bb02a2	Outlook
c7a4093872176c74	Paint Shop Pro
f5ac5390b9115fdb	PowerPoint 2007
9c7cc110ff56d1bd	PowerPoint 2010
1bc392b8e104a00e	Remote Desktop
1b4dd67f29cb1962	Windows Explorer
d7528034b5bd6f28	Windows Live Mail
b91050d8b077a4e8	Windows Media Center
74d7f43c1561fc1e	Windows Media Player
290532160612e071	WinRar
a8c43ef36da523b1	Word 2003
adecfb853d77462a	Word 2007
a7bd71699cd38d1c	Word 2010

# Windows Search



Il “Search” di Microsoft Windows consente agli utenti di cercare file, e-mail e altro tramite l’interfaccia di ricerca. Tutte queste informazioni vengono catalogate automaticamente nel file Windows.edb.

In Windows Vista, 7, 8, 10

***C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb***

In Windows 11 il file è stato rinominato ***Windows.db***

In Windows XP

***C:\Documents and Settings\All Users\Application Data\Microsoft\Search\Data\Applications\Windows\Windows.edb***

Il database può contenere i file cercati dall’utente, e-mail, ma anche indirizzi di posta elettronica e vari metadati. Questo database contiene una notevole quantità di dati. Per fare il parser di questo file possiamo utilizzare il programma ESE Database View della Nirsoft scaricabile all’indirizzo [http://www.nirsoft.net/utils/ese\\_database\\_view.html](http://www.nirsoft.net/utils/ese_database_view.html) che permette la navigazione nelle tabelle del database. Se il file è danneggiato, esiste in Windows uno strumento denominato "esentutl" che può aiutare a recuperarlo e ripararlo.

# Windows ShellBags

Le Shell Bags registrano le preferenze di visualizzazione, ricordano la posizione della cartella, la vista e la posizione degli elementi, contengono una interessante raccolta di informazioni relative alle cartelle navigate usando Windows Explorer. La cosa importante da sapere è che, le shell bags sono inizializzate nel momento in cui l'utente è entrato almeno una volta all'interno della cartella. Scorrerle si può quindi non solo, ricostruire una timeline piuttosto precisa relativamente a quanto compiuto dall'utente nell'esplorazione del file system, ma si possono trovare indicazioni anche in relazione a dischi rimovibili (cifrati) collegati e poi rimossi dal sistema e a cartelle di rete che un utente ha visitato  
Le Shell Bags si trovano nel seguente percorso:

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

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

*NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU*

*NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags*

Per estrarre i dati dalle Shell Bags bisogna fare il parsing da entrambi i file NTUSER.DAT e USRCLASS.DAT per ogni account presente sul pc.

# Windows ShellBags

Le chiavi più importanti nelle Shell Bags sono :

- **BagMRU:** memorizza lo storico di tutte le cartelle visualizzate dall'utente durante l'uso del computer. Le cartelle all'interno di BagMRU sono elencate tramite dei numeri progressivi

BagMRU è la cartella base, ovvero quella corrispondente al Desktop. BagMRU\0 corrisponderà a Risorse del computer, BagMRU\0\0 al disco C: e via così. In pratica la struttura contenuta all'interno di BarMRU è equivalente a quella del filesystem che ci mostra Windows nelle finestre di salvataggio dei file.

- **Bag:** contiene le impostazioni di visualizzazione delle cartelle contenute all'interno di BagMRU.

Per fare il parsing delle Shell Bags utilizzare il programma Shellbags Explorer (SBECmd) scaricabile da questo indirizzo <https://ericzimmerman.github.io/>

# Windows ShellBags

```
Xxx@DESKTOP-9CJUBC0 C:\Users\Xxx\Downloads\SBECmd
# SBECmd.exe -l --csv .
SBECmd version 2.0.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman

Command line: -l --csv .

Processing live registry. Disabling dedupe
All messages will be saved to C:\Users\Xxx\Downloads\SBECmd\!SBECmd_Messages.txt
Processing live registry
'C:\Users\Xxx\AppData\Local\Microsoft\Windows\usrClass.dat' is in use. Rerouting...
Two transaction logs found. Determining primary log...
Primary log: C:\Users\Xxx\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2, secondary log: C:\Users\Xxx\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Replaying log file: C:\Users\Xxx\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Replaying log file: C:\Users\Xxx\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
At least one transaction log was applied. Sequence numbers have been updated to 0xBDEE. New Checksum: 0xBA423367
Parse time: 2.81 seconds

Total ShellBags found: 883

Totals by bag type

Root folder: GUID: 13
Directory: 817
Drive letter: 9
History folder: 3
CDBurn: 3
MTP folder: 6
MTP storage: 1
MTP device: 1
Users property view: 14
Users property view: Drive letter: 5
GUID: Control panel: 4
Control Panel Category: 3
Variable: Users property view: 2
Network location: 1
Users Files Folder: 1

Finished processing live registry

Exported to: C:\Users\Xxx\Downloads\SBECmd\20230127_140740_DESKTOP-9CJUBC0_LIVE_REGISTRY.csv

Processing complete!

Processed live registry in 2.81 seconds!
Total ShellBags found: 883
```

# Windows ShellBags

AbsolutePath	ShellType	Value	LastWriteTime	MFTEntry	MFTSequenceNumber	ExtensionBlockCount	FirstInteracted	LastInteracted	HasExplore	Miscellaneous
Desktop\My Computer\D:\Forensics\VmWare Win	Directory	VmWare Win	09/01/2023 14:36	5616	1	1	03/03/2022 13:05		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Xry	Directory	Xry	09/01/2023 14:36	5926	2	1	15/03/2022 09:48		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Zimmermann	Directory	Zimmermann	09/01/2023 14:36	104076	4	1	03/05/2022 09:12		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\KAPE	Directory	KAPE	09/01/2023 14:36	53	63	1			VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Sans Sift	Directory	Sans Sift	09/01/2023 14:36	5587	1	1	11/05/2022 07:13		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Corsi Sans	Directory	Corsi Sans	09/01/2023 14:36	164	1	1		09/01/2023 14:36	VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Emotet Check	Directory	Emotet Check	09/01/2023 14:36	59	6	1	19/05/2022 08:44		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Adobe Acrobat Pro DC 2021.001..	Directory	Adobe Acrobat Pro DC 2021.001.20142 Portable	09/01/2023 14:36	561392	1	1	24/05/2022 05:28		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Ftk	Directory	Ftk	09/01/2023 14:36	440	1	1	26/05/2022 12:07		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Arsenal Image Mounter v2.0.010	Directory	Arsenal Image Mounter v2.0.010.0 x64	09/01/2023 14:36	153	1	1	30/05/2022 05:39		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Registro Windows	Directory	Registro Windows	09/01/2023 14:36	4850	1	1			VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Dtsearch	Directory	Dtsearch	09/01/2023 14:36	7051	27	1	20/07/2022 05:36		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Powergrep	Directory	Powergrep	09/01/2023 14:36	620	1	1			VERO	NTFS file system
Desktop\My Computer\D:\Forensics\WhatsApp Extractor	Directory	WhatsApp Extractor	09/01/2023 14:36	5619	1	1	16/08/2022 13:00		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Elcomsoft	Directory	Elcomsoft	09/01/2023 14:36	6536	3	1			VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Office Professional Plus 2010 sp1	Directory	Office Professional Plus 2010 sp1 x86 x64	09/01/2023 14:36	599	1	1	17/08/2022 08:48		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Encase 8	Directory	Encase 8	09/01/2023 14:36	430	1	1	28/10/2022 06:52		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Encase 6	Directory	Encase 6	09/01/2023 14:36	418	1	1	02/11/2022 06:09		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Encase 22.1	Directory	Encase 22.1	09/01/2023 14:36	6308	13	1	02/11/2022 06:14		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Phone Forensics	Directory	Phone Forensics	09/01/2023 14:36	614	1	1	02/11/2022 16:48		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\DataBreach	Directory	DataBreach	09/01/2023 14:36	22035	18	1	28/12/2022 13:15		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Registro Windows\RegRipper2.8	Directory	RegRipper2.8-master	30/05/2022 07:19	4853	1	1	30/05/2022 07:19	30/05/2022 07:19	VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Powergrep\PowerGREP.v4.6.3 x1	Directory	PowerGREP.v4.6.3 x64	20/07/2022 05:44	626	1	1	20/07/2022 05:44		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Powergrep\PowerGREP.v4.1.2.r1	Directory	PowerGREP.v4.1.2.retail-iOTA	20/07/2022 05:44	622	1	1	20/07/2022 05:44	20/07/2022 05:44	VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Elcomsoft\Elcomsoft Explorer Fc	Directory	Elcomsoft Explorer For WhatsApp Standard Edition 2.78.372	16/08/2022 13:01	6315	12	1	16/08/2022 13:01	16/08/2022 13:01	VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Office 2016\Microsoft Office Pro	Directory	Microsoft Office ProPlus 2016 VL64 Bit Preatt	02/03/2022 10:11	5693	8	1	02/03/2022 10:11	02/03/2022 10:11	VERO	NTFS file system
Desktop\My Computer\D:\Forensics\KAPE\kapec	Directory	kapec	19/05/2022 09:13	49	11	1	19/05/2022 09:13	19/05/2022 09:13	VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Corsi Sans\508 ADVANCED DIGIT	Directory	508 ADVANCED DIGITAL FORENSIC AND INCIDENT RESPONSI	09/01/2023 14:37	186	1	1	11/05/2022 07:14		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Corsi Sans\Corsi SANS ocr	Directory	Corsi SANS ocr	09/01/2023 14:37	5651	5	1	11/05/2022 07:14		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Corsi Sans\408	Directory	408	09/01/2023 14:37	165	1	1	11/05/2022 07:14		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Corsi Sans\408.2.0 WINDOWS FO	Directory	408.2.0 WINDOWS FORENSIC ANALYSIS	09/01/2023 14:37	174	1	1	11/05/2022 07:14	09/01/2023 14:37	VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Corsi Sans\585 ADVANCED SMAF	Directory	585 ADVANCED SMARTPHONE FORENSICS	09/01/2023 14:37	6526	1	1	28/12/2022 14:22		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Corsi Sans\508 ADVANCED INCID	Directory	508 ADVANCED INCIDENT RESPONCE AND THREAT HUNTING	09/01/2023 14:37	6742	20	1	28/12/2022 14:26		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Corsi Sans\500 WINDOWS FOREN	Directory	500 WINDOWS FORENSICS NEW	09/01/2023 14:37	6741	24	1	28/12/2022 14:27		VERO	NTFS file system
Desktop\My Computer\D:\Forensics\Corsi Sans\500 WINDOWS FOREN	Directory	500 WINDOWS FORENSICS NEW - Copia	09/01/2023 14:37	71017	7	1	30/12/2022 11:37		VERO	NTFS file system

# Windows ShellBags

BagPath	Slot	NodeSlot	MRUPositio	AbsolutePath	ShellType	Value	ChildBags	CreatedOn	ModifiedOn	AccessedOn	LastWriteTime	MFTEntry	MFTSequenceNumber	ExtensionBlockCount	FirstInteracted	LastInteracted
BagMRU	0	0	4	Desktop\Control Panel	Root folder: GUID	Control Panel	9				24/08/10 23:25			0		
BagMRU	1	0	1	Desktop\My Computer	Root folder: GUID	My Computer	6				24/08/10 23:25			0		
BagMRU	2	0	2	Desktop\User Libraries	Root folder: GUID	User Libraries	5				24/08/10 23:25			0		
BagMRU	3	0	3	Desktop\Shared Documents Folder (Users Files)	Root folder: GUID	Shared Documents Folder (Us	4				24/08/10 23:25			0		
BagMRU	4	0	0	Desktop\Recycle bin	Root folder: GUID	Recycle bin	0				24/08/10 23:25			0	04/08/10 03:44	24/08/10 23:25
BagMRU	5	0	5	Desktop\Search Folder	Users property view	Search Folder	0				24/08/10 23:25			3	19/08/10 03:43	
BagMRU	6	0	6	Desktop\Recent Places	Root folder: GUID	Recent Places	0				24/08/10 23:25			0	19/08/10 17:59	
BagMRU\0	0	24	1	Desktop\Control Panel\System and Security	Control Panel Category	System and Security	3				19/08/10 03:45			0		
BagMRU\0	1	23	3	Desktop\Control Panel\Network and Internet	Control Panel Category	Network and Internet	3				19/08/10 03:45			0		
BagMRU\0	2	0	4	Desktop\Control Panel\Appearance and Personalization	Control Panel Category	Appearance and Personalizati	1				19/08/10 03:45			0		
BagMRU\0	3	25	5	Desktop\Control Panel\User Accounts	Control Panel Category	User Accounts	1				19/08/10 03:45			0		
BagMRU\0	4	26	8	Desktop\Control Panel\Clock, Language, and Region	Control Panel Category	Clock, Language, and Region	0				19/08/10 03:45			0	06/06/10 21:16	
BagMRU\0	5	27	7	Desktop\Control Panel\Ease of Access	Control Panel Category	Ease of Access	0				19/08/10 03:45			0	06/06/10 21:16	
BagMRU\0	6	0	6	Desktop\Control Panel\Programs	Control Panel Category	Programs	1				19/08/10 03:45			0		
BagMRU\0	7	0	2	Desktop\Control Panel>All Control Panel Items	Control Panel Category	All Control Panel Items	1				19/08/10 03:45			0		
BagMRU\0	8	0	0	Desktop\Control Panel\Hardware and Sound	Control Panel Category	Hardware and Sound	1				19/08/10 03:45			0		19/08/10 03:45
BagMRU\0\0	0	1	2	Desktop\Control Panel\System and Security\Windows Update	GUID: Control panel	Windows Update	1				04/08/10 03:31			0		
BagMRU\0\0	1	53	0	Desktop\Control Panel\System and Security\System	GUID: Control panel	System	0				04/08/10 03:31			0	04/08/10 02:10	04/08/10 03:31
BagMRU\0\0	2	0	1	Desktop\Control Panel\System and Security\Windows Firewall	GUID: Control panel	Windows Firewall	1				04/08/10 03:31			0		
BagMRU\0\0\0	0	2	0	Desktop\Control Panel\System and Security\Windows Update\View update history	Variable: Users property view	View update history	0				29/04/10 05:55			0	29/04/10 05:55	29/04/10 05:55
BagMRU\0\0\2	0	55	0	Desktop\Control Panel\System and Security\Windows Firewall\Customize Settings	Variable: Users property view	Customize Settings	0				04/08/10 02:11			0	04/08/10 02:11	04/08/10 02:11
BagMRU\0\1	0	19	1	Desktop\Control Panel\Network and Internet\Network and Sharing Center	GUID: Control panel	Network and Sharing Center	1				04/08/10 03:11			0		
BagMRU\0\1	1	20	0	Desktop\Control Panel\Network and Internet\Network Connections	GUID: Control panel	Network Connections	0				04/08/10 03:11			0	02/05/10 21:13	04/08/10 03:11
BagMRU\0\1	2	28	2	Desktop\Control Panel\Network and Internet\Home Group Control Panel	GUID: Control panel	Home Group Control Panel (+)	0				04/08/10 03:11			0	06/06/10 21:17	
BagMRU\0\1\0	0	29	0	Desktop\Control Panel\Network and Internet\Network and Sharing Center	Variable: Users property view	Advanced sharing settings	0				06/06/10 21:17			0	06/06/10 21:17	06/06/10 21:17
BagMRU\0\2	0	21	0	Desktop\Control Panel\Appearance and Personalization\Personalization Control Panel	GUID: Control panel	Personalization Control Panel	1				23/05/10 23:09			0		23/05/10 23:09
BagMRU\0\2\0	0	51	0	Desktop\Control Panel\Appearance and Personalization\Personalization Control Panel	Variable: Users property view	Desktop Background	0				05/07/10 23:02			0	05/07/10 23:02	05/07/10 23:02
BagMRU\0\3	0	35	0	Desktop\Control Panel\User Accounts\User Accounts	GUID: Control panel	User Accounts	1				22/06/10 22:33			0		22/06/10 22:33
BagMRU\0\3\0	0	34	0	Desktop\Control Panel\User Accounts\User Accounts\Change Your Picture	Variable: Users property view	Change Your Picture	0				22/06/10 22:33			0	22/06/10 22:33	22/06/10 22:33
BagMRU\0\6	0	31	0	Desktop\Control Panel\Programs\Default Programs	GUID: Control panel	Default Programs	0				06/06/10 23:59			0	06/06/10 23:59	06/06/10 23:59
BagMRU\0\7	0	54	0	Desktop\Control Panel>All Control Panel Items\Windows Firewall	GUID: Control panel	Windows Firewall	0				04/08/10 02:10			0	04/08/10 02:10	04/08/10 02:10
BagMRU\0\8	0	0	0	Desktop\Control Panel\Hardware and Sound\Device Center\Devices and Peripherals	GUID: Control panel	Device Center(Devices and Pr	1				19/08/10 03:45			0		19/08/10 03:45
BagMRU\0\8\0	0	61	0	Desktop\Control Panel\Hardware and Sound\Device Center\Devices and Peripherals	Variable: Users property view	S3000	0				19/08/10 03:45			0	19/08/10 03:45	19/08/10 03:45
BagMRU\1	0	4	0	Desktop\My Computer\C:	Drive letter	C:	3				24/08/10 22:04			0		24/08/10 22:04
BagMRU\1	1	22	5	Desktop\My Computer\Norman.Peterson.lnk	Users Files Folder	Norman.Peterson.lnk	0	29/04/10 05:31	29/04/10 05:31	29/04/10 05:31	24/08/10 22:04	43123	2	2	23/05/10 23:16	
BagMRU\1	2	30	3	Desktop\My Computer\Z:	Drive letter	Z:	2				24/08/10 22:04			0		
BagMRU\1	3	36	1	Desktop\My Computer\E:	Drive letter	E:	4				24/08/10 22:04			0		
BagMRU\1	4	41	4	Desktop\My Computer\O:	Drive letter	O:	0				24/08/10 22:04			0	24/06/10 02:27	
BagMRU\1	5	79	2	Desktop\My Computer\S3000	MTP device	S3000	1				24/08/10 22:04			0		
BagMRU\1\0	0	5	0	Desktop\My Computer\C:\Users	Directory	Users	1	14/07/09 02:37	29/04/10 05:27	29/04/10 05:27	21/08/10 22:11	346	1	1		21/08/10 22:11
BagMRU\1\0	1	17	2	Desktop\My Computer\C:\PerfLogs	Directory	Perflogs	0	14/07/09 02:37	14/07/09 02:37	14/07/09 02:37	21/08/10 22:11	58	1	1	29/04/10 16:26	
BagMRU\1\0	2	78	1	Desktop\My Computer\C:\Windows	Directory	Windows	2	14/07/09 02:37	19/08/10 17:31	19/08/10 17:31	21/08/10 22:11	499	1	1		
BagMRU\1\0\0	0	6	0	Desktop\My Computer\C:\Users\Norman.Peterson	Directory	Norman.Peterson	2	29/04/10 05:27	29/04/10 05:27	29/04/10 05:27	29/04/10 16:10	40958	12	1		29/04/10 16:10

# Windows Shadow Copy

La Shadow Copy è una tecnologia inclusa in Microsoft Windows a partire da Windows Vista che permette di creare copie o istantanee di files nel computer, attualmente le shadow copy vengono chiamate anche “Versioni Precedenti”. Il funzionamento è parte integrante del Backup e Punti di Ripristino di Windows. In pratica il sistema crea delle copie di backup sul FileSystem corrente. In questo modo non è necessario avere privilegi amministrativi per ripristinare un file che risiede nel profilo utente. Ciò che viene registrato è solamente la “differenza” dal file precedente e non tutto il file. Quindi se il file non cambia non verrà effettuato il backup.

Per visualizzare se sono disponibili delle Shadow Copy su un pc mentre è acceso, utilizziamo il comando vssadmin in un prompt dei comandi come amministratore:

**vssadmin list shadows**

Tale comando ci restituirà la lista delle shadow copy eventualmente presenti nel computer



# Windows Shadow Copy

```
C:>\vssadmin list shadows
vssadmin 1.1 - Utilità da riga di comando di amministrazione
Servizio copia shadow del volume
(C) Copyright 2001-2005 Microsoft Corp.
```

Contenuto dell'ID gruppo di copie shadow: {1fe1a1ca-10cf-4c7a-b98e-68673271de43}  
Conteneva 1 copie shadow al momento della **creazione: 02/07/2017 00:00:10**  
ID copia shadow: {35f8ff5a-3567-4227-b871-553f611cd09b}  
**Volume originale: (C:)\\?\Volume{612a80ba-c2a3-11e6-9312-806e6f6e6963}\\**  
Volume copia shadow: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2  
**Computer di origine: xxxpc**  
Computer di servizio: xxxpc  
Provider: 'Microsoft Software Shadow Copy provider 1.0'  
Tipo: ClientAccessibleWriters  
Attributi: Permanente, Accessibile dal client, Senza rilascio automatico, Differenziale,  
Ripristinato automaticamente

# Windows Shadow Copy

Contenuto dell'ID gruppo di copie shadow: {63e0e875-c9f2-42dd-bc00-b6b60850811e}

Conteneva 1 copie shadow al momento della **creazione: 03/07/2017 18:59:33**

ID copia shadow: {a2d70ec3-8a50-4b30-aa9c-97d7e0084334}

**Volume originale:** (C):\?\Volume{612a80ba-c2a3-11e6-9312-806e6f6e6963}\

Volume copia shadow: \?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3

**Computer di origine:** xxxpc

Computer di servizio: xxxpc

Provider: 'Microsoft Software Shadow Copy provider 1.0'

Tipo: ClientAccessibleWriters

Attributi: Permanente, Accessibile dal client, Senza rilascio automatico, Differenziale,

Ripristinato automaticamente

Possiamo estrarre le Shadow Copy facendo un link simbolico alle shadow visualizzandole come se fossero cartelle di Windows, in questo modo potrebbe essere utile sfogliare o analizzare manualmente una directory contenente un volume di shadow copy.

# Windows Shadow Copy

```
mklink /d C:\provashadow \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\  
collegamento simbolico creato per C:\provashadow <<====>>  
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\
```

**Importante alla fine del comando bisogna obbligatoriamente inserire il Backslash altrimenti non riusciremo ad aprire il nostro link.**

Occorre creare il link inserendo una cartella casuale che possiamo chiamare provashadow e inserire la copia shadow presente sul pc.

Se invece stiamo analizzando un'immagine del disco possiamo montare il Volume con il tool Arsenal Image Mounter (<https://arsenalrecon.com/>) che permette di montare il disco in modalità scrittura temporanea in modo da mostrare le shadow, le modifiche effettuate sul disco verranno scritte in un file temporaneo e l'immagine del disco originale non verrà modificata, in questo modo possiamo utilizzare il programma Shadow Explorer scaricabile da <http://www.shadowexplorer.com/> che permette la visualizzazione della shadow in modalità grafica.

# Windows ShadowCopy

ShadowExplorer

C: 03/07/2017 18:59:33 Details

Name	Date Modified	Type	Size
\$Recycle.Bin	14/07/2009 07:32:39	Cartella di file	14
Documents and Settings	14/07/2009 05:20:08	Cartella di file	14
PerfLogs	14/06/2017 12:06:31	Cartella di file	14
PNotes.NET	14/05/2017 13:07:16	Cartella di file	14
Program Files	12/04/2011 13:00:25	Cartella di file	12
Program Files (x86)	14/07/2009 07:32:38	Cartella di file	14
ProgramData	14/07/2009 07:32:38	Cartella di file	14
Programmi	15/12/2016 09:49:53	Cartella di file	12
Recovery	14/07/2009 07:32:39	Cartella di file	14
SierraChart	16/06/2017 17:13:40	Cartella di file	14
System Volume Information	14/07/2009 07:32:38	Cartella di file	14
Users	12/04/2011 12:49:34	Cartella di file	14
Windows	14/07/2009 07:32:39	Cartella di file	14
addons	14/07/2009 07:32:39	Cartella di file	14
AppCompat	14/07/2009 05:20:08	Cartella di file	14
AppPatch	14/06/2017 12:06:31	Cartella di file	14
assembly	14/05/2017 13:07:16	Cartella di file	14
BitLockerDiscoveryVolumeCon...	12/04/2011 13:00:25	Cartella di file	12
Boot	14/07/2009 07:32:38	Cartella di file	14
Branding	14/07/2009 07:32:38	Cartella di file	14
CSC	15/12/2016 09:49:53	Cartella di file	12
Cursors	14/07/2009 07:32:39	Cartella di file	14
debug	16/06/2017 17:13:40	Cartella di file	14
diagnostics	14/07/2009 07:32:38	Cartella di file	14
DigitalLocker	12/04/2011 12:49:34	Cartella di file	14
Downloaded Program Files	14/07/2009 07:32:39	Cartella di file	14
ehome	10/12/2016 11:33:35	Cartella di file	12
en-US	12/04/2011 12:46:28	Cartella di file	14
Fonts	10/12/2016 11:07:03	Cartella di file	14
Globalization	12/04/2011 13:03:09	Cartella di file	14
Help	12/04/2011 12:49:33	Cartella di file	14
IME	12/04/2011 12:49:34	Cartella di file	14
inf	03/07/2017 11:50:43	Cartella di file	14
Installer	27/06/2017 16:02:53	Cartella di file	10
it-IT	10/12/2016 11:09:11	Cartella di file	12
L2Schemas	14/07/2009 07:32:39	Cartella di file	14
LiveKemelReports	14/07/2009 04:34:24	Cartella di file	14
Logs	29/12/2016 07:56:04	Cartella di file	14
Media	14/07/2009 07:32:40	Cartella di file	14
Microsoft .NET	14/05/2017 13:10:11	Cartella di file	14

# Windows Prefetch



Prefetching è un processo in cui il sistema operativo carica dati e codici delle applicazioni dal disco alla memoria prima che sia effettivamente necessario. La directory Prefetch viene popolata una volta che un'applicazione viene eseguita. In Windows XP e Vista, in particolare, l'applicazione di prefetch dati è utilizzata per eseguire le applicazioni in modo più efficiente nelle successive esecuzioni.

In pratica i file di prefetch sono utilizzati per ottimizzare l'esecuzione dei processi frequenti.

I file di prefetch sono memorizzati in una cartella denominata Prefetch situata nella cartella di sistema %SystemRoot%\Prefetch, normalmente in C:\Windows\Prefetch.

Il gestore della cache controlla tutti i file e le directory indicati per ciascuna applicazione o processo e li mappa in un file .pf.

La directory Prefetch fino a Windows 7 conteneva massimo 128 file, su Windows 8 e Windows 10, nella cartella Prefetch possono essere presenti fino a 1024 file. A partire da Windows 10, i file Prefetch vengono compressi.

In pc con Windows 7 che si avviano da unità SSD (Solid State Drive), la directory prefetch non esiste perché non è abilitata per impostazione predefinita.

# Windows Prefetch

Il file prefetch viene così nominato, nome dell'applicazione eseguita, trattino e la rappresentazione esadecimale dell' hash del percorso del file:

*Wordpad.exe-24533991(pf*

*NotePad.exe-336351A9(pf*

*Winzip32.exe-382A5A28(pf*

*Rundll32.exe-4ADD5E7F(pf*

All'interno del file sono indicate il numero di volte in cui l'applicazione è stata eseguita, il percorso originario dell'esecuzione e l'ultima volta dell'esecuzione.

Windows esamina regolarmente il contenuto dei file .pf e scrive i file e le directory utilizzati dal processo nel file layout.ini, che contiene i nomi di percorso originali dei file presenti nel Prefetch.

Per fare il parsing della cartella Prefetch si può utilizzare il programma della Nirsoft WinPrefetchview scaricabile da [http://www.nirsoft.net/utils/win\\_prefetch\\_view.html](http://www.nirsoft.net/utils/win_prefetch_view.html)

Esiste una versione aggiornata dei file Prefetch chiamata SuperFetch che è stata introdotta da Microsoft con lo scopo di analizzare le azioni effettuate dall'utente e memorizzarle nella Ram per un avvio più rapido delle applicazioni. È importante notare che non sostituisce il servizio Prefetch. Il SuperFetch consiste in una serie di file di database "Ag\*.db" situati nella cartella %SystemRoot%\Prefetch.

All'interno dei database possiamo trovare una vasta gamma di file che sono stati mappati in memoria, tra cui librerie, file zip, documenti, file di database, cartelle presenti su supporti rimovibili, cestino, cartelle temp e anche copie shadow.

Nei sistemi avviati su unità SSD, il SuperFetch può essere disattivato come il Prefetch.

Per il parsing del database è possibile utilizzare il programma SuperFetch Tree scaricabile da <http://www.tmurgent.com/appv/en/87-tools/performance-tools/141-superfetch-tools>

Nei Windows Server il file Prefetch è disabilitato di default

# Windows ShimCache

Microsoft ha introdotto lo ShimCache in Windows 95 e rimane ad oggi un meccanismo per garantire la compatibilità dei file binari più vecchi in nuove versioni dei sistemi operativi. Quando i nuovi sistemi operativi Microsoft vengono rilasciati qualche file binario potrebbe corrompersi, per risolvere questo problema Microsoft ha introdotto la ShimCache che permette ai programmi non aggiornati di funzionare sui sistemi più aggiornati.

In Windows XP questa struttura di dati viene memorizzato sotto la chiave di registro:

- **HKLM\CurrentControlSet\Control\Session Manager\AppCompatibility\AppCompatCache**

Sui Windows recenti i dati ShimCache vengono memorizzati sotto la chiave di registro:

- **SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache\AppCompatCache**

Nella ShimCache possiamo ottenere informazioni su tutti i file che sono stati eseguiti nel sistema da quando è stato riavviato e tiene traccia delle dimensioni e la data dell'ultima modifica.

Inoltre nella ShimCache possiamo trovare degli eseguibili che non sono stati eseguiti ma sono stati “sfogliati” per esempio attraverso explorer.exe. Questo è molto importante perché possiamo trovare traccia di eseguibili che si trovavano sul sistema, ma non sono stati eseguiti. In Windows XP la ShimCache mantiene fino a 96 voci, ma da Windows 7 la ShimCache può mantenere fino a 1024 voci.

# Windows ShimCache

Per fare il parsing possiamo utilizzare il programma AppCompatCacheParser scaricabile all'indirizzo

<https://f001.backblazeb2.com/file/EricZimmermanTools/AppCompatCacheParser.zip>

```
$ AppCompatCacheParser.exe -f C:\Users\XxX\Desktop\SYSTEM --csv  
C:\Users\XxX\Desktop\App\
```

*AppCompatCache Parser version 0.9.7.0*

*Author: Eric Zimmerman (saericzimmerman@gmail.com)*

<https://github.com/EricZimmerman/AppCompatCacheParser>

*Processing hive 'C:\Users\XxX\Desktop\SYSTEM'*

*Found 48 cache entries for Windows10Creators in ControlSet001*

*Results saved to*

*'C:\Users\XxX\Desktop\App\Windows10Creators\_SYSTEM\_AppCompatCache.tsv'*

# Windows ShimCache

ControlSet	CacheEntryPosition	Path	LastModifiedTimeUTC	Executed
1	1	C:\WINDOWS\microsoft.net\framework64\v2.0.50727\ngen.exe	17/03/17 17:53	Yes
1	2	C:\WINDOWS\microsoft.net\framework\v2.0.50727\ngen.exe	03/03/17 20:10	Yes
1	3	C:\Windows\System32\ie4uininit.exe	18/03/17 20:56	Yes
1	4	C:\WINDOWS\system32\unregmp2.exe	18/03/17 04:54	Yes
1	5	C:\WINDOWS\SysWOW64\regsvr32.exe	18/03/17 20:58	Yes
1	6	C:\WINDOWS\system32\regsvr32.exe	18/03/17 20:57	Yes
1	7	C:\WINDOWS\system32\DllHost.exe	18/03/17 20:58	Yes
1	8	C:\\$WINDOWS.~BT\Sources\mghost.exe	17/03/17 20:41	Yes
1	9	C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\Ngen.exe	18/03/17 20:59	Yes
1	10	C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\Ngen.exe	18/03/17 21:00	No
1	11	C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\aspnet_regiis.exe	17/03/17 17:53	Yes
1	12	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe	03/03/17 20:10	Yes
1	19	C:\WINDOWS\system32\AUDIODG.EXE	18/03/17 20:57	Yes
1	20	C:\Program Files\Realtek\Audio\HDA\DTSAudioService64.exe	17/02/17 23:12	No
1	21	C:\WINDOWS\syswow64\WOWReg32.exe	18/03/17 20:58	Yes
1	22	C:\Windows\System32\WUDFHost.exe	18/03/17 20:57	Yes
1	23	C:\Program Files\NVIDIA Corporation\Display\nvtray.exe	09/02/17 22:57	Yes
1	24	C:\WINDOWS\system32\RunDll32.EXE	18/03/17 20:58	No
1	25	C:\Program Files\NVIDIA Corporation\Display\nvxdsync.exe	09/02/17 22:57	No
1	26	C:\temp\NVIDIA\ControlPanelInstallerTemp\setup.exe	09/02/17 22:57	Yes
1	28	C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.exe	09/02/17 23:13	Yes

File simili dove possiamo trovare informazioni su i programmi eseguiti sono il **RecentFileCache.bcf** presente nel percorso C:\Windows\AppCompat\Programs\ sostituito da Windows 8 dal file **Amcache.hve** inserito nello stesso percorso.

# ADS (Alternate Data Streams)

Gli alternate data streams (ADS) sono, flussi di dati alternativi ed è una particolarità del filesystem NTFS di Windows.

Gli ADS sono stati creati per rendere compatibile Windows con il filesystem HFS di Apple, infatti questo filesystem utilizza anch'esso una struttura dati simile ad un ADS (chiamati metadati).

NTFS memorizza i nomi dei file, directory, data di creazione/modifica e il contenuto dei file nella MFT (Master File Table). La particolarità, è che ogni file può avere più di un flusso di dati (ovvero il contenuto).

Gli ADS vengono utilizzati per memorizzare insiemi di informazioni aggiuntive rispetto a quelle che normalmente vengono conservate in qualunque tipo di file, proprio questa caratteristica è stata spesso utilizzata in passato per nascondere malware.

In realtà, però, gli ADS sono utilizzati per finalità assolutamente legittime: il browser e il sistema operativo, ad esempio, annotano la provenienza dei file in modo da allertare l'utente nel caso la loro apertura potesse nascondere un'insidia.

Gli Ads vengono utilizzati anche da vari programmi come Dropbox che memorizza informazioni di appoggio sui file sincronizzati con i suoi server cloud o gli antivirus che sfruttano questa funzionalità per contrassegnare i file scansionati in modo da non controllarli una seconda volta se non hanno subito cambiamenti.



# ADS (Alternate Data Streams)

Per cercare i file che hanno gli Ads tramite prompt dei comandi di windows eseguiamo questo comando dir /r | find ":\$DATA" si troveranno diversi file che hanno un corrispettivo con lo stesso nome e il suffisso :Zone.Identifier:\$DATA. Si tratta proprio dei file con un ADS.

```
XXX@DESKTOP-9CJUBC0 C:\Users\XXX\Downloads
$ dir /r | find ":$DATA"
449 AMP_Quantower_(1).exe:Zone.Identifier:$DATA
196 avg-antivirus-free-setup-21103213.zip:Zone.Identifier:$DATA
    7 ChromeSetup.exe:SmartScreen:$DATA
121 driver_booster_setup_(2).exe:Zone.Identifier:$DATA
649 emocheck_v2.2_x86.exe:Zone.Identifier:$DATA
152 EvtxECmd.zip:Zone.Identifier:$DATA
128 evtxECmd_2_tln.exe:Zone.Identifier:$DATA
110 exiftool-12.41.zip:Zone.Identifier:$DATA
154 FBReader_1.999.16.0_x64.msix:Zone.Identifier:$DATA
158 fulleventlogview-x64.zip:Zone.Identifier:$DATA
147 hashmyfiles-x64.zip:Zone.Identifier:$DATA
303 hfsexplorer-2021.10.9-bin.zip:Zone.Identifier:$DATA
184 hfsexplorer-2021.10.9-setup.exe:Zone.Identifier:$DATA
140 hfs_win_uc_trial_(1).msi:Zone.Identifier:$DATA
137 ipnetinfo.zip:Zone.Identifier:$DATA
131 it.csv:Zone.Identifier:$DATA
195 Italy-b2c-email-list-sample.xlsx:Zone.Identifier:$DATA
157 KapeFiles-master_(1).zip:Zone.Identifier:$DATA
165 KapeFiles-master.zip:Zone.Identifier:$DATA
670 logpresso-log4j2-scan-3.0.1-win64.7z:Zone.Identifier:$DATA
151 MFTECmd.zip:Zone.Identifier:$DATA
155 MFTExplorer.zip:Zone.Identifier:$DATA
157 mimikatz-master.zip:Zone.Identifier:$DATA
645 mimikatz_trunk.7z:Zone.Identifier:$DATA
163 netpass-x64.zip:Zone.Identifier:$DATA
157 networkusagelogview-x64.zip:Zone.Identifier:$DATA
    87 PSTools.zip:Zone.Identifier:$DATA
145 qemu-img-win-x64-2_3_0.zip:Zone.Identifier:$DATA
185 realtek-rtl2838uhidir-277257.zip:Zone.Identifier:$DATA
160 RegistryExplorer.zip:Zone.Identifier:$DATA
107 RegRipper3.0-master.zip:Zone.Identifier:$DATA
169 rtlsdr_win.zip:Zone.Identifier:$DATA
129 Streams.zip:Zone.Identifier:$DATA
182 tabella_riepilogative_aree_protette.xls:Zone.Identifier:$DATA
240 TeamViewer_Setup_x64.exe:Zone.Identifier:$DATA
160 TimelineExplorer.zip:Zone.Identifier:$DATA
147 Tools-master.zip:Zone.Identifier:$DATA
129 unicode_2_ascii.exe:Zone.Identifier:$DATA
    83 usbdevview-x64.zip:Zone.Identifier:$DATA
128 volatility_2.6_win64_standalone.zip:Zone.Identifier:$DATA
```

# ADS (Alternate Data Streams)

Per vedere il contenuto dell'Ads sempre da prompt possiamo digitare il seguente comando  
more <nomefile>:Zone.Identifier

Come si può vedere dallo screenshot ci dice che il file è stato scaricato da Internet e dove è stato scaricato.

La lettura del contenuto degli ADS può essere effettuata anche via PowerShell usando il comando Get-Content nomefile.zip -Stream Zone.Identifier.

Con Remove-Item è possibile rimuovere gli ADS.

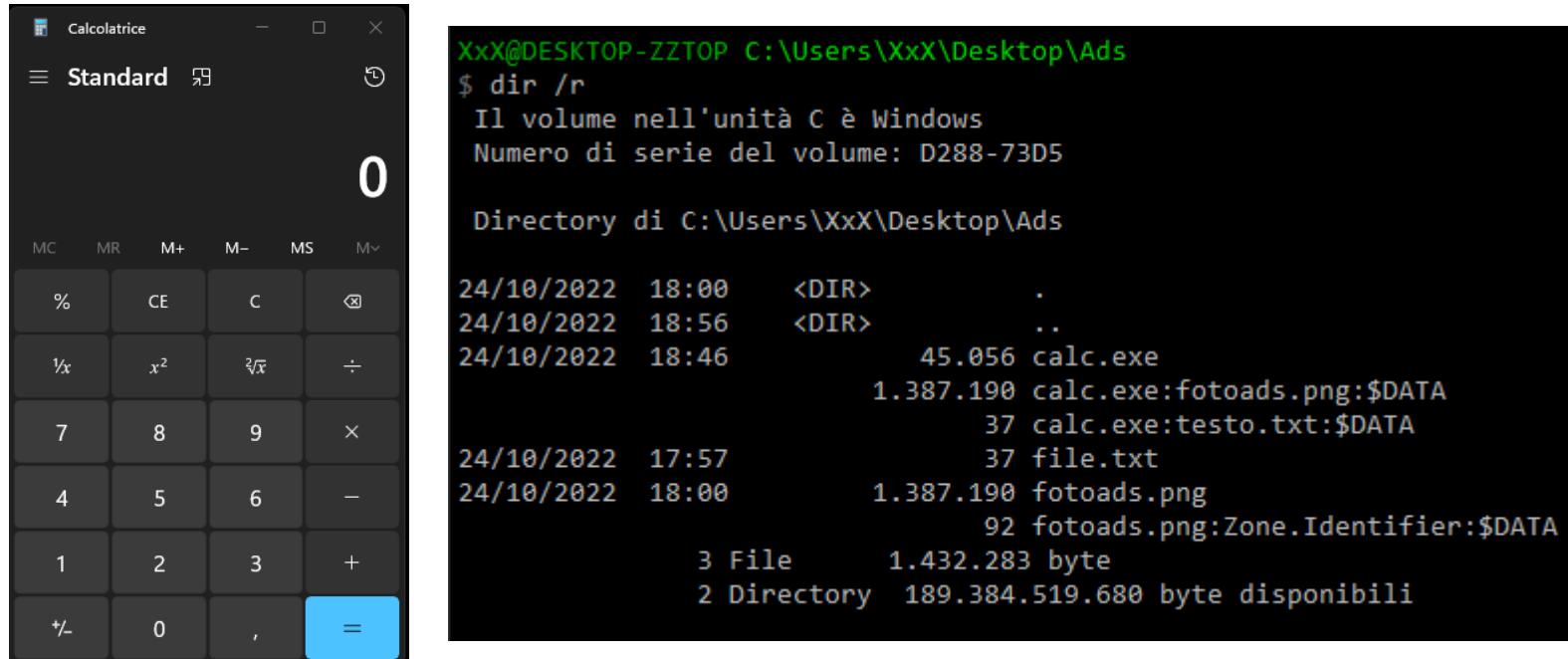
```
Xxx@DESKTOP-9CJUBC0 C:\Users\XXX\Downloads
$ more <Streams.zip>:Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://learn.microsoft.com/
HostUrl=https://download.sysinternals.com/files/streams.zip
```

Zone	ZoneId
Local machine	0
Local intranet	1
Trusted sites	2
Internet	3
Restricted sites	4

```
PS C:\Users\XXX\Downloads> Get-Content .\OSSTMM.3.pdf -Stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://www.redhotcyber.com/post/vulnerability-assessment-e-penetration-test-scopriamo-le-loro-differenze/
HostUrl=https://www.isecom.org/OSSTMM.3.pdf
PS C:\Users\XXX\Downloads> []
```

# ADS (Alternate Data Streams)

Possiamo nascondere qualsiasi cosa dentro gli Ads nell'esempio utilizzeremo la calcolatrice di windows per nascondere sia un file di testo che una foto.



The image shows a screenshot of a Windows desktop environment. On the left, there is a standard Windows calculator window with the number '0' displayed. On the right, there is a terminal window with the following text:

```
XxX@DESKTOP-ZZTOP C:\Users\XxX\Desktop\Ads
$ dir /r
Il volume nell'unità C è Windows
Numero di serie del volume: D288-73D5

Directory di C:\Users\XxX\Desktop\Ads

24/10/2022 18:00    <DIR>    .
24/10/2022 18:56    <DIR>    ..
24/10/2022 18:46                45.056 calc.exe
                                1.387.190 calc.exe:fotoads.png:$DATA
                                37 calc.exe:testo.txt:$DATA
                                37 file.txt
24/10/2022 17:57
24/10/2022 18:00                1.387.190 fotoads.png
                                92 fotoads.png:Zone.Identifier:$DATA
                                3 File      1.432.283 byte
                                2 Directory 189.384.519.680 byte disponibili
```

# ADS (Alternate Data Streams)

```
XxX@DESKTOP-ZZTOP C:\Users\XxX\Desktop\Ads
$ type file.txt > calc.exe:testo.txt

XxX@DESKTOP-ZZTOP C:\Users\XxX\Desktop\Ads
$ type fotoads.png > calc.exe:fotoads.png
```

```
XxX@DESKTOP-ZZTOP C:\Users\XxX\Desktop\Ads
$ more <calc.exe:testo.txt
"Stringa di testo per esempio ADS"
```

```
PS C:\Users\XxX\Desktop\Ads> start .\calc.exe:fotoads.png
PS C:\Users\XxX\Desktop\Ads> []
```

[CHI SIAMO](#)[CORSI ITS ▾](#)[CORSI PROFESSIONALI](#)[DOCENTI](#)[STUDENTI](#)[AZIENDE](#)[ERASMUS](#)[CONTATTI](#)

# ADS (Alternate Data Streams)

Da Powershell con il comando Get-Item –path .\calc.exe –stream \* possiamo vedere quanti Ads ci sono in un file.

```
PS C:\Users\XxX\Desktop\Ads> Get-Item -path .\calc.exe -stream *

PSPath          : Microsoft.PowerShell.Core\FileSystem::C:\Users\XxX\Desktop\Ads\calc.exe::$DATA
PSParentPath    : Microsoft.PowerShell.Core\FileSystem::C:\Users\XxX\Desktop\Ads
PSChildName    : calc.exe::$DATA
PSDrive         : C
PSProvider       : Microsoft.PowerShell.Core\FileSystem
PSIsContainer   : False
FileName        : C:\Users\XxX\Desktop\Ads\calc.exe
Stream          : ::$DATA
Length          : 45056

PSPath          : Microsoft.PowerShell.Core\FileSystem::C:\Users\XxX\Desktop\Ads\calc.exe:fotoads.png
PSParentPath    : Microsoft.PowerShell.Core\FileSystem::C:\Users\XxX\Desktop\Ads
PSChildName    : calc.exe:fotoads.png
PSDrive         : C
PSProvider       : Microsoft.PowerShell.Core\FileSystem
PSIsContainer   : False
FileName        : C:\Users\XxX\Desktop\Ads\calc.exe
Stream          : fotoads.png
Length          : 1387190

PSPath          : Microsoft.PowerShell.Core\FileSystem::C:\Users\XxX\Desktop\Ads\calc.exe:testo.txt
PSParentPath    : Microsoft.PowerShell.Core\FileSystem::C:\Users\XxX\Desktop\Ads
PSChildName    : calc.exe:testo.txt
PSDrive         : C
PSProvider       : Microsoft.PowerShell.Core\FileSystem
PSIsContainer   : False
FileName        : C:\Users\XxX\Desktop\Ads\calc.exe
Stream          : testo.txt
Length          : 37
```

# ADS (Alternate Data Streams)

Bisogna ricordarci che gli Ads funzionano solo nei pc con file system Ntfs, se copiamo il file su un disco perdiamo gli Ads, infatti riceveremo un messaggio di avviso che il file contiene attributi che non verranno copiati.

L'Hash del file non cambia in un file con gli Ads.

Esistono programmi che scansionano il disco alla ricerca di Ads e permettono la rimozione di un Ads dal file. (es. Streams scaricabile da <https://learn.microsoft.com/en-us/sysinternals/downloads/streams> )

Possiamo inserire fino a 256 mila stream alternativi per ogni singolo file, possiamo aggiungere qualsiasi file, incluse cartelle.

Gli antivirus generalmente riconoscono se in un file c'è un Ads malevolo.

# Windows Event

I registri eventi forniscono una grande quantità di informazioni che possono aiutare l'investigatore a ricostruire tutte le operazioni che si sono verificate sul sistema.

In Windows tutto quello che avviene è riferibile al contesto di un account. Possiamo identificare i riferimenti ad utenti specifici così come informazioni sulle attività del sistema operativo Windows eseguite tramite account speciali come System e NetworkService.

- Event ID, Categories Event ci aiutano a trovare rapidamente eventi rilevanti che sono avvenuti nel sistema.
- I timestamp sono una parte fondamentale dei registri degli eventi, fornendo un contesto temporale per gli eventi. Con sistemi che registrano migliaia di eventi, i timestamp possono aiutare l'investigatore a focalizzare la propria attenzione.

# Windows Event

- In un ambiente in rete, comunemente troveremo riferimenti a sistemi diversi dall'host, poiché le risorse sono accessibili in remoto. In origine, solo il nome di Netbios era registrato negli eventi, rendendo molto più difficile il monitoraggio e l'attribuzione di un determinato evento. Nei sistemi post-Windows 2000, gli indirizzi IP vengono registrati nei registri degli eventi
- Il servizio di registrazione eventi può essere configurato per memorizzare informazioni molto dettagliate sull'utilizzo di vari oggetti di sistema. Ad esempio, questo può aiutare a identificare l'accesso tentato a file non autorizzati in un sistema.

I file di log in Windows NT /Win 2000/ Xp /Win Server 2003 sono nel percorso:

- ***%systemroot% \System32 \config***

con estensione .evt ed hanno i seguenti nomi  
SecEvent.evt, AppEvent.evt, SysEvent.evt

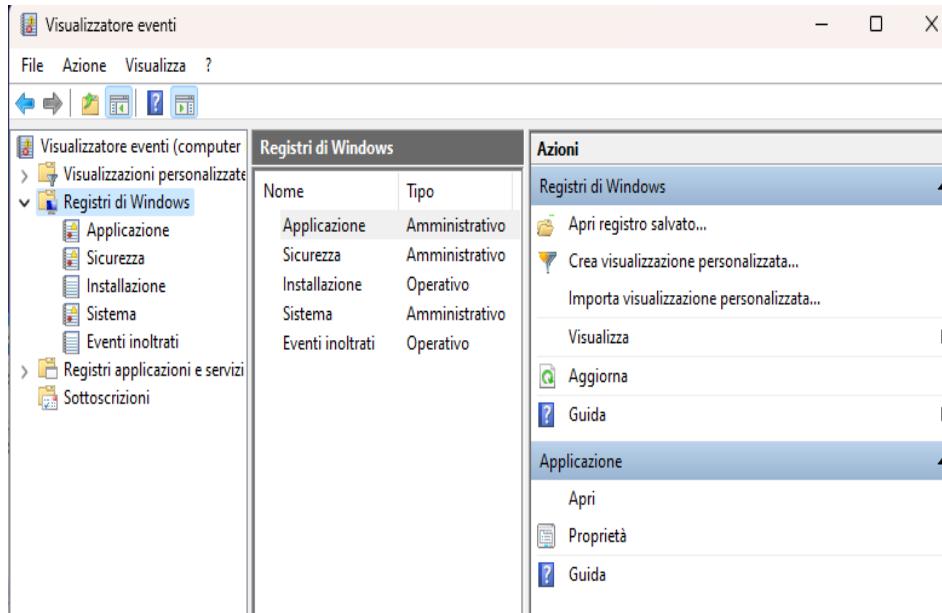
In Windows Vista/Win7/Win8/Win10 sono nel percorso:

- ***%systemroot% \System32 \winevt \logs***

Con estensione .evtx hanno i seguenti nomi  
Security.evtx, Application.evtx, System.evtx, etc.

# Windows Event

I registri vengono memorizzati in formato binario, complicando la ricerca di stringhe e vengono implementati utilizzando un buffer circolare. Il buffer circolare scrive ed (eventualmente) sovrascrive le voci più vecchie.



A partire da Vista e Server 2008, sono state apportate modifiche significative alle strutture del registro eventi, ai tipi di registro e alle posizioni del registro. I registri eventi hanno storicamente richiesto un enorme carico a livello di prestazioni sui sistemi e quindi il nuovo formato, utilizzando l'estensione .evtx, è stato creato per risolvere questo ed altri problemi.

Inoltre, il nuovo formato di registro consente di inviare i registri a un collettore di log remoto, quindi è **importante ricordare che i registri possono essere disponibili su server esterni.**

# Windows Event

## Tipi di Event Log

### Security

Registra il controllo degli accessi e le impostazioni di sicurezza

Eventi basati su controlli e politiche di gruppo

Esempio: accesso non riuscito, accesso alla cartella

### System

Contiene eventi relativi a servizi Windows, componenti di sistema, driver, risorse, ecc.

Esempio: servizio interrotto, system reboot

### Application

Eventi software non correlati al sistema operativo

Esempio: il server SQL non è in grado di accedere a un database

### Custom

Registri applicazione personalizzati

Esempio: Server Logs incluso Directory Service, Server DNS

# Windows Event

**Visualizzatore eventi**

**Sicurezza** Numero di eventi: 30.638

Filtrati: Registro: Security; Origine: ID evento: 4648. Numero di eventi: 210

Parole chiave	Data e ora	Origine	ID evento	Categoria attività
Controllo riuscito	28/12/2022 14:04:38	Microsoft Windows security auditing.	4648	Logon
Controllo riuscito	28/12/2022 13:51:20	Microsoft Windows security auditing.	4648	Logon
Controllo riuscito	28/12/2022 13:45:13	Microsoft Windows security auditing.	4648	Logon
Controllo riuscito	28/12/2022 13:45:02	Microsoft Windows security auditing.	4648	Logon
Controllo riuscito	28/12/2022 12:46:43	Microsoft Win		Filtro registro corrente
Controllo riuscito	28/12/2022 10:47:29	Microsoft Win		
Controllo riuscito	28/12/2022 10:47:07	Microsoft Win		
Controllo riuscito	28/12/2022 09:47:36	Microsoft Win		
Controllo riuscito	28/12/2022 09:47:18	Microsoft Win		
Controllo riuscito	28/12/2022 09:19:08	Microsoft Win		
Controllo riuscito	28/12/2022 09:18:29	Microsoft Win		
Controllo riuscito	28/12/2022 08:49:55	Microsoft Win		
Controllo riuscito	28/12/2022 08:47:49	Microsoft Win		
Controllo riuscito	28/12/2022 08:19:39	Microsoft Win		

**Evento 4648, Microsoft Windows security auditing.**

**Generale** **Dettagli**

È stato tentato un accesso utilizzando credenziali esplicite.

**Soggetto:**

- ID sicurezza: DESKTOP-ZZTOP\XxX
- Nome account: XxX
- Domino account: DESKTOP-ZZTOP
- ID accesso: 0x42D70
- GUID accesso: (00000000-0000-0000-0000-000000000000)

**Account di cui sono state utilizzate le credenziali:**

- Nome account: pippo
- Domino account: DESKTOP-ZZTOP
- GUID accesso: (00000000-0000-0000-0000-000000000000)

**Server di destinazione:**

- Nome server di destinazione: nas380xx
- Informazioni aggiuntive: nas380xx

**Informazioni sul processo:**

- ID processo: 0x4

**Nome registro:** Sicurezza  
**Origine:** Microsoft Windows security  
**Registrato:** 28/12/2022 14:04:38  
**ID evento:** 4648  
**Livello:** Informazioni  
**Utente:** N/D  
**Opcode:** Informazioni  
**Altre informazioni:** [Guida registro eventi](#)

**Azioni**

**Sicurezza**

- Apri registro salvato...
- Creare visualizzazione personalizzata...
- Importa visualizzazione personalizzata...
- Cancella registro...
- Filtro registro corrente...**
- Cancella filtro
- Proprietà
- Trova...
- Salva file di registro filtrato con nome...
- Associa un'attività al registro...
- Salva filtro in una visualizzazione personalizzata...
- Visualizza
- Aggiorna
- Guida

**Evento 4648, Microsoft Windows security auditing.**

- Proprietà evento
- Associa attività all'evento...
- Salva eventi selezionati...
- Copia
- Aggiorna
- Guida

# Windows Event

**Visualizzatore eventi**

**Sicurezza** Numero di eventi: 30.638

Parole chiave	Data e ora	Origine	ID evento	Categoria attività
Controllo riuscito	28/12/2022 14:22:04	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	28/12/2022 14:22:04	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	28/12/2022 14:22:04	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	28/12/2022 14:22:04	Microsoft Windows security auditing.	4624	Logon
<b>Controllo riuscito</b>	<b>28/12/2022 14:04:38</b>	<b>Microsoft Windows security auditing.</b>	<b>4648</b>	<b>Logon</b>
Controllo riuscito	28/12/2022 14:04:28	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	28/12/2022 14:04:28	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	28/12/2022 14:04:28	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	28/12/2022 14:04:28	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	28/12/2022 14:04:19	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/12/2022 14:04:19	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/12/2022 14:04:17	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/12/2022 13:51:20	Microsoft Windows security auditing.	4648	Logon
Controllo riuscito	28/12/2022 13:50:33	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	28/12/2022 13:50:33	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	28/12/2022 13:50:24	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/12/2022 13:50:19	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/12/2022 13:50:18	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/12/2022 13:50:11	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/12/2022 13:49:54	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/12/2022 13:49:54	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/12/2022 13:49:34	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/12/2022 13:45:13	Microsoft Windows security auditing.	4648	Logon
Controllo riuscito	28/12/2022 13:45:02	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	28/12/2022 13:45:02	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	28/12/2022 13:45:02	Microsoft Windows security auditing.	4634	Logoff
Controllo riuscito	28/12/2022 13:45:02	Microsoft Windows security auditing.	4634	Logoff

**Eventi 4648, Microsoft Windows security auditing.**

**Generale** **Dettagli**

Account di cui sono state utilizzate le credenziali:  
 Nome account: pippo  
 Dominio account: DESKTOP-ZZTOP  
 GUID accesso: {00000000-0000-0000-0000-000000000000}

Server di destinazione:

Nome registro:	Sicurezza		
Origine:	Microsoft Windows security	Registrato:	28/12/2022 14:04:38
ID evento:	4648	Categoria attività:	Logon
Livello:	Informazioni	Parole chiave:	Controllo riuscito
Utente:	N/D	Computer:	DESKTOP-ZzTop
Opcode:	Informazioni		
Altre informazioni:	<a href="#">Guida registro eventi</a>		



# Windows Event

Proprietà evento - Evento 4648, Microsoft Windows security auditing.

Generale Dettagli

È stato tentato un accesso utilizzando credenziali esplicite.

Soggetto:

ID sicurezza:	DESKTOP-ZZTOP\XxX
Nome account:	XxX
Dominio account:	DESKTOP-ZZTOP
ID accesso:	0x42D70
GUID accesso:	{00000000-0000-0000-0000-000000000000}

Account di cui sono state utilizzate le credenziali:

Nome account:	pippo
Dominio account:	DESKTOP-ZZTOP
GUID accesso:	{00000000-0000-0000-0000-000000000000}

Server di destinazione:

Nome server di destinazione:	[REDACTED]
Informazioni aggiuntive:	[REDACTED]

Informazioni sul processo:

ID processo:	0x4
Nome processo:	

Informazioni di rete:

Indirizzo di rete:	192.168.1.15
Porta:	445

Questo evento viene generato quando un processo tenta di far accedere un account specificando esplicitamente le credenziali dell'account. Generalmente si verifica in configurazioni di tipo batch, ad esempio attività pianificate, oppure quando si utilizza il comando RUNAS.

Nome registro: Sicurezza  
Origine: Microsoft Windows security Registrato: 28/12/2022 14:04:38  
ID evento: 4648 Categoria attività: Logon  
Livello: Informazioni Parole chiave: Controllo riuscito  
Utente: N/D Computer: DESKTOP-ZzTop  
Opcode: Informazioni  
Altre informazioni: [Guida registro eventi](#)

Copia Chiudi

# Windows Event

Proprietà evento - Evento 4624, Microsoft Windows security auditing.

**Generale** **Dettagli**

Accesso di un account riuscito.

Soggetto:

ID sicurezza:	SYSTEM
Nome account:	DESKTOP-ZZTOPS
Dominio account:	WORKGROUP
ID accesso:	0x3E7

Informazioni di accesso:

Tipo di accesso:	2	← Logon Type
Modalità amministrativa limitata:	-	
Credential Guard remoto:	-	
Account virtuale:	No	
Token elevato:	No	

Livello rappresentazione: Rappresentazione

Nuovo accesso:

ID sicurezza:	DESKTOP-ZZTOP\XxX
Nome account:	XxX
Dominio account:	DESKTOP-ZZTOP
ID accesso:	0x1BE1242
ID accesso collegato:	0x1BE120A
Nome account di rete:	-
Dominio account di rete:	-
GUID accesso:	{00000000-0000-0000-0000-000000000000}

Informazioni sul processo:

ID processo:	0xc08
Nome processo:	C:\Windows\System32\svchost.exe

Informazioni di rete:

Nome Workstation:	DESKTOP-ZZTOP
Indirizzo rete di origine:	127.0.0.1
Porta di origine:	0

Informazioni di autenticazione dettagliate:

Processo di accesso:	User32
Pacchetto di autenticazione:	Negotiate
Servizi transitati:	-
Nome pacchetto (solo NTLM):	-
Lunghezza chiave:	0

Nome registro: Sicurezza  
 Origine: Microsoft Windows security  
 ID evento: 4624  
 Livello: Informazioni  
 Utente: N/D  
 Opcode: Informazioni  
 Altre informazioni: [Guida registro eventi](#)

Registrato: 28/12/2022 09:47:18  
 Categoria attività: Logon  
 Parole chiave: Controllo riuscito  
 Computer: DESKTOP-ZzTop

**EventID**      **Computer**      **Timestamp**      **Logon Type**      **Account**

**Copia**      **Chiudi**

# Windows Event

## **Tipo di accesso**

2 Interattivo (accesso alla tastiera e schermo del sistema)

3 Rete (cioè la connessione alla cartella condivisa in questo computer da altrove in rete)

4 Batch (attività pianificata)

5 Servizio (avvio del servizio)

7 Sblocco (postazione di lavoro non controllata con screen saver protetto da password)

8 - Network logon sending credentials in cleartext (Autenticazione con password non cifrata)

9 - Different credentials used than logged on user — RunAs/netonly (Accesso utente locale con credenziali diverse)

10 Remote Interactive (Servizi terminal, Desktop remoto o assistenza remota)

11 Cached Interactive (accesso con credenziali di dominio memorizzati nella cache)



# Windows Event

Per le attività di analisi forensi, security.evtx è sicuramente il file più utile in quanto contiene log di accesso, creazione/modifica utenti e gruppi, modifiche dei privilegi degli account, modifiche di policy, accesso a share e cartelle e altri tipi di informazioni, tutti relativi alla sicurezza del sistema.

Per ogni log esiste la possibilità di loggare sia gli eventi avvenuti con successo, sia quelli falliti.

I principali eventi di security sono questi:

# Windows Event

## SECURITY EVENT CATEGORY

- **Account Logon:** eventi archiviati nel sistema che ha autorizzato l'accesso (ovvero, controller di dominio o sistema locale per account non di dominio)
- **Account Management:** manutenzione e modifiche dell'account
- **Directory Service:** Tentativo di accesso agli oggetti di Active Directory
- **Logon Events:** ogni istanza di accesso/disconnessione sul sistema locale
- **Object Access:** Accesso agli oggetti identificati nel system access control list
- **Policy Change:** Modifica dei diritti utente, delle politiche di controllo o delle politiche di attendibilità
- **Privilege Use:** Ogni caso di un account che esercita un diritto utente
- **Process Tracking:** Avvio del processo, uscita, accesso agli oggetti, ecc.
- **System Events:** Avvio e arresto del sistema; azioni che influiscono sul registro di sicurezza

# Windows Event

## Event ID rilevanti per le indagini

- EventID 1102 (The audit log was cleared), segnala che è stata effettuata la cancellazione dei log Security. È una delle tipiche azioni dell'attaccante effettuate per cancellare le proprie tracce.
- EventID 1100 identifica l'arresto dell'event logging che avviene subito prima di uno shutdown del sistema.
- EventID 4704 (A user right was assigned), fa parte della categoria “Policy Change” e viene generato quando vengono modificati i diritti di un utente.
- EventID 4738 (A user account was changed), fa parte della categoria “Account Management”. Evento che traccia chi e quali modifiche sono state apportate ad un account.
- EventID 4720 / 4726: An account was created / deleted
- EventID 4634/4647: Successful Logoff
- EventID 4648: Logon using explicit credentials (RunAs)
- EventID 4740 (A user account was locked out), fa parte della categoria “Account Management” e segnala che un account è stato bloccato a causa di ripetuti tentativi di accesso con password errata.

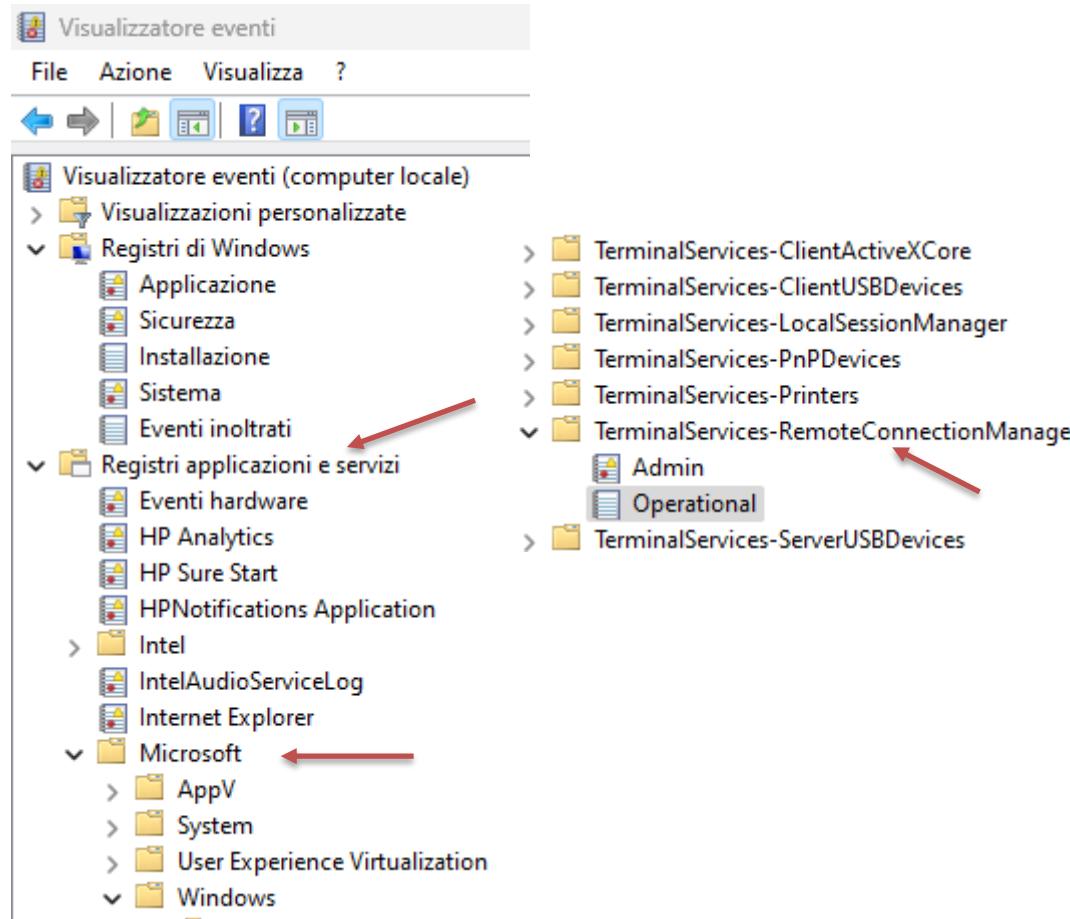
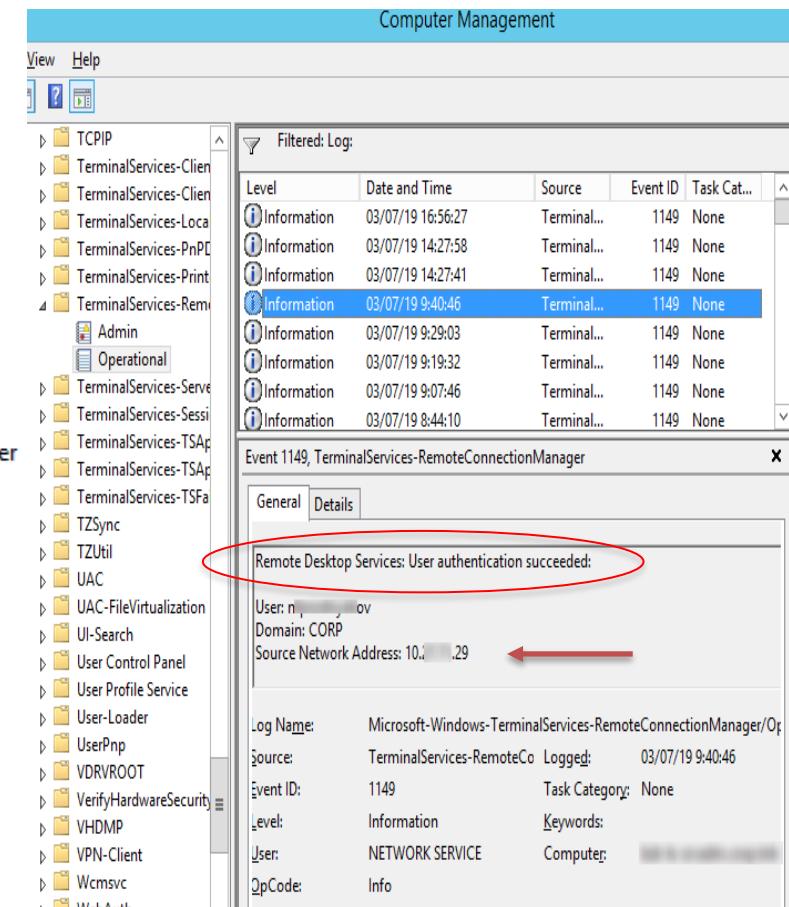
# Windows Event

## Event ID rilevanti per le indagini

- EventID 4624 (An account was successfully logged on).
- EventID 4625 (An account failed to log on), fa parte della categoria “Logon/Logoff”. Utili per individuare e monitorare tutti i tentativi di logon falliti.
- EventID 4672 (Special privileges assigned to new logon), fa parte della categoria “Logon/Logoff” e viene registrato a seguito di un evento 4624. È utile per monitorare l’accesso di un “super user” cioè degli Amministratori di Sistema.
- EventID 1149 RDP Connection (User authentication succeeded) evento molto importante per vedere se qualcuno si è connesso con Remote Desktop al Pc
- EventID 4778 indica che una sessione RDP è stata riconnessa.
- EventID 4779 indica che una sessione remota è stata disconnessa.
- EventID 4798 (A user’s local group membership was enumerated).
- EventID 4799 (A security-enabled local group membership was enumerated).

Fanno parte della categoria “Account Management”. Il primo (4798) si genera quando un processo enumera i gruppi locali alla quale l’utente appartiene, il secondo evento (4799) si genera quando un processo enumera i membri di un “gruppo locale”. Entrambi gli eventi possono indicare una attività tipica di un attaccante che ha compromesso un PC e vuole verificare ed esaminare gli account locali.

# Windows Event

The screenshot shows the Computer Management console with the "Filtered Log" window open. The log table shows several events, with the last one highlighted:

Level	Date and Time	Source	Event ID	Task Cat...
Information	03/07/19 16:56:27	Terminal...	1149	None
Information	03/07/19 14:27:58	Terminal...	1149	None
Information	03/07/19 14:27:41	Terminal...	1149	None
Information	03/07/19 9:40:46	Terminal...	1149	None
Information	03/07/19 9:29:03	Terminal...	1149	None
Information	03/07/19 9:19:32	Terminal...	1149	None
Information	03/07/19 9:07:46	Terminal...	1149	None
Information	03/07/19 8:44:10	Terminal...	1149	None

The detailed view for Event ID 1149, source "TerminalServices-RemoteConnectionManager", shows the following information:

General Details

Remote Desktop Services: User authentication succeeded:  
 User: n...ov  
 Domain: CORP  
 Source Network Address: 10.1.1.29

Log Name: Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational  
 Source: TerminalServices-RemoteConnectionManager  
 Event ID: 1149  
 Level: Information  
 User: NETWORK SERVICE  
 OpCode: Info  
 Logged: 03/07/19 9:40:46  
 Task Category: None  
 Keywords: Computer: [redacted]

A red circle highlights the message "Remote Desktop Services: User authentication succeeded:" and a red arrow points to the "Source Network Address" field.

# Windows Event

Ultimate IT SECURITY

December 2022 Patch Tuesday "Patch Tuesday - And Another Year" SuperCHARGER

User name:   
Password:   
[Login](#) / [Forgot?](#)  
[Register](#)

Security Log Windows SharePoint SQL Server Exchange | Training Tools Newsletter Webinars Blog

Webinars Training Encyclopedia Quick Reference Book

**Encyclopedia**

- Event IDs
- All Event IDs
- Audit Policy

Go To Event ID:  Go

Security Log Quick Reference Chart  
  
Download now!

Tweet

Share 

## Windows Security Log Events

All Sources  Windows Audit  SharePoint Audit (LOGbinder for SharePoint)  SQL Server Audit (LOGbinder for SQL Server)  Exchange Audit (LOGbinder for Exchange)  Sysmon (MS Sysinternals Sysmon)

Windows Audit Categories: All categories Subcategories: All subcategories

Windows Versions: All events Win2000, XP and Win2003 only Win2008, Win2012R2, Win2016 and Win10+, Win2019

Category: All

Windows 1100 The event logging service has shut down.  
Windows 1101 Audit events have been dropped by the transport.  
Windows 1102 The audit log was cleared.  
Windows 1104 The security Log is now full.  
Windows 1105 Event log automatic backup.  
Windows 1108 The event logging service encountered an error.  
Windows 4608 Windows is starting up.  
Windows 4609 Windows is shutting down.  
Windows 4610 An authentication package has been loaded by the Local Security Authority.  
Windows 4611 A trusted logon process has been registered with the Local Security Authority.  
Windows 4612 Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.  
Windows 4614 A notification package has been loaded by the Security Account Manager.  
Windows 4615 Invalid use of LPC port.  
Windows 4616 The system time was changed.  
Windows 4618 A monitored security event pattern has occurred.  
Windows 4621 Administrator recovered system from CrashOnAuditFail.  
Windows 4622 A security package has been loaded by the Local Security Authority.  
Windows 4624 An account was successfully logged on.  
Windows 4625 An account failed to log on.  
Windows 4626 User/Device claims information.  
Windows 4627 Group membership information.  
Windows 4634 An account was logged off.  
Windows 4646 IKE DoS-prevention mode started.  
Windows 4647 User initiated logoff.

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>

# Browser Forensics – Google Chrome



Google Chrome è stato introdotto nel 2008, è diventato molto diffuso, grazie soprattutto alla sua interfaccia semplice, alla profonda integrazione con i prodotti Google. Chrome è basato sul motore di layout WebKit, utilizzato anche dal browser Apple Safari e Microsoft Edge. Dal punto di vista forense, tutti gli artefatti di Chrome sono archiviati in un'unica posizione, sotto il profilo dell'utente:

Windows XP

*"%userprofile%\Impostazioni locali\Dat applicazioni\Google\Chrome\User Data\Default"*

Windows 7 in poi

*"%userprofile%\AppData\Local\Google\Chrome\User Data\Default"*

La maggior parte degli artefatti conservati da Chrome si trova in database SQLite, il che li rende facilmente accessibili. I dati memorizzati non sono sempre nella forma più leggibile. Ad esempio i timestamp sono in formato Webkit Time e devono essere convertiti. Per i dati come le preferenze, i segnalibri e le estensioni caricate, il browser utilizza il codice JSON.

Chrome memorizza un gran numero di informazioni sulla cronologia in diversi file SQLite archiviati nella cartella \User Data\Default. (I database SQLite utilizzati da Chrome non hanno estensioni di file).

## DB History

La cronologia del browser Chrome viene memorizzata nel file History per 90 giorni.

Il database della History memorizza anche informazioni quali la cronologia dei download (gestore dei download), il completamento automatico (download manager) e i segmenti.

Questi ultimi vengono utilizzati per identificare le pagine visitate maggiormente.

Per analizzare il database possiamo utilizzare sia un programma che legge i DB Sqlite, sia il programma della Nirsoft Chrome History View.

I programmi possono essere scaricati da:

<https://sqlitebrowser.org/>

[https://www.nirsoft.net/utils/chrome\\_history\\_view.html](https://www.nirsoft.net/utils/chrome_history_view.html)



# Browser Forensics – Google Chrome

ChromeHistoryView

File Edit View Options Help

URL	Title	Visited On	Visit Count	Typed Count	Referrer	Visit Duration	Visit ID	Profile	URL Length	Transition Type	Transition Qualifiers	History File
https://www.redhotcyber.com/	Home Page - Red Hot Cyber	05/12/2022 12:43:39	26	1		00:00:32.499	79	Default	28	Auto Bookmark	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/	Home Page - Red Hot Cyber	07/12/2022 11:08:45	26	1			182	Default	28	Auto Bookmark	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/	Home Page - Red Hot Cyber	14/12/2022 16:06:29	26	1			545	Default	28	Auto Bookmark	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/	Home Page - Red Hot Cyber	09/12/2022 07:56:14	26	1			224	Default	28	Auto Bookmark	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/	Home Page - Red Hot Cyber	24/01/2023 07:15:41	26	1		06:40:15.287	1212	Default	28	Auto Bookmark	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/	Home Page - Red Hot Cyber	24/01/2023 13:55:57	26	1		00:00:09.754	1222	Default	28	Reload	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/	Home Page - Red Hot Cyber	12/12/2022 11:52:45	26	1		01:06:12.844	387	Default	28	Reload	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/#google_vignette	Il darknet si evolve: la droga verrà...	09/12/2022 07:56:38	10	0	https://www.redhotcyber.com/		226	Default	44	Link	Chain Start	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/#google_vignette	Il darknet si evolve: la droga verrà...	12/12/2022 07:36:06	10	0	https://www.redhotcyber.com/		304	Default	44	Link	Chain Start	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/#google_vignette	Il darknet si evolve: la droga verrà...	14/12/2022 16:06:50	10	0	https://www.redhotcyber.com/		546	Default	44	Link	Chain Start	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/#google_vignette	Il darknet si evolve: la droga verrà...	18/01/2023 08:59:34	10	0	https://www.redhotcyber.com/	00:00:09.424	1048	Default	44	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/#google_vignette	Il darknet si evolve: la droga verrà...	23/01/2023 08:01:36	10	0	https://www.redhotcyber.com/	00:00:34.105	1085	Default	44	Link	Chain Start	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/#google_vignette	Il darknet si evolve: la droga verrà...	07/12/2022 11:09:11	10	0	https://www.redhotcyber.com/		183	Default	44	Link	Chain Start	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/#google_vignette	Il darknet si evolve: la droga verrà...	05/01/2023 08:26:45	10	0	https://www.redhotcyber.com/		910	Default	44	Link	Chain Start	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/#google_vignette	Il darknet si evolve: la droga verrà...	10/01/2023 10:09:13	10	0	https://www.redhotcyber.com/		955	Default	44	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/#google_vignette	Il darknet si evolve: la droga verrà...	12/01/2023 08:20:16	10	0	https://www.redhotcyber.com/		1028	Default	44	Link	Chain Start	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/#google_vignette	Il darknet si evolve: la droga verrà...	27/12/2022 15:59:45	10	0	https://www.redhotcyber.com/		751	Default	44	Link	Chain Start	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/2/	Home Page - Red Hot Cyber	05/01/2023 08:26:47	11	0	https://www.redhotcyber.com/#google_vig...	00:00:25.683	911	Default	35	Link	Chain End,Client Redirect	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/2/	Home Page - Red Hot Cyber	05/12/2022 12:44:12	11	0	https://www.redhotcyber.com/	00:01:13.575	81	Default	35	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/2/	Home Page - Red Hot Cyber	09/12/2022 07:56:44	11	0	https://www.redhotcyber.com/#google_vig...	04:53:27.228	227	Default	35	Link	Chain End,Client Redirect	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/2/	Home Page - Red Hot Cyber	12/12/2022 07:36:09	11	0	https://www.redhotcyber.com/#google_vig...	00:14:46.038	305	Default	35	Link	Chain End,Client Redirect	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/2/	Home Page - Red Hot Cyber	07/12/2022 11:10:33	11	0	https://www.redhotcyber.com/#google_vig...	00:00:43.643	184	Default	35	Link	Chain End,Client Redirect	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/2/	Home Page - Red Hot Cyber	30/12/2022 07:01:48	11	0	https://www.redhotcyber.com/	00:00:14.723	868	Default	35	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/2/	Home Page - Red Hot Cyber	10/01/2023 10:17:41	11	0	https://www.redhotcyber.com/	00:02:55.110	957	Default	35	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/2/	Home Page - Red Hot Cyber	12/01/2023 08:20:19	11	0	https://www.redhotcyber.com/#google_vig...	00:00:15.711	1029	Default	35	Link	Chain End,Client Redirect	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/2/	Home Page - Red Hot Cyber	27/12/2022 15:59:48	11	0	https://www.redhotcyber.com/#google_vig...	00:00:24.677	752	Default	35	Link	Chain End,Client Redirect	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/2/	Home Page - Red Hot Cyber	18/01/2023 08:59:43	11	0	https://www.redhotcyber.com/#google_vig...	07:41:03.306	1049	Default	35	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/2/	Home Page - Red Hot Cyber	14/12/2022 16:06:52	11	0	https://www.redhotcyber.com/#google_vig...	00:00:11.907	547	Default	35	Link	Chain End,Client Redirect	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/2/#google_vig...	Home Page - Red Hot Cyber	30/12/2022 07:02:03	1	0	https://www.redhotcyber.com/page/2/		869	Default	51	Link	Chain Start	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/3/	Home Page - Red Hot Cyber	05/01/2023 08:27:10	3	0	https://www.redhotcyber.com/page/2/	00:00:24.935	912	Default	35	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/3/	Home Page - Red Hot Cyber	10/01/2023 10:18:06	3	0	https://www.redhotcyber.com/page/2/	00:00:23.769	958	Default	35	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/3/	Home Page - Red Hot Cyber	27/12/2022 16:00:12	3	0	https://www.redhotcyber.com/page/2/	00:13:47.272	753	Default	35	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/page/4/	Home Page - Red Hot Cyber	05/01/2023 08:27:35	1	0	https://www.redhotcyber.com/page/3/	00:00:13.392	914	Default	35	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/altre-265-milio...	Altri 265 milioni di euro di multa p...	05/12/2022 12:50:17	1	0	https://www.redhotcyber.com/post/attacco...	00:01:01.992	84	Default	105	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/attacco-inform...	Attacco informatico al Ministero d...	05/12/2022 12:45:05	1	0	https://www.redhotcyber.com/page/2/	00:05:11.504	82	Default	134	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/attacco-inform...	Attacco informatico all'Azienda O...	30/12/2022 07:02:13	1	0	https://www.redhotcyber.com/	05:35:33.728	871	Default	111	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/blocco-dei-voli...	Blocco dei voli negli Stati Uniti ca...	12/01/2023 08:20:15	1	0	https://www.redhotcyber.com/	00:00:46.328	1027	Default	110	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/dei-ricercatori...	Dei ricercatori di sicurezza scopri...	05/01/2023 08:24:40	1	0	https://www.redhotcyber.com/	00:01:05.598	909	Default	140	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/google-home-int...	Google Home compromesso e int...	05/01/2023 08:27:13	1	0	https://www.redhotcyber.com/page/2/	00:00:13.392	913	Default	100	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/il-darknet-si-ev...	Il darknet si evolve: la droga verrà...	23/01/2023 08:02:10	1	0	https://www.redhotcyber.com/#google_vig...	00:01:20.577	1089	Default	110	Link	Chain End,Client Redirect	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/il-server-di-co...	Il server di CommuteAir espone la ...	26/01/2023 07:30:00	1	0	https://www.redhotcyber.com/	00:01:02.891	1267	Default	159	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/interventi-chiru...	Interventi chirurgici rimandati". Si...	09/12/2022 07:56:27	1	0	https://www.redhotcyber.com/	00:01:46.088	225	Default	113	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/la-polizia-post...	La Polizia Postale smaschera una tr...	12/01/2023 08:20:35	1	0	https://www.redhotcyber.com/page/2/	00:01:52.744	1030	Default	107	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/litaliana-benet...	Attacco informatico al colosso ital...	23/01/2023 08:03:33	1	0	https://www.redhotcyber.com/	00:01:41.359	1092	Default	72	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/phisher-sofistic...	Phisher sofisticati ma un po' pastic...	01/12/2022 08:43:30	1	0	https://www.redhotcyber.com/	01:41:41.443	32	Default	129	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/ragnar-locker-s...	Ragnar Locker sbaglia target in Be...	05/12/2022 12:44:11	1	0	https://www.redhotcyber.com/	00:00:41.239	80	Default	127	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/ransomware-d...	Ransomware Data Room – Novem...	05/12/2022 12:45:26	1	0	https://www.redhotcyber.com/page/2/	00:05:55.087	83	Default	68	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/un-mercato-un...	Un mercato underground italiano ...	12/01/2023 08:20:10	1	0	https://www.redhotcyber.com/	00:01:55.316	1026	Default	123	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/uno-studio-cin...	Violato l'algoritmo RSA 2048? Sco...	05/01/2023 08:24:24	1	0	https://www.redhotcyber.com/	00:02:18.482	908	Default	95	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...
https://www.redhotcyber.com/post/vipersoftx-si-e...	ViperSoftX si è diffuso in Italia. 93...	01/12/2022 08:28:42	1	0	https://www.redhotcyber.com/	00:14:43.540	5	Default	142	Link	Chain Start,Chain End	C:\Users\XXX\AppData\Local\Google\Chro...

# Browser Forensics – Google Chrome

DB Browser for SQLite - C:\Users\XxX\Desktop\History

File Modifica Visualizza Strumenti Aiuto

Nuovo Database Apri Database Salva le modifiche Ripristina le modifiche Apri Progetto Salva Progetto Collega Database Chiudi Database

Struttura database Naviga nei dati Modifica Pragmas Esegui SQL

Tabella: urls

Filtra in qualsiasi colonna

	<b>id</b>	<b>url</b>	<b>title</b>	<b>visit_count</b>	<b>typed_count</b>	<b>last_visit_time</b>	<b>hidden</b>
	2071	https://www.altensione.net/...	Videocorso per sistemi Mikrotik	3	0	13319276399740625	0
	2072	https://www.altensione.net/	Il Metodo Reti IP Formula è il corso reti che ti ...	2	2	13319276313994647	0
	2073	https://www.altensione.net/home	Il Metodo Reti IP Formula è il corso reti che ti ...	2	0	13319276313994647	0
	2074	https://mail.google.com/mail/u/0/#inbox/...	Account Corsi MikroTik creato! - ...	2	0	13319276629739506	0
	2075	https://mail.google.com/mail/u/0/#inbox/...	Prodotti resi: risparmia fino al 50% - ...	2	0	13319276637262276	0
	2076	https://www.google.com/url?q=https://...	Amazon.it	1	0	13319276642904588	0
	2077	https://www.amazon.it/gp/r.html?...	Amazon.it	1	0	13319276642904588	0
	2078	https://www.amazon.it/gp/s?...	Amazon.it	1	0	13319276642904588	0
	2079	https://www.amazon.it/s?...	Amazon.it	1	0	13319276643660895	0
	2080	https://www.enel.it/	Entra nel Mercato Libero: Offerte Luce e Gas   E...	1	0	1331927669357968	0
	2081	https://www.enel.it/content/enel-it/it/login	Accesso all'Area Clienti Enel Energia	1	0	13319276677065524	0
	2082	https://www.enel.it/login	Accesso all'Area Clienti Enel Energia	1	0	13319276677065524	0
	2083	https://accounts.enel.com/samlssso		1	0	13319276689746217	0
	2084	https://www.enel.it/it/area-clienti/	area-clienti	1	0	13319276690466767	0
	2085	https://www.enel.it/content/enel-it/it/area-clienti.../	Forniture Area Clienti   Enel Energia	1	0	13319276694538720	0
	2086	https://www.enel.it/it/area-clienti/residenziale	Forniture Area Clienti   Enel Energia	2	0	13319276948289176	0
	2087	https://www.enel.it/it/area-clienti/residenziale/...	Bollette Area Clienti   Enel Energia	1	0	13319276701645221	0
	2088	file:///C:/Users/XxX/Downloads/...	Fattura_000004296225184.pdf	1	0	13319276722919363	0
	2089	https://www.enel.it/content/enel-it/it/area-clienti.../	Area Clienti Enel Energia	1	0	13319276962051298	0
	2090	https://www.enel.it/it/area-clienti/residenziale/...	Area Clienti Enel Energia	1	0	13319276962051298	0
	2091	https://www.enel.it/bin/samllogout?wso2=true	Entra nel Mercato Libero: Offerte Luce e Gas   E...	1	0	13319277012304051	0
	2092	https://accounts.enel.com/samlssso?...	Entra nel Mercato Libero: Offerte Luce e Gas   E...	1	0	13319277012304051	0
	2093	https://www.enel.it/bin/samllogout	Entra nel Mercato Libero: Offerte Luce e Gas   E...	1	0	13319277012304051	0
	2094	https://www.enel.it/it	Entra nel Mercato Libero: Offerte Luce e Gas   E...	1	0	13319277012304051	0
	2095	https://www.bmedonline.it/ecm/?login=true	Banca Mediolanum S.p.A.   Accesso clienti	3	0	13319277268094633	0
	2096	https://www.bmedonline.it/ecm/homed_new.ht...	BMedOnline   NewUi	2	0	13319277043221939	0
	2097	https://sso-c-pro.mediolanum.it/oam/server/...	BMedOnline   NewUi	1	0	13319277043221939	0
	2098	https://www.bmedonline.it/obrar.cgi?...	BMedOnline   NewUi	1	0	13319277043221939	0
	2099	https://www.bmedonline.it/lr/	BMedOnline   NewUi	1	0	13319277044997916	0
	2100	https://www.bmedonline.it/lr/ib-production-v2	BMedOnline   NewUi	2	0	13319277044997916	0

DCode v5.5

File Tools Theme Help

Time Decoding Time Encoding

Name	Timestamp
⌚ Apple Absolute Time (ns) (UTC)	2001-06-04 03:47:56.6770655 Z
⌚ Apple Absolute Time (ns)	2001-06-04 05:47:56.6770655 +02:00
⌚ Chromium Time Microseconds (UTC)	2023-01-27 07:04:37.0655240 Z
⌚ Chromium Time Microseconds	2023-01-27 08:04:37.0655240 +01:00
⌚ Microsoft Ticks (Local)	0043-03-17 19:54:27.7065524
⌚ Unix Microseconds (UTC)	2392-01-27 07:04:37.0655240 Z
⌚ Unix Microseconds	2392-01-27 08:04:37.0655240 +01:00
⌚ Windows Filetime (UTC)	1643-03-17 19:54:27.7065524 Z
⌚ Windows Filetime	1643-03-17 20:54:27.7065524 +01:00

Chrome memorizza l'ora nel formato Webkit come Safari e Opera. Il formato Webkit memorizza il numero di microsecondi dalla mezzanotte UTC del 1° gennaio 1601. Per decodificarlo è possibile utilizzare Dcode scaricabile da <https://www.digital-detective.net/dcode/>

# Browser Forensics – Google Chrome

Domande Investigative	History
Qual è l'Url Visitata	urls
Titolo pagina visitata	urls -> title
Quando è stato visitato il sito per la prima volta?	visits -> visit_time
Quando è stato visitato il sito per l'ultima volta?	urls -> last_visit_time
Quante visite sono state effettuate al sito?	urls -> visit_count

# Browser Forensics – Google Chrome

Altro file interessante ai fini investigativi è la cache di Chrome che contiene numerose file scaricati dai siti web che abbiamo visitato, nella cache troviamo oltre alla pagine web anche video, foto e audio.

Tramite il programma Chrome Cache View ([https://www.nirsoft.net/utils/chrome\\_cache\\_view.html](https://www.nirsoft.net/utils/chrome_cache_view.html)) possiamo visualizzare queste informazioni.

La cache di Chrome si trova nel percorso :

*"%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Cache*



# Browser Forensics – Google Chrome

Filename	URL	Content Type	File Size	Last Accessed	Server Last Modified	Server Name	Server Response	Web Site	Content En...	Cache Name	Server IP Address	Deleted File
135.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		790.233	01/02/2023 13:53:10	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000448	8.241.93.122	No	
135532930-2191...	https://img-prod.tgcom24.mediaset.it/images/2023/01/31/135532930-21912ee6-9ead-4...	image/jpeg	16.258	01/02/2023 13:43:17	31/01/2023 14:55:34	AmazonS3	HTTP/1.1 200	https://mediaset.it	data_3 [25223168]	81.74.231.138	No	
136.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		851.824	01/02/2023 13:53:13	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000449	8.241.93.122	No	
136.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		24.386	01/02/2023 13:53:13	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_00044a	8.241.93.122	No	
137.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		824.497	01/02/2023 13:53:16	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_00044b	8.241.93.122	No	
137.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		24.293	01/02/2023 13:53:16	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_00044c	8.241.93.122	No	
138.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		24.205	01/02/2023 13:53:19	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_00044d	8.241.93.122	No	
138.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		903.314	01/02/2023 13:53:19	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_00044e	8.241.93.122	No	
139.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		24.683	01/02/2023 13:53:22	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_00044f	8.241.93.122	No	
139.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		531.405	01/02/2023 13:53:22	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000450	8.241.93.122	No	
14.jpg.jifif	https://maptiles.shodan.io/data/openmaptiles_satellite/5/7/14.jpg	image/jpeg	9.320	01/02/2023 14:43:15	18/08/2019 23:26:30	cloudflare	HTTP/1.1 200	https://shodan.io	data_3 [1941504]	104.18.13.238	No	
14.jpg.jifif	https://maptiles.shodan.io/data/openmaptiles_satellite/5/5/14.jpg	image/jpeg	1.555	01/02/2023 14:43:15	18/08/2019 23:26:30	cloudflare	HTTP/1.1 200	https://shodan.io	data_2 [1075200]	104.18.13.238	No	
14.jpg.jifif	https://maptiles.shodan.io/data/openmaptiles_satellite/5/11/14.jpg	image/jpeg	2.309	01/02/2023 14:43:15	18/08/2019 23:26:30	cloudflare	HTTP/1.1 200	https://shodan.io	data_2 [7700480]	104.18.13.238	No	
14.jpg.jifif	https://maptiles.shodan.io/data/openmaptiles_satellite/5/2/14.jpg	image/jpeg	2.300	01/02/2023 14:43:15	18/08/2019 23:26:30	cloudflare	HTTP/1.1 200	https://shodan.io	data_2 [7757824]	104.18.13.238	No	
14.jpg.jifif	https://maptiles.shodan.io/data/openmaptiles_satellite/5/3/14.jpg	image/jpeg	1.285	01/02/2023 14:43:15	18/08/2019 23:26:30	cloudflare	HTTP/1.1 200	https://shodan.io	data_2 [7659520]	104.18.13.238	No	
14.jpg.jifif	https://maptiles.shodan.io/data/openmaptiles_satellite/5/9/14.jpg	image/jpeg	7.847	01/02/2023 14:43:15	18/08/2019 23:26:30	cloudflare	HTTP/1.1 200	https://shodan.io	data_3 [2031616]	104.18.13.238	No	
14.jpg.jifif	https://maptiles.shodan.io/data/openmaptiles_satellite/5/6/14.jpg	image/jpeg	4.659	01/02/2023 14:43:15	18/08/2019 23:26:30	cloudflare	HTTP/1.1 200	https://shodan.io	data_3 [8536064]	104.18.13.238	No	
14.jpg.jifif	https://maptiles.shodan.io/data/openmaptiles_satellite/5/10/14.jpg	image/jpeg	4.611	01/02/2023 14:43:15	18/08/2019 23:26:30	cloudflare	HTTP/1.1 200	https://shodan.io	data_3 [2498560]	104.18.13.238	No	
14.jpg.jifif	https://maptiles.shodan.io/data/openmaptiles_satellite/5/4/14.jpg	image/jpeg	1.201	01/02/2023 14:43:15	18/08/2019 23:26:30	cloudflare	HTTP/1.1 200	https://shodan.io	data_2 [5079040]	104.18.13.238	No	
14.jpg.jifif	https://maptiles.shodan.io/data/openmaptiles_satellite/5/8/14.jpg	image/jpeg	8.905	01/02/2023 14:43:15	18/08/2019 23:26:30	cloudflare	HTTP/1.1 200	https://shodan.io	data_3 [1974272]	104.18.13.238	No	
14.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		817.756	01/02/2023 13:44:20	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000354	8.241.93.122	No	
14.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		24.744	01/02/2023 13:44:20	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000355	8.241.93.122	No	
140.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		24.393	01/02/2023 13:53:25	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000452	8.241.93.122	No	
140.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		861.601	01/02/2023 13:53:25	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000451	8.241.93.122	No	
141.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		836.300	01/02/2023 13:53:28	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000454	8.241.93.122	No	
141.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		24.214	01/02/2023 13:53:28	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000453	8.241.93.122	No	
142.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		24.609	01/02/2023 13:53:31	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000456	8.241.93.122	No	
142.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		849.459	01/02/2023 13:53:31	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000455	8.241.93.122	No	
143.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		757.912	01/02/2023 13:53:34	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000458	8.241.93.122	No	
143.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		24.308	01/02/2023 13:53:34	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000457	8.241.93.122	No	
143122.htm	https://forum.qnap.com/viewtopic.php?t=143122	text/html	18.453	01/02/2023 14:41:34	01/01/1601 01:00:00	Apache	HTTP/1.1 200 OK	https://qnap.com	gzip	f_000802	113.196.74.119	No
143128077-101b...	https://img-prod.tgcom24.mediaset.it/images/2023/01/31/143128077-101b0536-763f-4...	image/jpeg	9.123	01/02/2023 13:43:36	31/01/2023 15:31:34	AmazonS3	HTTP/1.1 200	chrome-extension://m...	data_3 [26157056]	81.74.224.43	No	
143128077-101b...	https://img-prod.tgcom24.mediaset.it/images/2023/01/31/143128077-101b0536-763f-4...	image/jpeg	9.123	01/02/2023 13:43:36	31/01/2023 15:31:34	AmazonS3	HTTP/1.1 200	https://mediaset.it	data_3 [24715264]	81.74.231.138	No	
144.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		931.183	01/02/2023 13:53:37	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_00045a	8.241.93.122	No	
144.m4s	https://vod05.msf.cdn.mediaset.net/farmunica/2023/01/1252217_18608e8d845f89/dashr...		24.359	01/02/2023 13:53:36	31/01/2023 18:44:23	origin/0.1-	HTTP/1.1 200	https://mediaset.it	f_000459	8.241.93.122	No	

# Browser Forensics – Google Chrome



Visualizza il  
file Online

Copia il file  
dalla Cache

Basic Settings

Camera Name:	Megapixel IP cam
Primary Stream:	Codec: H264
	Resolution: QSXGA (2592x1944)
	Bit Rate: 8000 kbps (500~10000)
	Frame Rate: 10 FPS
	I-frame Interval: 1 ~ 5
Secondary Stream:	Codec: OFF
	Resolution: ...
	Bit Rate: 4000 Kbps (500~4000)
	Frame Rate: 30 FPS
	I-frame Interval: 1 ~ 5
Third Stream:	Codec: MJPEG
	Resolution: VGA (640x480)

Immagine presente nella Cache

ChromeCacheView: C:\Users\XxX\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache

File Edit View Options Help

Filename	URL
95.pb	<a href="https://maptiles.shodan.io/data/v3/8/137/95.pb">https://maptiles.shodan.io/data/v3/8/137/95.pb</a>
3.19	<a href="https://app.gitbook.com/public/fonts/SourceCodePro/SourceCodePro-Bold.woff">https://app.gitbook.com/public/fonts/SourceCodePro/SourceCodePro-Bold.woff</a>
3.19	<a href="https://app.gitbook.com/public/fonts/SourceCodePro/SourceCodePro-Medium.woff">https://app.gitbook.com/public/fonts/SourceCodePro/SourceCodePro-Medium.woff</a>
26.pb	<a href="https://maptiles.shodan.io/data/v3/6/15/26.pb">https://maptiles.shodan.io/data/v3/6/15/26.pb</a>
366.pb	<a href="https://maptiles.shodan.io/data/v3/10/535/366.pb">https://maptiles.shodan.io/data/v3/10/535/366.pb</a>
155_camera_cod...	<a href="https://www.unifore.net/images/article/155_camera_codec.jpg.jfif">https://www.unifore.net/images/article/155_camera_codec.jpg.jfif</a>
155_camera_cod...	<a href="https://www.unifore.net/images/article/155_camera_codec.jpg.jfif">https://www.unifore.net/images/article/155_camera_codec.jpg.jfif</a>
3.19	<a href="https://app.gitbook.com/public/fonts/SourceCodePro/SourceCodePro-Black.woff">https://app.gitbook.com/public/fonts/SourceCodePro/SourceCodePro-Black.woff</a>

# Browser Forensics – Google Chrome

Properties

<b>Filename:</b>	155_camera_codec.jpg.jfif
<b>URL:</b>	<a href="https://www.unifore.net/images/article/155_camera_codec.jpg.jfif">https://www.unifore.net/images/article/155_camera_codec.jpg.jfif</a>
<b>Content Type:</b>	image/jpeg
<b>File Size:</b>	58.036
<b>Last Accessed:</b>	01/02/2023 14:16:14
<b>Server Time:</b>	01/02/2023 14:16:13
<b>Server Last Modified:</b>	17/07/2015 05:21:28
<b>Expire Time:</b>	08/12/2023 06:24:48
<b>Server Name:</b>	cloudflare
<b>Server Response:</b>	HTTP/1.1 200
<b>Web Site:</b>	<a href="https://unifore.net">https://unifore.net</a>
<b>Frame:</b>	<a href="https://unifore.net">https://unifore.net</a>
<b>Content Encoding:</b>	
<b>Cache Name:</b>	f_0005e2
<b>Cache Control:</b>	public, max-age=31536000, proxy-revalidate
<b>ETag:</b>	
<b>Server IP Address:</b>	172.67.153.173
<b>URL Length:</b>	59
<b>Deleted File:</b>	No

**OK**

**Last Accessed:** Fornisce la data e l'ora in cui il contenuto nella cache è stato richiesto e visualizzato per l'ultima volta dall'utente.

**Server Time:** l'ora in cui il file memorizzato nella cache è stato salvato su disco; è un'indicazione della prima volta che la pagina URL è stata visualizzata.

**Server Last Modified:** Indica quando la versione più recente della pagina o del file è stata modificata sul server web. I server Web restituiscono questo timestamp come parte delle intestazioni di risposta http.

**Expire Time:** viene impostato dal sito web che fornisce il contenuto, consentendogli di stabilire la durata di vita prevista per la pagina. I processi analizzano frequentemente la cache ed eliminano i contenuti in cache che sono scaduti.

Tutti gli orari sono memorizzati in UTC.

# Browser Forensics – Google Chrome

## Cookie

I cookie permettono di capire quali siti web sono stati visitati e quali attività sono state svolte.

Sono piccoli file di testo (< 4 KB) memorizzati per personalizzare l'esperienza dell'utente sul sito web.

I cookie forniscono all'investigatore le seguenti informazioni:

- Sito web di emissione (ad esempio, facebook.com)
- Account utente responsabile (ad esempio, francesco)
- Orario di creazione e di ultimo accesso del cookie
- Tutti i dati che il sito web desidera includere nel file di testo.

Ricordate che vengono salvati solo i cookie persistenti!

I cookie sono fondamentali per il web e forniscono un interessante archivio di informazioni all'investigatore forense.

I cookie consentono di ricordare i dati di autenticazione in modo che non debbano essere inseriti in ogni pagina.

I cookie si trovano nel percorso *C:\Users\XxX\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb*

# Browser Forensics – Google Chrome

## Cookie

Cosa possiamo ricavare dall'analisi dei cookie?

Possiamo ricostruire un elenco di siti web visitati da uno specifico profilo utente (tutti i dati del browser sono memorizzati per account utente).

Per ogni sito web, possiamo identificare la prima e l'ultima volta che è stato visitato (anche se altri artefatti come la cronologia del browser possono fornire una visione più completa).

Potremmo essere in grado di visualizzare le informazioni memorizzate nel cookie stesso, a partire dalla versione di Chrome V33 i valori dei cookie sono criptati. Chrome utilizza le librerie di crittografia di Windows (DPAPI) per eseguire la crittografia. In questo modo, ogni dato crittografato nel database è legato all'autenticazione Windows dell'utente.

E' ancora possibile decodificare i Cookie effettuando un'estrazione live, tramite il software Hindsight Crome Forensics Tools scaricabile da (<https://github.com/obsidianforensics/hindsight>)

# Browser Forensics – Google Chrome



Lanciamo il programma Hindsight, che aprirà un server web al percorso `http://localhost:8080/`, nella pagina ci chiede il percorso del profilo da analizzare.

Per vedere il percorso andiamo su una pagina di Chrome e digitiamo `chrome://version/` si apre la schermata dove vediamo il percorso del profilo da inserire nel programma.



# Hindsight

Web Artifact Analysis

Hindsight is a free tool for analyzing web artifacts. To get started, select the 'Input Type' below and fill out the 'Input Path' field. Review the plugins and options on the right, and hit the 'Run' button at the bottom.

**Inputs**

**Input Type:** Chrome

**Profile Path:**

**Cache Path:**

**Description:** Chrome is a free web browser from Google that runs on Windows, macOS, Linux, ChromeOS, iOS, and Android. Each user's web history and configuration information is stored under their user directory, so there may be multiple sets of browser data on the system. 

**Available Decryption:** Windows  Mac  Linux

**Default Locations:**

- Windows XP: \[userdir]\Local Settings\Application Data\Google\Chrome\User Data
- Vista/7/8/10: \[userdir]\AppData\Local\Google\Chrome\User Data
- Linux: \[userdir]/.config/google-chrome
- OSX/macOS: \[userdir]\Library\Application Support\Google\Chrome\Default
- iOS: Applications\com.google.chrome.ios\Library\Application Support\Google\Chrome
- Android: /userdata/data/com.android.chrome/app\_chrome

**Plugin Selector**

- Chrome Extension Names [v20210424]
- Generic Timestamp Decoder [v20160907]
- Google Analytics Cookie Parser [v20170130]
- Google Searches [v20160912]
- Load Balancer Cookie Decoder [v20200213]
- Quantcast Cookie Parser [v20160907]
- Query String Parser [v20170225]
- Time Discrepancy Finder [v20170129]
- Unfurl [v20210424]

**Options Selector**

Log Path:

Timezone:

Copy files before opening?

Temp Path:

# Browser Forensics – Google Chrome



## Results

Hindsight - Web Artifact Analysis

### Summary

Input Path: C:\Users\Xxx\AppData\Local\Google\Chrome\User Data\Profile 1  
 Input Type: Chrome  
 Profile Paths:  
     • C:\Users\Xxx\AppData\Local\Google\Chrome\User Data\Profile 1

### Parsed Artifacts

Detected Chrome version:	95-96
URL records:	565
Download records:	2
Cache records:	0
GPU Cache records:	0
Local Storage records:	523
Bookmark records:	2
Autofill records:	2
Login Data records:	1
Preference Items:	231
Extensions:	14
Extension Cookie records:	7
Session Storage records:	405
Site Characteristics records:	110
File System Items:	2

### Plugin Results

Chrome Extension Names [v20210424]:	- 23 extension URLs parsed -
Generic Timestamp Decoder [v20160907]:	- 0 timestamps parsed -
Google Analytics Cookie Parser [v20170130]:	- 0 cookies parsed -
Google Searches [v20160912]:	- 195 searches parsed -
Load Balancer Cookie Decoder [v20200213]:	- 0 cookies parsed -
Quantcast Cookie Parser [v20160907]:	- 0 cookies parsed -
Query String Parser [v20170225]:	- 142 query strings parsed -
Time Discrepancy Finder [v20170129]:	- 0 differences parsed -
Unfurl [v20210424]:	- 27 values parsed -

[Save XLSX](#) [Save JSONL](#) [Save SQLite DB](#)

[View SQLite DB in Browser](#)

[Start New Analysis Session](#)

Una volta terminata l'elaborazione,  
 possiamo visualizzare i dati salvandoli  
 in un file Excel, Json o Database Sql,  
 per la successiva analisi.



GRAZIE PER L'ATTENZIONE