

Università degli Studi di Salerno

Dipartimento di Informatica

Analisi Artefatti di Windows

_ X

Corso@di# Digital Forensics |

Raffaele Pizzolante
Seminario Didattico



Importanza degli Artefatti di Windows

Importanza degli Artefatti di Windows | 1/6

- Un sistema operativo è un software particolarmente **complesso** ed **articolato**
- Se adeguatamente supportato, è in **continua evoluzione**
 - Sono previsti **aggiornamenti** di diverse tipologie
 - Nuove release/major release
 - Cadenza semestrale o annuale
 - Minor release/aggiornamenti cumulativi
 - Patch di sicurezza
 - Implementazione di feature
 - Aggiornamenti relativi al software di sistema

Importanza degli Artefatti di Windows | 2/6

- Durante l'esecuzione di un S.O., vengono utilizzate diverse strutture
 - Alcune sono direttamente accessibili (o parzialmente accessibili) dall'utente
 - Altre strutture sono accessibili ed utilizzabili esclusivamente al S.O.
- All'interno di tali strutture, possono esservi diversi artefatti (file, stringhe di testo, ecc.), i quali vengono memorizzati dal S.O., per diversi obiettivi

Importanza degli Artefatti di Windows | 2/6

- Migliorare l'esperienza dell'utente e/o agevolare alcune azioni dell'utente
- Migliorare le performance di sistema
- Ricordare alcune azioni dell'utente, per fornire adeguati suggerimenti, in futuro, ottimizzando l'operatività dell'utente stesso

- All'interno di tali strutture, possono esservi diversi **artefatti** (file, stringhe di testo, ecc.), i quali vengono memorizzati dal S.O., per

diversi obiettivi:

Importanza degli Artefatti di Windows | 3/6

- Durante l'investigazione forense, è **necessario analizzare gli artefatti**, siano essi prodotti, in automatico, dal sistema o dall'utente (direttamente e/o indirettamente)
- Da essi è possibile delineare delle ipotesi sul comportamento dell'utente

OSSERVAZIONE

- È sempre utile avere più conferme possibili alle ipotesi
 - Le conferme dovrebbero provenire da più fonti indipendenti di tracce (ad esempio, artefatti reperiti da strutture diverse, ecc.)

Importanza degli Artefatti di Windows | 3/6

- Durante l'investigazione forense, è necessario analizzare gli artefatti, siano essi prodotti, in automatico, dal sistema o dall'utente (direttamente e/o

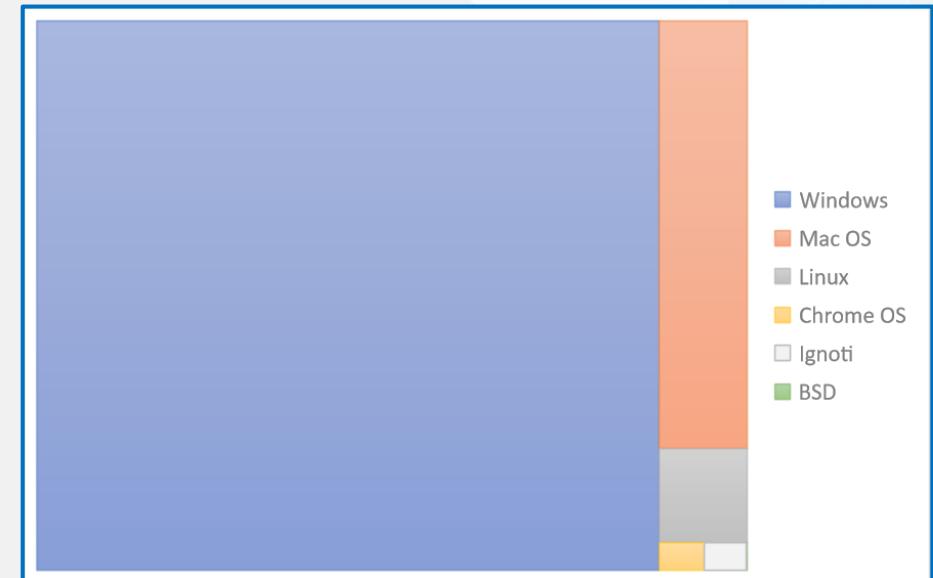
L'investigazione forense dei sistemi basati su **Microsoft™ Windows®**, risulta particolarmente importante, in virtù della diffusione di quest'ultimo (anche in contesti organizzativi)

- Le conferme dovrebbero provenire da più fonti indipendenti di tracce (ad esempio, artefatti reperiti da strutture diverse, ecc.)

Importanza degli Artefatti di Windows | 4/6

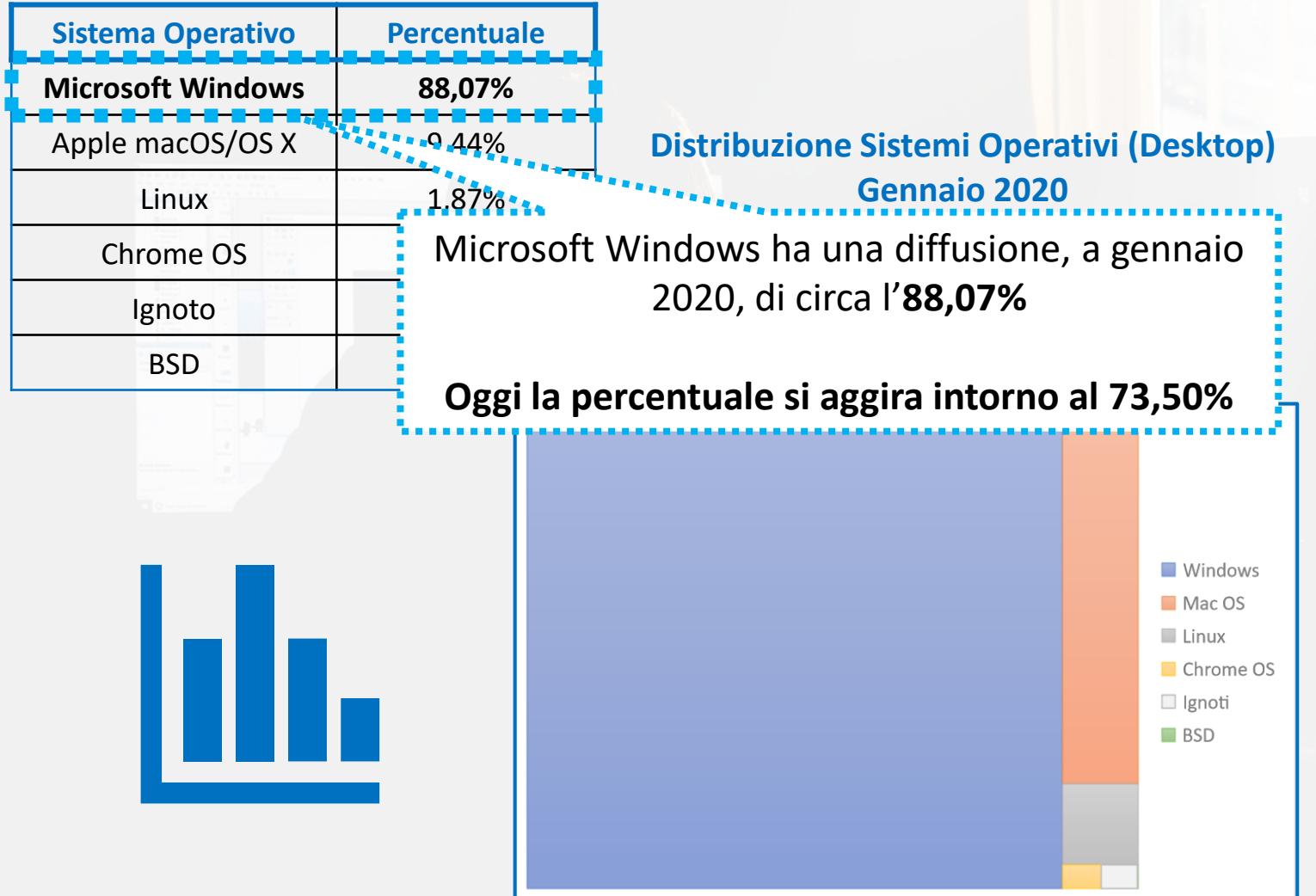
Sistema Operativo	Percentuale
Microsoft Windows	88,07%
Apple macOS/OS X	9,44%
Linux	1,87%
Chrome OS	0,41%
Ignoto	0,19%
BSD	0,02%

Distribuzione Sistemi Operativi (Desktop)
Gennaio 2020



Fonte dei Dati: <https://netmarketshare.com/> (Sezione: Operating Systems → Desktop)

Importanza degli Artefatti di Windows | 4/6



Importanza degli Artefatti di Windows | 5/6

- Ci focalizzeremo su diverse **fonti di artefatti** e sui relativi aspetti forensi, al fine di estrarre tracce per l'investigazione forense
- In genere, tali artefatti sono creati automaticamente e memorizzati in **varie strutture** del sistema
 - Alcuni artefatti sono creati durante **alcune procedure**, svolte dal sistema
- Diversi elementi di Windows, utilizzati quotidianamente dagli utenti, **possono essere fonte di tracce/evidenze**
 - È necessario quindi conoscere le **principali fonti ed individuare possibili artefatti**, i quali, se analizzati, potrebbero fornire utili informazioni

Importanza degli Artefatti di Windows | 6/6



Alcune Fonti di Artefatti



La Fase di Boot di Windows



La Fase di Boot di Windows

Caratteristiche e Importanza | 1/2

- La **fase di boot** di un computer è una fase potenzialmente rilevante, per l'investigazione forense
- Alcune **motivazioni**:
 - Possibilità di identificare i **file modificati durante il processo di boot**
 - Per cui, anche in caso di eventuali avvii accidentali, è possibile determinare quali siano i file alterati dal S.O.
 - Possibilità di **esaminare i processi di avvio**, al fine di individuare eventuali software malevoli
 - *Esempio*: rootkit, virus, ecc.

La Fase di Boot di Windows

Caratteristiche e Importanza | 1/2

- La fase di boot di un computer è una fase potenzialmente rilevante, per l'investigazione forense
- Alcune motivazioni:

È importante affrontare anche una eventuale fase di malware analysis, per individuare software malevoli, i quali potrebbero aver alterato file ed eseguito operazioni all'insaputa dell'utente

- Possibilità di **esaminare i processi di avvio**, al fine di individuare eventuali software malevoli
 - *Esempio:* rootkit, virus, ecc.

La Fase di Boot di Windows

Caratteristiche e Importanza | 2/2

- La fase di boot di un computer è una fase potenzialmente rilevante, per l'investigazione forense
- Alcuni punti da considerare:
 - In virtù delle precedenti osservazioni, è utile **approfondire i concetti chiave della fase di boot di Windows**

file alterati dal S.O.

- Possibilità di esaminare i processi di avvio, al fine di individuare eventuali software malevoli
 - Esempio: rootkit, virus, ecc.

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 1/15

Fase di Boot di Windows 7

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 1/15

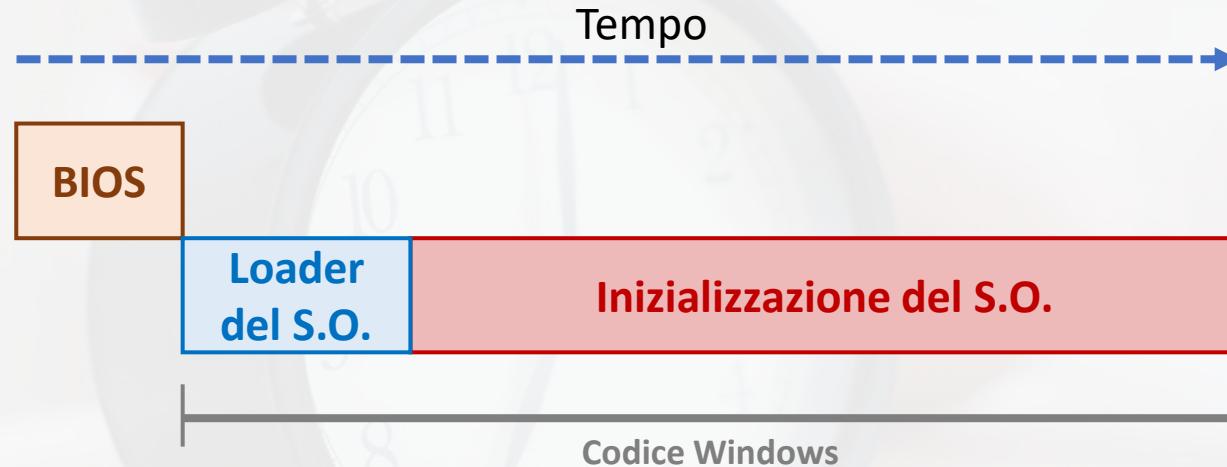
Fase di Boot di Windows 7

Verranno discussi i concetti chiave, relativi alla fase di boot di Microsoft Windows 7, i quali sono **documentati direttamente da Microsoft**

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 1/15

Fase di Boot di Windows 7



La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 2/15

Fase di Boot di Windows 7



La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 3/15

Basic Input-Output System (BIOS)

Permette l'**intermediazione** tra l'**hardware** e il **S.O.**

Contiene una **sequenza di istruzioni** che è **indispensabile** per l'avvio del S.O.
e per far sì che il S.O. possa controllare correttamente l'hardware

Le istruzioni sono generalmente memorizzate all'interno di una memoria
ROM (Read-Only Memory)/PROM (Programmable ROM)



Un chip di memoria (ospitato sulla scheda madre), contenente il BIOS

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 3/15

Basic Input-Output System (BIOS)

Permette l'intermediazione tra l'hardware e il S.O.

Contiene una **sequenza di istruzioni** che è indispensabile per l'avvio del S.O.
e per far sì che il S.O. possa controllare correttamente l'hardware

Le istruzioni sono generalmente memorizzate all'interno di una memoria ROM (Read-Only Memory)/PROM (Programmable ROM)

Unified Extensible Firmware Interface (UEFI)

A partire dal **2017**, il BIOS è stato **sostituito con l'UEFI**

L'**UEFI** estende le funzionalità del BIOS e fornisce una **GUI più avanzata**, rispetto a quella fornita dal BIOS,
per la **configurazione del sistema**

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 4/15

- Durante la **fase di inizializzazione** del sistema (prima del boot del S.O.), vengono eseguite le seguenti operazioni:
 - Identificazione dei dispositivi hardware
 - Inizializzazione dei suddetti dispositivi
 - Power-On Self Test (POST)

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 4/15

- Durante la **fase di inizializzazione** del sistema (prima del boot del S.O.), vengono eseguite le seguenti operazioni:
 - Identificazione dei dispositivi hardware
 - Inizializzazione dei suddetti dispositivi
 - **Power-On Self Test (POST)**

Fase di **testing automatico**, che permette di verificare il **corretto funzionamento** delle componenti e delle periferiche hardware

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 4/15

- Durante la fase di inizializzazione del sistema (prima del boot) vengono eseguite le seguenti operazioni:

Principali Operazioni della Fase di POST

- Test automatico dell'alimentazione del sistema
- Caricamento del codice del BIOS
 - Test dell'integrità del suddetto codice
- Individuazione della causa che ha portato all'avvio del processo di POST (accensione, ripresa dallo stand-by, ecc.)
- Individuazione della RAM
 - Determinazione delle dimensioni
 - Fase di verifica
- Individuazione dei dispositivi di sistema e dei bus
 - Fase di catalogazione ed inizializzazione
- Eventuale avvio del BIOS della scheda video
- Lettura delle impostazioni relative alla configurazione di avvio

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 4/15

OSSERVAZIONE IMPORTANTE | 1/2

- Du
b

La **configurazione di avvio** costituisce un potenziale elemento rilevante per una indagine forense

Infatti, essa esplicita **tutti i dispositivi che possono contenere un S.O.**, che può essere avviato sulla macchina in esame

Viene inoltre specificata anche una **priorità** a ciascun dispositivo (utile qualora venissero individuati più dispositivi con un S.O.)

Conoscendo queste informazioni, l'**investigatore** potrebbe **delineare delle ipotesi e valutare diversi scenari investigativi**

- Fase di catalogazione ed inizializzaz.
- Eventuale avvio del BIOS della scheda video
- Lettura delle impostazioni relative alla configurazione di avvio

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 4/15

- Du

OSSERVAZIONE IMPORTANTE | 2/2

Esempio (Semplificato)

Si supponga che la macchina sulla quale si sta indagando abbia una configurazione tale da poter permettere l'**avvio di un S.O. da una penna USB, con elevata priorità**

In virtù di tale informazione, l'investigatore dovrebbe considerare anche l'**ipotesi che un malintenzionato abbia potuto utilizzare un S.O. live** (tecnica anti-forense), avviandolo da una penna USB

- Fase di catalogazione ed inizializzaz.
- Eventuale avvio del BIOS della scheda video.
- Lettura delle impostazioni relative alla configurazione di avvio

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 4/15

- Durante la fase di inizializzazione del sistema (prima del boot) vengono eseguite le seguenti operazioni:

Principali Operazioni della Fase di POST

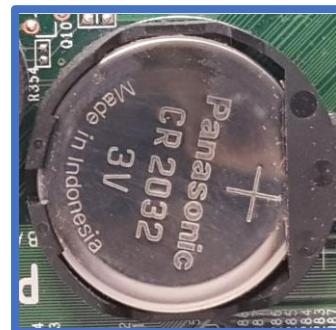
- Test automatico dell'alimentazione del sistema
- Caricamento del codice del BIOS
 - Test dell'integrità del suddetto codice
- Individuazione della causa che ha portato all'avvio del processo di POST (accensione, ripresa dallo stand-by, ecc.)
- Individuazione della RAM
 - Determinazione delle dimensioni
 - Fase di verifica
- Individuazione dei dispositivi di sistema e dei bus
 - Fase di catalogazione ed inizializzazione
- Eventuale avvio del BIOS della scheda video
- Lettura delle impostazioni relative alla configurazione di avvio
 - Tali impostazioni sono memorizzate nel CMOS

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 4/15

- Durante la fase di inizializzazione del sistema (prima del boot) il **CMOS** (Complementary Metal-Oxide Semiconductor) è un semiconduttore che **svolge la funzione di una piccolissima RAM** e contiene le **impostazioni del BIOS**

Assorbe poca energia elettrica e **deve necessariamente essere alimentato da una batteria** (se la batteria si scarica, le impostazioni del BIOS, vengono tipicamente resettate a quelle di fabbrica)



Batteria del CMOS (ospitata sulla scheda madre)

- Lettura delle impostazioni relative alla configurazione di avvio
 - Tali impostazioni sono memorizzate nel **CMOS**

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 4/15

- Durante la **fase di inizializzazione** del sistema (prima del boot del S.O.), vengono eseguite le seguenti operazioni:
 - Identificazione dei dispositivi hardware
 - Inizializzazione dei suddetti dispositivi
 - Power-On Self Test (POST)
 - Identificazione del dispositivo di avvio e lettura del Master Boot Record (MBR)
 - Avvio del Boot Manager, denominato Windows Boot Manager nel S.O. Windows (Bootmgr.exe)
 - Il Windows Boot Manager ha il compito di individuare il loader di Windows (Winload.exe), nella partizione di boot di Windows
 - Inizia poi la fase successiva:
 - **Loader del S.O. (OS Loader)**

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 6/15

Fase di Boot di Windows 7



La Fase di Boot di Windows

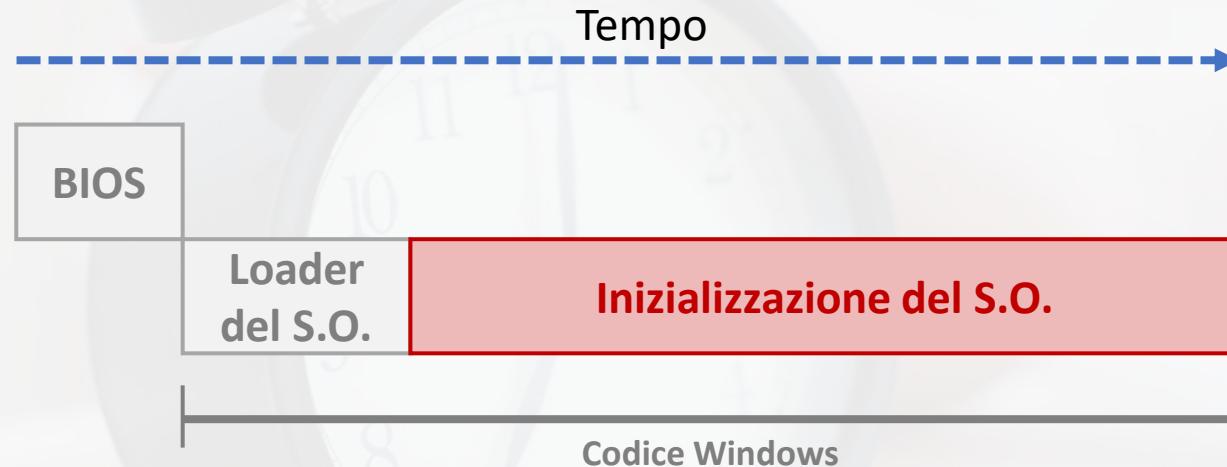
Nozioni, Concetti e Principali Sottofasi | 7/15

- L'eseguibile Windows Loader (`Winload.exe`) effettua le seguenti operazioni:
 - Avvia i **driver essenziali e minimali** per la lettura di dati dal disco fisso (o dal supporto di memorizzazione prescelto)
 - Inizializza il sistema ad **un punto in cui il Kernel** di Windows **può iniziare la sua esecuzione**
- Al momento dell'avvio del Kernel, vengono **caricati in memoria**, i seguenti elementi:
 - Registro di sistema
 - Alcuni Driver
 - Vengono caricati in memoria tutti **i driver, che sono necessari nelle fasi successive**
 - Tali driver sono contrassegnati come **BOOT_START**

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 8/15

Fase di Boot di Windows 7



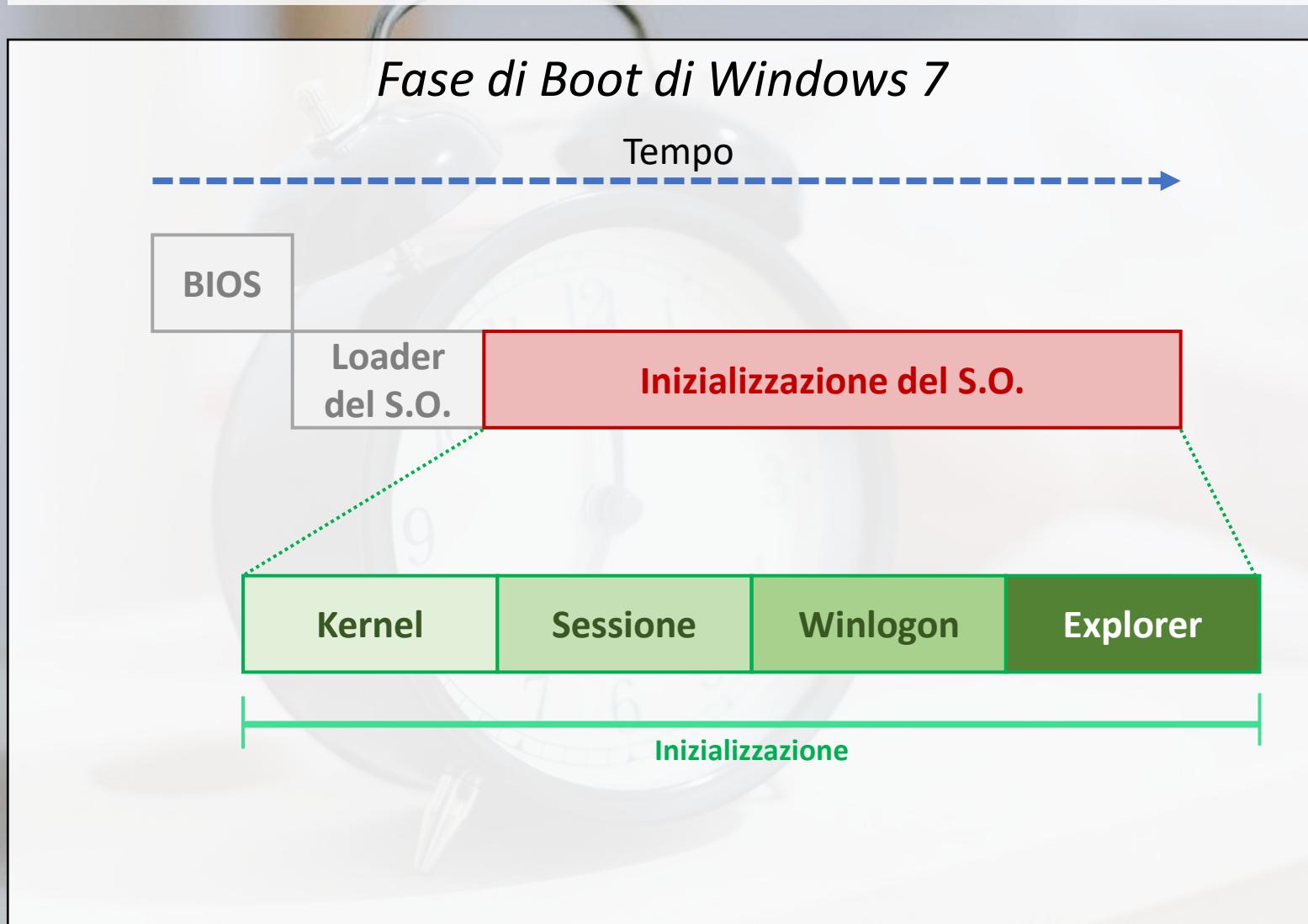
La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 9/15

- Nella fase di **inizializzazione del S.O.**, viene eseguita la maggior parte delle operazioni di avvio
- Questa fase può essere suddivisa in **quattro sotto-fasi principali**:
 - Inizializzazione del **Kernel**
 - Inizializzazione della **Sessione**
 - Inizializzazione di accesso a Windows (**Winlogon**)
 - Inizializzazione dell'Interfaccia Grafica (**Explorer**)

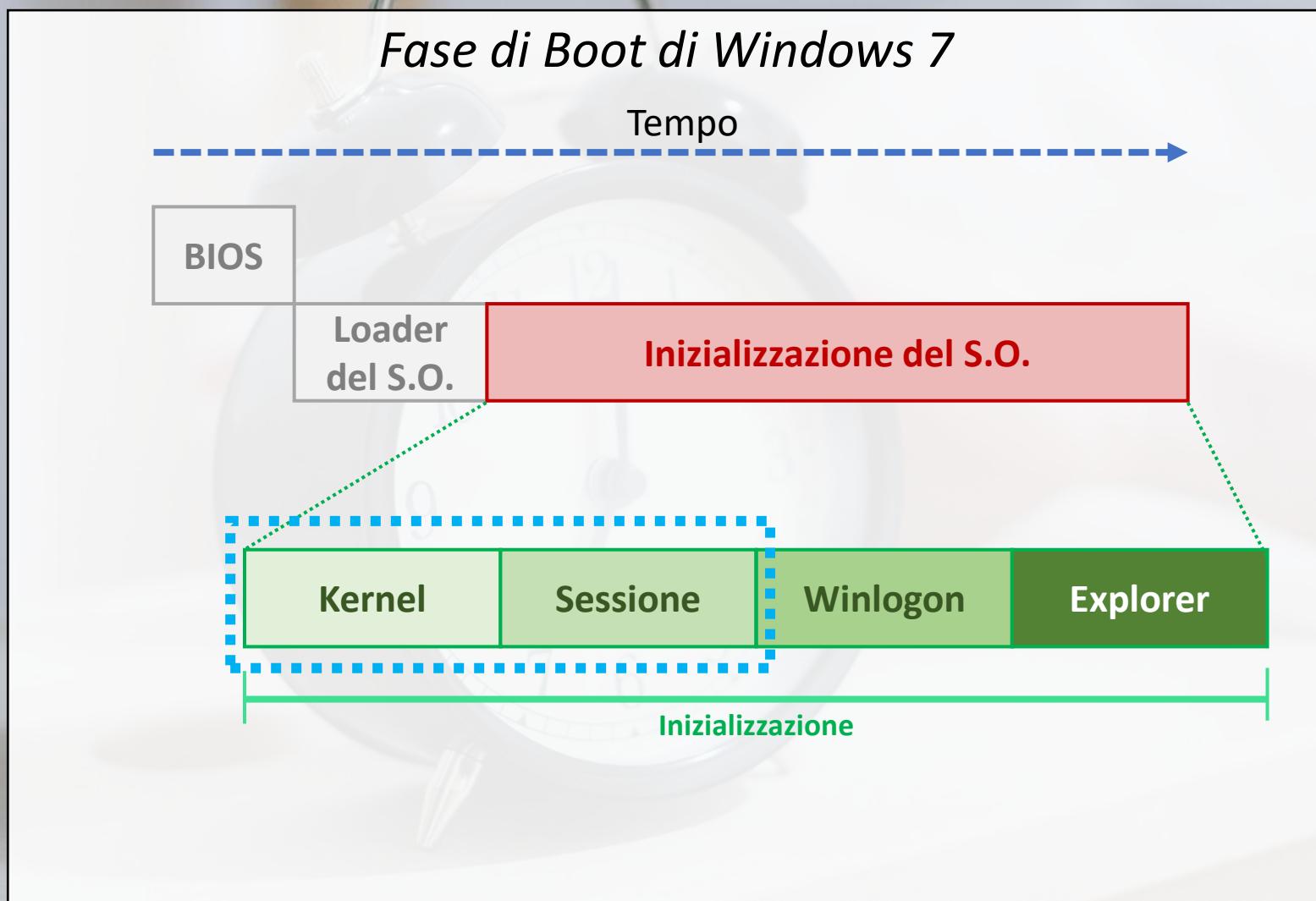
La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 10/15



La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 11/15



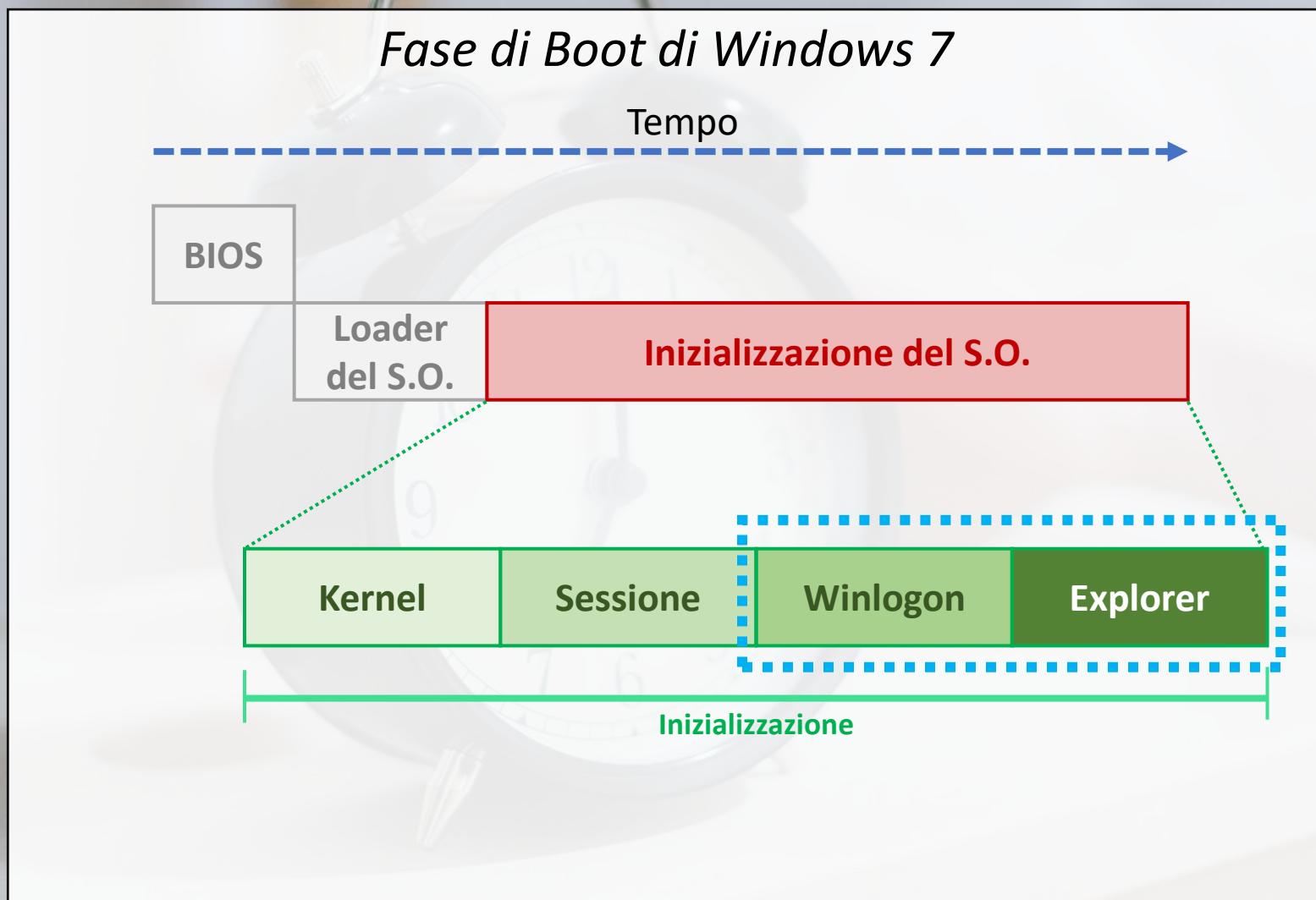
La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 12/15

- **Inizializzazione del Kernel**
 - In questa fase vengono inizializzate tutte le strutture dati e le componenti del Kernel
 - Viene poi inizializzato il Plug and Play (PnP) manager, il quale inizializza i driver, contrassegnati come *BOOT_START* (tali driver sono stati precedentemente caricati in memoria)
- **Inizializzazione della Sessione**
 - Il controllo passa al gestore di sessione: processo smss.exe
 - smss.exe provvede a:
 - Inizializzare il registro (caricato in memoria, precedentemente)
 - Inizializzare i dispositivi ed i driver (non contrassegnati come *BOOT_START*)
 - Avvia alcuni processi relativi a sottosistemi del S.O.

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 13/15



La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 14/15

- **Inizializzazione di Winlogon**
 - Il controllo passa al gestore del logon (`Winlogon.exe`)
 - Appare la schermata di logon (autenticazione), vengono avviati determinati servizi, vengono avviati eventuali script per la gestione di privilegi (Group Policy), ecc.
- **Inizializzazione di Explorer**
 - Viene avviato il Desktop Window Manager (DWM), il quale provvede all'avvio dell'ambiente desktop, visualizzandolo per la prima volta (nella fase di boot)

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 15/15

Fase di Boot di Windows 7

Tempo



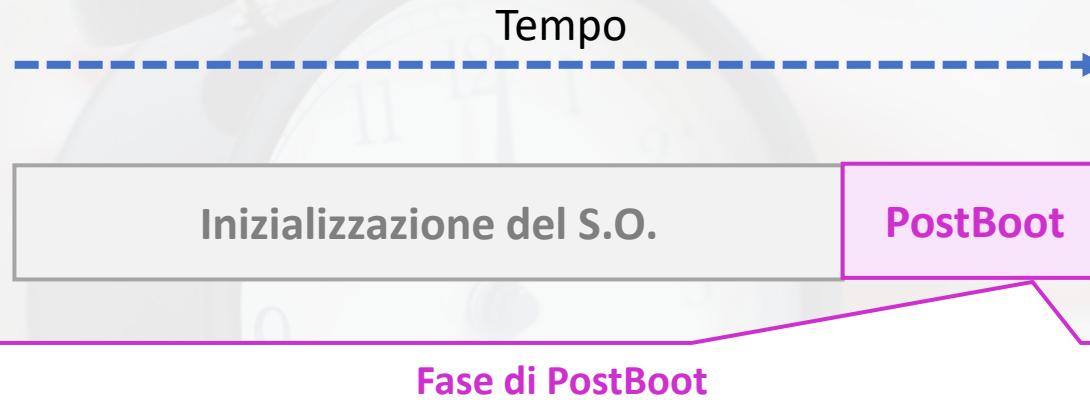
Inizializzazione del S.O.

PostBoot

La Fase di Boot di Windows

Nozioni, Concetti e Principali Sottofasi | 15/15

Fase di Boot di Windows 7



La fase di PostBoot include lo svolgimento di diverse attività in background, che devono essere avviate, sebbene il desktop risulti visualizzato ed utilizzabile, ad esempio:

- Avvio di servizi
- Avvio di programmi in background (ad es., DropBox, OneDrive, ecc.)
- Aggiunta di *tray icon* (icone nell'area vicino l'orologio di Windows)
- Ecc.

Analisi del Registro di Sistema

Analisi del Registro di Sistema

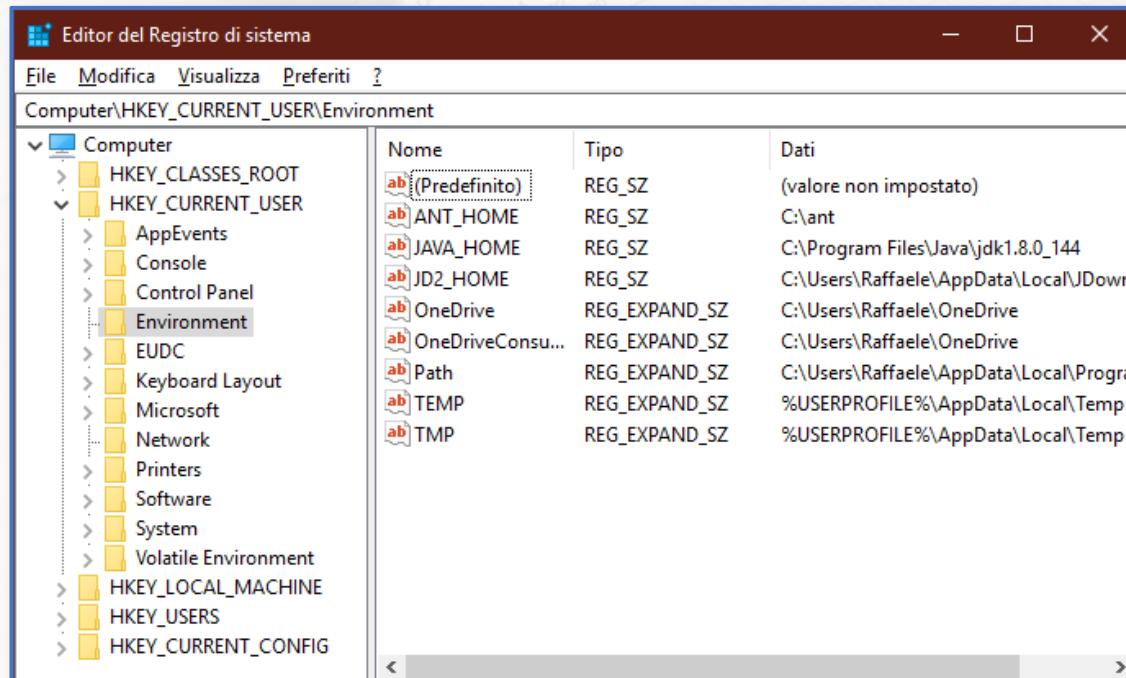
Caratteristiche, Struttura e Importanza | 1/6

- Il **registro di sistema** è una componente di Windows, che **memorizza molteplici informazioni**, alle quali il S.O. fa continuamente riferimento, durante l'utilizzo
- Ad esempio, vengono memorizzati:
 - Settaggi e preferenze di Windows stesso e di eventuali applicazioni installate
 - Settaggi e preferenze degli utenti
 - Settaggi e preferenze dell'hardware del sistema
- Inoltre, il registro di sistema, tiene traccia di alcune attività degli utenti
- Dal punto di vista forense, il **registro di sistema** è **potenzialmente una enorme risorsa**
 - In esso, infatti, sono contenuti migliaia di valori

Analisi del Registro di Sistema

Caratteristiche, Struttura e Importanza | 2/6

- Windows fornisce il tool **Editor del Registro di sistema**, il quale permette di visualizzare e modificare il registro di sistema
 - NOTA:** Tool utilizzabile esclusivamente in un *live system* (permette di visualizzare/modificare esclusivamente il registro di sistema, della macchina su cui il tool è utilizzato)

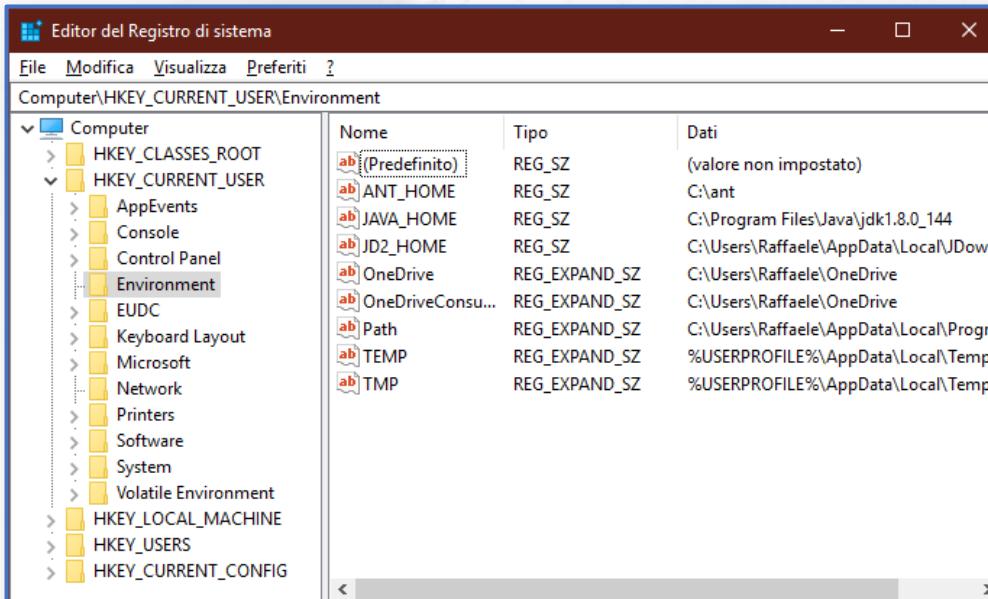


Interfaccia Utente del tool Editor del Registro di sistema (Windows 10)

Analisi del Registro di Sistema

Caratteristiche, Struttura e Importanza | 3/6

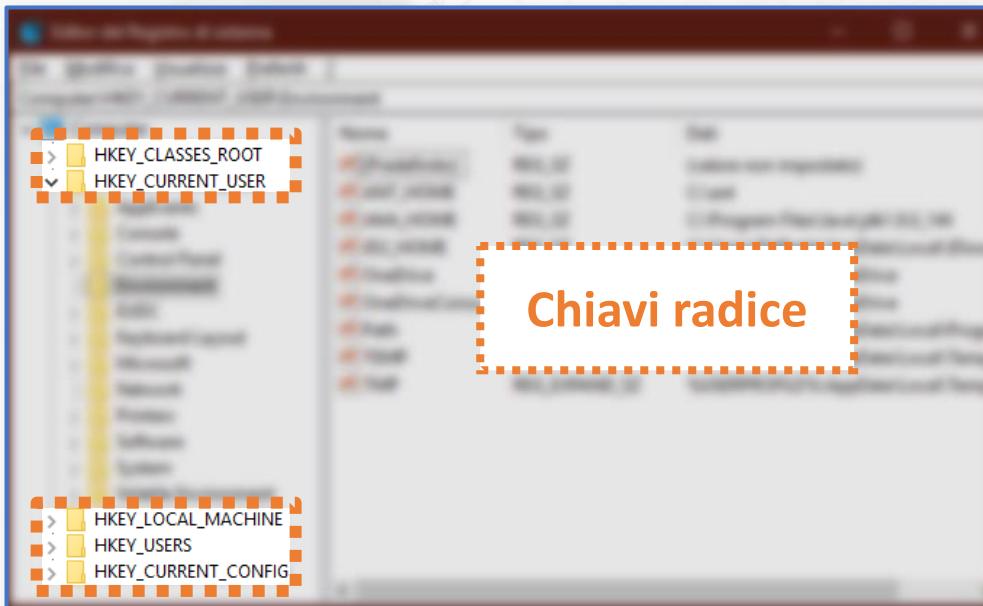
- Il registro ha una specifica struttura gerarchica
- Presenta **cinque chiavi radice (root keys)**
 - All'interno di ogni chiave radice, sono presenti delle **sotto-chiavi (sub-keys)**
 - Ciascuna sotto-chiave, può contenere, a sua volta, altre sotto-chiavi e/o **valori (values)**



Analisi del Registro di Sistema

Caratteristiche, Struttura e Importanza | 4/6

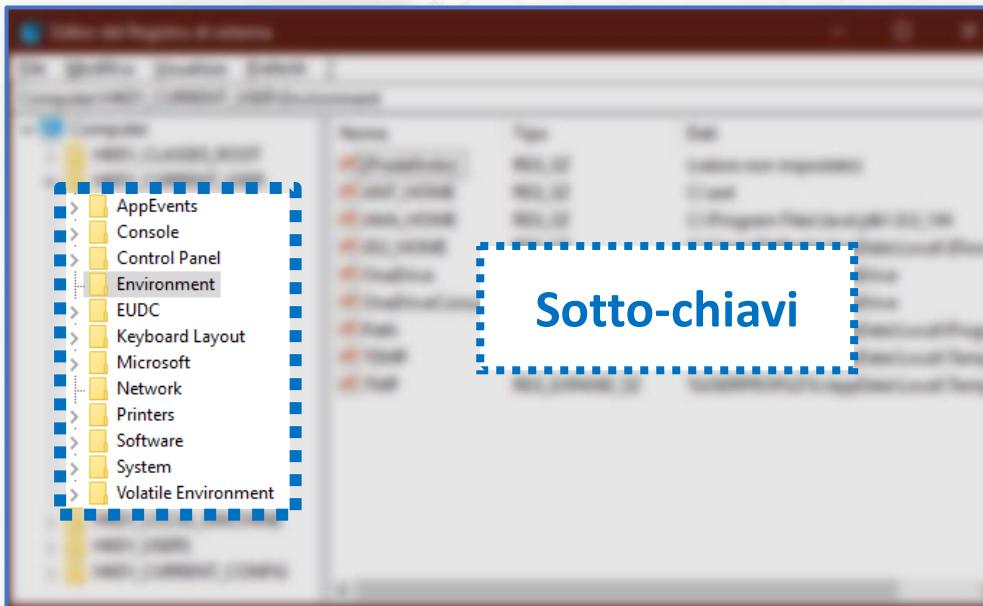
- Il registro ha una specifica struttura gerarchica
- Presenta **cinque chiavi radice (root keys)**
 - All'interno di ogni chiave radice, sono presenti delle **sotto-chiavi (sub-keys)**
 - Ciascuna sotto-chiave, può contenere, a sua volta, altre sotto-chiavi e/o **valori (values)**



Analisi del Registro di Sistema

Caratteristiche, Struttura e Importanza | 4/6

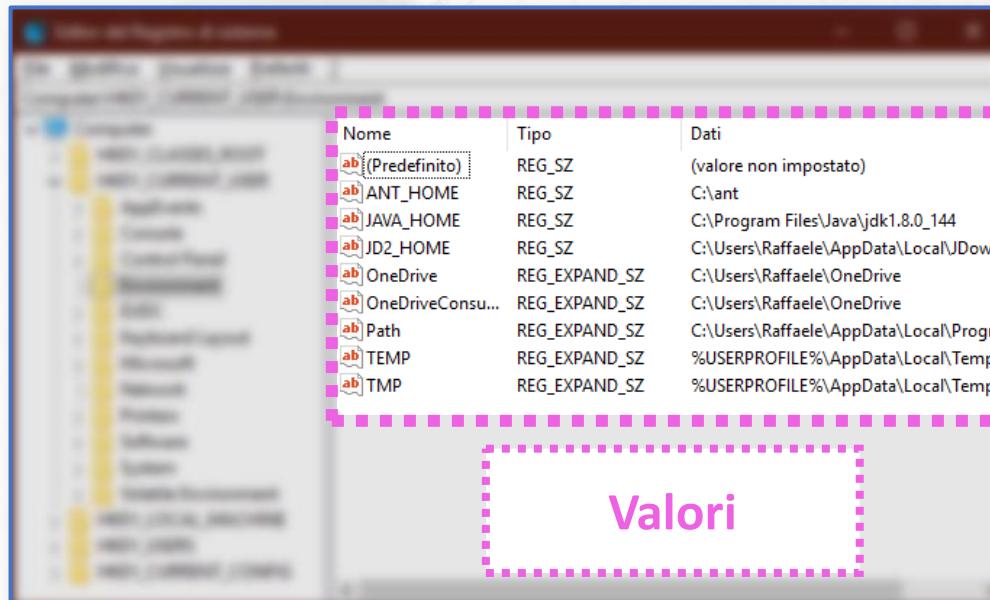
- Il registro ha una specifica struttura gerarchica
- Presenta **cinque chiavi radice (root keys)**
 - All'interno di ogni chiave radice, sono presenti delle **sotto-chiavi (sub-keys)**
 - Ciascuna sotto-chiave, può contenere, a sua volta, altre sotto-chiavi e/o **valori (values)**



Analisi del Registro di Sistema

Caratteristiche, Struttura e Importanza | 4/6

- Il registro ha una specifica struttura gerarchica
- Presenta **cinque chiavi radice (root keys)**
 - All'interno di ogni chiave radice, sono presenti delle **sotto-chiavi (sub-keys)**
 - Ciascuna sotto-chiave, può contenere, a sua volta, altre sotto-chiavi e/o **valori (values)**



Analisi del Registro di Sistema

Caratteristiche, Struttura e Importanza | 5/6

- Ogni **valore** è costituito da tre elementi:
 - *Nome* del valore (Prima Colonna)
 - *Dati* contenuti nel valore (Terza Colonna)
 - *Tipo* dei dati, contenuti nel valore (Seconda Colonna)

Nome	Tipo	Dati
ab (Predefinito)	REG_SZ	(valore non impostato)
ab ANT_HOME	REG_SZ	C:\ant
ab JAVA_HOME	REG_SZ	C:\Program Files\Java\jdk1.8.0_144
ab JD2_HOME	REG_SZ	C:\Users\Raffaele\AppData\Local\JDwn
ab OneDrive	REG_EXPAND_SZ	C:\Users\Raffaele\OneDrive
ab OneDriveConsu...	REG_EXPAND_SZ	C:\Users\Raffaele\OneDrive
ab Path	REG_EXPAND_SZ	C:\Users\Raffaele\AppData\Local\Progra
ab TEMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp
ab TMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp

Analisi del Registro di Sistema

Caratteristiche, Struttura e Importanza | 5/6

- Ogni valore è costituito da tre elementi:
 - Nome* del valore (Prima Colonna)
 - Dati* contenuti nel valore (Terza Colonna)
 - Tipo dei dati, contenuti nel valore (Seconda Colonna)**

Esempi di Tipi

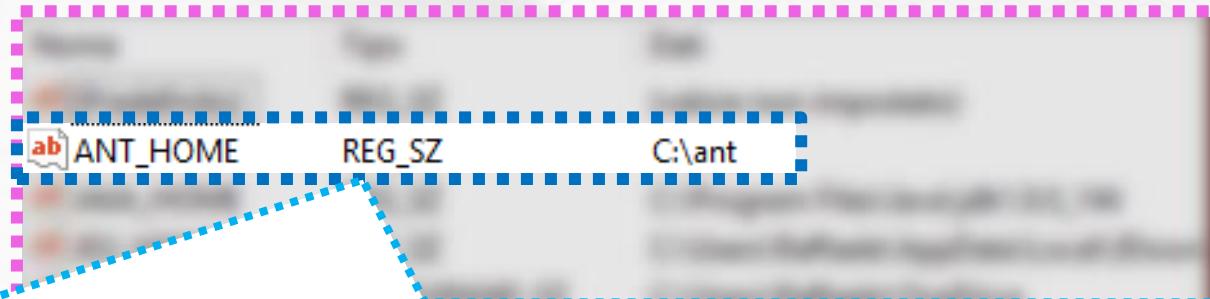
Stringhe (REG_SZ, REG_EXPAND_SZ, ...), numeri (REG_DWORD, ...), dati binari (REG_BINARY), ecc.

OneDriveConsu...	REG_EXPAND_SZ	C:\Users\Raffaele\OneDrive
Path	REG_EXPAND_SZ	C:\Users\Raffaele\AppData\Local\Progra
TEMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp
TMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp

Analisi del Registro di Sistema

Caratteristiche, Struttura e Importanza | 5/6

- Ogni **valore** è costituito da tre elementi:
 - *Nome* del valore (Prima Colonna)
 - *Dati* contenuti nel valore (Terza Colonna)
 - *Tipo* dei dati, contenuti nel valore (Seconda Colonna)



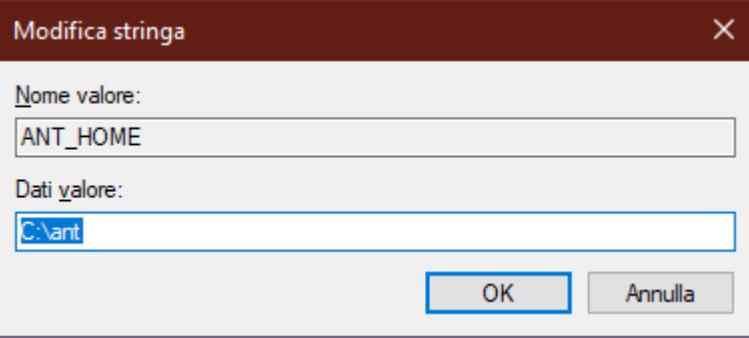
Ogni riga rappresenta un **valore** del registro

Esempio: Il valore evidenziato è denominato ANT_HOME (*Nome*) ed il contenuto (elemento *Dati*) è uguale a C:\ant (si tratta di una stringa, come specificato dall'elemento *Tipo*, che è uguale a REG_SZ)

Analisi del Registro di Sistema

Caratteristiche, Struttura e Importanza | 5/6

- Ogni **valore** è costituito da tre elementi:
 - Nome* del valore (Prima Colonna)
 - Dati* contenuti nel valore (Terza Colonna)
 - Tipo* dei dati, contenuti nel valore (Seconda Colonna)

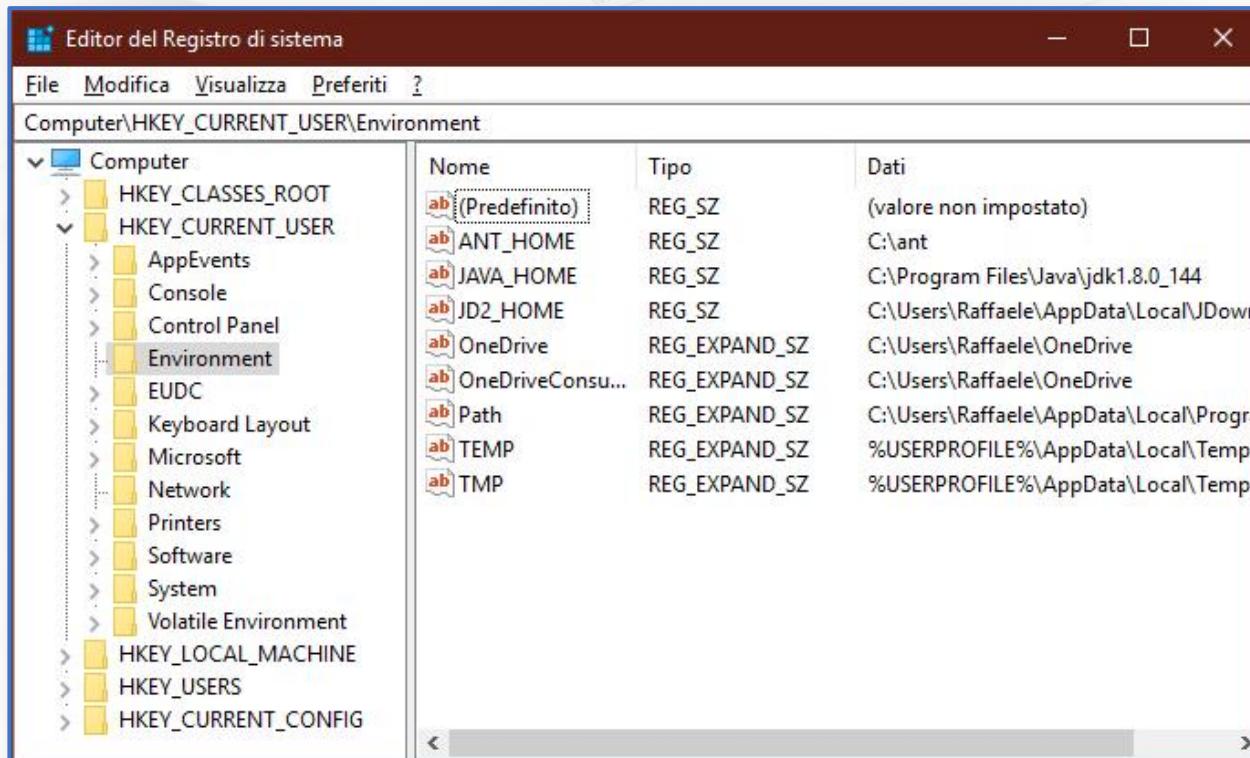


Dal tool Editor del Registro di sistema, facendo doppio click su un valore, sarà possibile visualizzarne/modificarne il contenuto (elemento *Dati*), tramite una nuova schermata

Analisi del Registro di Sistema

Caratteristiche, Struttura e Importanza | 6/6

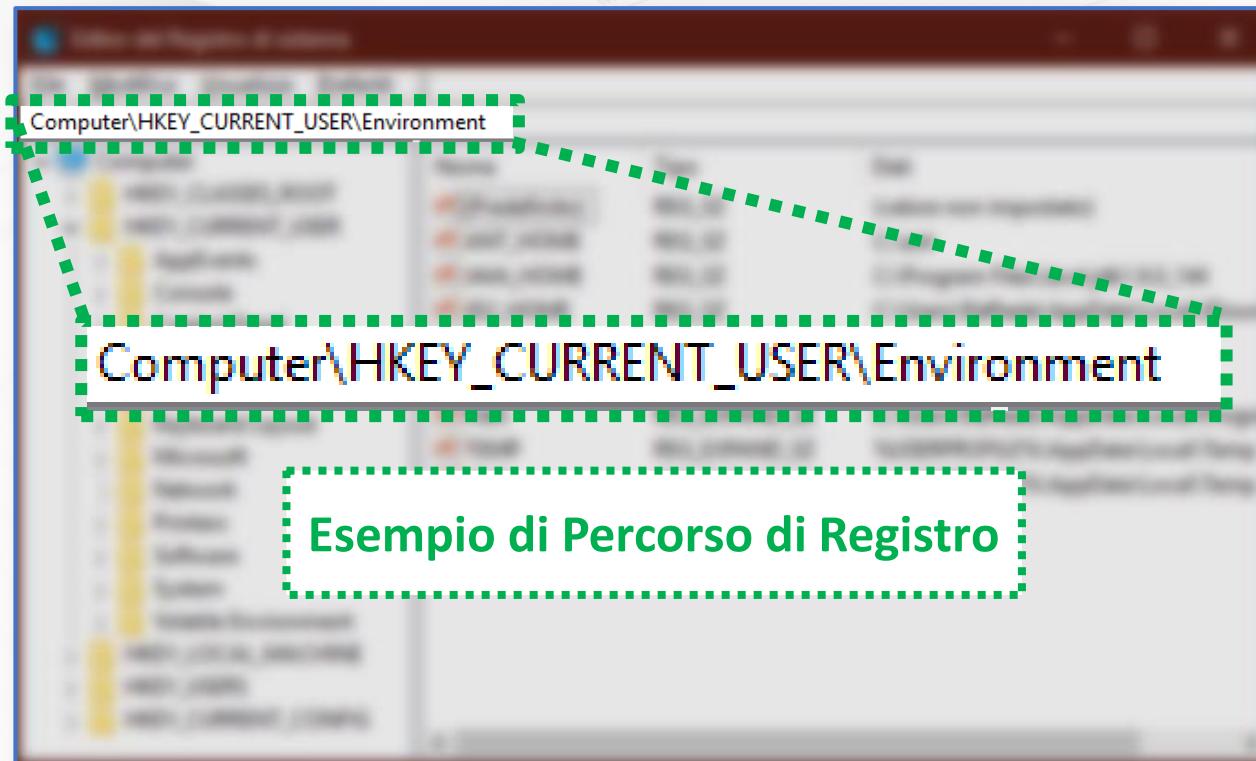
- Per accedere ad uno specifico valore o ad una specifica chiave radice/sotto-chiave, è possibile utilizzare un **percorso di registro** (che ha un formato simile a quello dei percorsi nel file system)



Analisi del Registro di Sistema

Caratteristiche, Struttura e Importanza | 6/6

- Per accedere ad uno specifico valore o ad una specifica chiave radice/sotto-chiave, è possibile utilizzare un **percorso di registro** (che ha un formato simile a quello dei percorsi nel file system)



Analisi del Registro di Sistema

Chiavi Radice

- Le **cinque chiavi radice** del registro di sistema, sono le seguenti:
 - **HKEY_CLASSES_ROOT**
 - **HKEY_LOCAL_MACHINE**
 - **HKEY_CURRENT_USER**
 - **HKEY_USERS**
 - **HKEY_CURRENT_CONFIG**
- Ogni chiave radice:
 - Ha il compito di memorizzare specifiche informazioni ed impostazioni del sistema in uso e/o degli utenti
 - È memorizzata all'interno del file system, in uno o più file specifici, chiamati ***registry hive file*** (o ***hive file***)
 - Letteralmente, *hive* significa *alveare*

Analisi del Registro di Sistema

Chiavi Radice

- Le **cinque chiavi radice** del registro di sistema, sono le seguenti:
 - **HKEY_CLASSES_ROOT**
 - HKEY_LOCAL_MACHINE
 - HKEY_CURRENT_USER
 - HKEY_USERS
 - HKEY_CURRENT_CONFIG
- Ogni chiave radice:
 - Ha il compito di memorizzare specifiche informazioni ed impostazioni del sistema in uso e/o degli utenti
 - È memorizzata all'interno del file system, in uno o più file specifici, chiamati ***registry hive file*** (o ***hive file***)

Analisi del Registro di Sistema

Chiave Radice HKCR | 1/4

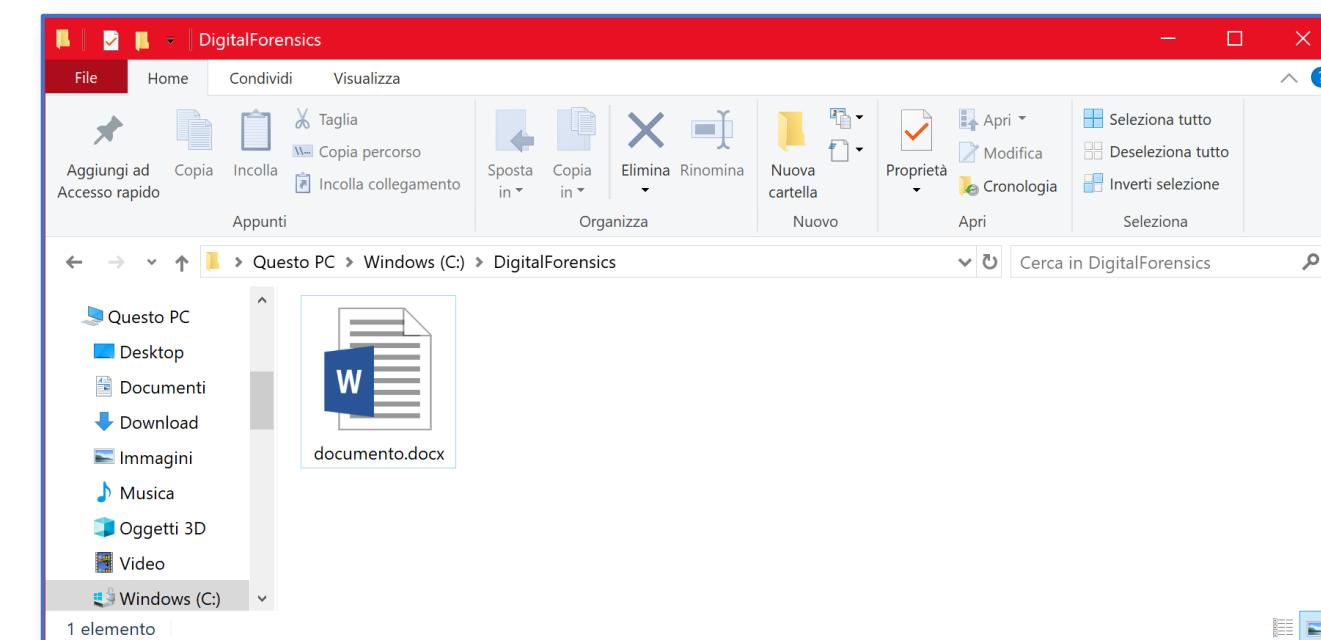
- La chiave radice **HKEY_CLASSES_ROOT** (talvolta, chiamata anche **HKCR**, per brevità), definisce il comportamento di Windows, in risposta ad alcune azioni eseguite dall'utente, tramite Esplora Risorse
 - Esplora Risorse è una componente della UI di Windows, che permette di «navigare» nel file system, svolgere operazioni sui file (ad esempio, rinominare un file), ecc.

Analisi del Registro di Sistema

Chiave Radice HKCR | 1/4

- La chiave radice **HKEY_CLASSES_ROOT** (talvolta, chiamata anche **HKCR**, per brevità), definisce il comportamento di Windows, in risposta ad alcune azioni eseguite dall'utente, tramite **Esplora Risorse**

- Esplora Risorse è una componente della UI di



Interfaccia Utente | Componente Esplora Risorse di Windows

Analisi del Registro di Sistema

Chiave Radice HKCR | 1/4

- La chiave radice **HKEY_CLASSES_ROOT** (talvolta, chiamata anche **HKCR**, per brevità), definisce il comportamento di Windows, in risposta ad alcune azioni eseguite dall'utente, tramite Esplora Risorse
 - Esplora Risorse è una componente della UI di Windows, che permette di «navigare» nel file system, svolgere operazioni sui file (ad esempio, rinominare un file), ecc.

Il suddetto comportamento può essere modificato da un utente (questa modifica sarà valida, esclusivamente, in riferimento all'utente che la ha apportata)

Analisi del Registro di Sistema

Chiave Radice HKCR | 2/4

Esempio di Azioni dell'Utente

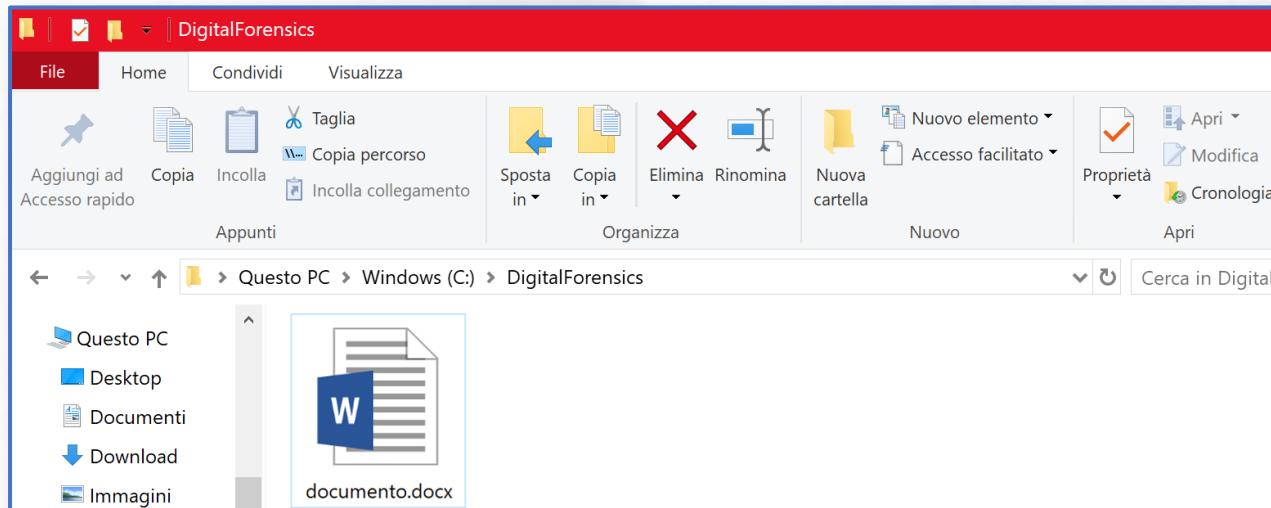
1. Click su determinati tasti di Esplora Risorse, i quali si attivano, alla selezione di un file
2. Click su determinate entry del menu contestuale, associato ad un file (tale menu si apre mediante un click, con il tasto destro del mouse, su un file, tramite Esplora Risorse)
3. Doppio click su un file, tramite Esplora Risorse

Analisi del Registro di Sistema

Chiave Radice HKCR | 2/4

Esempio di Azioni dell'Utente

1. Click su determinati tasti di Esplora Risorse, i quali si attivano, alla selezione di un file
2. Click su determinate entry del menu contestuale, associato ad un file (tale menu si apre mediante un click, con il tasto destro del mouse, su un file, tramite Esplora Risorse)
3. Doppio click su un file, tramite Esplora Risorse



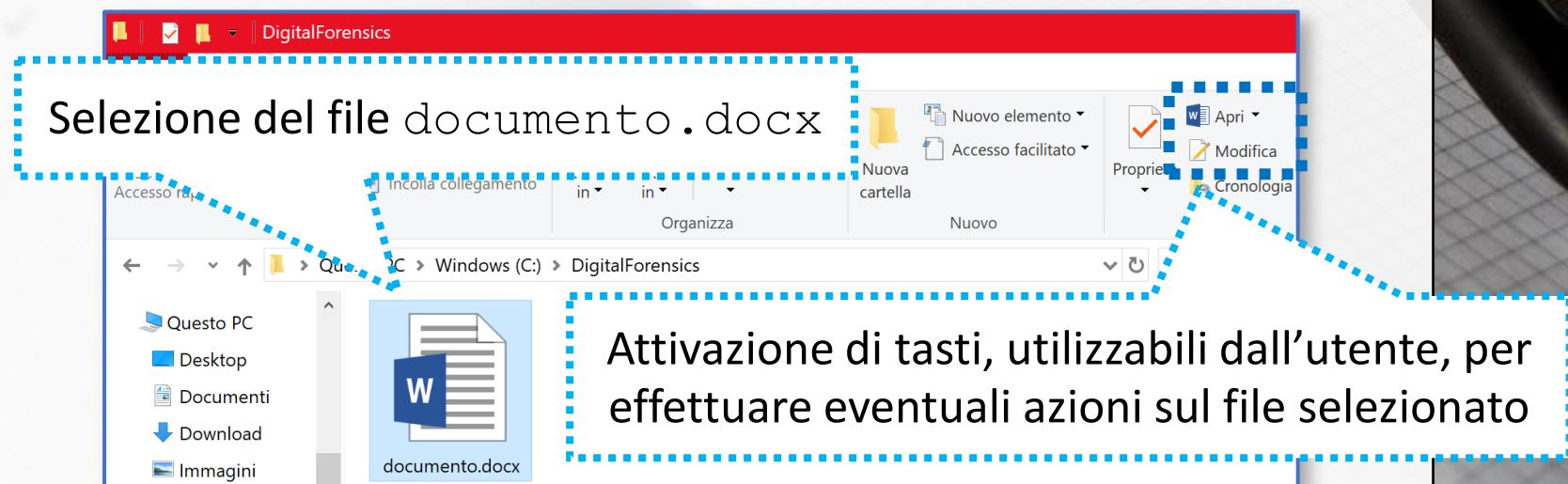
Esplora Risorse

Analisi del Registro di Sistema

Chiave Radice HKCR | 2/4

Esempio di Azioni dell'Utente

1. Click su determinati tasti di Esplora Risorse, i quali si attivano, alla selezione di un file
2. Click su determinate entry del menu contestuale, associato ad un file (tale menu si apre mediante un click, con il tasto destro del mouse, su un file, tramite Esplora Risorse)
3. Doppio click su un file, tramite Esplora Risorse



Esplora Risorse

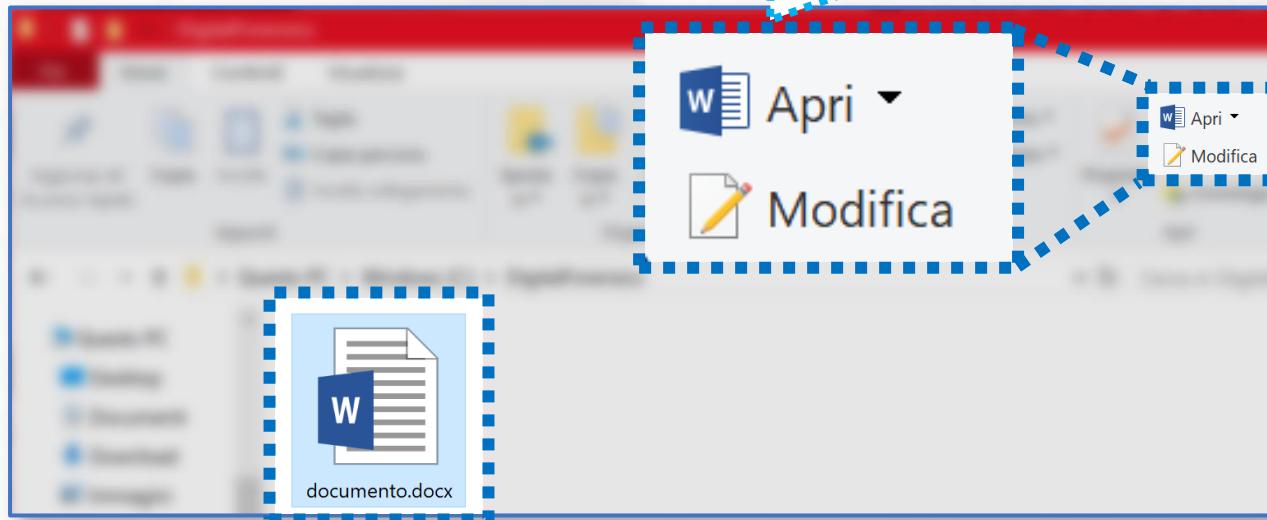
Analisi del Registro di Sistema

Chiave Radice HKCR | 2/4

Ad esempio, in risposta al click sul tasto «**Apri**», Windows utilizzerà il programma, specificato nella chiave radice **HKCR** (che, in questo caso, si suppone essere Microsoft Word), per aprire il file selezionato **documento.docx**

Questo comportamento è quindi specificato nella chiave radice **HKCR** ed è il medesimo per tutti i file con estensione **.docx**

- un file, tramite Esplora Risorse)
3. Doppio click su un file, tramite Esplora R



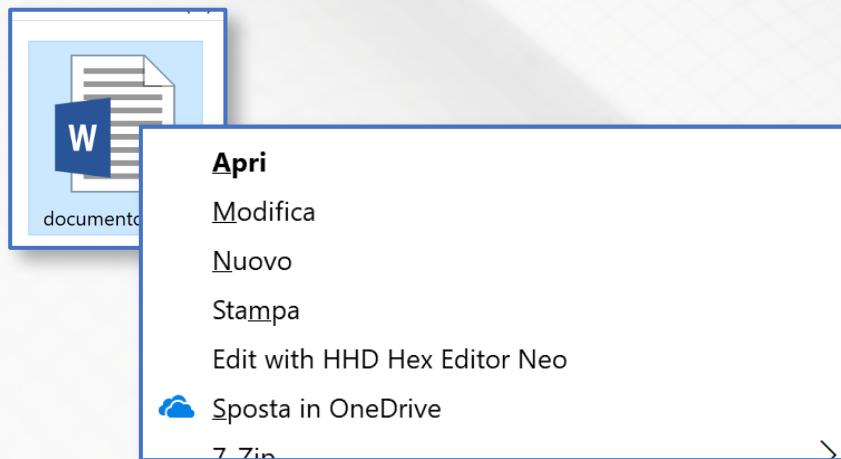
Esplora Risorse

Analisi del Registro di Sistema

Chiave Radice HKCR | 2/4

Esempio di Azioni dell'Utente

1. Click su determinati tasti di Esplora Risorse, i quali si attivano, alla selezione di un file
2. **Click su determinate entry del menu contestuale, associato ad un file (tale menu si apre mediante un click, con il tasto destro del mouse, su un file, tramite Esplora Risorse)**
3. Doppio click su un file, tramite Esplora Risorse



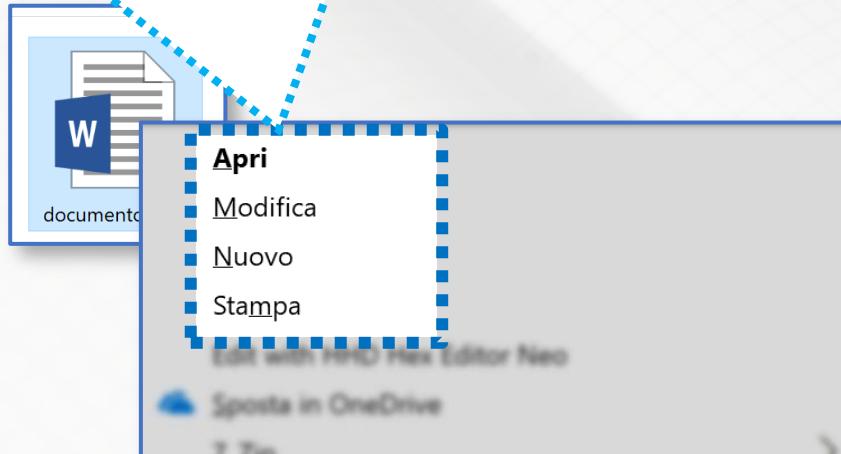
Analisi del Registro di Sistema

Chiave Radice HKCR | 2/4

Ad esempio, in risposta ad un click sulla entry «Stampa» del menu contestuale, Windows utilizzerà il programma, specificato nella chiave radice **HKCR**, per la stampa del file selezionato **documento.docx**

Medesimo comportamento per tutti i file con estensione **.docx**

3. Doppio clic su **documento.docx** (o su qualsiasi altro file con estensione .docx) nell'Esplora Risorse



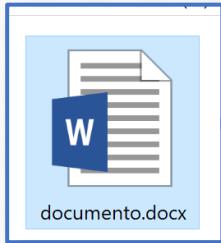
Esplora Risorse | Menu Contestuale *relativo al file* documento.docx

Analisi del Registro di Sistema

Chiave Radice HKCR | 2/4

Esempio di Azioni dell'Utente

1. Click su determinati tasti di Esplora Risorse, i quali si attivano, alla selezione di un file
2. Click su determinate entry del menu contestuale, associato ad un file (tale menu si apre mediante un click, con il tasto destro del mouse, su un file, tramite Esplora Risorse)
- 3. Doppio click su un file, tramite Esplora Risorse**



Esplora Risorse



Analisi del Registro di Sistema

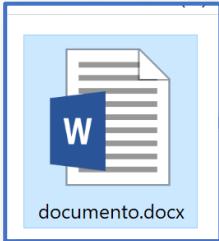
Chiave Radice HKCR | 2/4

Ad esempio, in risposta ad un doppio click su un file (in questo caso **documento.docx**), Windows utilizzerà il programma, specificato nella chiave radice **HKCR** (anche in questo caso, si suppone essere Microsoft Word), per aprire tale file

Medesimo comportamento per tutti i file con estensione **.docx**

3.

Doppio c...



Esplora Risorse

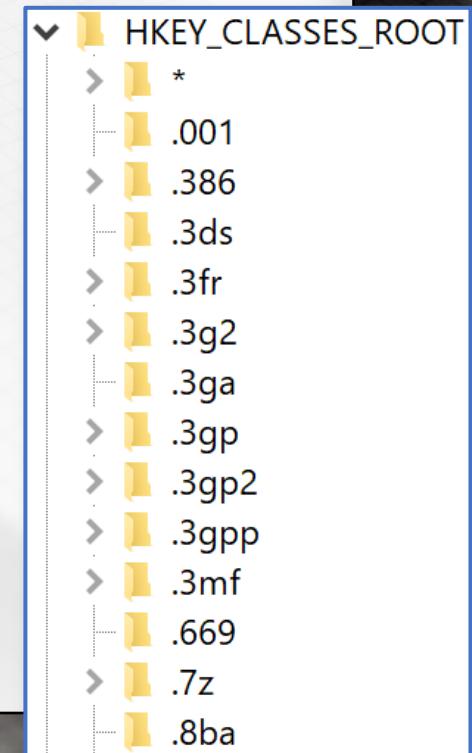
...ite Esplora Risorse



Analisi del Registro di Sistema

Chiave Radice HKCR | 3/4

- All'interno di **HKEY_CLASSES_ROOT**, è possibile individuare una sotto-chiave, per ognuna delle estensioni, note al sistema
 - Ciascuna di tali sotto-chiavi ha il medesimo **nome** dell'**estensione** a cui fa riferimento
- *Esempio*
 - La sotto-chiave **.png** definisce il comportamento di Windows, in risposta alle azioni dell'utente, effettuate su file con estensione **.png** (tramite Esplora Risorse)



Analisi del Registro di Sistema

Chiave Radice HKCR | 4/4

Esempio | Utilizzo della Chiave Radice HKCR

In un live system, si intende individuare quale programma è utilizzato da Windows, in risposta all'azione di apertura di file con estensione .docx (eseguita dall'utente, tramite Esplora Risorse)

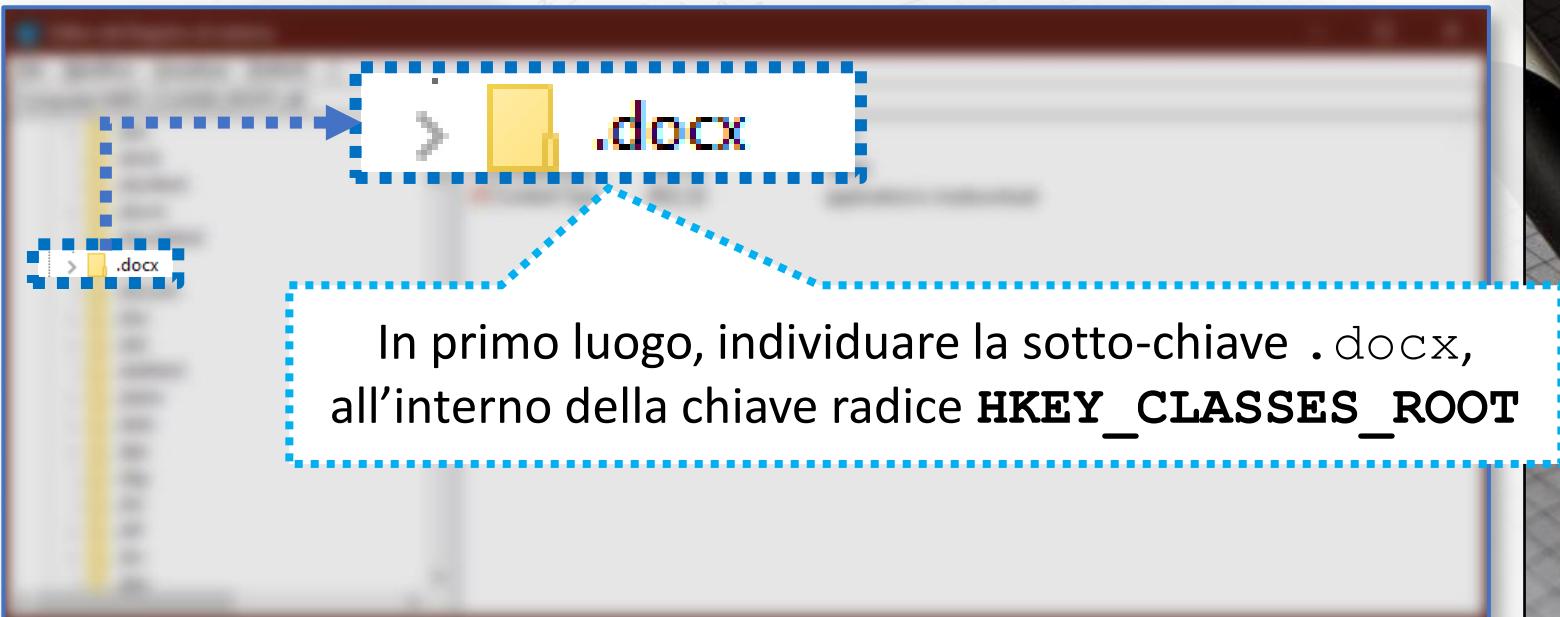
NOTA: È possibile utilizzare il tool Editor del Registro di sistema

Analisi del Registro di Sistema

Chiave Radice HKCR | 4/4

Esempio | Passo 1 di 6

In un live system, si intende individuare quale programma è utilizzato da Windows, in risposta all'azione di apertura di file con estensione .docx (eseguita dall'utente, tramite Esplora Risorse)

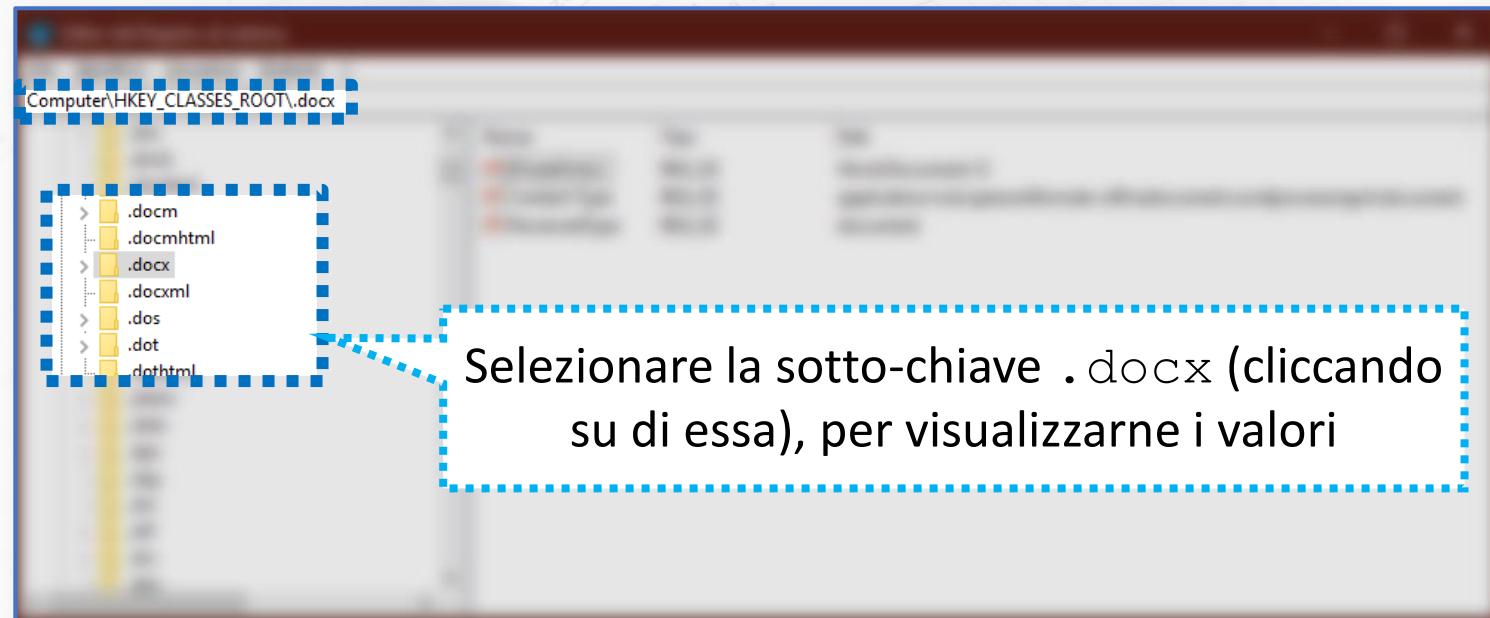


Analisi del Registro di Sistema

Chiave Radice HKCR | 4/4

Esempio | Passo 2 di 6

In un live system, si intende individuare quale programma è utilizzato da Windows, in risposta all'azione di apertura di file con estensione .docx (eseguita dall'utente, tramite Esplora Risorse)



Analisi del Registro di Sistema

Chiave Radice HKCR | 4/4

Esempio | Passo 3 di 6

Considerare il contenuto (elemento *Dati*) del valore denominato (Predefinito), che è uguale a: **Word.Document.12**

(ato da Windows, in risposta
ente, tramite Esplora Risorse)

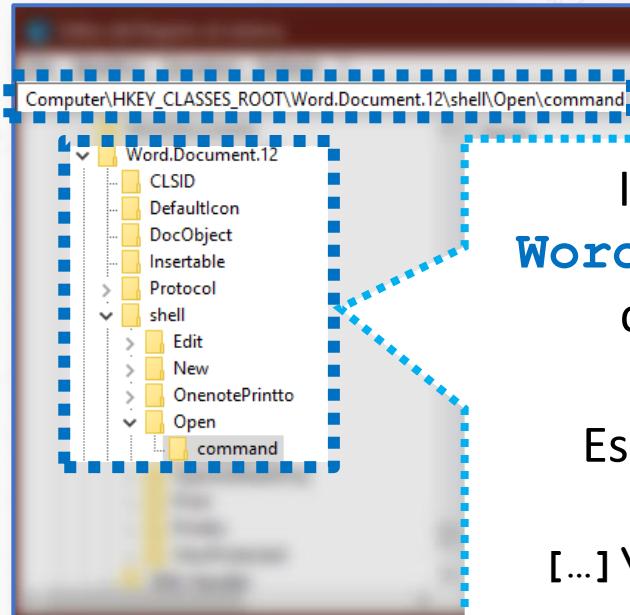
 (Predefinito)	REG_SZ	Word.Document.12
 Content Type	REG_SZ	application/vnd.openxmlformats-officedocument.wordprocessingml.document
 PerceivedType	REG_SZ	document

Analisi del Registro di Sistema

Chiave Radice HKCR | 4/4

Esempio | Passo 4 di 6

In un live system, si intende individuare quale programma è utilizzato da Windows, in risposta all'azione di apertura di file con estensione .docx (eseguita dall'utente, tramite Esplora Risorse)



Individuare la sotto-chiave denominata **Word.Document.12**, contenuta sempre nella chiave-radice **HKEY_CLASSES_ROOT**

Espandere la suddetta sotto-chiave, fino al seguente percorso di registro:
[...] \Word.Document.12\shell\Open\command

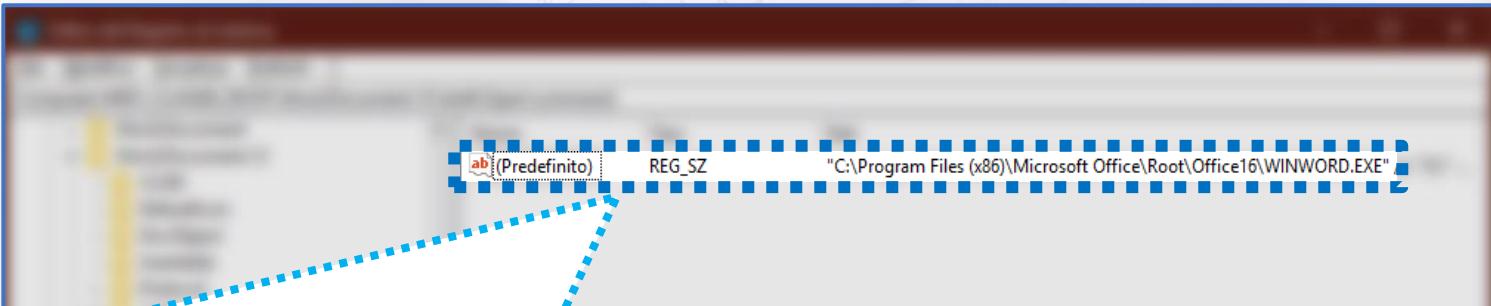
NOTA: **shell** fa riferimento all'interfaccia grafica di Windows ed **Open** all'azione di **apertura** del file

Analisi del Registro di Sistema

Chiave Radice HKCR | 4/4

Esempio | Passo 5 di 6

In un live system, si intende individuare quale programma è utilizzato da Windows, in risposta all'azione di apertura di file con estensione .docx (eseguita dall'utente, tramite Esplora Risorse)



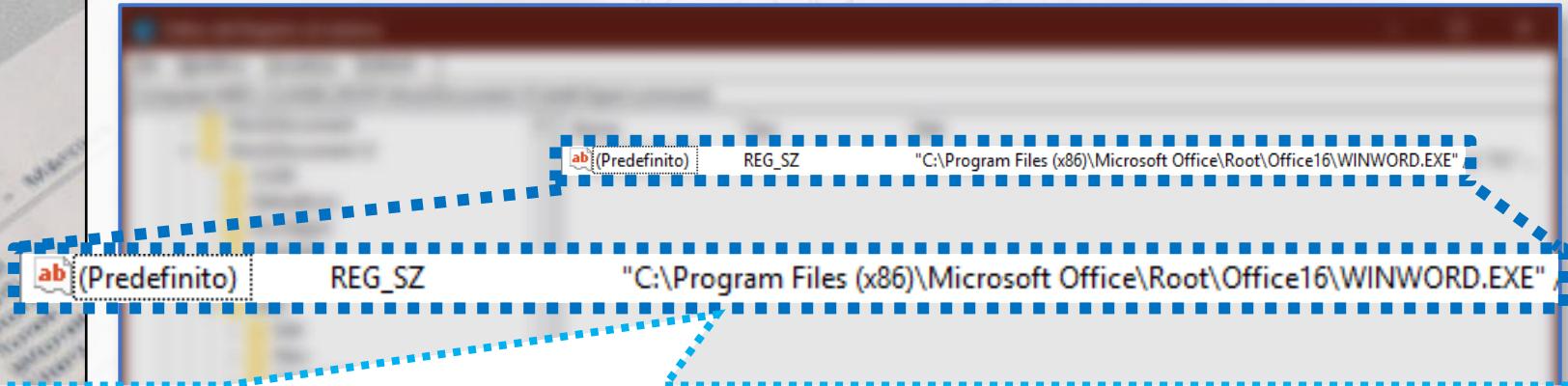
(Predefinito) è l'unico valore della sotto-chiave **command** (al percorso di registro: [...] \Word.Document.12\shell\Open\command)

Analisi del Registro di Sistema

Chiave Radice HKCR | 4/4

Esempio | Passo 6 di 6

In un live system, si intende individuare quale programma è utilizzato da Windows, in risposta all'azione di apertura di file con estensione .docx (eseguita dall'utente, tramite Esplora Risorse)



Nel contenuto (elemento *Dati*) del valore (Predefinito), è specificato, in questo caso, il percorso (nel file system) relativo all'**eseguibile del programma**, utilizzato da Windows, per l'apertura dei file con estensione .docx:

C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE

Analisi del Registro di Sistema

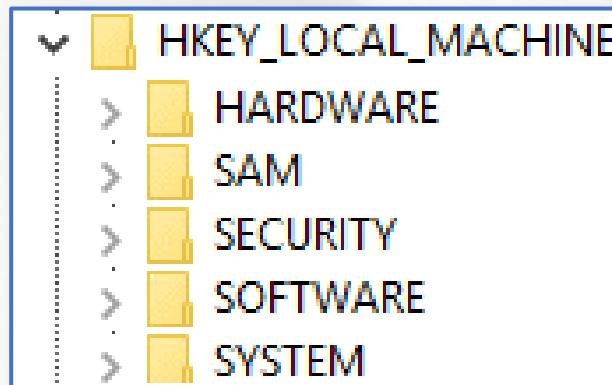
Chiavi Radice

- Le **cinque chiavi radice** del registro di sistema, sono le seguenti:
 - `HKEY_CLASSES_ROOT`
 - **`HKEY_LOCAL_MACHINE`**
 - `HKEY_CURRENT_USER`
 - `HKEY_USERS`
 - `HKEY_CURRENT_CONFIG`
- Ogni chiave radice:
 - Ha il compito di memorizzare specifiche informazioni ed impostazioni del sistema in uso e/o degli utenti
 - È memorizzata all'interno del file system, in uno o più file specifici, chiamati **registry hive file** (o **hive file**)

Analisi del Registro di Sistema

Chiave Radice HKLM | 1/4

- La chiave radice **HKEY_LOCAL_MACHINE** (o **HKLM**) contiene informazioni sulla configurazione della macchina
- Tale chiave radice è **indipendente dall'utente autenticato**



Analisi del Registro di Sistema

Chiave Radice HKLM | 2/4

- La chiave radice **HKEY_LOCAL_MACHINE** contiene cinque sotto-chiavi:
 - System
 - Software
 - SAM
 - Security
 - Hardware

Analisi del Registro di Sistema

Chiave Radice HKLM | 3/4

- La chiave radice **HKEY_LOCAL_MACHINE** contiene cinque sotto-chiavi:
 - **System**
 - Contiene settaggi, preferenze ed informazioni del sistema, come, ad esempio, il nome della macchina, il fuso orario, le interfacce di rete, i dispositivi di memorizzazione collegati al sistema, ecc.
 - Software
 - SAM
 - Security
 - Hardware

Analisi del Registro di Sistema

Chiave Radice HKLM | 3/4

- La chiave radice **HKEY_LOCAL_MACHINE** contiene cinque sotto-chiavi:
 - System
 - **Software**
 - Contiene settaggi e preferenze, relative ad applicazioni installate ed a servizi installati, nel sistema
 - SAM
 - Security
 - Hardware

Analisi del Registro di Sistema

Chiave Radice HKLM | 3/4

- La chiave radice **HKEY_LOCAL_MACHINE** contiene cinque sotto-chiavi:
 - System
 - Software
 - **SAM**
 - Acronimo di Security Account Manager (SAM)
 - Contiene informazioni di sicurezza, in merito agli utenti ed a eventuali gruppi di utenti
 - Contiene tutte le informazioni relative ad i permessi degli utenti, forniti dall'amministratore
 - Contiene il *nome utente* (username), il SID (acronimo di Secure ID: si tratta di un identificativo univoco associato a ciascun utente) e le relative password (crittografate) degli utenti
 - Security
 - Hardware

Analisi del Registro di Sistema

Chiave Radice HKLM | 3/4

- La chiave radice **HKEY_LOCAL_MACHINE** contiene cinque sotto-chiavi:
 - System
 - Software
 - **SAM**
 - Acronimo di Security Account Manager (SAM)
 - Contiene informazioni di sicurezza, in merito agli utenti ed a eventuali gruppi
 - Con forniti
 - Con ID: utenti
 - Security
 - Hardware

OSSERVAZIONE

Per ragioni di sicurezza, Windows non permette l'accesso a questa sotto-chiave (essa appare vuota), sul sistema in uso

Può essere però estratta, dalla macchina in uso, ed analizzata su un'altra macchina

Analisi del Registro di Sistema

Chiave Radice HKLM | 3/4

- La chiave radice **HKEY_LOCAL_MACHINE** contiene cinque sotto-chiavi:
 - System
 - Software
 - SAM
 - **Security**
 - Contiene eventuali policy di sicurezza
 - Hardware

Analisi del Registro di Sistema

Chiave Radice HKLM | 3/4

- La chiave radice **HKEY_LOCAL_MACHINE** contiene cinque sotto-chiavi:
 - System
 - Software
 - SAM
 - **Security**
 - Contiene eventuali policy di sicurezza
 - Hardware

OSSERVAZIONE

Analogamente alla sotto-chiave SAM, anche questa chiave non può essere direttamente acceduta, sul sistema in uso

Analisi del Registro di Sistema

Chiave Radice HKLM | 3/4

- La chiave radice **HKEY_LOCAL_MACHINE** contiene cinque sotto-chiavi:
 - System
 - Software
 - SAM
 - Security
 - **Hardware**
 - Informazioni, settaggi ed impostazioni dei dispositivi collegati al sistema
 - Tali informazioni sono memorizzate in fase di boot

Analisi del Registro di Sistema

Chiave Radice HKLM | 4/4

Esempio | Utilizzo della Chiave Radice HKLM

In un live system, si intende conoscere la tipologia del dispositivo di memorizzazione (ad esempio, penna USB, disco fisso, ecc.), collegato al sistema, al quale è stata associata la lettera **E**:

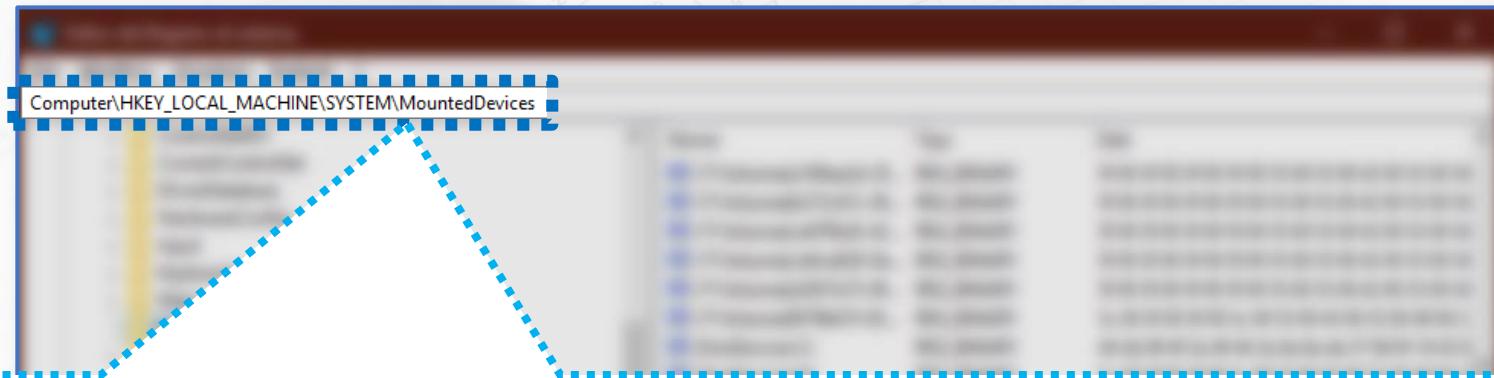
NOTA: È possibile utilizzare il tool Editor del Registro di sistema

Analisi del Registro di Sistema

Chiave Radice HKLM | 4/4

Esempio | Passo 1 di 3

In un live system, si intende conoscere la tipologia del dispositivo di memorizzazione (ad esempio, penna USB, disco fisso, ecc.), collegato al sistema, al quale è stata associata la lettera **E**:



Al percorso **HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices**, è possibile individuare tutti i **dispositivi di memorizzazione**, che sono **collegati al sistema o che sono stati collegati, precedentemente**

Analisi del Registro di Sistema

Chiave Radice HKLM | 4/4

Esempio | Passo 1 di 3

In un live system, si intende conoscere la tipologia del dispositivo di memorizzazione (ad esempio, penna USB, disco fisso, ecc.), collegato al sistema, al quale è stata associata la lettera **E**:



Analisi del Registro di Sistema

Chiave Radice HKLM | 4/4

Esempio | Passo 2 di 3

In un live system, si intende conoscere la tipologia del dispositivo di memorizzazione (ad esempio, penna USB, disco fisso, ecc.), collegato al sistema, al quale è stata associata la lettera **E**:

Lista dei Dispositivi di Memorizzazione

 \DosDevices\C:	REG_BINARY	44 4d 49 4f 3a 49 44 3a 6e 6e de 57 66 f0 18 43 8
 \DosDevices\D:	REG_BINARY	5c 00 3f 00 3f 00 5c 00 53 00 43 00 53 00 49 00 2
 \DosDevices\E:	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54
 \DosDevices\F:	REG_BINARY	44 4d 49 4f 3a 49 44 3a f4 d0 45 25 d3 96 20 4b a
 \DosDevices\G:	REG_BINARY	5c 00 3f 00 3f 00 5c 00 44 00 54 00 4c 00 49 00 54
 \DosDevices\H:	REG_BINARY	44 4d 49 4f 3a 49 44 3a c4 c4 2c 4f 7c 8a da 47 a
 \DosDevices\I:	REG_BINARY	44 4d 49 4f 3a 49 44 3a 54 ab 8b 91 0d 4a 18 4f b
 \DosDevices\J:	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54
 \DosDevices\K:	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54

Analisi del Registro di Sistema

Chiave Radice HKLM | 4/4

Esempio | Passo 2 di 3

In un live system, si intende conoscere la tipologia del dispositivo di memorizzazione (ad esempio, penna USB, disco fisso, ecc.), collegato al sistema, al quale è stata associata la lettera **E**:

Lista dei Dispositivi di Memorizzazione

C:
D:
E:
F:
G:
H:
I:
J:
K:

Ciascuna lettera è un riferimento logico ad un dispositivo o ad una unità di memorizzazione, collegata al sistema (o che è stata collegata, precedentemente)

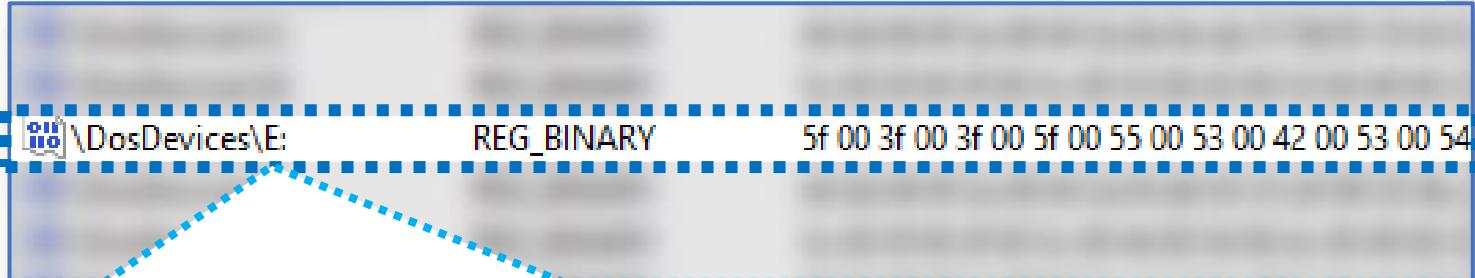
Analisi del Registro di Sistema

Chiave Radice HKLM | 4/4

Esempio | Passo 2 di 3

In un live system, si intende conoscere la tipologia del dispositivo di memorizzazione (ad esempio, penna USB, disco fisso, ecc.), collegato al sistema, al quale è stata associata la lettera **E**:

Lista dei Dispositivi di Memorizzazione



Effettuando un doppio click, sul valore evidenziato (riferito al dispositivo di memorizzazione, associato alla lettera **E:**), verrà aperta nuova schermata, la quale permetterà la visualizzazione e/o la modifica del contenuto (elemento *Dati*)

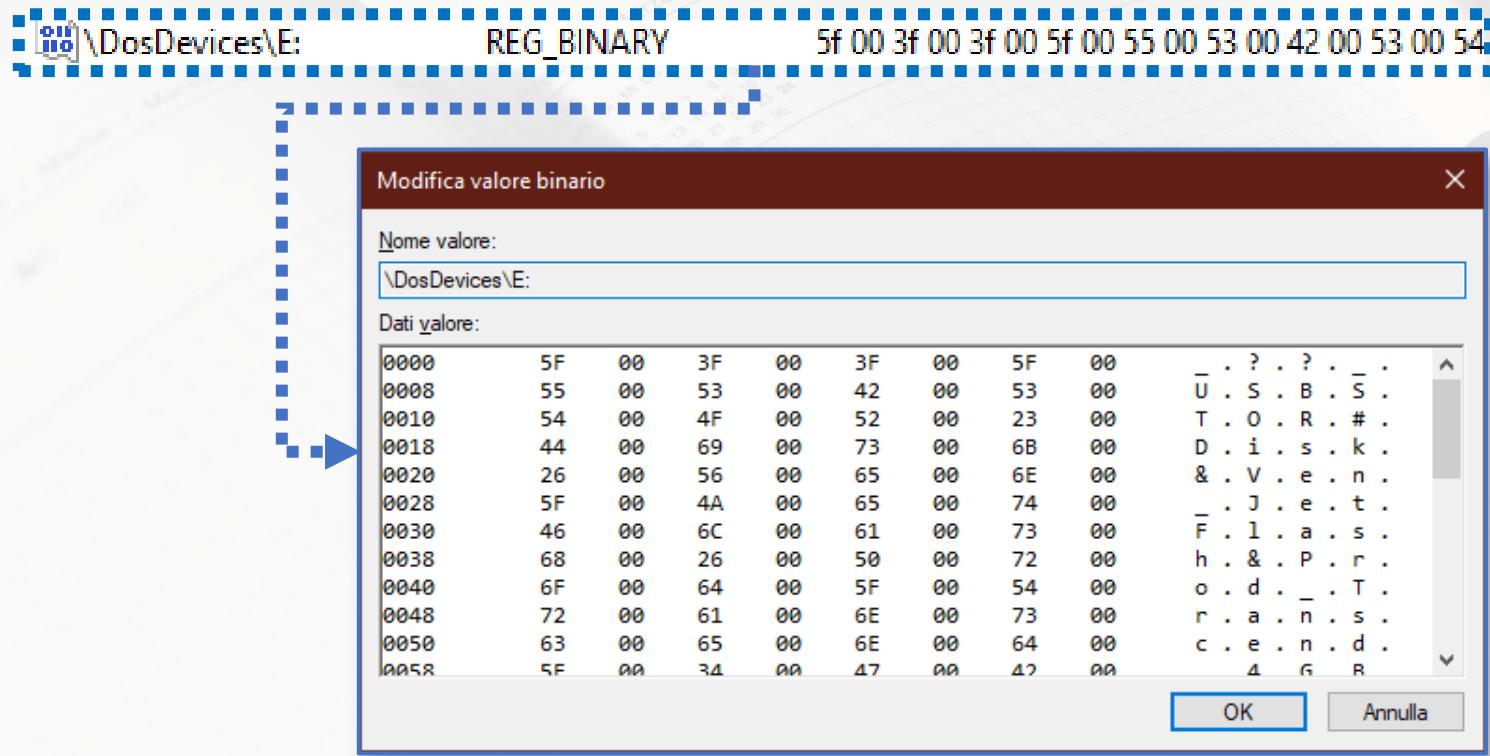
NOTA: Trattandosi di dati binari (elemento *Tipo* uguale a `REG_BINARY`), verranno mostrate due rappresentazioni (esadecimale e testuale)

Analisi del Registro di Sistema

Chiave Radice HKLM | 4/4

Esempio | Passo 3 di 3

In un live system, si intende conoscere la tipologia del dispositivo di memorizzazione (ad esempio, penna USB, disco fisso, ecc.), collegato al sistema, al quale è stata associata la lettera **E**:



Analisi del Registro di Sistema

Chiave Radice HKLM | 4/4

Esempio | Passo 3 di 3

In un live system, si intende conoscere la tipologia del dispositivo di memorizzazione (ad esempio, penna USB, disco fisso, ecc.), collegato al sistema, al quale è stata associata la lettera **E**:

 \DosDevices\E: REG_BINARY 5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54

Rappresentazione testuale, del contenuto (elemento *Dati*), relativo al valore selezionato

5F	00	3F	00	3F	00	5F	00	..	?	?	?
55	00	53	00	42	00	53	00	U	.	S	.	S	.
54	00	4F	00	52	00	23	00	T	.	O	.	R	#
44	00	69	00	73	00	6B	00	D	.	i	.	s	k
26	00	56	00	65	00	6E	00	&	.	V	.	e	n
5F	00	4A	00	65	00	74	00	..	J	.	e	e	t
46	00	6C	00	61	00	73	00	F	.	1	.	a	s
68	00	26	00	50	00	72	00	h	.	&	.	P	r
6F	00	64	00	5F	00	54	00	o	d	.	_	T	.
72	00	61	00	6E	00	73	00	r	.	a	.	n	s
63	00	65	00	6E	00	64	00	c	e	.	n	d	.
5F	00	34	00	47	00	42	00	4	G	R			

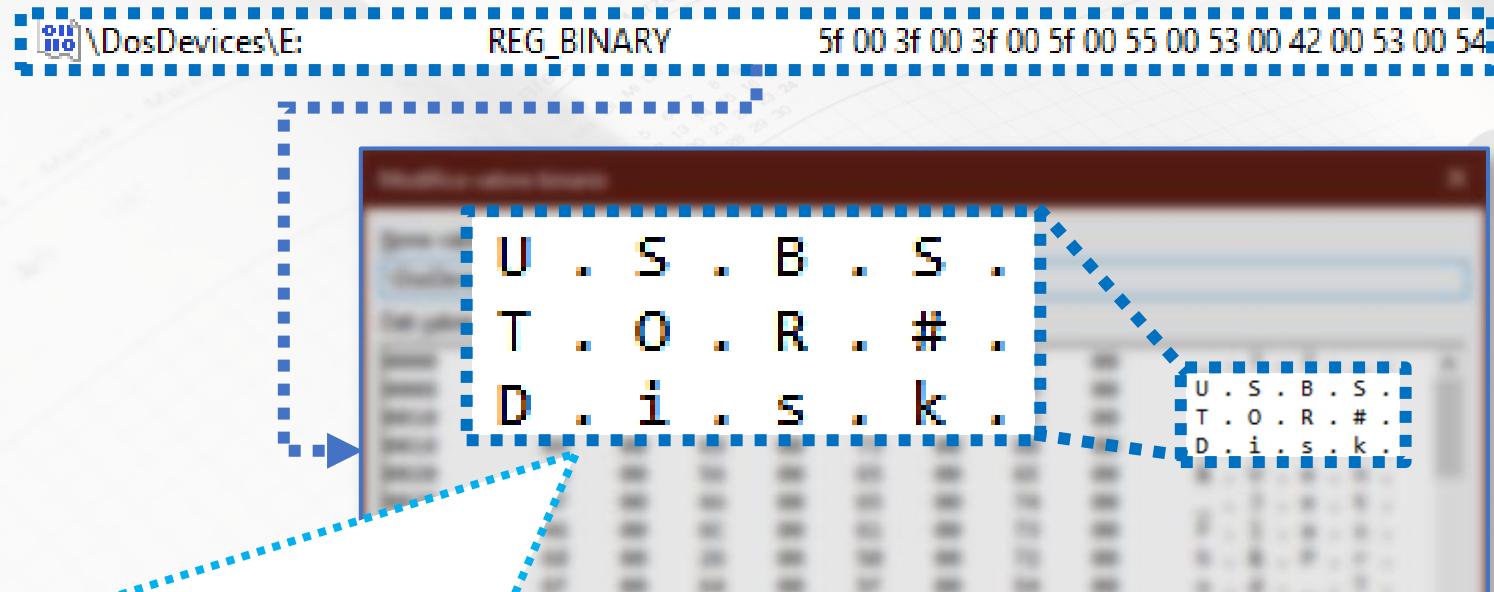
Rappresentazione in esadecimale, del contenuto (elemento *Dati*), relativo al valore selezionato

Analisi del Registro di Sistema

Chiave Radice HKLM | 4/4

Esempio | Passo 3 di 3

In un live system, si intende conoscere la tipologia del dispositivo di memorizzazione (ad esempio, penna USB, disco fisso, ecc.), collegato al sistema, al quale è stata associata la lettera **E**:



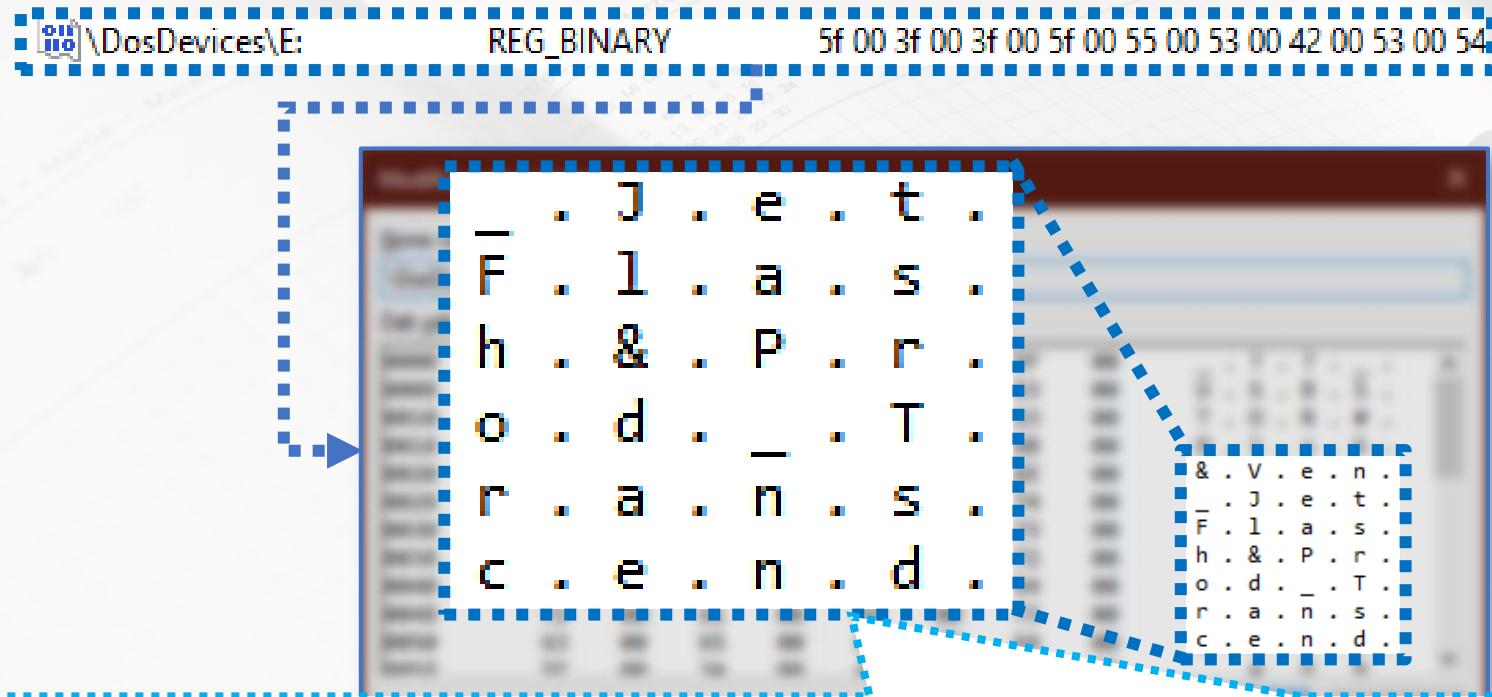
Dalla rappresentazione testuale, è possibile individuare la stringa «**USB STOR Disk**», la quale indica che la tipologia del dispositivo è una penna (o un dispositivo similare), collegato ad una porta USB del sistema

Analisi del Registro di Sistema

Chiave Radice HKLM | 4/4

Esempio | Passo 3 di 3

In un live system, si intende conoscere la tipologia del dispositivo di memorizzazione (ad esempio, penna USB, disco fisso, ecc.), collegato al sistema, al quale è stata associata la lettera **E**:



Inoltre, è possibile individuare le stringhe «**Jet Flash**» e «**Transcend**», le quali si riferiscono rispettivamente al modello del dispositivo USB ed alla marca

Analisi del Registro di Sistema

Chiave Radice HKLM | 4/4

Esempio | Passo 3 di 3

In un live system, si intende conoscere la tipologia del dispositivo di memorizzazione (ad esempio, penna USB, disco fisso, ecc.), collegato al sistema, al quale è stata associata la lettera **E**:

 \DosDevices\E: REG_BINARY 5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54

In questo caso, è possibile individuare la stringa «**4 GB**», la quale fa verosimilmente riferimento alla dimensione del supporto (ovvero, 4 GB)

4 . G . B .
4 G R

Analisi del Registro di Sistema

Chiavi Radice

- Le **cinque chiavi radice** del registro di sistema, sono le seguenti:
 - HKEY_CLASSES_ROOT
 - HKEY_LOCAL_MACHINE
 - **HKEY_CURRENT_USER**
 - HKEY_USERS
 - HKEY_CURRENT_CONFIG
- Ogni chiave radice:
 - Ha il compito di memorizzare specifiche informazioni ed impostazioni del sistema in uso e/o degli utenti
 - È memorizzata all'interno del file system, in uno o più file specifici, chiamati ***registry hive file*** (o ***hive file***)

Analisi del Registro di Sistema

Chiave Radice HKCU | 1/2

- In Windows, a ciascun utente è associato un *profilo*
- Un profilo specifica la configurazione e le preferenze, per Windows stesso e per eventuali altri software, relative ad un determinato utente
 - Ad esempio, lo sfondo del desktop, i colori degli elementi dell'interfaccia grafica, la dimensione delle finestre, le impostazioni del mouse, ecc.
- Inoltre, a ciascun profilo è associata una *cartella di profilo*, in cui l'utente può memorizzare i suoi file (ad esempio, documenti, immagini, video, download, ecc.)
 - Il percorso di tale cartella è tipicamente il seguente:
C:\Users\<NomeUtente>

Analisi del Registro di Sistema

Chiave Radice HKCU | 2/2

- Quando un utente effettua l'autenticazione con successo, Windows ne caricherà il relativo profilo
 - In tal modo, l'utente autenticato potrà fruire del suo ambiente operativo (Windows ed eventuali altri software), in accordo alla sua configurazione e preferenze, e potrà fruire dei suoi file

La **configurazione** e le **preferenze**, relative al profilo dell'utente autenticato, sono memorizzate nella chiave radice **HKEY_CURRENT_USER** (o **HKCU**)

In tale chiave radice, inoltre, potrebbero essere presenti anche tracce di attività dell'utente autenticato

Analisi del Registro di Sistema

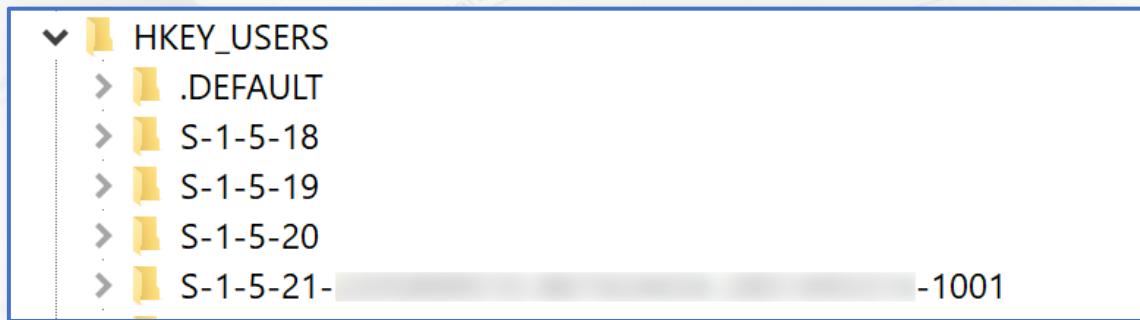
Chiavi Radice

- Le **cinque chiavi radice** del registro di sistema, sono le seguenti:
 - HKEY_CLASSES_ROOT
 - HKEY_LOCAL_MACHINE
 - HKEY_CURRENT_USER
 - **HKEY_USERS**
 - HKEY_CURRENT_CONFIG
- Ogni chiave radice:
 - Ha il compito di memorizzare specifiche informazioni ed impostazioni del sistema in uso e/o degli utenti
 - È memorizzata all'interno del file system, in uno o più file specifici, chiamati ***registry hive file*** (o ***hive file***)

Analisi del Registro di Sistema

Chiave Radice HKU | 1/4

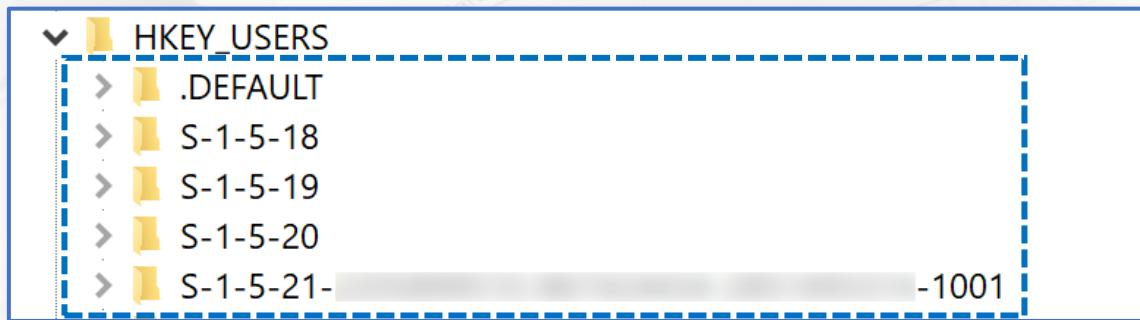
- La chiave radice **HKEY_USERS** (o **HKU**) memorizza le configurazioni e le preferenze, relative ai profili degli utenti autenticati, nel sistema



Analisi del Registro di Sistema

Chiave Radice HKU | 1/4

- La chiave radice **HKEY_USERS** (o **HKU**) memorizza le configurazioni e le preferenze, relative ai profili degli utenti autenticati, nel sistema



Analisi del Registro di Sistema

Chiave Radice HKU | 1/4

- La chiave radice **HKEY_USERS** (o **HKU**) memorizza le configurazioni e le preferenze, relative ai profili degli utenti autenticati, nel sistema



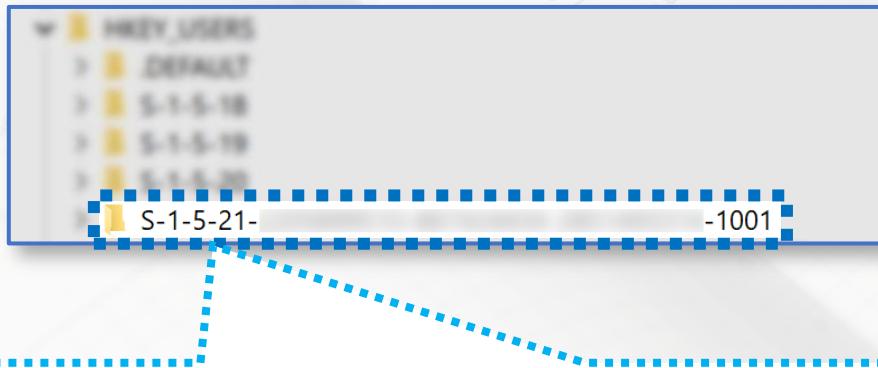
In questo esempio, sono presenti cinque sotto-chiavi, relative ai profili degli utenti autenticati, nel sistema:

- Quattro fanno riferimento ad **utenti «speciali»** di Windows
 - Tali utenti sono gestiti/utilizzati dal S.O. e servono per eseguire servizi o altre attività di sistema
- Una fa riferimento all'**utente** (autenticato) [NOTA: è riportato il relativo SID]
 - Tutti gli utenti (non «speciali»), hanno un SID che inizia per **S-1-5-21**
 - Tramite ciò è stato possibile dedurre che la sotto-chiave, evidenziata in verde, facesse riferimento ad un utente (non «speciale»)

Analisi del Registro di Sistema

Chiave Radice HKU | 2/4

- La chiave radice **HKEY_USERS** (o **HKU**) memorizza le configurazioni e le preferenze, relative ai profili degli utenti autenticati, nel sistema



Questa sotto-chiave memorizza quindi la **configurazione** e le **preferenze**, relative al profilo dell'utente autenticato

Contiene le stesse informazioni della chiave radice **HKEY_CURRENT_USER**, discussa precedentemente

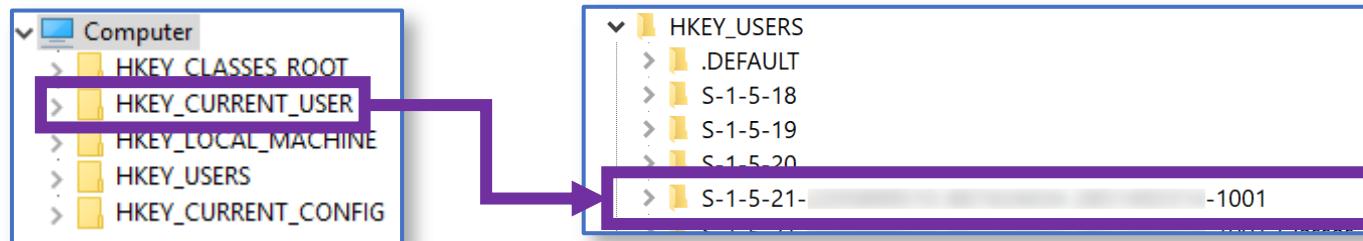
Analisi del Registro di Sistema

Chiave Radice HKU | 2/4

- La chiave radice **HKEY_USERS** (o **HKU**) memorizza le

OSSERVAZIONE

- Infatti, la chiave radice **HKEY_CURRENT_USER** (discussa precedentemente), è un *alias* che fa riferimento alla chiave radice **HKEY_USERS (HKU)**



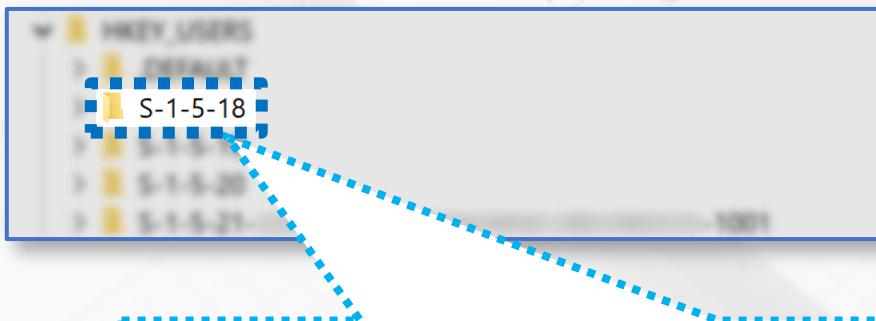
HKEY_CURRENT_USER

HKEY_USERS\<SIDUtenteAutenticato>

Analisi del Registro di Sistema

Chiave Radice HKU | 2/4

- La chiave radice **HKEY_USERS** (o **HKU**) memorizza le configurazioni e le preferenze, relative ai profili degli utenti autenticati, nel sistema

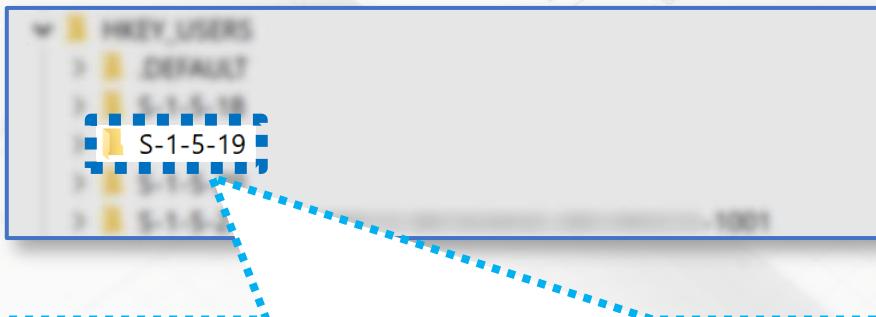


La sotto-chiave **S-1-5-18**, fa riferimento al profilo dell'**utente «speciale»** di Windows, denominato **Sistema (System)**

Analisi del Registro di Sistema

Chiave Radice HKU | 2/4

- La chiave radice **HKEY_USERS** (o **HKU**) memorizza le configurazioni e le preferenze, relative ai profili degli utenti autenticati, nel sistema

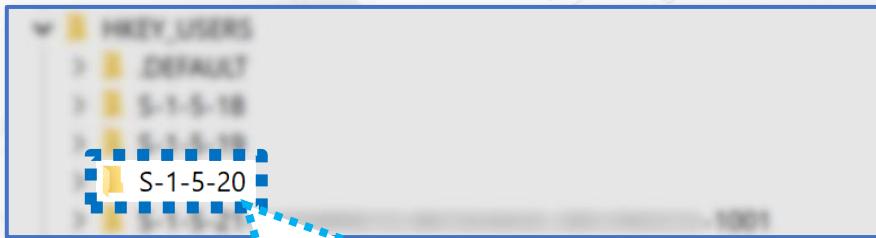


La sotto-chiave **S-1-5-19**, fa riferimento al profilo dell'**utente «speciale»** di Windows, denominato **Servizio Locale (LocalService)**

Analisi del Registro di Sistema

Chiave Radice HKU | 2/4

- La chiave radice **HKEY_USERS** (o **HKU**) memorizza le configurazioni e le preferenze, relative ai profili degli utenti autenticati, nel sistema



La sotto-chiave **S-1-5-20**, fa riferimento al profilo dell'**utente «speciale»** di Windows, denominato **Servizio di Rete (NetworkService)**

Analisi del Registro di Sistema

Chiave Radice HKU | 2/4

- La chiave radice memorizza le configurazioni e le preferenze autenticati.



La sotto-chiave **.DEFAULT** memorizza la configurazione e le preferenze, in riferimento al profilo di un **utente «speciale»**, denominato **utente di Default**

Quando viene creato un nuovo utente, esso non avrà alcun profilo, pertanto, Windows ne creerà uno nuovo, che sarà una copia del profilo dell'utente di Default (includendo la configurazione e le preferenze)

In tal modo, potrà essere fornito un ambiente operativo di base, al nuovo utente, il quale potrà essere personalizzato, successivamente

NOTA: La copia del profilo, discussa sopra, verrà eseguita solo quando il nuovo utente effettuerà la prima autenticazione

Analisi del Registro di Sistema

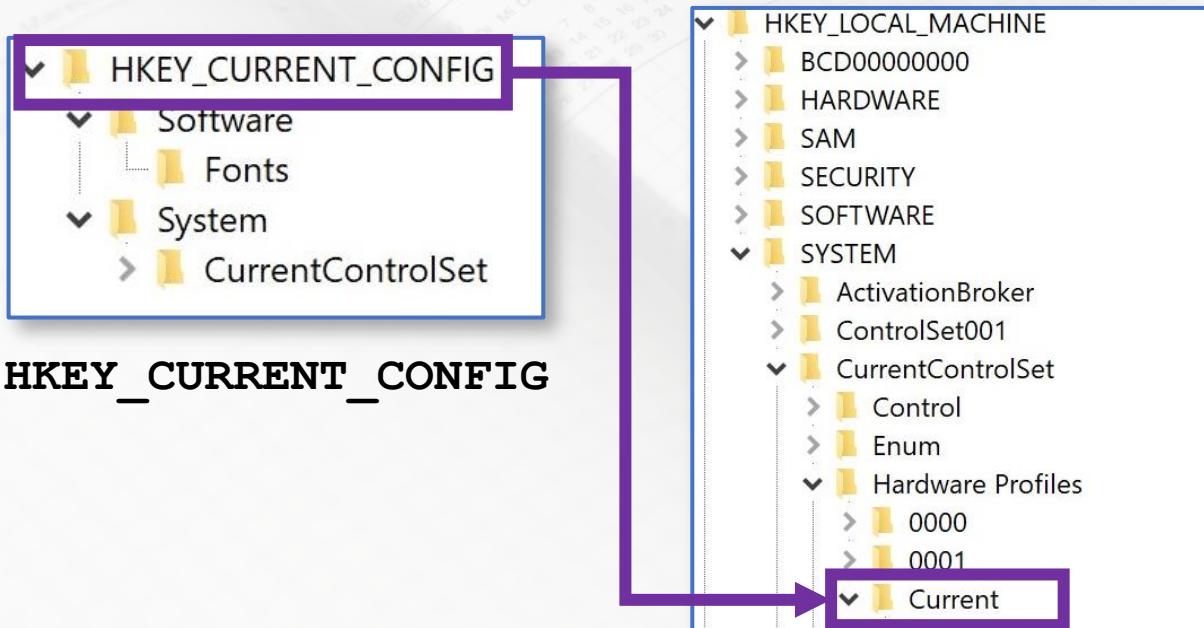
Chiavi Radice

- Le **cinque chiavi radice** del registro di sistema, sono le seguenti:
 - **HKEY_CLASSES_ROOT**
 - **HKEY_LOCAL_MACHINE**
 - **HKEY_CURRENT_USER**
 - **HKEY_USERS**
 - **HKEY_CURRENT_CONFIG**
- Ogni chiave radice:
 - Ha il compito di memorizzare specifiche informazioni ed impostazioni del sistema in uso e/o degli utenti
 - È memorizzata all'interno del file system, in uno o più file specifici, chiamati ***registry hive file*** (o ***hive file***)

Analisi del Registro di Sistema

Chiave Radice HKCC

- **HKEY_CURRENT_CONFIG** (o **HCC**) è un *alias* che fa riferimento alla chiave radice **HKEY_LOCAL_MACHINE (HKLM)**
 - Memorizza informazioni riguardanti il profilo hardware, utilizzato dalla macchina, all'avvio del sistema



HKEY_CURRENT_CONFIG
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current

Analisi del Registro di Sistema

Percorsi degli Hive nel File System | 1/3

- In precedenza, abbiamo osservato che ogni chiave radice è memorizzata in uno (o più) file (detti anche *hive file*), all'interno del file system
 - Nella seguente tabella, sono riportate alcune corrispondenze tra chiavi radici ed i percorsi degli hive file, nel file system (riportati in blu)

HKEY_CURRENT_USER

È memorizzato nell'hive file **NTUSER.DAT**, il quale è localizzato all'interno della cartella di profilo, dell'utente autenticato (posizione tipica: **C:\Users\<NomeUtente>**)

HKEY_LOCAL_MACHINE

System	C:\Windows\System32\config\System
SAM	C:\Windows\System32\config\SAM
Security	C:\Windows\System32\config\Security
Software	C:\Windows\System32\config\Software

Analisi del Registro di Sistema

Percorsi degli Hive nel File System | 2/3

- In precedenza, abbiamo osservato che ogni chiave radice è memorizzata in uno (o più) file (detti anche *hive file*), all'interno del file system
 - Nella seguente tabella, sono riportate alcune corrispondenze tra chiavi radici ed i percorsi degli hive file, nel file system (riportati in **blu**)

HKEY_CURRENT_USER

È memorizzato nell'hive file **NTUSER.DAT**, il quale è localizzato all'interno della cartella di profilo, dell'utente autenticato (posizione tipica: **C:\Users\<NomeUtente>**)

HKEY_LOCAL_MACHINE

System	C:\Windows\system32\config\System
SAM	C:\Windows\system32\config\SAM

La cartella **C:\Users\<NomeUtente>** è accessibile anche dalla locazione
C:\Documents and Settings\<NomeUtente>

Analisi del Registro di Sistema

Percorsi degli Hive nel File System | 3/3

OSSERVAZIONE IMPORTANTE

Queste informazioni sono rilevanti, poiché da una immagine forense (acquisita da un dead system o da un live system) è possibile accedere ai vari *hive file*, al fine di effettuare l'analisi forense del registro

HKEY_CURRENT_USER

È memorizzato nell'hive file **NTUSER.DAT**, il quale è localizzato all'interno della cartella di profilo, dell'utente autenticato (posizione tipica: **C:\Users\<NomeUtente>**)

HKEY_LOCAL_MACHINE

System	C:\Windows\System32\config\System
SAM	C:\Windows\System32\config\SAM
Security	C:\Windows\System32\config\Security
Software	C:\Windows\System32\config\Software

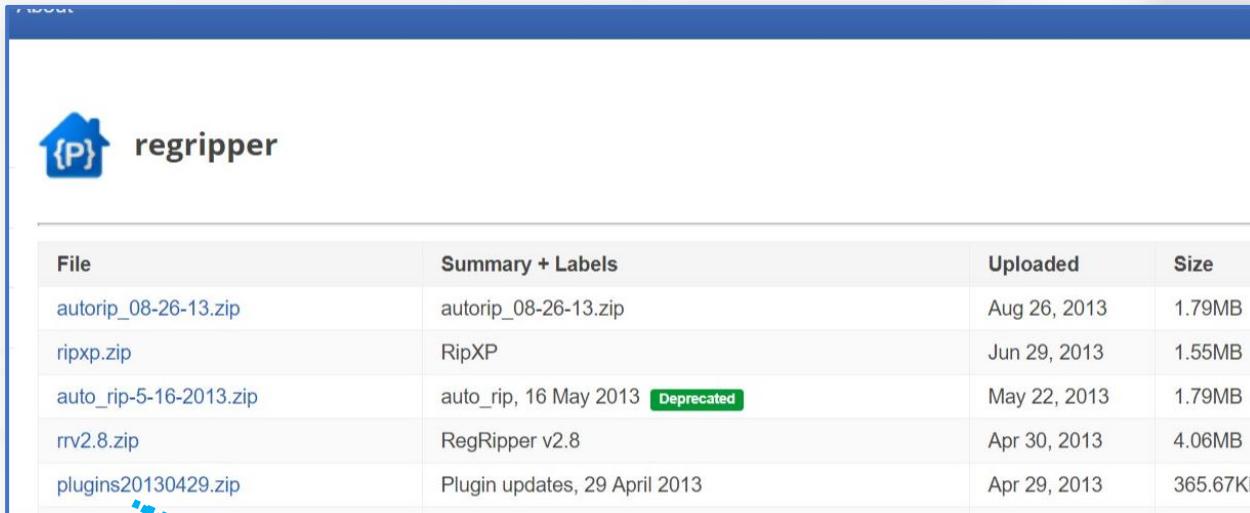
Analisi del Registro di Sistema

Il tool RegRipper | 1/4

- Per l'analisi degli hive file di registro, è possibile utilizzare il tool **RegRipper**
- Il tool RegRipper, scritto in Perl, è Open-Source ed è gratuitamente scaricabile
 - È in grado di effettuare il parsing della struttura del registro (analizzando gli hive file), **focalizzandosi sulle aree di interesse forense**
- Presenta un'interfaccia utente semplice e funzionale
- L'eseguibile è scaricabile al seguente link:
 - <https://code.google.com/p/regripper/>

Analisi del Registro di Sistema

Il tool RegRipper | 2/4



The screenshot shows a list of files uploaded to the regripper project on Google Code. The files are:

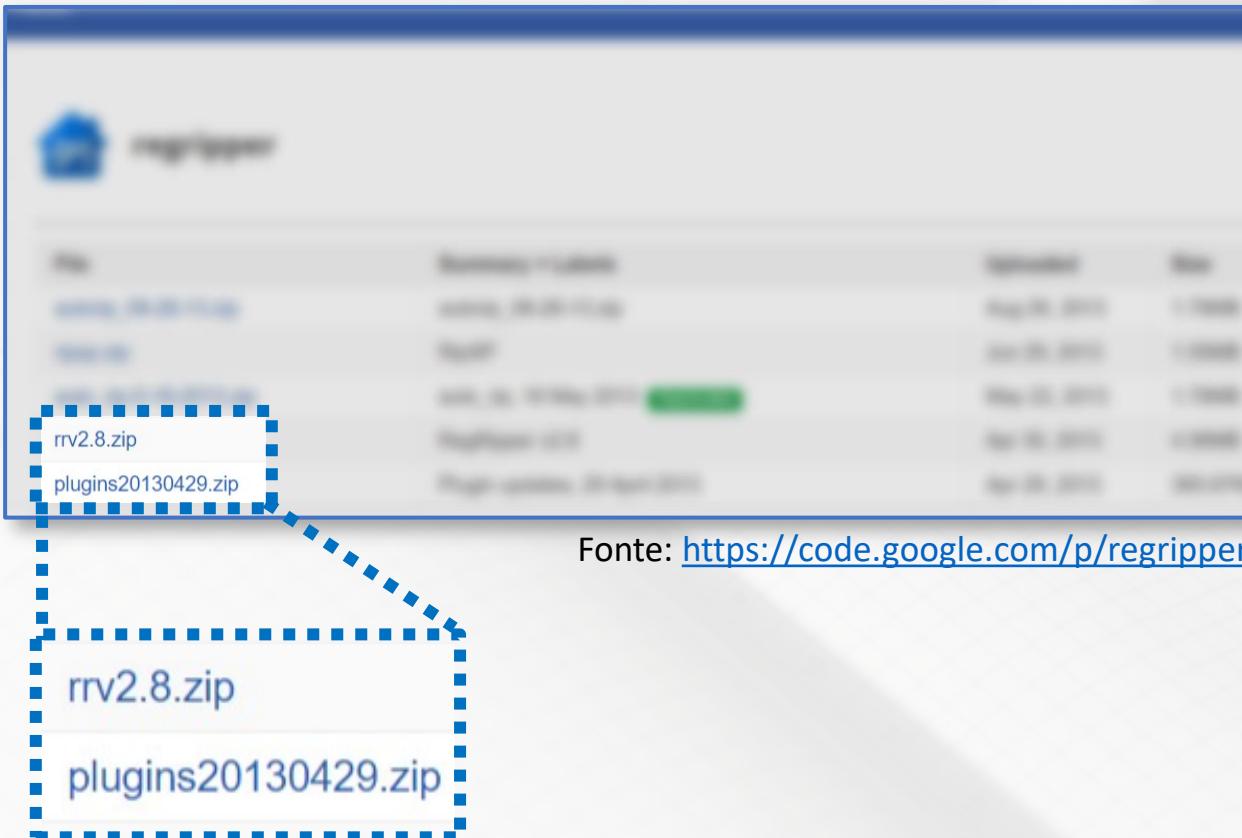
File	Summary + Labels	Uploaded	Size
autorip_08-26-13.zip	autorip_08-26-13.zip	Aug 26, 2013	1.79MB
ripxp.zip	RipXP	Jun 29, 2013	1.55MB
auto_rip-5-16-2013.zip	auto_rip, 16 May 2013 <small>Deprecated</small>	May 22, 2013	1.79MB
rrv2.8.zip	RegRipper v2.8	Apr 30, 2013	4.06MB
plugins20130429.zip	Plugin updates, 29 April 2013	Apr 29, 2013	365.67KB

Fonte: <https://code.google.com/p/regripper/>

NOTA: Oltre l'eseguibile, è necessario scaricare anche i plugin di RegRipper

Analisi del Registro di Sistema

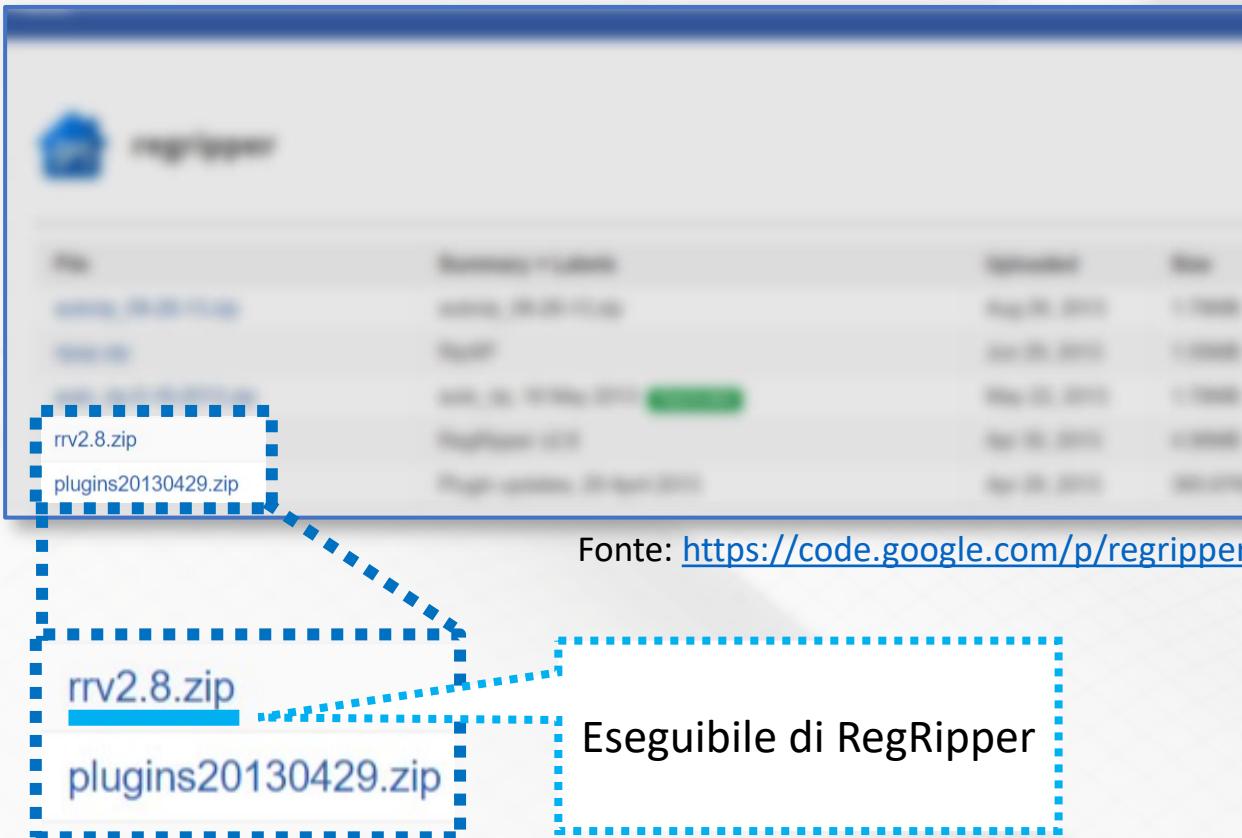
Il tool RegRipper | 2/4



Fonte: <https://code.google.com/p/regripper/>

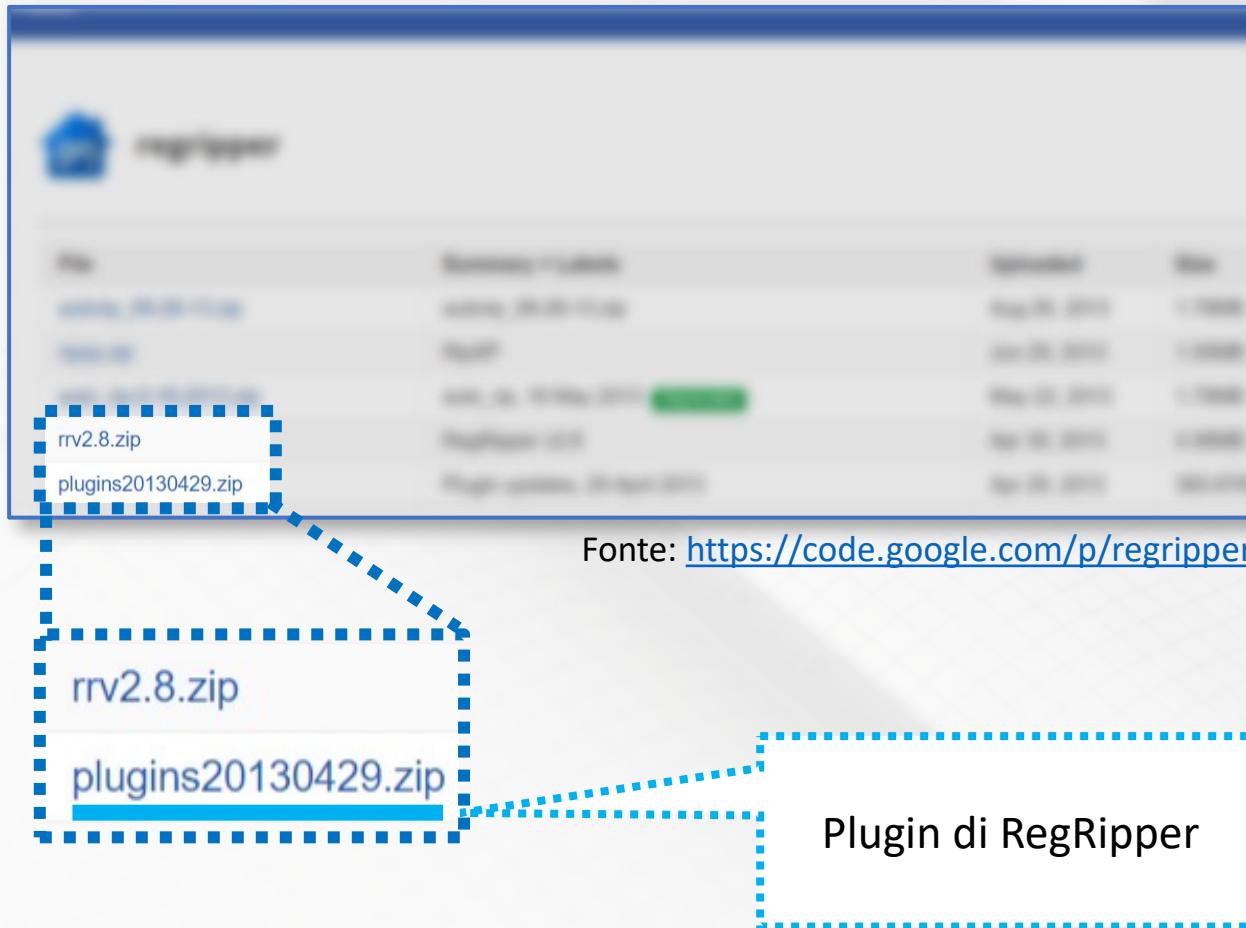
Analisi del Registro di Sistema

Il tool RegRipper | 2/4



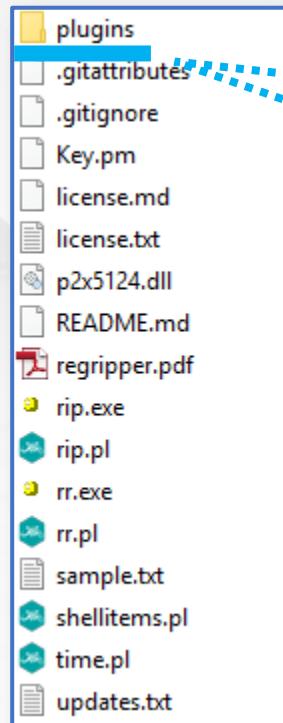
Analisi del Registro di Sistema

Il tool RegRipper | 2/4



Analisi del Registro di Sistema

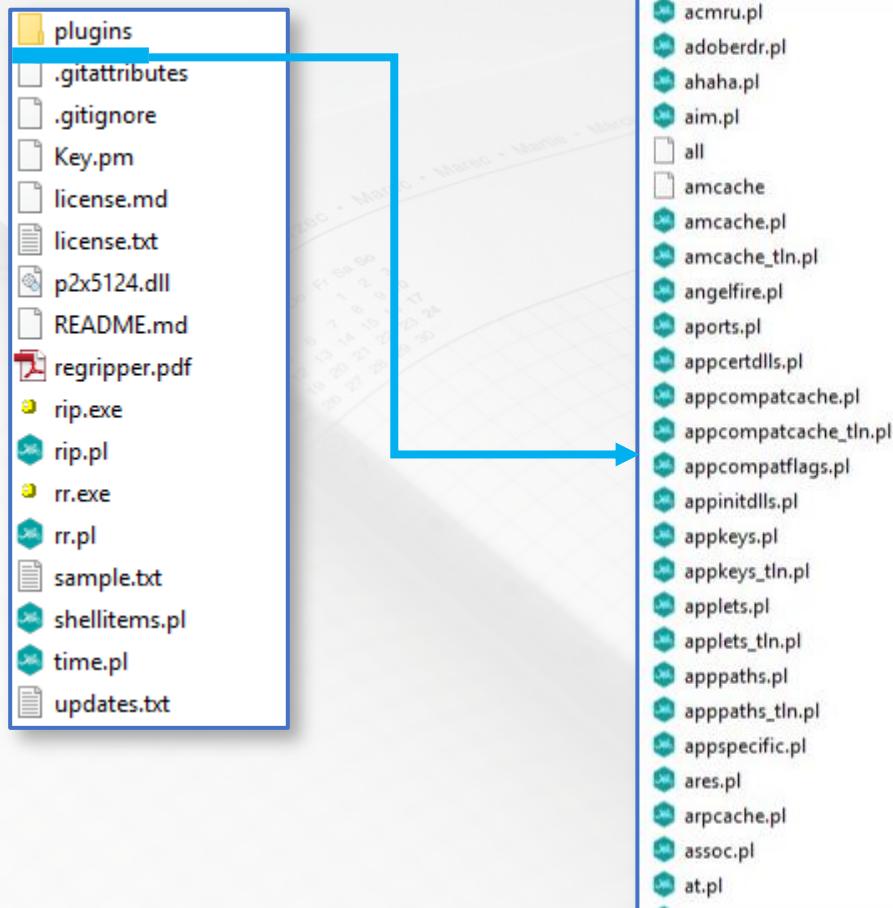
Il tool RegRipper | 3/4



I plugin vanno memorizzati tutti nella cartella plugin

Analisi del Registro di Sistema

Il tool RegRipper | 3/4

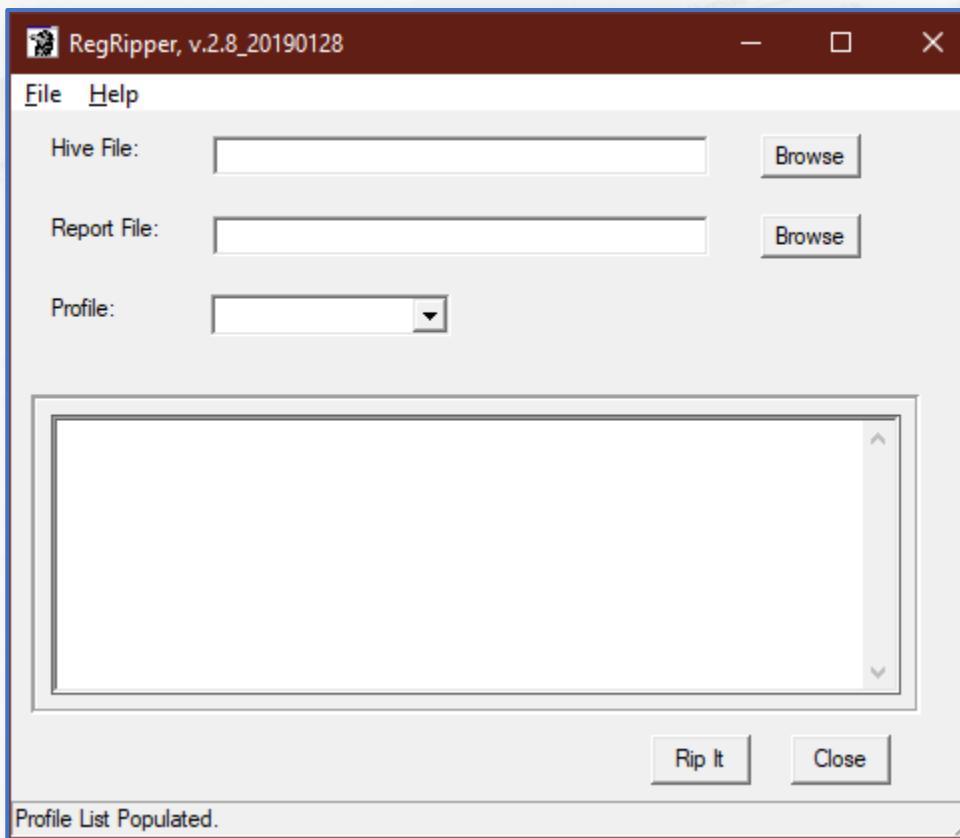


Cartella plugin

Analisi del Registro di Sistema

Il tool RegRipper | 4/4

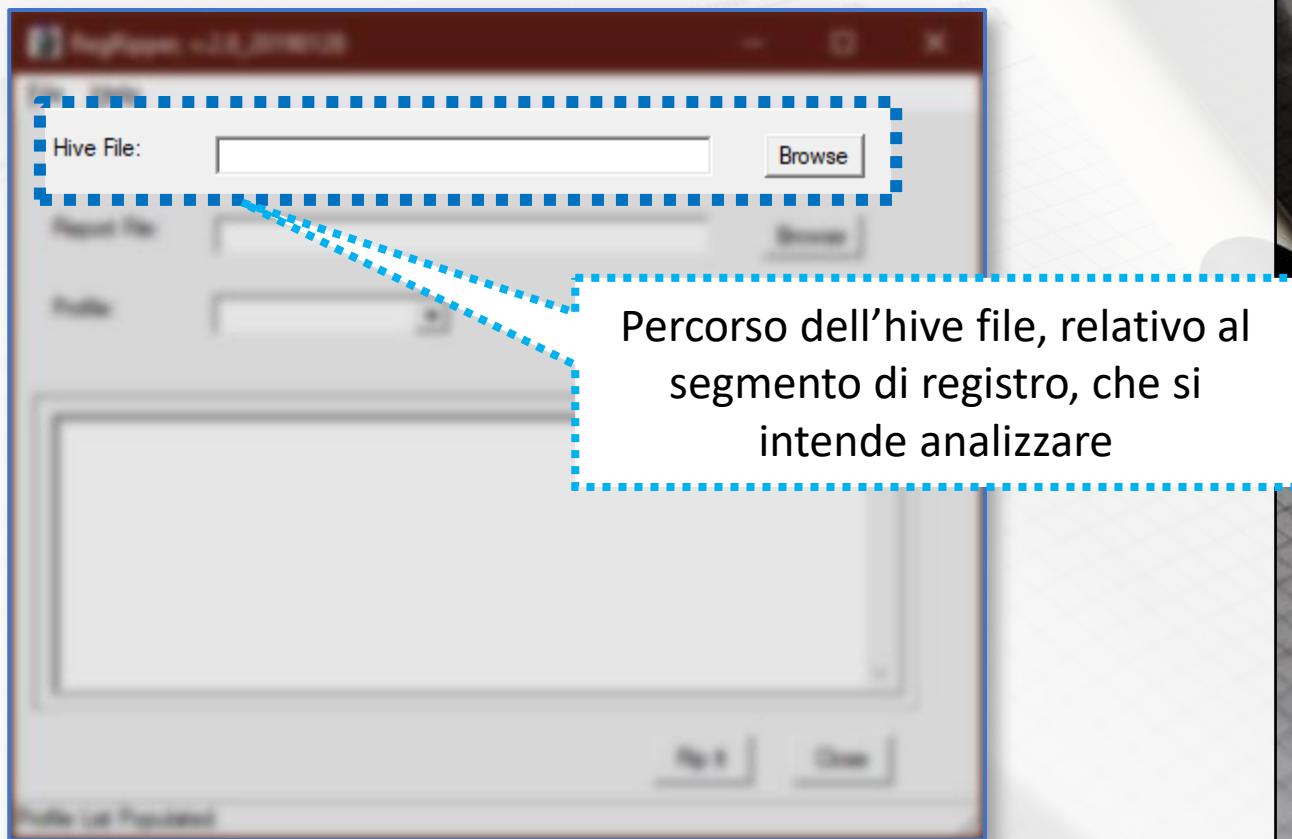
- *Interfaccia Grafica del tool RegRipper*



Analisi del Registro di Sistema

Il tool RegRipper | 4/4

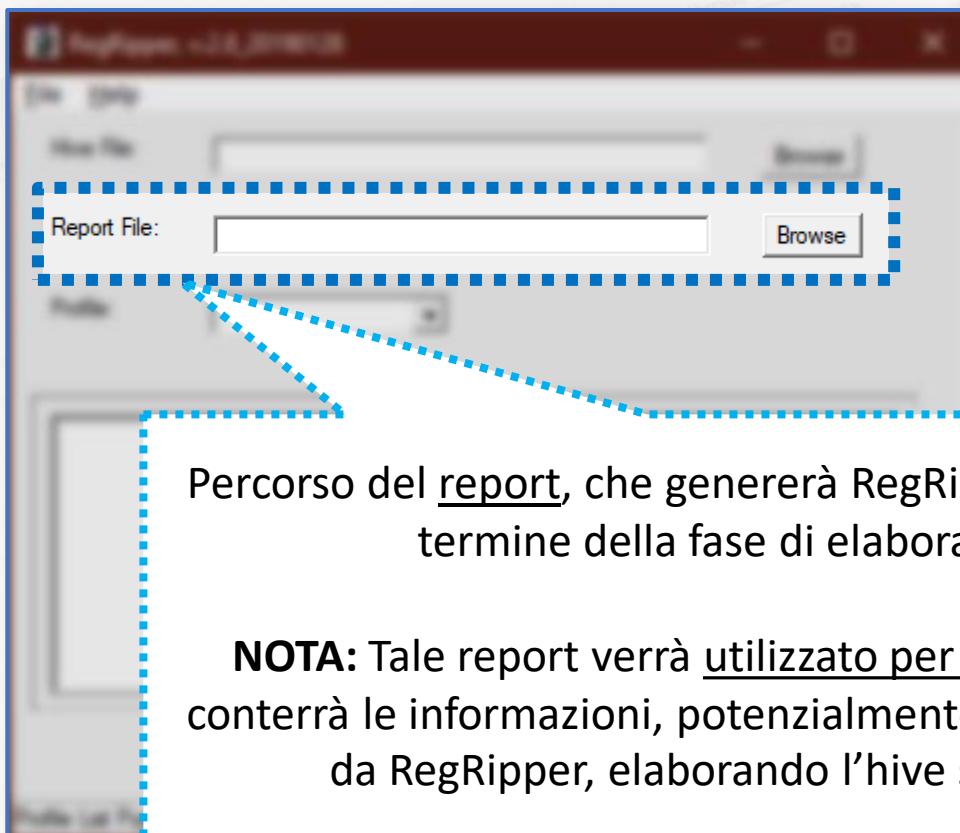
- *Interfaccia Grafica del tool RegRipper*



Analisi del Registro di Sistema

Il tool RegRipper | 4/4

- *Interfaccia Grafica del tool RegRipper*



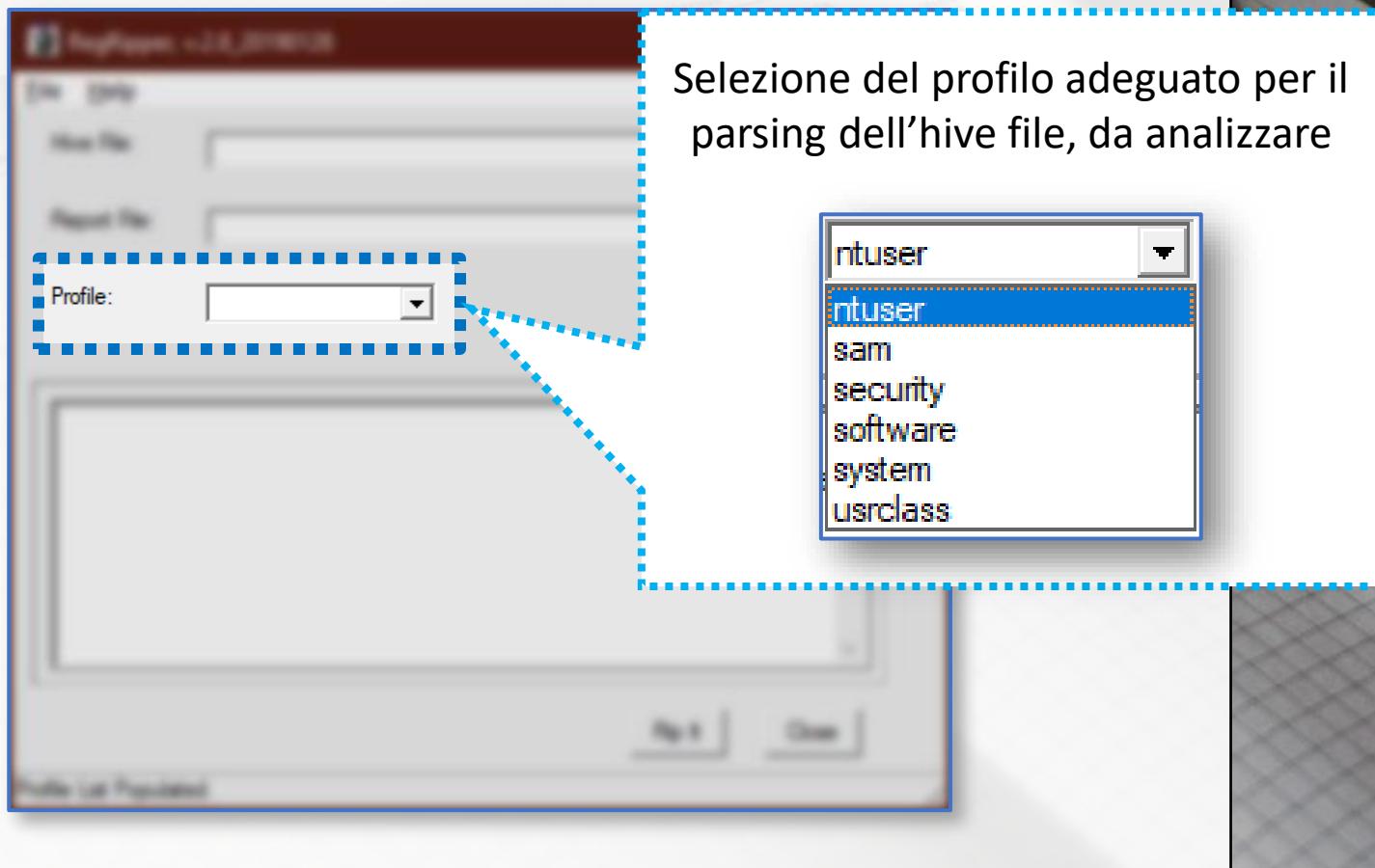
Percorso del report, che genererà RegRipper, in output, al termine della fase di elaborazione

NOTA: Tale report verrà utilizzato per l'analisi, poiché conterrà le informazioni, potenzialmente utili, individuate da RegRipper, elaborando l'hive specificato

Analisi del Registro di Sistema

Il tool RegRipper | 4/4

- *Interfaccia Grafica del tool RegRipper*



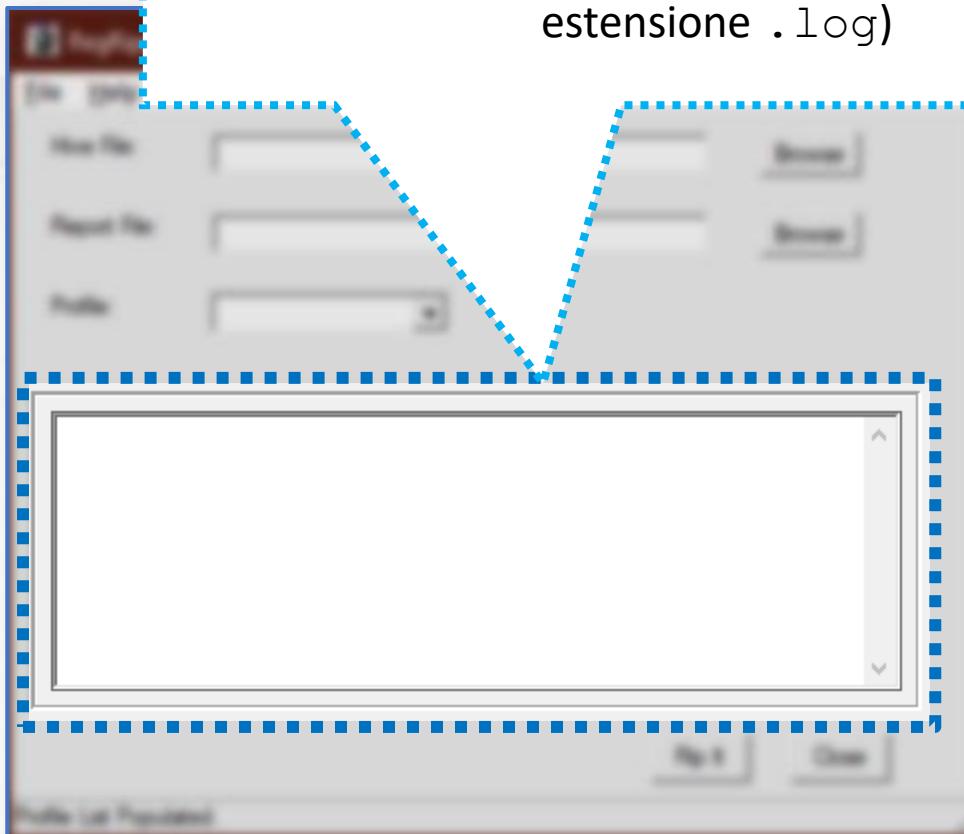
Analisi del Registro di Sistema

Il tool RegRipper | 4/4

- *Interfaccia Grafica*

Log della fase di elaborazione

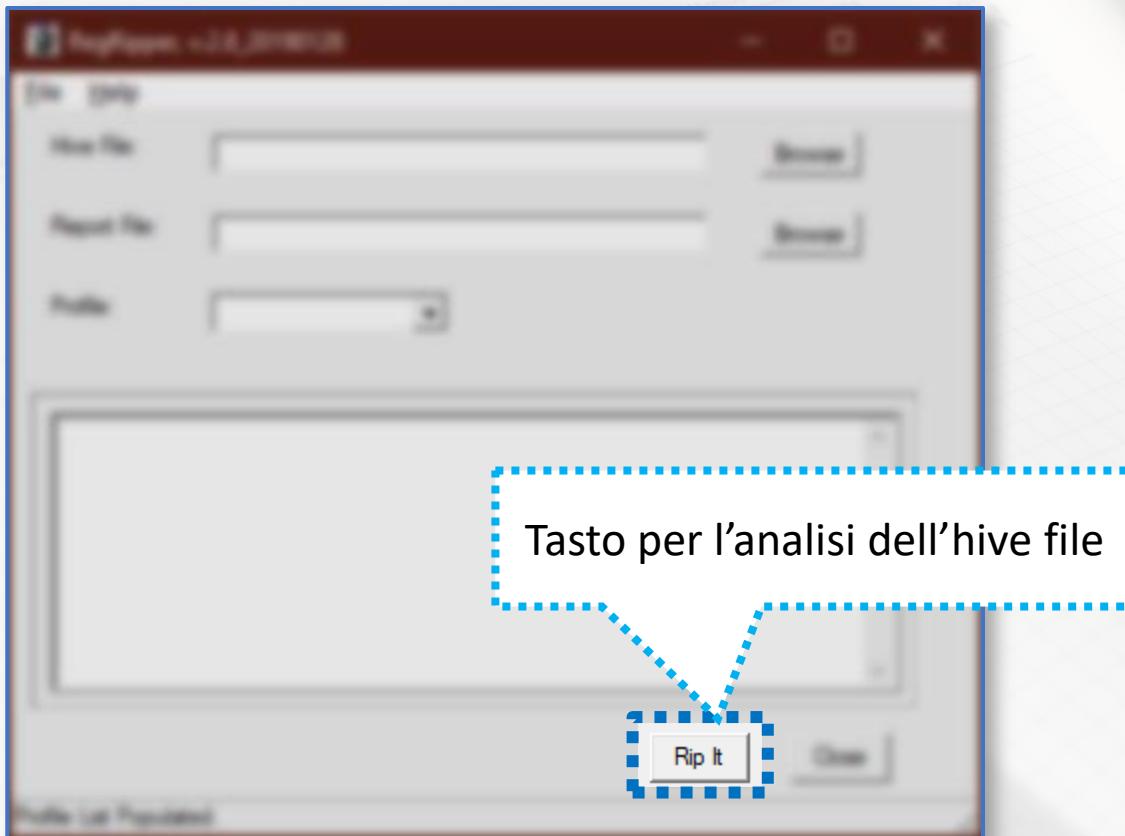
NOTA: Il log è memorizzato anche in un file (con estensione .log)



Analisi del Registro di Sistema

Il tool RegRipper | 4/4

- *Interfaccia Grafica del tool RegRipper*



lipiec

16

July / July / Lipiec

Poniedziałek
Monday / niedziela
Eustachego, Benedykta i Mał-



Analisi dei Registri degli Eventi

Analisi dei Registri degli Eventi

Caratteristiche Principali | 1/5

- Durante l'esecuzione di un software complesso, come il S.O., accadono innumerevoli **eventi**
 - La natura degli eventi è vastissima
- La maggior parte di essi è *registrata* dal S.O., mediante un sistema di memorizzazione, denominato **Event Logging**
 - Gli eventi vengono memorizzati all'interno di registri degli eventi (detti anche **event log** o, più semplicemente, **log**)
- Tali registri contengono informazioni importanti, derivanti dal software e dall'hardware
 - Le informazioni sono provenienti anche da applicativi, oltre che dal S.O., al fine di notificare eventuali informazioni all'utente
 - I registri possono essere utilizzati anche per la realizzazione di super timeline

Analisi dei Registri degli Eventi

Caratteristiche Principali | 2/5

- Tutti gli eventi, in Windows, sono gestiti e memorizzati dal servizio Event Logging (**Event Logging Service**)
- Gli eventi sono tutti registrati in ordine cronologico
 - In tal modo, è possibile individuare:
 - Eventuali criticità/problemi nell'ambito del S.O. e della sicurezza
 - Attività dell'utente
 - Utilizzo di risorse del sistema
- È necessario sottolineare, però, che le informazioni registrate, sono dipendenti dalla configurazione del S.O.
 - Ad esempio, è possibile disabilitare completamente il logging degli eventi

Analisi dei Registri degli Eventi

Caratteristiche Principali | 3/5

Possibili Informazioni Utili per l'Investigazione Forense fornite da un singolo Evento, memorizzato all'interno di un Registro

Tipologia

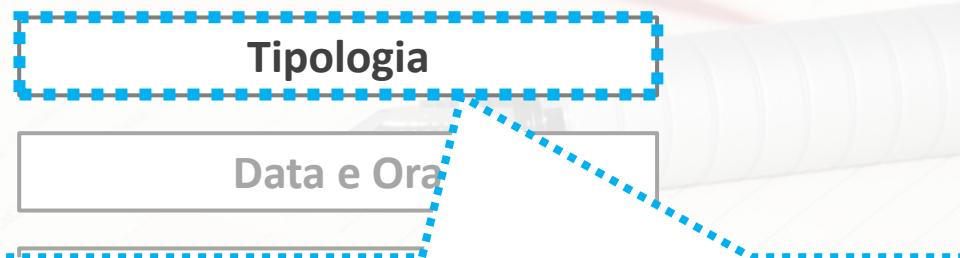
Data e Ora

Elementi Coinvolti/Acceduti

Analisi dei Registri degli Eventi

Caratteristiche Principali | 3/5

Possibili Informazioni Utili per l'Investigazione Forense fornite da un singolo Evento, memorizzato all'interno di un Registro

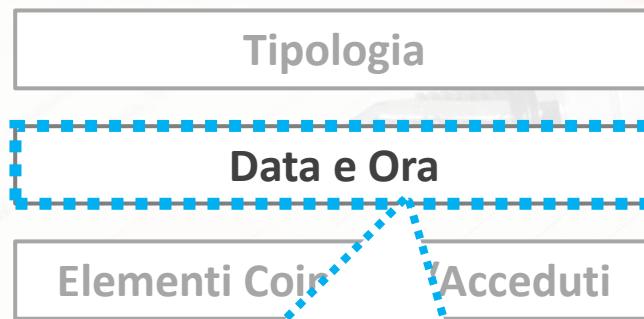


Tramite alcune informazioni, relative ad un evento, come l'**ID dell'evento** (*Event ID*) e/o **categoria dell'evento** (*Event Category*), è possibile individuare la tipologia di un evento

Analisi dei Registri degli Eventi

Caratteristiche Principali | 3/5

Possibili Informazioni Utili per l'Investigazione Forense fornite da un singolo Evento, memorizzato all'interno di un Registro

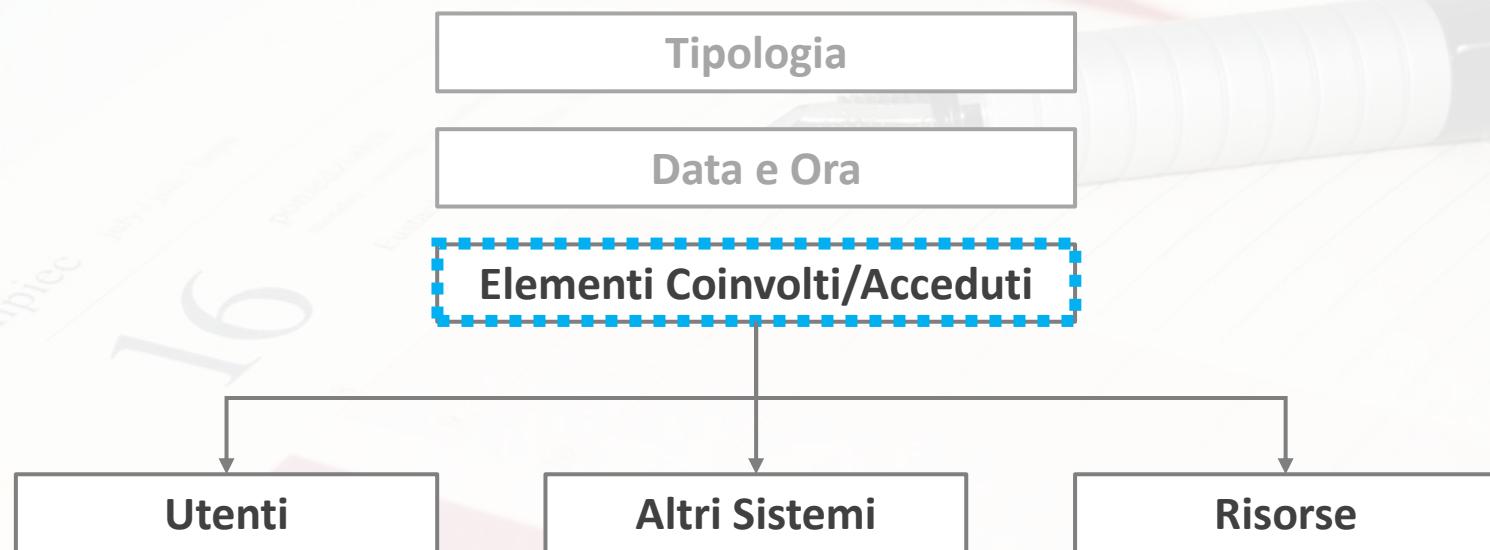


Per ciascun evento, viene riportato un *timestamp*, utile per contestualizzare la finestra temporale, in cui un certo evento ha avuto luogo

Analisi dei Registri degli Eventi

Caratteristiche Principali | 3/5

Possibili Informazioni Utili per l'Investigazione Forense fornite da un singolo Evento, memorizzato all'interno di un Registro

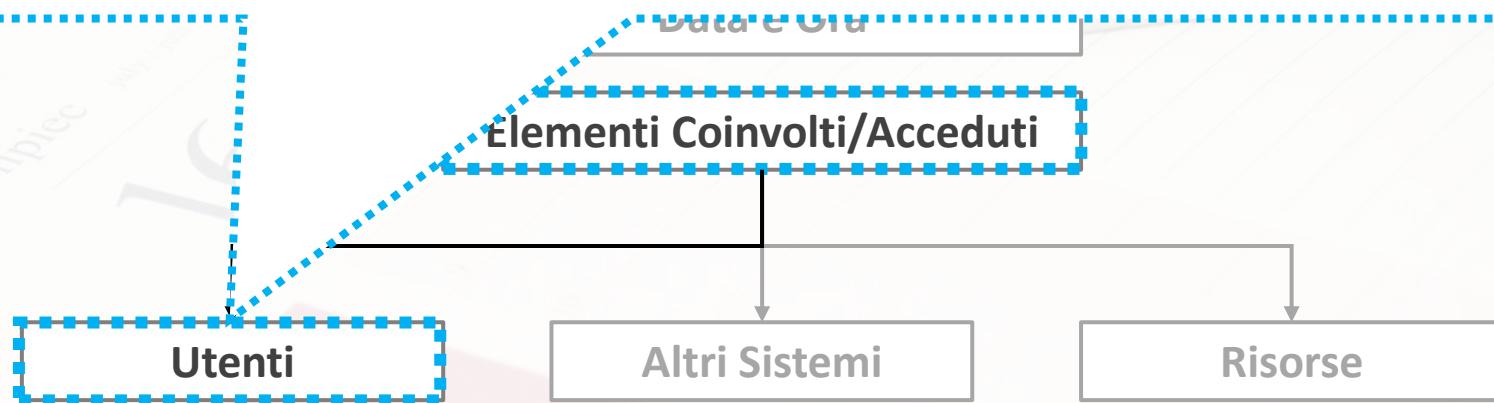


Analisi dei Registri degli Eventi

Caratteristiche Principali | 3/5

Vengono specificati gli utenti, coinvolti in un certo evento

NOTA: Si fa riferimento anche agli utenti «*speciali*» di Windows (ad esempio, l'utente speciale *Sistema*, l'utente speciale *Servizio di Rete*, ecc.), poiché alcuni eventi sono riferiti ad azioni svolte direttamente da Windows, tramite gli utenti speciali

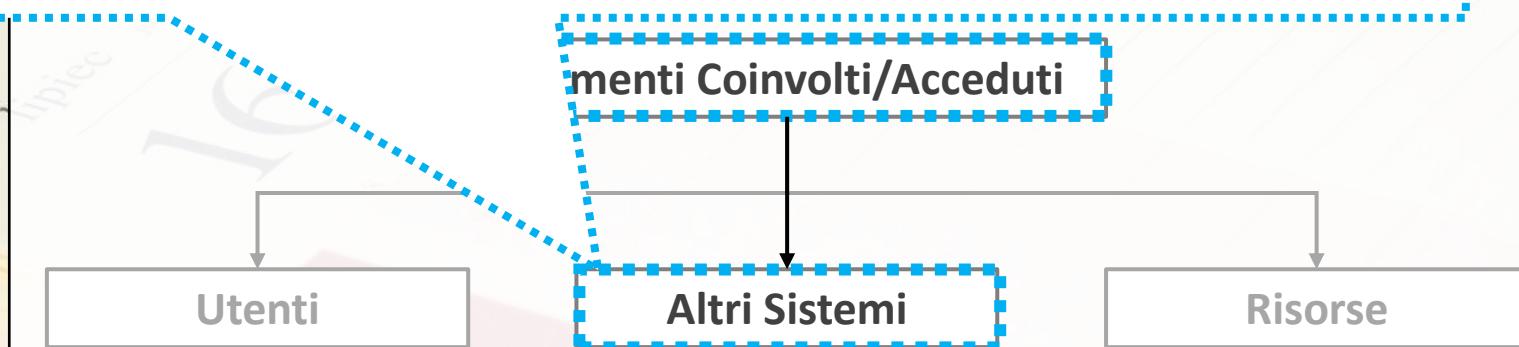


Analisi dei Registri degli Eventi

Caratteristiche Principali | 3/5

In ambiente di rete, i registri hanno solitamente molteplici riferimenti ad account di sistemi remoti

Nelle versioni più recenti di Windows, viene mantenuto anche l'indirizzo IP, all'interno dei log

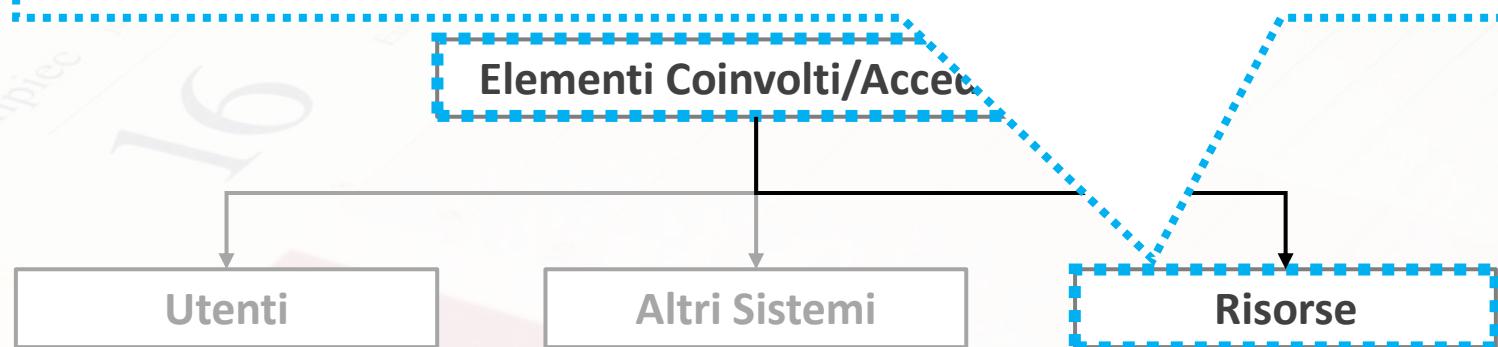


Analisi dei Registri degli Eventi

Caratteristiche Principali | 3/5

Possibili Informazioni Utili per l'Investigazione Forense fornite da un singolo Evento, memorizzato all'interno di un Registro

In base alla granularità della configurazione, i log possono riportare diverse informazioni in relazione a molteplici risorse del S.O.



Analisi dei Registri degli Eventi

Caratteristiche Principali | 4/5

- I registri (log) sono quindi una risorsa significativa, dal punto di vista forense, poiché, in essi, potrebbero essere presenti potenziali informazioni utili

Memorizzazione nel File System

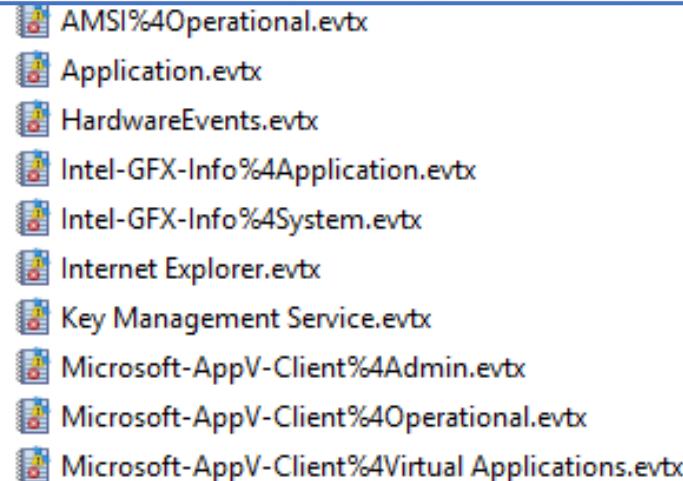
- Sono memorizzati in file con estensione .evtx, dal sistema di Event Logging
- La cartella in cui sono memorizzati è tipicamente la seguente:
 - C:\Windows\System32\WinEvt\Logs
 - NOTA:** Il percorso di tale cartella può comunque essere modificata dal registro di sistema

Analisi dei Registri degli Eventi

Caratteristiche Principali | 5/5

- Inoltre, è anche possibile impostare che i log vengano inviati ad un host remoto
 - Quindi, bisogna considerare anche l'eventuale possibilità che non tutti i log siano memorizzati all'interno della macchina, che si sta analizzando

Il numero totale di log è **superiore a 70**



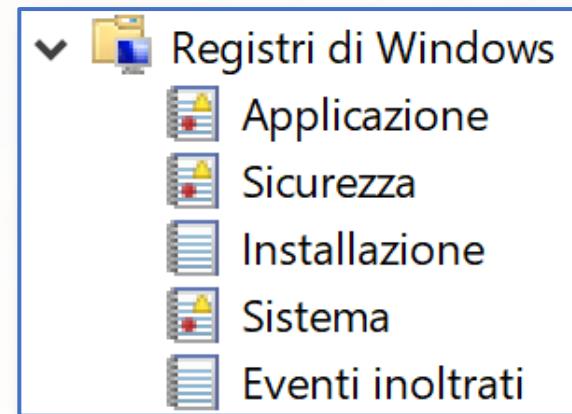
Alcuni dei file di log
(Alcune applicazioni hanno appositi file di log)

Analisi dei Registri degli Eventi

Principali Tipologie | 1/6

Alcune delle Principali Tipologie di Log

- Registro di Applicazione (Application Log)
- Registro di Sicurezza (Security Log)
- Installazione (Setup)
- Registro degli Eventi di Sistema (System Log)
- Eventi Inoltrati (Forwarded Events)



Analisi dei Registri degli Eventi

Principali Tipologie | 2/6

Alcune delle Principali Tipologie di Log

- **Registro di Applicazione (Application Log)**
 - È uno spazio utilizzato dalle applicazioni, che intendono registrare degli eventi significativi
 - *Esempio*
 - Un anti-virus potrebbe voler memorizzare eventi come l'individuazione di un malware, ecc.
- Registro di Sicurezza (Security Log)
- Installazione (Setup)
- Registro degli Eventi di Sistema (System Log)
- Eventi Inoltrati (Forwarded Events)

Analisi dei Registri degli Eventi

Principali Tipologie | 3/6

Alcune delle Principali Tipologie di Log

- Registro di Applicazione (Application Log)
- **Registro di Sicurezza (Security Log)**
 - Vengono registrati eventi relativi a controlli sulle politiche di accesso e di sicurezza locali e di gruppo
 - Maggiori dettagli nelle prossime slide
- Installazione (Setup)
- Registro degli Eventi di Sistema (System Log)
- Eventi Inoltrati (Forwarded Events)

Analisi dei Registri degli Eventi

Principali Tipologie | 4/6

Alcune delle Principali Tipologie di Log

- Registro di Applicazione (Application Log)
- Registro di Sicurezza (Security Log)
- **Installazione (Setup)**
 - Vengono memorizzate informazioni relative a Windows ed all'installazione di aggiornamenti
 - *Esempio*
 - Aggiornamenti di sicurezza
 - Installazione di patch
 - Ecc.
- Registro degli Eventi di Sistema (System Log)
- Eventi Inoltrati (Forwarded Events)

Analisi dei Registri degli Eventi

Principali Tipologie | 5/6

Alcune delle Principali Tipologie di Log

- Registro di Applicazione (Application Log)
- Registro di Sicurezza (Security Log)
- Installazione (Setup)
- **Registro degli Eventi di Sistema (System Log)**
 - Registra principalmente informazioni riguardanti le operazioni di sistema e la manutenzione di Windows
 - *Esempio*
 - Fallimento dell'avvio di un servizio, in fase di boot della macchina
- Eventi Inoltrati (Forwarded Events)

Analisi dei Registri degli Eventi

Principali Tipologie | 6/6

Alcune delle Principali Tipologie di Log

- Registro di Applicazione (Application Log)
- Registro di Sicurezza (Security Log)
- Installazione (Setup)
- Registro degli Eventi di Sistema (System Log)
- **Eventi Inoltrati (Forwarded Events)**
 - Registra eventi provenienti da computer remoti

Analisi dei Registri degli Eventi

Registro degli Eventi di Sicurezza (*Cenni*) | 1/3

- Prima che un utente possa eseguire una determinata operazione, sono necessari, talvolta, dei **controlli di sicurezza**
 - Il S.O. effettua i controlli di sicurezza per verificare se l'utente abbia o meno i privilegi necessari, per svolgere l'operazione che desidera
- I controlli di sicurezza vengono memorizzati nel **registro degli eventi di sicurezza**
 - Ciò permette di individuare lo svolgimento o meno (in base all'esito del controllo) di determinate operazioni, soggette a controlli di sicurezza
 - Ad esempio, l'autenticazione al sistema, accesso a un file protetto, ecc.

Analisi dei Registri degli Eventi

Registro degli Eventi di Sicurezza (*Cenni*) | 1/3

- Prima che un utente possa eseguire una determinata operazione, sono necessari, talvolta, dei controlli di sicurezza

• Il S.O. effettua i controlli di sicurezza per verificare se

OSSERVAZIONE IMPORTANTE

Alla luce delle caratteristiche del **registro degli eventi di sicurezza**, è facile osservare che essi costituiscano un elemento importante, per l'investigazione

~~base di esito dei controlli, di determinate operazioni,~~

soggette a controlli di sicurezza

- Ad esempio, l'autenticazione al sistema, accesso a un file protetto, ecc.

Analisi dei Registri degli Eventi

Registro degli Eventi di Sicurezza (Cenni) | 3/3

Possibili Motivi per cui viene Memorizzato un Evento di Sicurezza

Tipo di Evento	Descrizione
Errore (Critical/Error)	Notifica di un problema significativo <ul style="list-style-type: none"><i>Esempio:</i> Perdita di dati
Avviso (Warning)	Notifica di un problema non significativo <ul style="list-style-type: none"><i>Esempio:</i> Spazio in esaurimento
Informazioni (Information)	Notifica di una operazione eseguita con successo <ul style="list-style-type: none"><i>Esempio:</i> Corretto avvio di un servizio
Controllo Riuscito (Success Audit)	Notifica che un controllo, relativo allo svolgimento di una certa operazione, ha avuto esito positivo <ul style="list-style-type: none"><i>Esempio:</i> Autenticazione con successo di un utente
Controllo Fallito (Failure Audit)	Notifica che un controllo, relativo allo svolgimento di una certa operazione, ha avuto esito negativo <ul style="list-style-type: none"><i>Esempio:</i> Accesso ad una risorsa, senza avere permessi (accesso negato)

Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | Caratteristiche | 1/6

- Il tool **Visualizzatore Eventi (Event Viewer)** è un tool integrato in Windows
 - Permette di visualizzare tutti i registri del sistema in uso
- Gli eventi sono visualizzati in maniera molto dettagliata

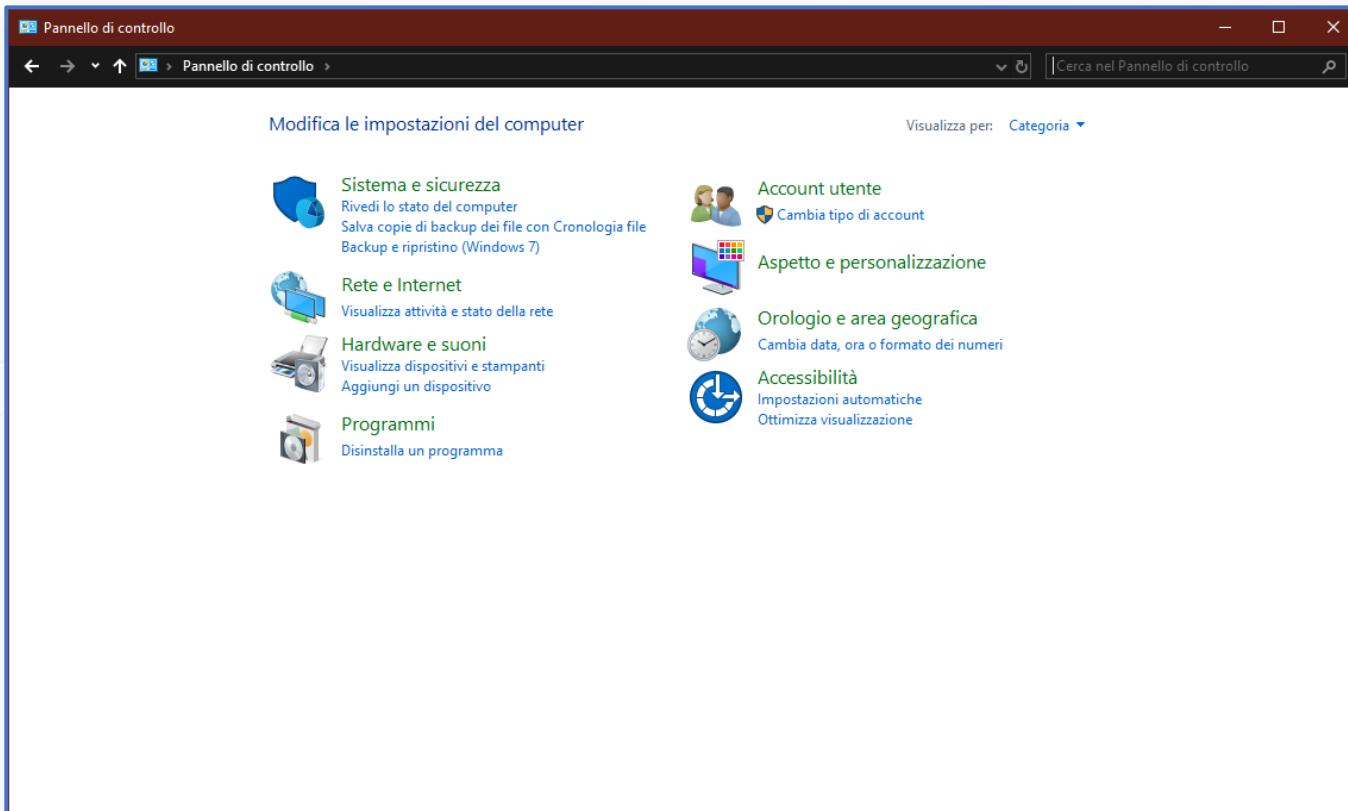
PRINCIPALE SVANTAGGIO

- L'analisi del registro può essere particolarmente complessa, per via di una interfaccia utente molto dettagliata, ma al contempo complessa

Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 2/6

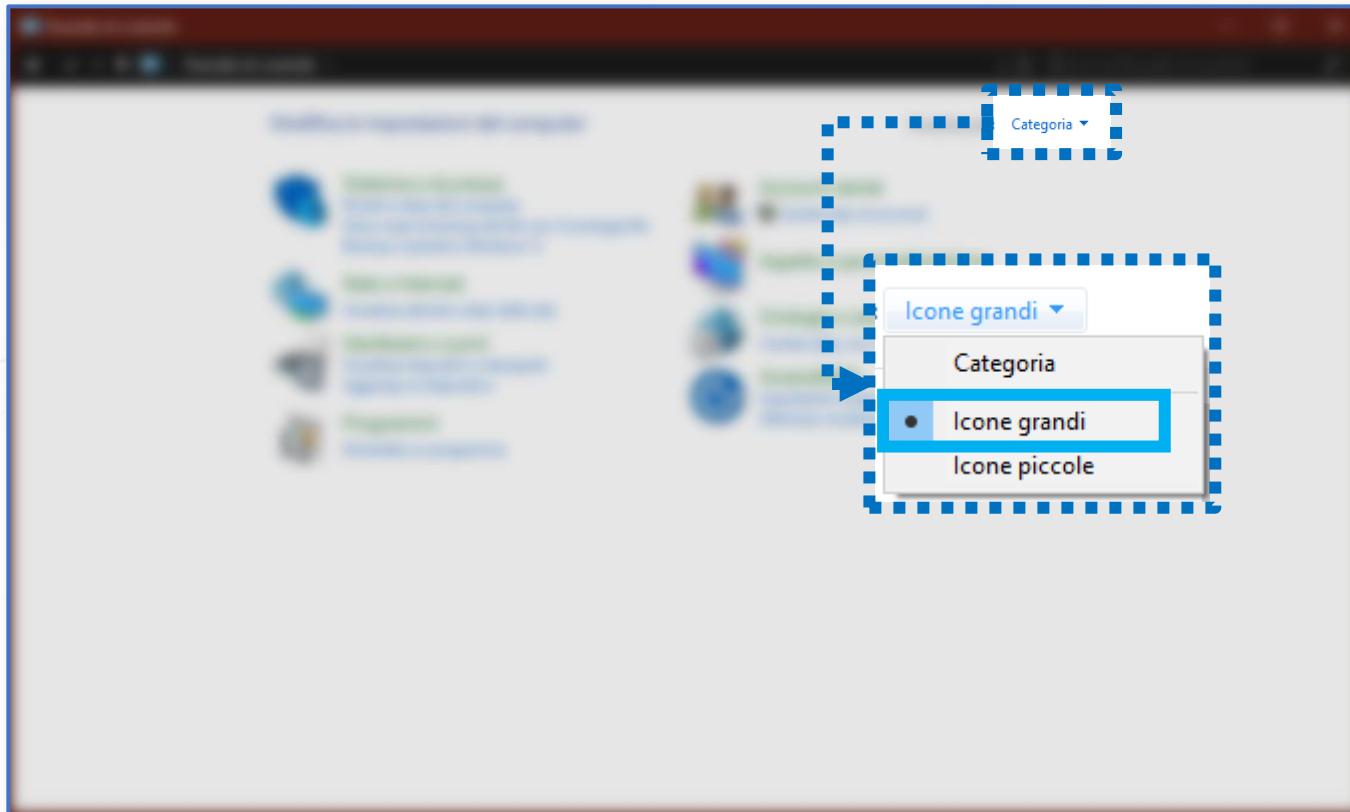
- Avvio del Tool dal Pannello di Controllo | Windows 10 | 1/3



Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 2/6

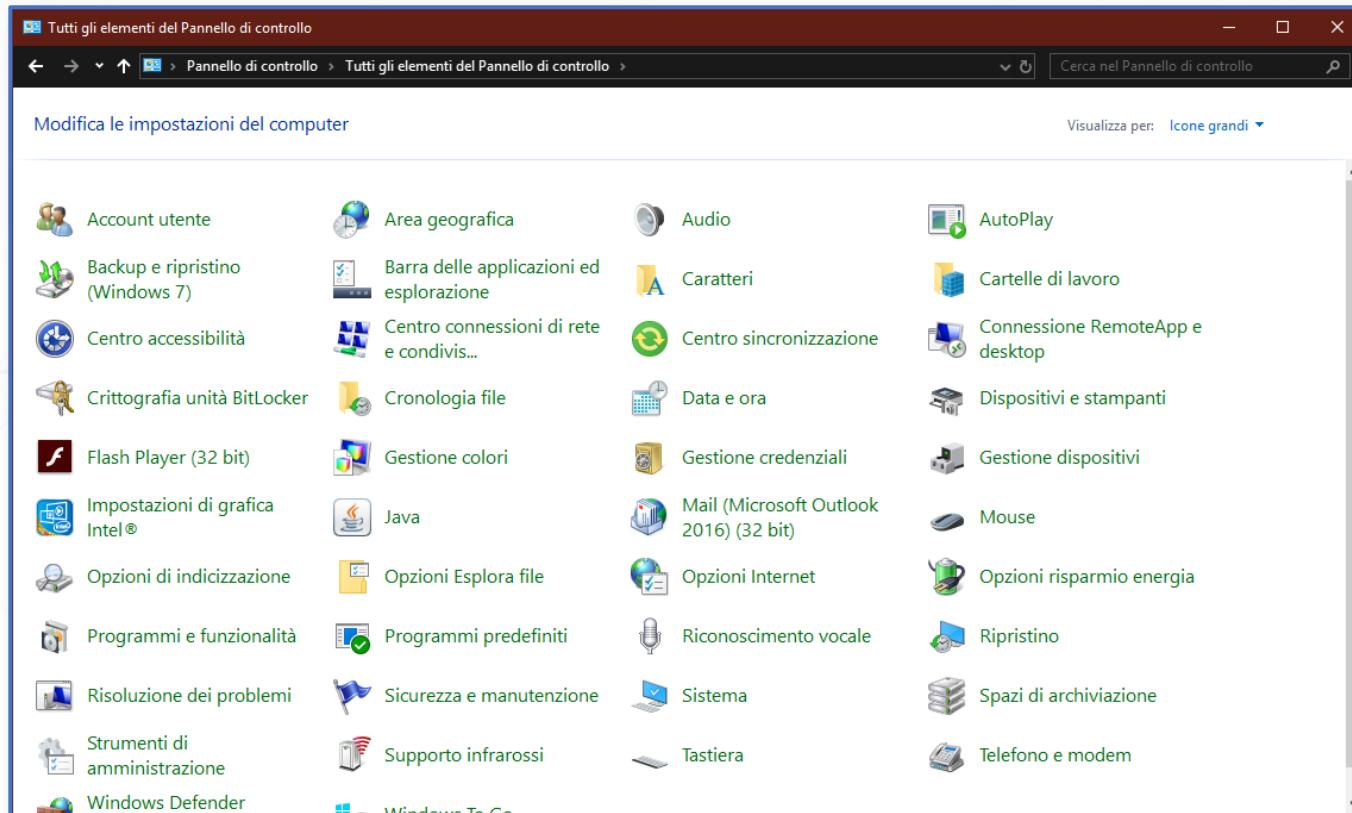
- Avvio del Tool dal Pannello di Controllo | Windows 10 | 2/3



Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 2/6

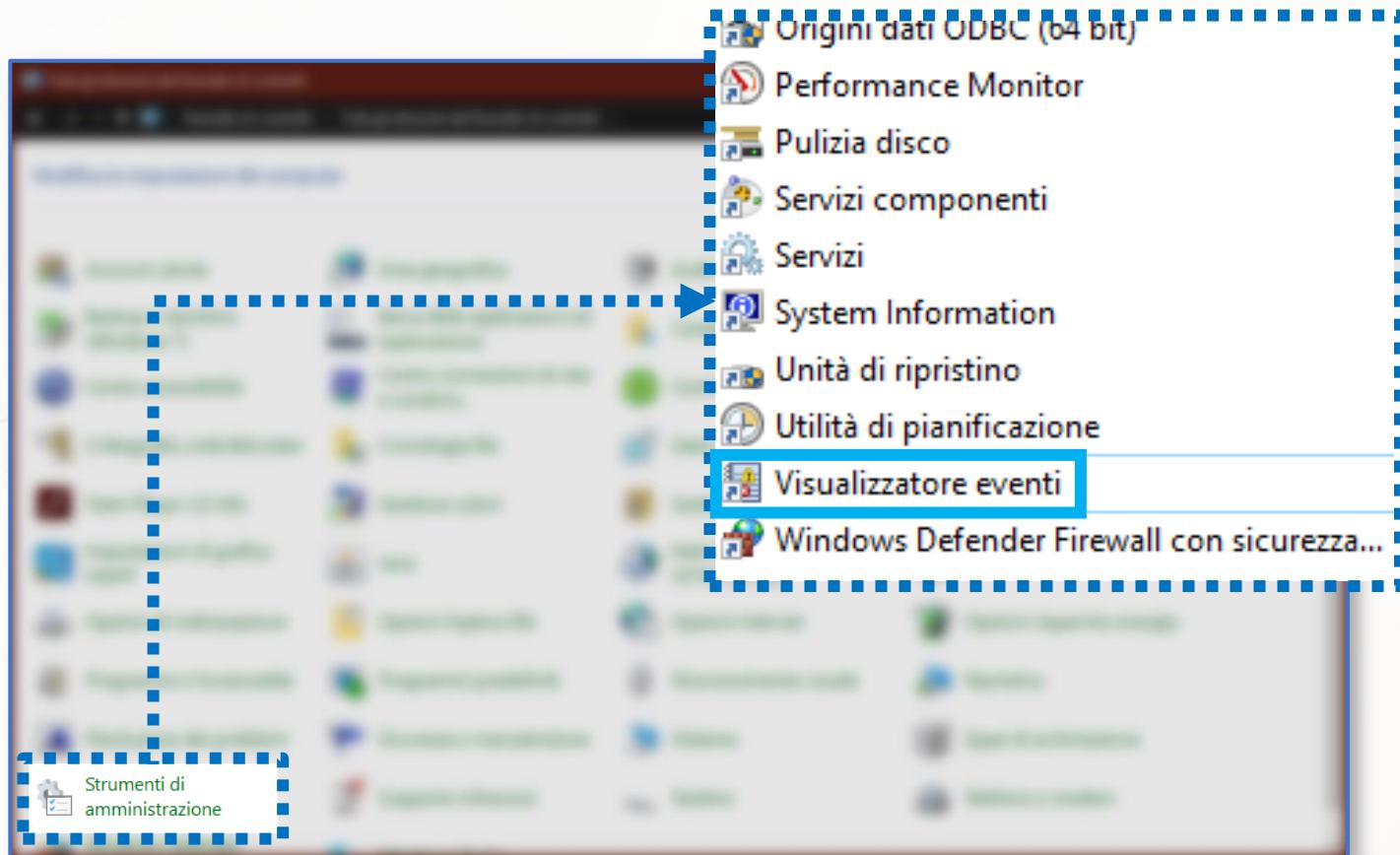
- Avvio del Tool dal Pannello di Controllo | Windows 10 | 3/3



Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 2/6

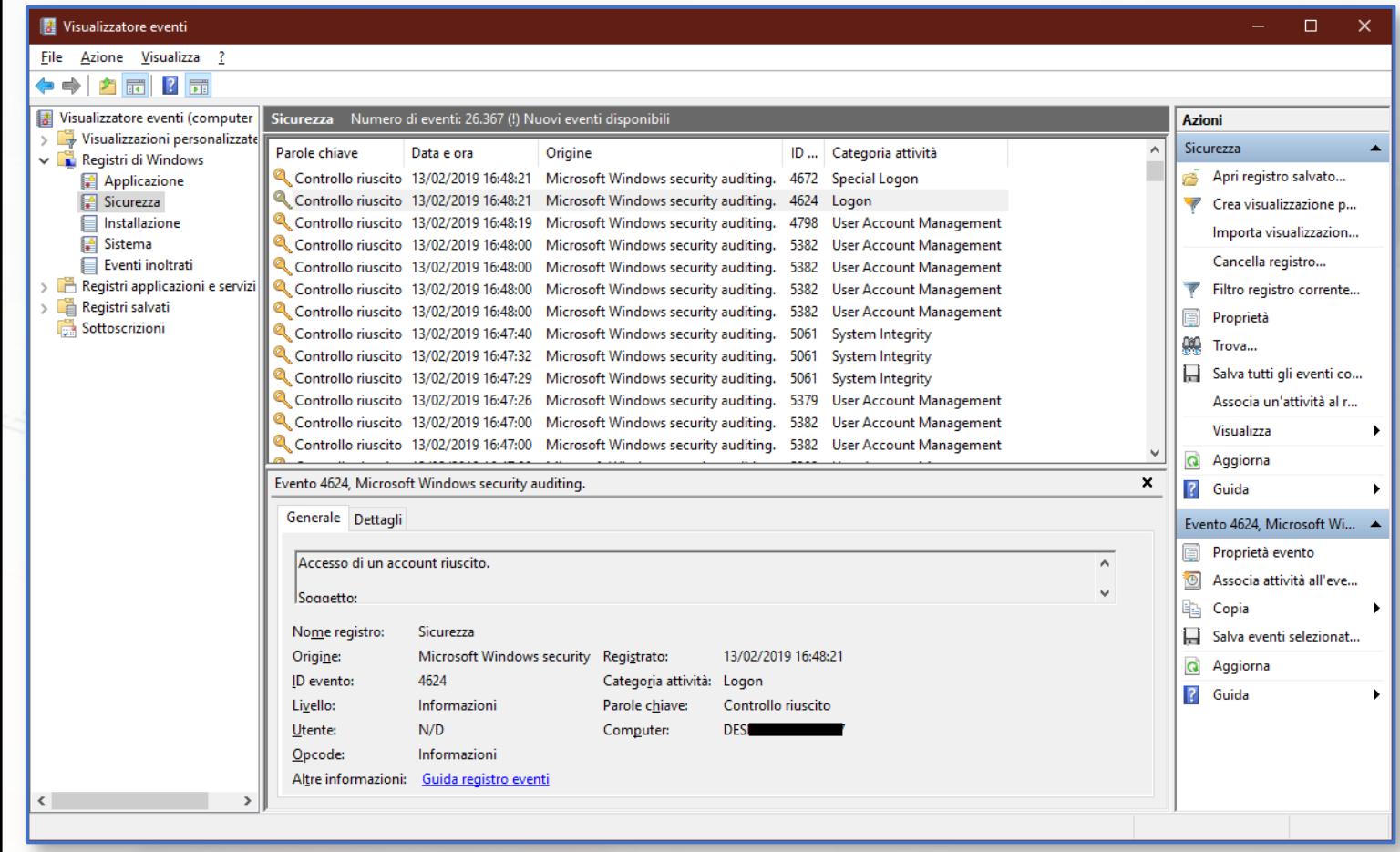
- Avvio del Tool dal Pannello di Controllo | Windows 10 | 3/3



Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 3/6

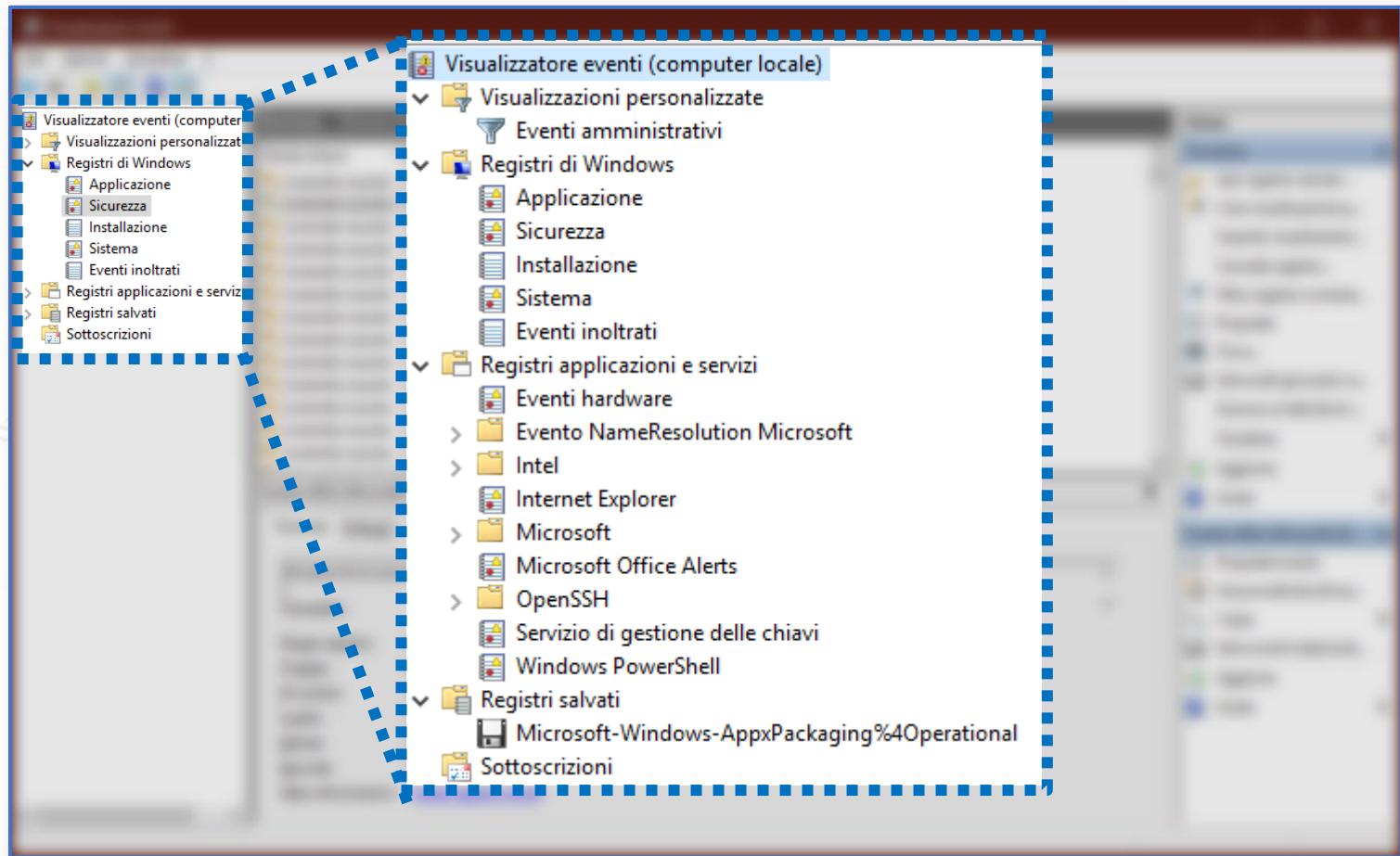
- *Interfaccia Grafica* | 1/12



Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 3/6

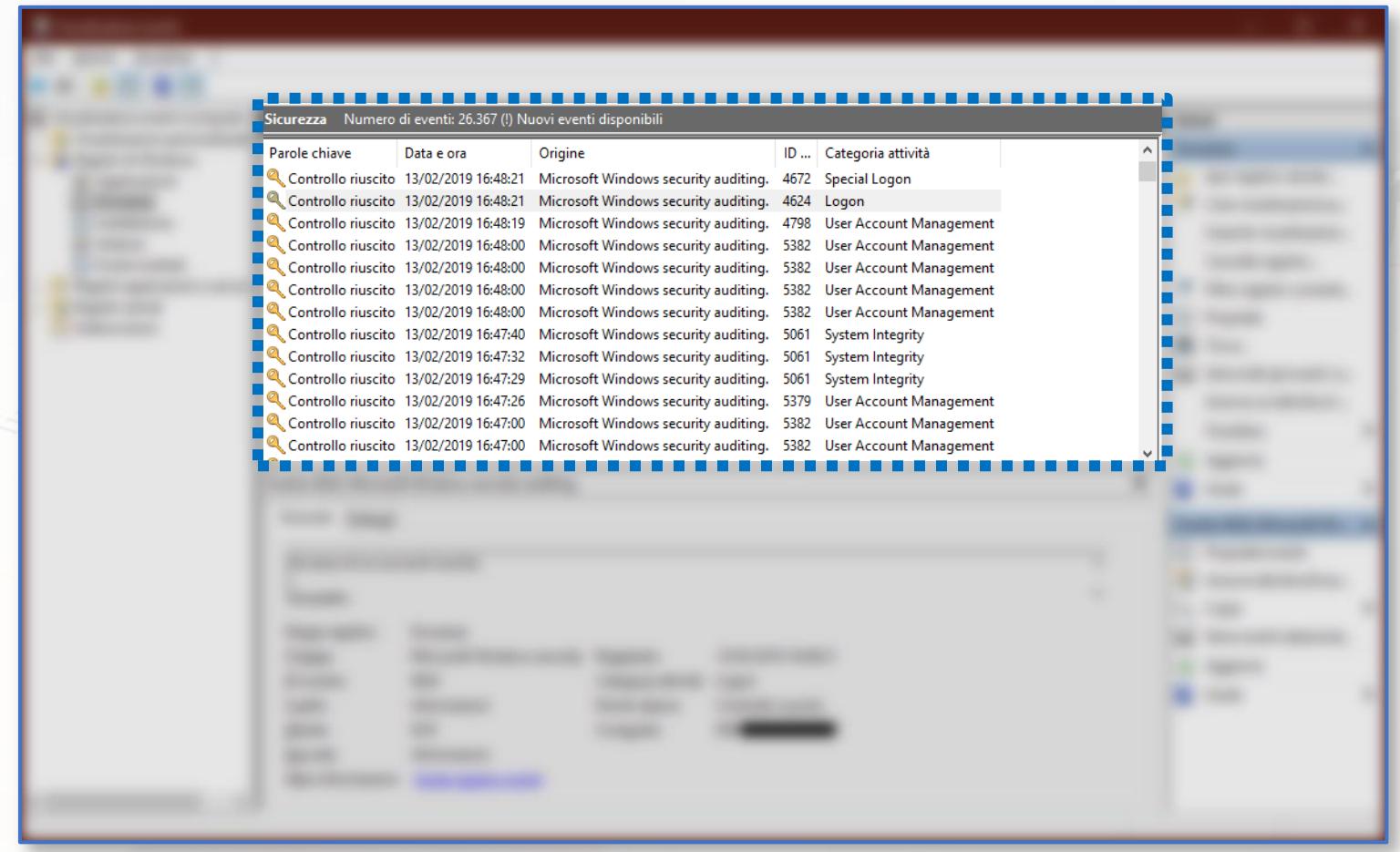
- *Interfaccia Grafica | Elenco dei Registri | 2/12*



Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 3/6

- *Interfaccia Grafica | Elenco degli Eventi di un Registro | 3/12*



Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 4/6

- *Interfaccia Grafica | Elenco degli Eventi di un Registro | 4/12*

Parole chiave	Data e ora	Origine	ID ...	Categoria attività
🔍 Controllo riuscito	13/02/2019 16:48:21	Microsoft Windows security auditing.	4672	Special Logon
🔍 Controllo riuscito	13/02/2019 16:48:21	Microsoft Windows security auditing.	4624	Logon
🔍 Controllo riuscito	13/02/2019 16:48:19	Microsoft Windows security auditing.	4798	User Account Management
🔍 Controllo riuscito	13/02/2019 16:48:00	Microsoft Windows security auditing.	5382	User Account Management
🔍 Controllo riuscito	13/02/2019 16:48:00	Microsoft Windows security auditing.	5382	User Account Management
🔍 Controllo riuscito	13/02/2019 16:48:00	Microsoft Windows security auditing.	5382	User Account Management
🔍 Controllo riuscito	13/02/2019 16:48:00	Microsoft Windows security auditing.	5382	User Account Management
🔍 Controllo riuscito	13/02/2019 16:47:40	Microsoft Windows security auditing.	5061	System Integrity
🔍 Controllo riuscito	13/02/2019 16:47:32	Microsoft Windows security auditing.	5061	System Integrity
🔍 Controllo riuscito	13/02/2019 16:47:29	Microsoft Windows security auditing.	5061	System Integrity
🔍 Controllo riuscito	13/02/2019 16:47:26	Microsoft Windows security auditing.	5379	User Account Management
🔍 Controllo riuscito	13/02/2019 16:47:00	Microsoft Windows security auditing.	5382	User Account Management
🔍 Controllo riuscito	13/02/2019 16:47:00	Microsoft Windows security auditing.	5382	User Account Management

Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 4/6

- *Interfaccia Grafica | Elenco degli Eventi di un Registro | 5/12*

The screenshot shows a graphical user interface for viewing event logs. On the left, there is a sidebar titled "Parole chiave" (Keywords) containing a list of search results, each with a magnifying glass icon and the text "Controllo riuscito". To the right of this sidebar is a large main pane displaying a list of events. A callout box with a blue dashed border points from the text "in questo caso, sono tutti *controlli riusciti*" to the list of events in the main pane.

Parole chiave

Controllo riuscito

Tipo di Evento (in questo caso, sono tutti *controlli riusciti*)

Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 4/6

- *Interfaccia Grafica | Elenco degli Eventi di un Registro | 6/12*

Parole chiave

- Controllo riuscito

Tipo di Evento (in questo caso, sono tutti *controlli riusciti*)

Ulteriori Esempi di Tipi di Evento

Icona	Data	Sorgente	ID	Dettagli
Errore	13/02/2019 21:04:15	DistributedCOM	10000	Nessuna
Errore	13/02/2019 19:38:13	DistributedCOM	10000	Nessuna
Avviso	13/02/2019 19:17:50	DNS Client Ev...	1014	(1014)
Informazioni	13/02/2019 18:57:41	Service Contro...	7040	Nessuna
Errore	13/02/2019 18:38:13	DistributedCOM	10000	Nessuna
Avviso	13/02/2019 18:15:12	DNS Client Ev...	1014	(1014)
Errore	13/02/2019 17:38:13	DistributedCOM	10000	Nessuna
Informazioni	13/02/2019 17:30:38	Kernel-General	16	Nessuna
Informazioni	13/02/2019 17:08:54	Service Contro...	7040	Nessuna
Informazioni	13/02/2019 17:06:44	Service Contro...	7040	Nessuna

Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 4/6

- *Interfaccia Grafica | Elenco degli Eventi di un Registro | 7/12*

Data e ora
13/02/2019 16:48:21
13/02/2019 16:48:21
13/02/2019 16:48:19
13/02/2019 16:48:00
13/02/2019 16:48:00
13/02/2019 16:48:00
13/02/2019 16:48:00
13/02/2019 16:47:40
13/02/2019 16:47:32
13/02/2019 16:47:29
13/02/2019 16:47:26
13/02/2019 16:47:00
13/02/2019 16:47:00

Data e Ora (timestamp)

Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 4/6

- *Interfaccia Grafica | Elenco degli Eventi di un Registro | 8/12*

Origine dell'evento

Origine

Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 4/6

- *Interfaccia Grafica | Elenco degli Eventi di un Registro | 9/12*

ID dell'evento
4672
4624
4798
5382
5382
5382
5382
5061
5061
5061
5379
5382
5382

Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 4/6

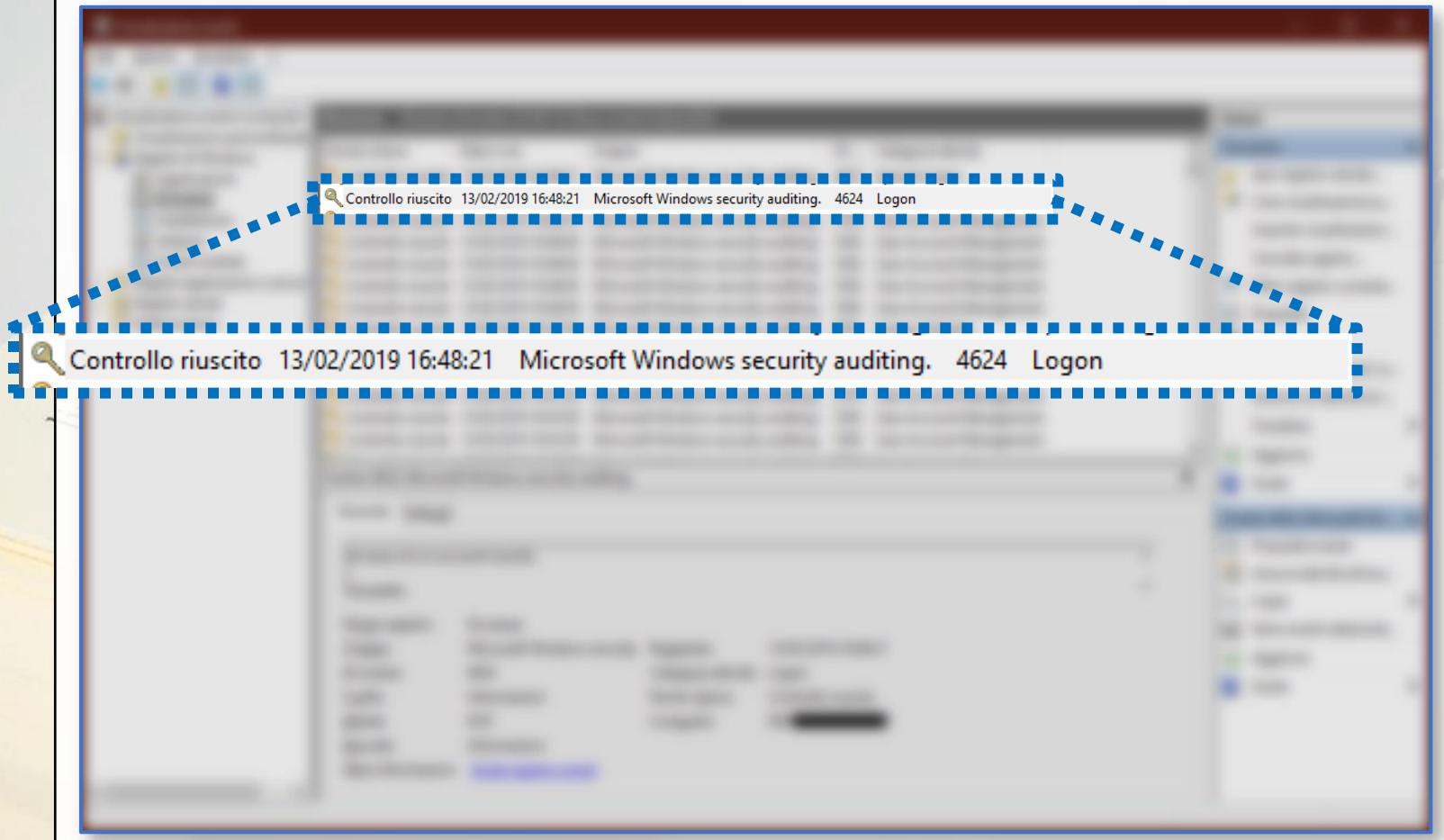
- *Interfaccia Grafica | Elenco degli Eventi di un Registro | 10/12*

Categoria dell'evento
Categoria attività
Special Logon
Logon
User Account Management
System Integrity
System Integrity
System Integrity
User Account Management
User Account Management
User Account Management

Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 5/6

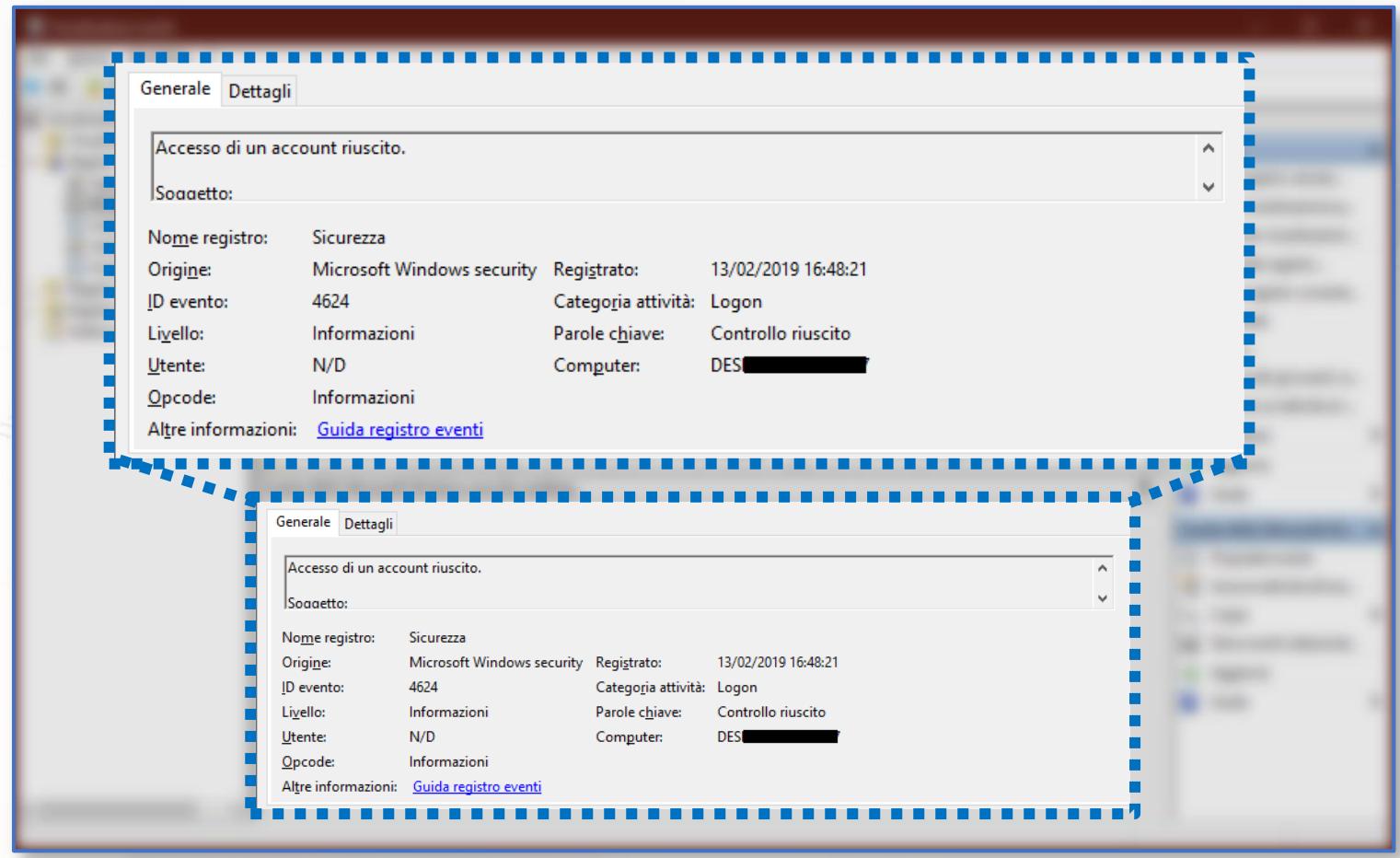
- *Interfaccia Grafica | Dettaglio di un Evento di un Registro | 11/12*



Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 5/6

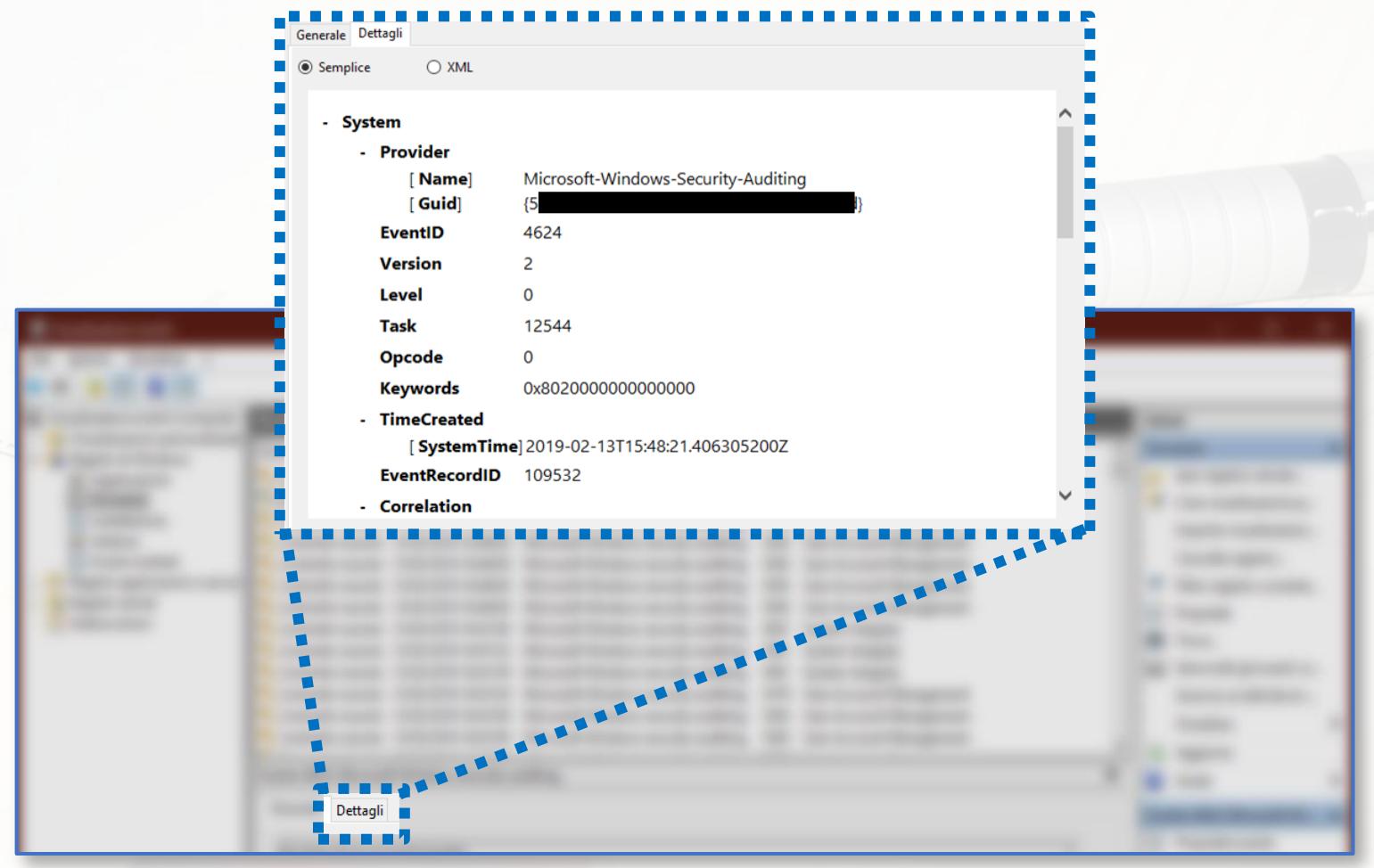
- *Interfaccia Grafica | Dettaglio di un Evento di un Registro | 12/12*



Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 6/6

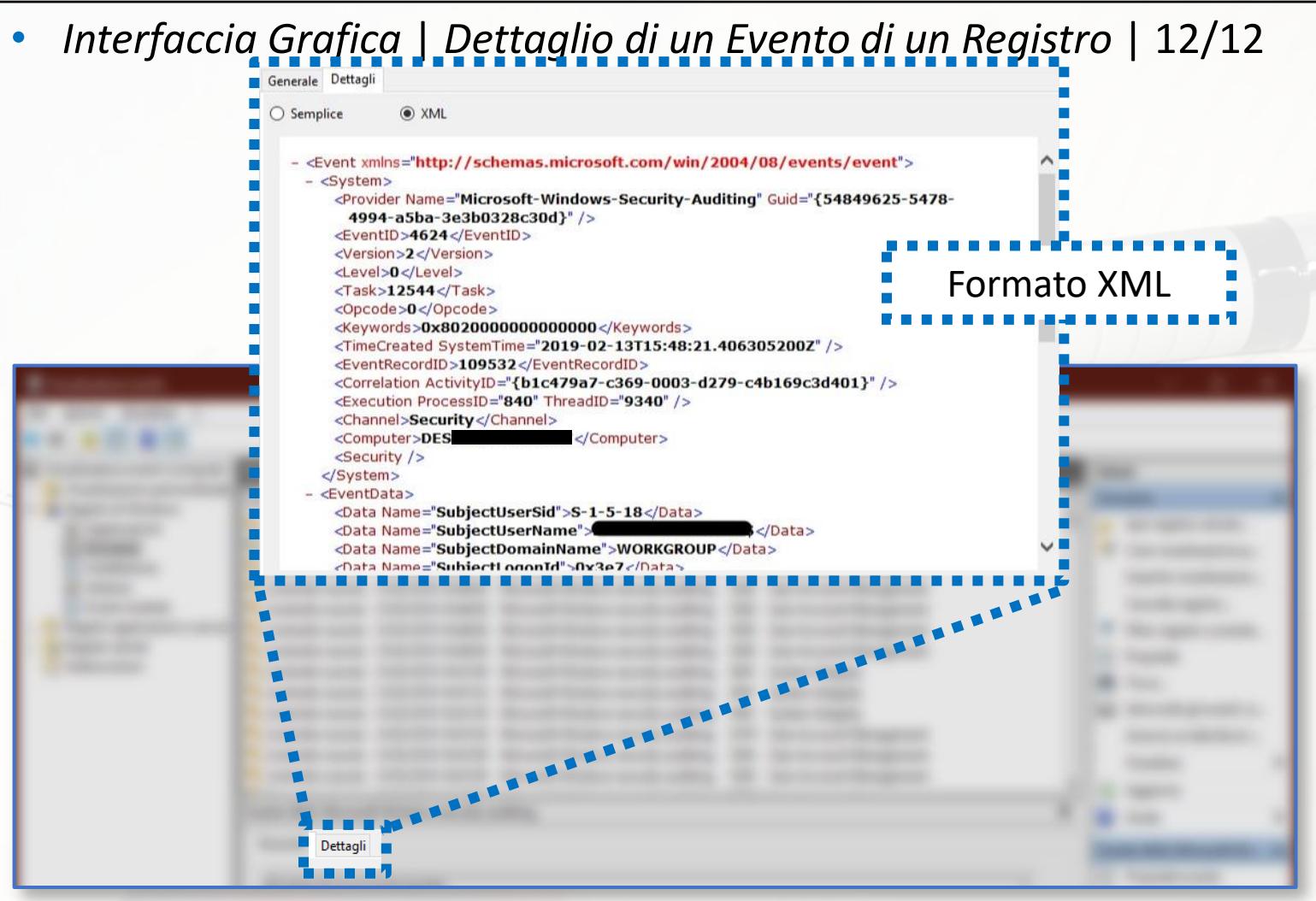
- *Interfaccia Grafica | Dettaglio di un Evento di un Registro | 12/12*



Analisi dei Registri degli Eventi

Il tool Visualizzatore Eventi | 6/6

- *Interfaccia Grafica | Dettaglio di un Evento di un Registro | 12/12*



Analisi dei Registri degli Eventi

Esportazione dei Registri | 1/6

- Affinché possa essere svolta un'analisi dei registri, è necessario preliminarmente **esportarli**
- La modalità di esportazione, varia in virtù del fatto che ci si trovi a lavorare su un:
 - *Live System*
 - *Dead System*



Analisi dei Registri degli Eventi

Esportazione dei Registri | 2/6

- Affinché possa essere svolta un'analisi dei registri, è necessario preliminarmente esportarli
- La modalità di esportazione, varia in virtù del fatto che ci si trovi a lavorare su un:
 - ***Live System***
 - ***Dead System***



Analisi dei Registri degli Eventi

Esportazione dei Registri | 2/6

- Affinché possa essere svolta un'analisi dei registri, è necessario preliminarmente esportarli
- La modalità di esportazione, varia in virtù del fatto che ci si trovi a lavorare su un:

- Live System
- Dead System

OSSERVAZIONE IMPORTANTE

Quando si lavora con un live system, è necessario considerare che i file di log, sono costantemente utilizzati

Analisi dei Registri degli Eventi

Esportazione dei Registri | 2/6

- Affinché possa essere svolta un'analisi dei registri, è necessario preliminarmente esportarli
- La modalità di esportazione, varia in virtù del fatto che ci si trovi a lavorare su un:
 - *Live System*
 - *Prima Possibilità*
 - *Seconda Possibilità*
 - *Dead System*



Analisi dei Registri degli Eventi

Esportazione dei Registri | 2/6

- Affinché possa essere svolta un'analisi dei registri, è necessario preliminarmente esportarli
- La modalità di esportazione, varia in virtù del fatto che ci si trovi a lavorare su un:
 - *Live System*
 - Prima Possibilità
 - Seconda Possibilità
 - *Dead System*

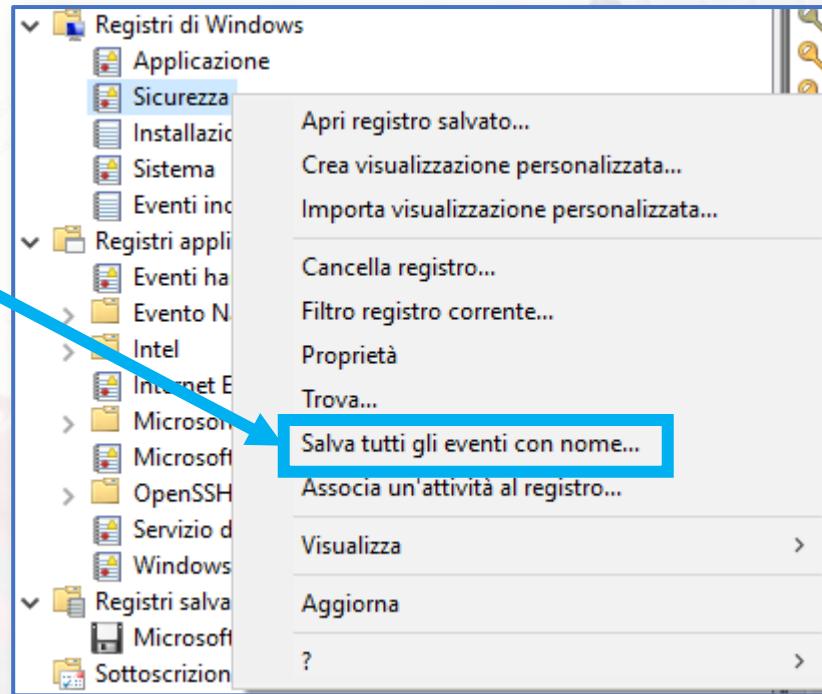


Analisi dei Registri degli Eventi

Esportazione dei Registri | 3/6

- **Prima Possibilità | 1/2**

- Utilizzare il tool Visualizzatore Eventi e cliccare, con il tasto destro, sul registro di interesse
- Selezionare la voce «**Salva tutti gli eventi con nome...**»

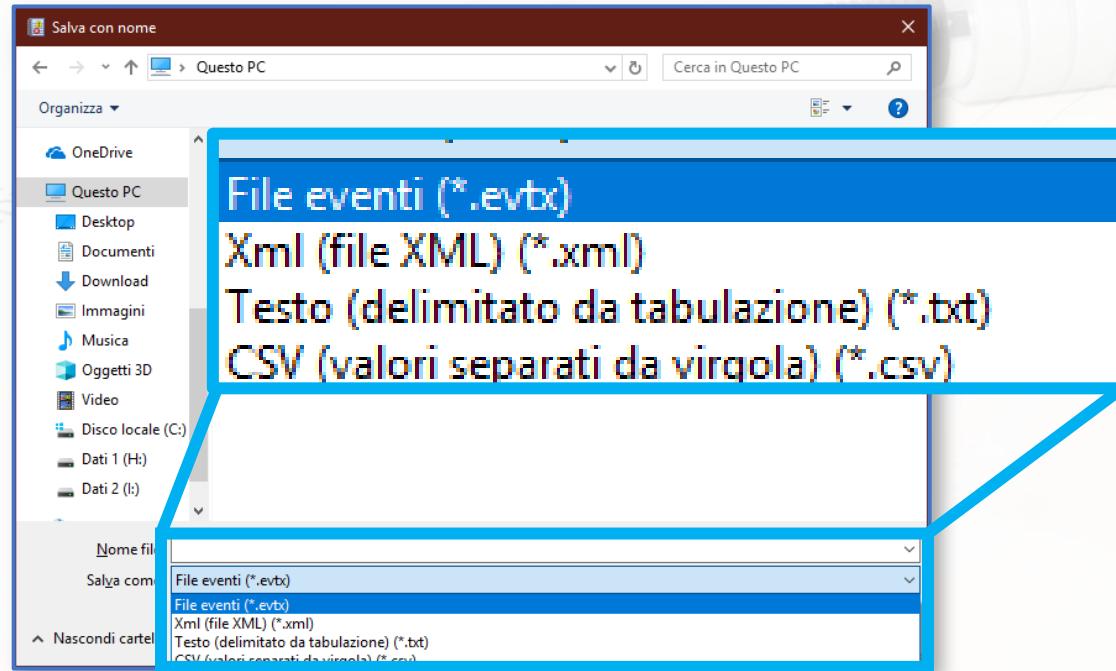


Analisi dei Registri degli Eventi

Esportazione dei Registri | 3/6

- **Prima Possibilità | 2/2**

- Verrà fornita la possibilità di esportare il log, in diversi formati: formato utilizzato per i file di log (.evtx), file XML (.xml), file testuale (.txt) e file CSV (.csv)



Analisi dei Registri degli Eventi

Esportazione dei Registri | 2/6

- Affinché possa essere svolta un'analisi dei registri, è necessario preliminarmente esportarli
- La modalità di esportazione, varia in virtù del fatto che ci si trovi a lavorare su un:
 - ***Live System***
 - ***Prima Possibilità***
 - ***Seconda Possibilità***
 - ***Dead System***



Analisi dei Registri degli Eventi

Esportazione dei Registri | 4/6

- **Seconda Possibilità**

- Acquisire una **immagine forense** del disco fisso in cui sono memorizzati i log, mediante un tool dedicato
- Una volta acquisita l'immagine forense, si può trattare il sistema, in maniera *offline*, come se si trattasse un **dead system**
 - Lavorando quindi con l'immagine forense
- Pertanto, a questo punto, è possibile seguire i passi discussi nella procedura relativa all'esportazione in un dead system

Analisi dei Registri degli Eventi

Esportazione dei Registri | 5/6

- Affinché possa essere svolta un'analisi dei registri, è necessario preliminarmente esportarli
- La modalità di esportazione, varia in virtù del fatto che ci si trovi a lavorare su un:
 - *Live system*
 - **Dead System**



Analisi dei Registri degli Eventi

Esportazione dei Registri | 6/6

- Effettuare il mounting dell'immagine forense, precedentemente acquisita
 - In tal modo, si potrà avere accesso ai file contenuti in tale immagine
- Recuperare i file di log (.evt x), dall'apposita cartella
- I file .evt x sono in formato binary XML, pertanto, **non possono essere analizzati direttamente**
- Vi sono però diversi tool che permettono l'analisi dei file di log degli eventi
 - Approfondiremo il tool **FullEventLogView**

Analisi dei Registri degli Eventi

Il tool FullEventLogView | Caratteristiche | 1/9

- Il tool **FullEventLogView** è sviluppato da NirSoft ed è gratuitamente scaricabile
 - Prevede la visualizzazione dei registri degli eventi, da diverse fonti:
 - Computer locale
 - Computer remoto sulla rete
 - File .evtx
 - Permette anche l'esportazione dei registri, in diversi formati (fra cui, il formato HTML)
- Disponibile unicamente per sistemi Windows-based
 - 32 bit e 64 bit
- Fornisce una pratica e semplice interfaccia grafica, ma è possibile specificare determinate opzioni anche tramite linea di comando
- Ulteriori informazioni e maggiori dettagli:
 - https://www.nirsoft.net/utils/full_event_log_view.html

Analisi dei Registri degli Eventi

Il tool FullEventLogView | 2/9

- *Interfaccia Utente di FullEventLogView | 1/9*

The screenshot shows the FullEventLogView application window. The title bar reads "FullEventLogView". The menu bar includes "File", "Edit", "View", "Options", and "Help". Below the menu is a toolbar with icons for opening files, saving, printing, and other functions. The main area is a table displaying log entries:

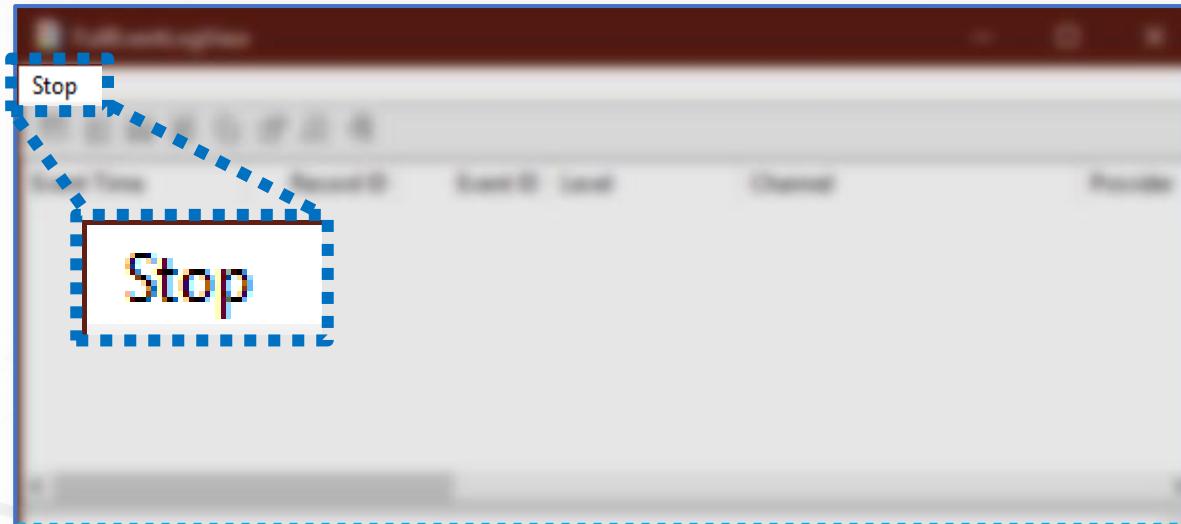
Event Time	Record ID	Event ID	Level	Channel	Provide
07/02/2019 12:0...	17827	20	Information	Microsoft-Windows-Audio/Pl...	Microso
07/02/2019 12:1...	17828	20	Information	Microsoft-Windows-Audio/Pl...	Microso
07/02/2019 12:1...	17829	20	Information	Microsoft-Windows-Audio/Pl...	Microso
07/02/2019 12:1...	11770	3	Information	Microsoft-Windows-Bits-Clie...	Microso
07/02/2019 12:1...	11771	209	Information	Microsoft-Windows-Bits-Clie...	Microso
07/02/2019 12:1...	11772	59	Information	Microsoft-Windows-Bits-Clie...	Microso
07/02/2019 12:1...	11773	60	Information	Microsoft-Windows-Bits-Clie...	Microso
07/02/2019 12:1...	11774	60	Information	Microsoft-Windows-Bits-Clie...	Microso

At the bottom left, it says "11686 item(s)". At the bottom right, it says "NirSoft Freeware. <http://www.nirsoft.net>".

Analisi dei Registri degli Eventi

Il tool FullEventLogView | 3/9

- *Interfaccia Utente di FullEventLogView | 2/9*



OSSERVAZIONE

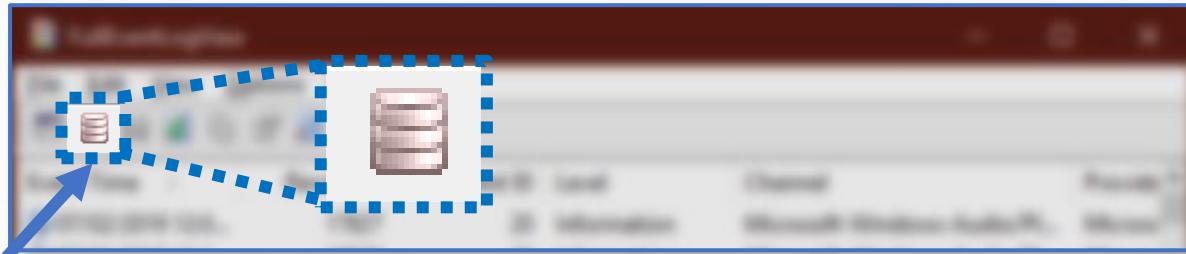
FullEventLogView avvia automaticamente il reperimento di informazioni sugli eventi all'interno del sistema in uso

Tale operazione può essere fermata, cliccando su **Stop**

Analisi dei Registri degli Eventi

Il tool FullEventLogView | 4/9

- Selezione Origine Dati (Data Source) | 3/9



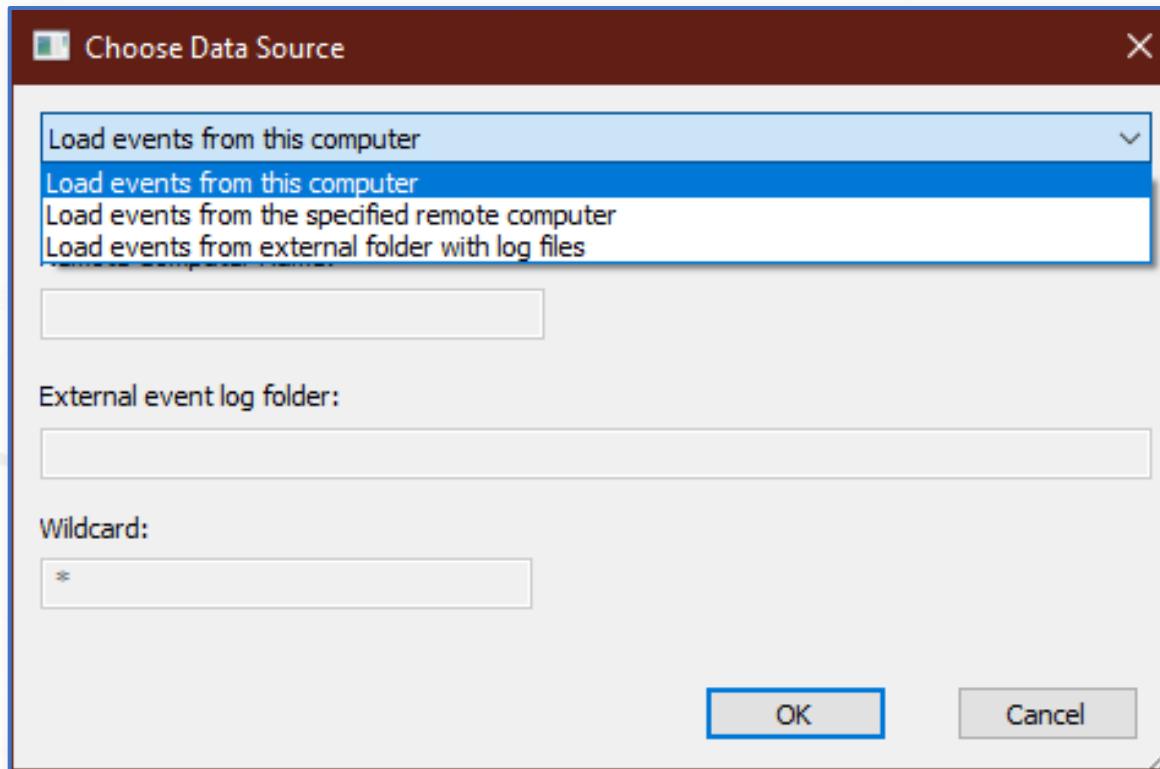
oppure



Analisi dei Registri degli Eventi

Il tool FullEventLogView | 5/9

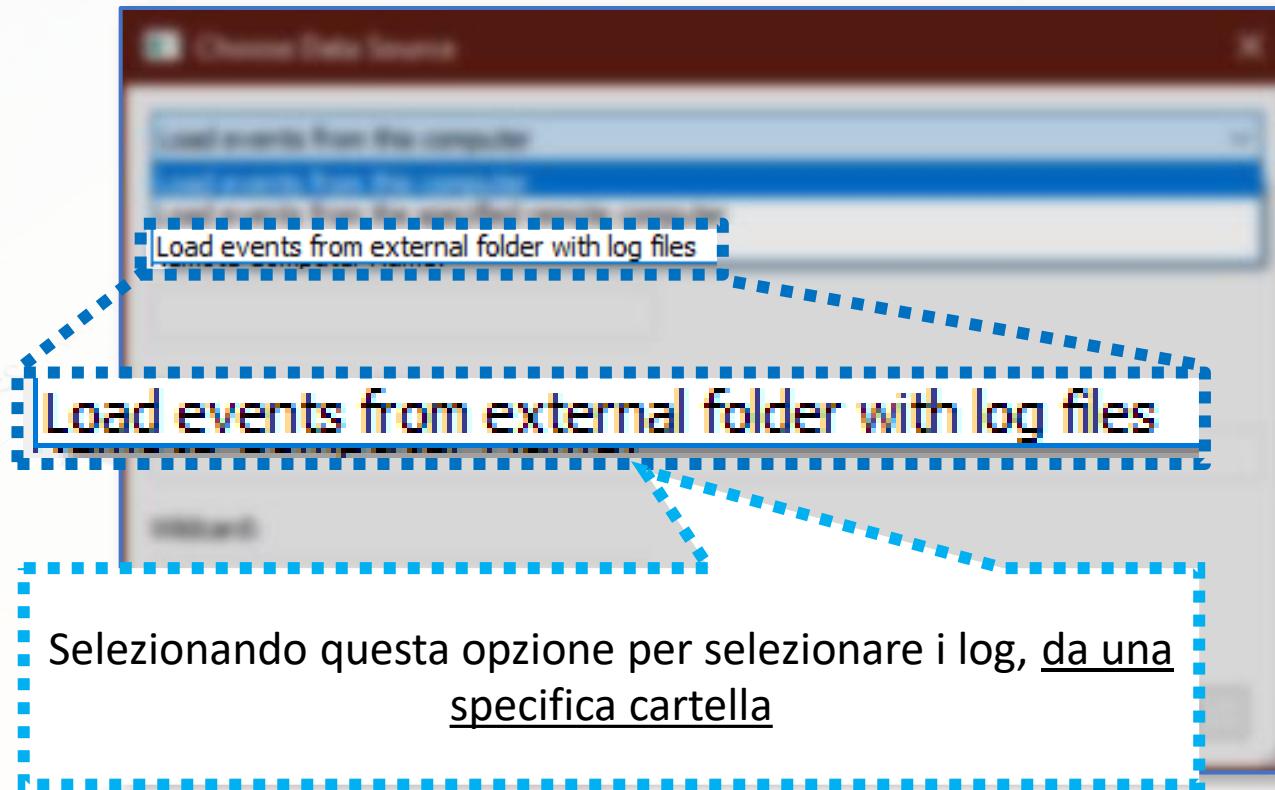
- *Selezione Origine Dati (Data Source) | 4/9*



Analisi dei Registri degli Eventi

Il tool FullEventLogView | 5/9

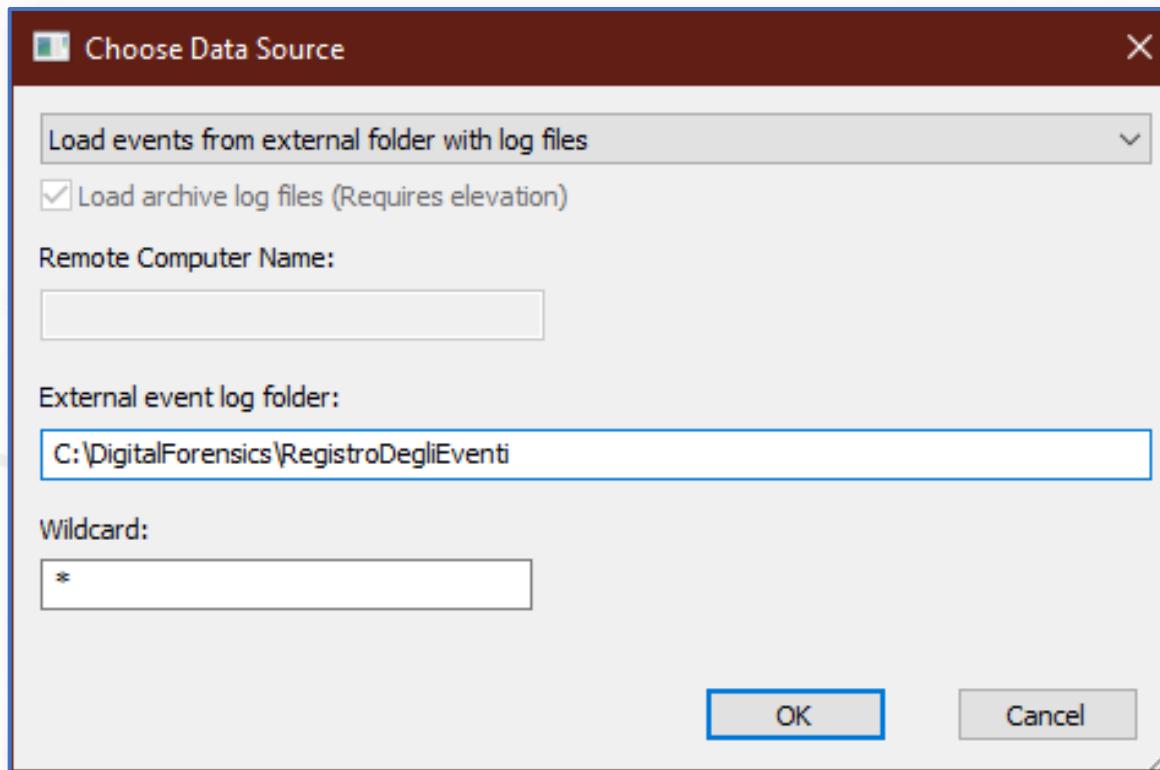
- Selezione Origine Dati (Data Source) | 4/9



Analisi dei Registri degli Eventi

Il tool FullEventLogView | 6/9

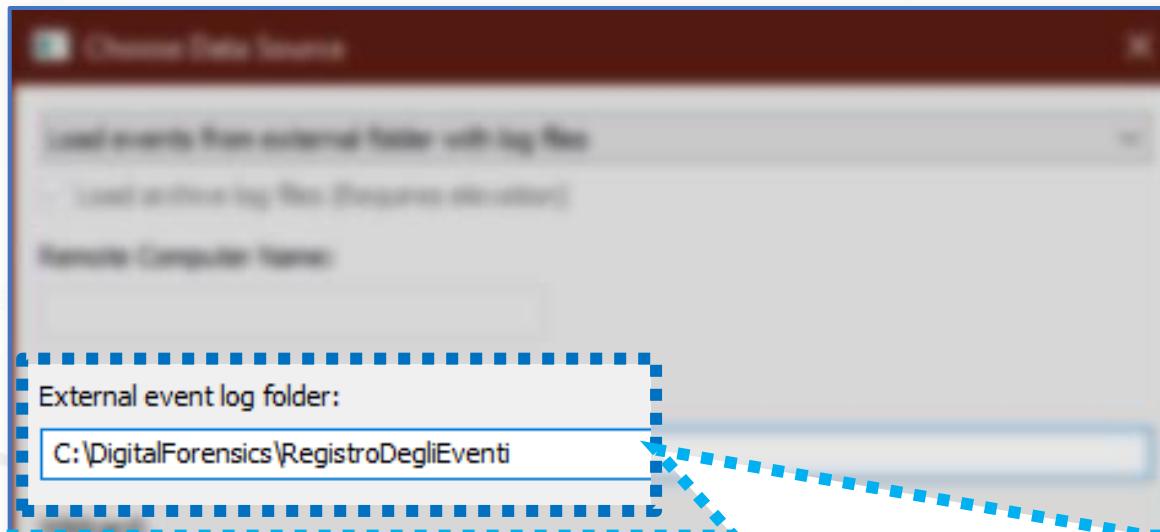
- *Selezione Origine Dati (Data Source) | 5/9*



Analisi dei Registri degli Eventi

Il tool FullEventLogView | 6/9

- *Selezione Origine Dati (Data Source) | 5/9*



Specificare la cartella che contiene il log, indicandone il percorso

I log dovrebbero essere acceduti dal drive «*virtuale*» (sul quale è stato effettuato il mounting dell’immagine forense, precedentemente acquisita)

NOTA: In questo esempio, unicamente per comodità di redazione, sono stati acceduti da una cartella locale

Analisi dei Registri degli Eventi

Il tool FullEventLogView | 7/9

- *Lista degli Eventi e Descrizione dell'Evento selezionato | 6/9*

The screenshot shows the FullEventLogView application window. The main pane displays a table of event logs with columns: Event Time, Record ID, Event ID, Level, Channel, and Provider. The provider column shows 'Microsoft' for most entries. The fourth row, corresponding to the selected event, has a yellow warning icon, a timestamp of 07/02/2019 12:20:00, a Record ID of 16560, an Event ID of 1534, a Level of Warning, a Channel of Application, and a Provider of Microsoft. Below the table, a message box contains the text: "Impossibile notificare al profilo l'evento Load per il componente {B31118B2-1F49-48E5-B6F5-BC21CAEC56FB}. Codice di errore: See Tracelogging for error details." At the bottom left, it says "6713 item(s), 1 Selected". At the bottom right, it includes the copyright notice "NirSoft Freeware. http://www.nirsoft.net".

Event Time	Record ID	Event ID	Level	Channel	Provider
07/02/2019 12:1...	16557	16384	Information	Application	Microsoft
07/02/2019 12:2...	16558	1534	Warning	Application	Microsoft
07/02/2019 12:2...	16559	1534	Warning	Application	Microsoft
07/02/2019 12:2...	16560	1534	Warning	Application	Microsoft
07/02/2019 12:2...	5192	100	Information	Microsoft-Client-Licensing-Pl...	Microsoft
07/02/2019 12:2...	5193	101	Information	Microsoft-Client-Licensing-Pl...	Microsoft
07/02/2019 12:3...	5194	102	Information	Microsoft-Client-Licensing-Pl...	Microsoft
...

Impossibile notificare al profilo l'evento Load per il componente {B31118B2-1F49-48E5-B6F5-BC21CAEC56FB}. Codice di errore: See Tracelogging for error details.

6713 item(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

Analisi dei Registri degli Eventi

Il tool FullEventLogView | 7/9

- Lista degli Eventi e Descrizione dell'Evento selezionato | 6/9*

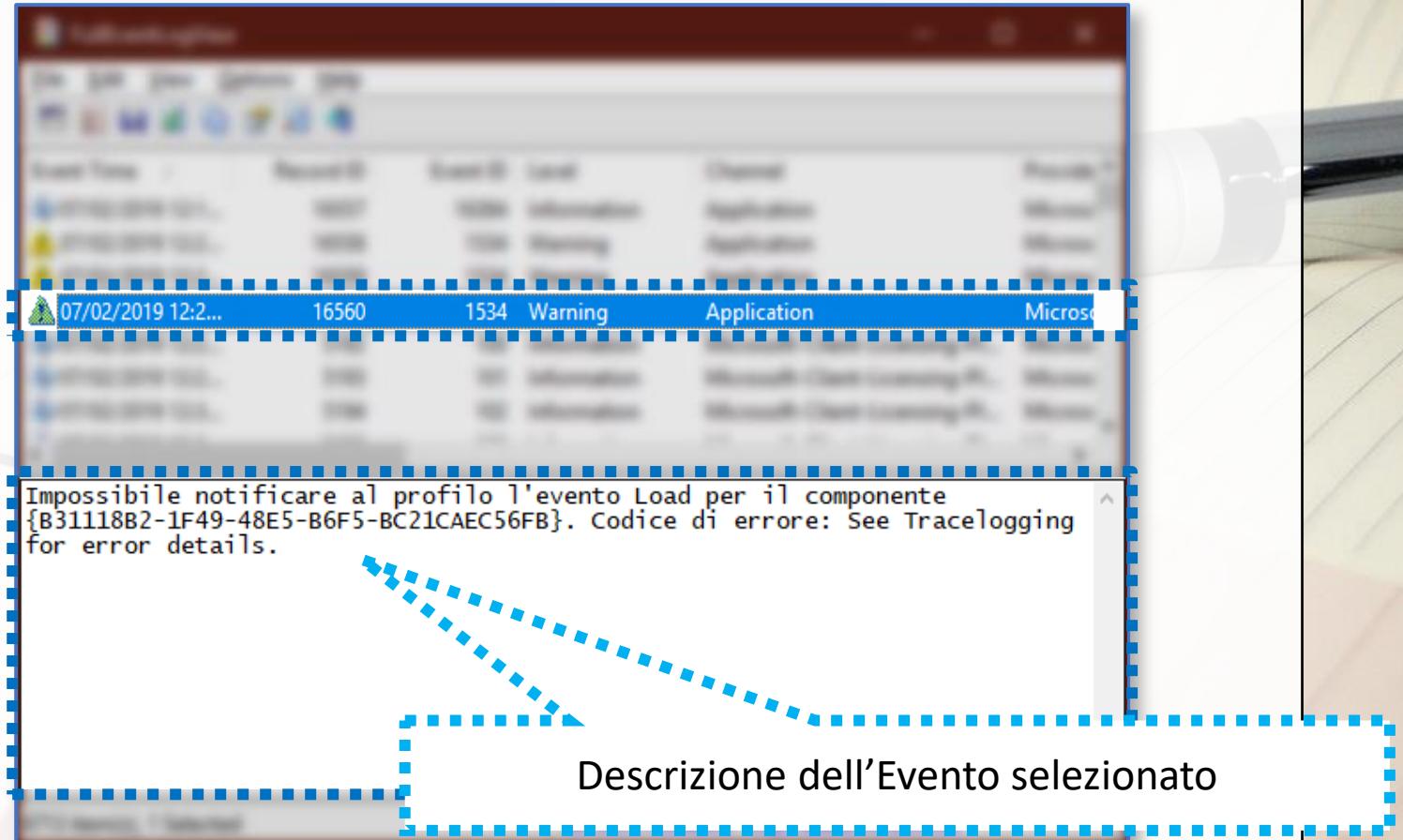
The screenshot shows a Windows application window titled "FullEventLogView". Inside the window, there is a table titled "Lista degli Eventi, contenuti nel Registro specificato". The table has columns: Event Time, Record ID, Event ID, Level, Channel, and Provider. The "Event Time" column includes icons for information (blue i), warning (yellow exclamation mark), and error (red exclamation mark). The "Event ID" column lists event IDs such as 16557, 16558, 16559, 16560, 5192, 5193, and 5194. The "Level" column shows levels like Information, Warning, and Error. The "Channel" and "Provider" columns both show "Microsoft" for most entries. The fourth row, which corresponds to Event ID 16560, is highlighted with a blue selection bar and is also outlined by a large blue dashed box. Below this table, there is a large, semi-transparent text area containing event details, which is also partially enclosed by a blue dashed box.

Event Time	Record ID	Event ID	Level	Channel	Provider
07/02/2019 12:1...	16557	16384	Information	Application	Microso...
07/02/2019 12:2...	16558	1534	Warning	Application	Microso...
07/02/2019 12:2...	16559	1534	Warning	Application	Microso...
07/02/2019 12:2...	16560	1534	Warning	Application	Microso...
07/02/2019 12:2...	5192	100	Information	Microsoft-Client-Licensing-Pl...	Microso...
07/02/2019 12:2...	5193	101	Information	Microsoft-Client-Licensing-Pl...	Microso...
07/02/2019 12:3...	5194	102	Information	Microsoft-Client-Licensing-Pl...	Microso...

Analisi dei Registri degli Eventi

Il tool FullEventLogView | 7/9

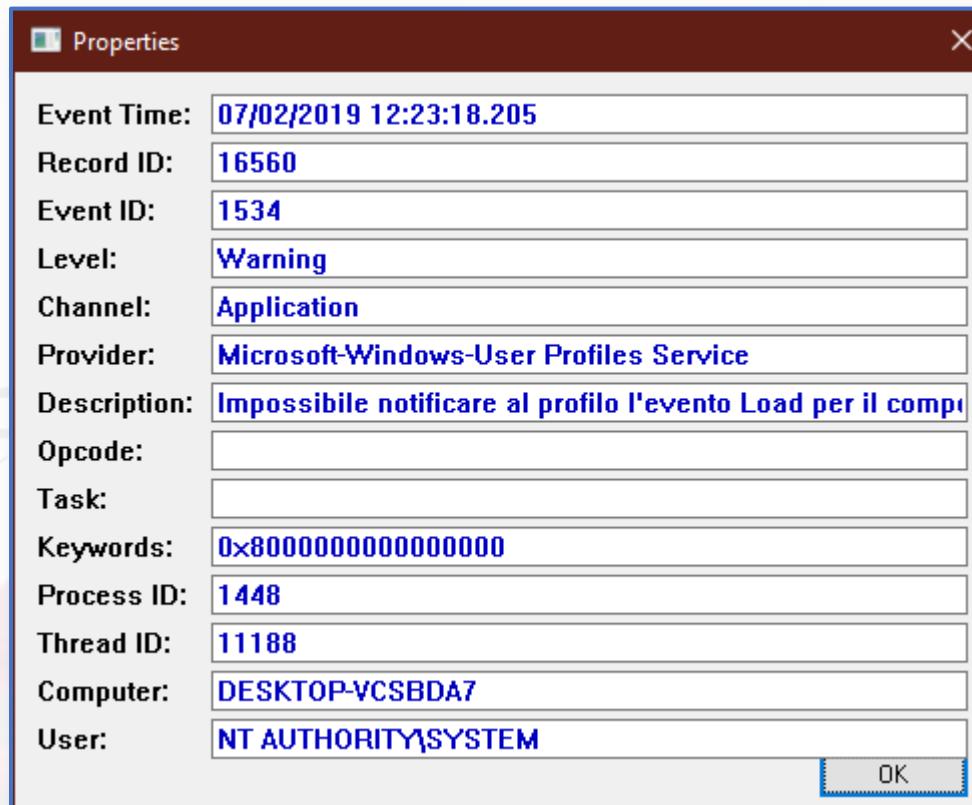
- Lista degli Eventi e Descrizione dell'Evento selezionato | 6/9*



Analisi dei Registri degli Eventi

Il tool FullEventLogView | 8/9

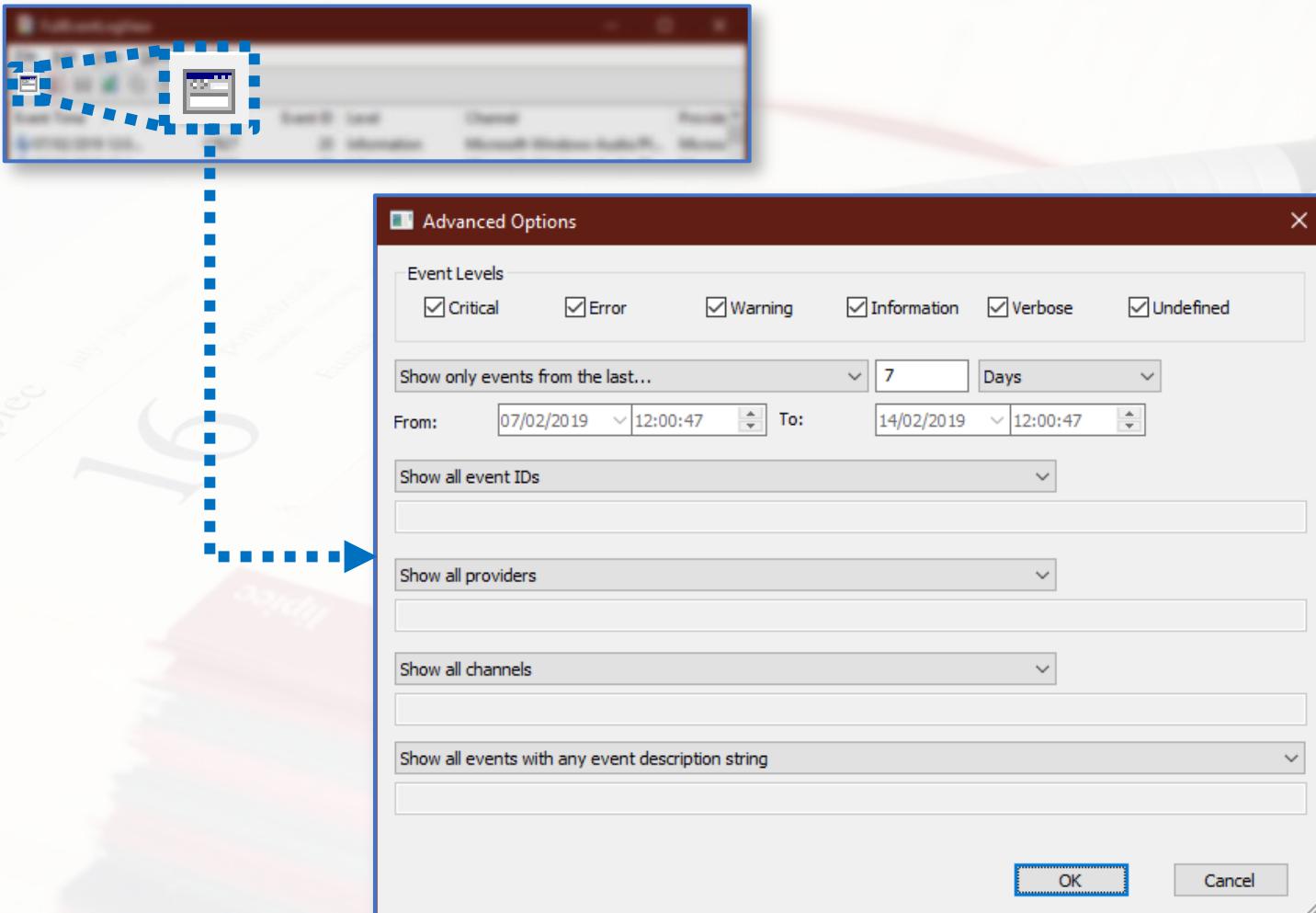
- Proprietà di un Evento | 7/9



Analisi dei Registri degli Eventi

Il tool FullEventLogView | 9/9

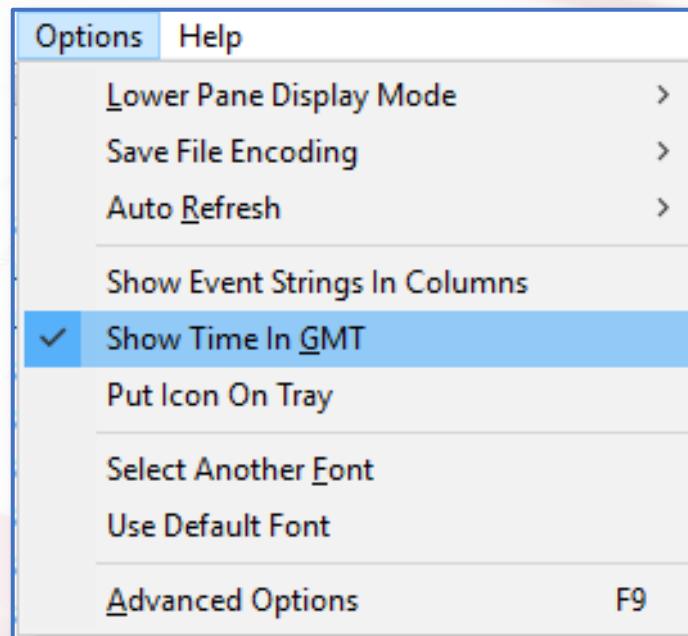
- *Opzioni Avanzate (Advanced Options) | 8/9*



Analisi dei Registri degli Eventi

Il tool FullEventLogView | 9/9

- *Mostrare Data e Ora nel Fuso Orario GMT | 9/9*



2.3

ИЗИКИ

24.2

ОРГАНІСКА
ХИМИЯ

1.4

ХИМИЧЕСКАЯ
АММІАКІЯ

5

26.89

ПОГРАД
АДІВІ

28.6

СИСТЕМА
ЖИВОТИН

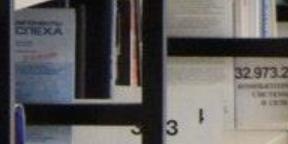
1.8

28

28.7

ІНІЦІАТИВА

La Cartella Prefetch



La Cartella Prefetch

Caratteristiche e Importanza | 1/6

- In Windows, è presente una cartella speciale, denominata **Prefetch** (letteralmente, *recuperare in anticipo*), che potrebbe contenere informazioni utili, per l'indagine
- **Obiettivo:** Ridurre i tempi di avvio dei programmi

Idee di Base del Funzionamento

- Al **primo avvio** di un dato programma P , Windows ne analizzerà il comportamento, nell'arco dei primi 10 secondi di esecuzione
 - Registrerà le informazioni in merito ai file utilizzati da P , per il suo avvio
 - Tali informazioni saranno memorizzate, in un apposito file (detto *file di prefetch*), associato al programma P , che verrà memorizzato nella cartella Prefetch
- Al **successivo avvio** di P , grazie al file di prefetch, associato a P (creato al primo avvio di P), Windows sarà in grado di precaricare, in memoria, i file che P utilizzerà, per l'avvio
 - In tal modo, sarà possibile ridurre i tempi di avvio di P

La Cartella Prefetch

Caratteristiche e Importanza | 2/6

- Tipicamente, ad ogni programma è associato un *file di prefetch*, il quale contiene le seguenti informazioni:
 - Il nome dell'eseguibile del programma
 - Il percorso, nel file system, dell'eseguibile
 - Numero di volte che il programma è stato eseguito
 - Utile, ad esempio, per individuare il programma più utilizzato dall'utente
 - Data e ora delle esecuzioni recenti del programma
 - Una lista di file utilizzati dal programma, per il suo avvio
- Tutte queste informazioni potrebbero rivelarsi particolarmente interessanti, dal punto di vista forense
 - Grazie ad esse, infatti, è possibile arricchire il quadro generale dell'indagine

La Cartella Prefetch

Caratteristiche e Importanza | 3/6

- La cartella Prefetch è tipicamente la seguente:
 - C :\Windows\Prefetch
 - Oppure, più in generale:
 - <CartellaWindows>\Prefetch
- I file di prefetch hanno estensione .pf
- Il nome di un file prefetch ha la seguente struttura:

<NOME_ESEGUIBILE>-<VALORE_HASH>.pf

- Esempio

CHROME . EXE-CCF9F3FC . pf	
CHROME . EXE	Nome dell'eseguibile
CCF9F3FC	Valore di Hash
.pf	Estensione del file prefetch

La Cartella Prefetch

Caratteristiche e Importanza | 4/6

- Da Windows 8 in poi, la cartella Prefetch può contenere fino a **1024 file di prefetch** (associati ad altrettanti eseguibili)
 - Invece, da Windows XP a Windows 7, tale cartella poteva contenere al massimo **128 file di prefetch**
- Quando il limite massimo di file prefetch è raggiunto, Windows elimina i file di prefetch più datati, per fare spazio ai nuovi
- **OSSERVAZIONE:** In fase di investigazione forense, è importante considerare il numero massimo di file di prefetch, nella cartella Prefetch
 - Ad esempio, in una cartella Prefetch, contenente il numero massimo di file prefetch, è probabile che alcuni file di prefetch, più datati, non siano presenti, poiché eliminati automaticamente

La Cartella Prefetch

Caratteristiche e Importanza | 5/6

- La funzionalità di prefetching (pre-caricamento) può essere anche utilizzata per ridurre i tempi, relativi alla fase di boot di Windows (funzionalità denominata *ReadyBoot*)
- Dal registro di sistema è possibile specificare il comportamento del prefetching, nelle seguenti modalità:
 1. Disabilitazione totale del prefetching
 2. Abilitazione del prefetching solo per migliorare le performance di avvio delle applicazioni
 3. Abilitazione del prefetching solo per migliorare le performance di boot di Windows
 4. Abilitazione di entrambi i punti 2. e 3.

La Cartella Prefetch

Caratteristiche e Importanza | 6/6

- Un file potenzialmente interessante, contenuto all'interno della cartella Prefetch, è il file layout.ini
[NOTA: Non è un file di prefetch]
- layout.ini contiene una lista di file, i quali sono utilizzati con maggior frequenza, dal S.O., nell'ambito delle operazioni di prefetching
- Tale file è tipicamente utilizzato per ottimizzare la *deframmentazione* del disco fisso
 - I file, listati da layout.ini, dovrebbero essere memorizzati in locazioni contigue del disco fisso, per ottimizzare le performance degli accessi ad essi

La Cartella Prefetch

Caratteristiche e Importanza | 6/6

- Un file potenzialmente interessante, contenuto all'interno della cartella Prefetch, è il file `layout.ini`
[NOTA: Non è un file di prefetch]
- **`layout.ini`** contiene una lista di file, i quali sono utilizzati con maggiore frequenza, dal S.O., nell'ambito delle operazioni.

Esempio | Contenuto del File `layout.ini` (Parziale)

```
[OptimalLayoutFile]
Version=1
C:\WINDOWS\SYSTEM32\NTOSKRNL.EXE
C:\WINDOWS\SYSTEM32\PSHED.DLL
C:\WINDOWS\SYSTEM32\BOOTVID.DLL
C:\WINDOWS\SYSTEM32\KDCOM.DLL
C:\WINDOWS\SYSTEM32\CI.DLL
C:\WINDOWS\SYSTEM32\DRIVERS\MSRPC.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\CNG.SYS
C:\WINDOWS\SYSTEM32\HAL.DLL
C:\WINDOWS\SYSTEM32\CONFIG\SYSTEM
C:\WINDOWS\SYSTEM32\C_1252.NLS
C:\WINDOWS\SYSTEM32\C_850.NLS
[...]
```

La Cartella Prefetch

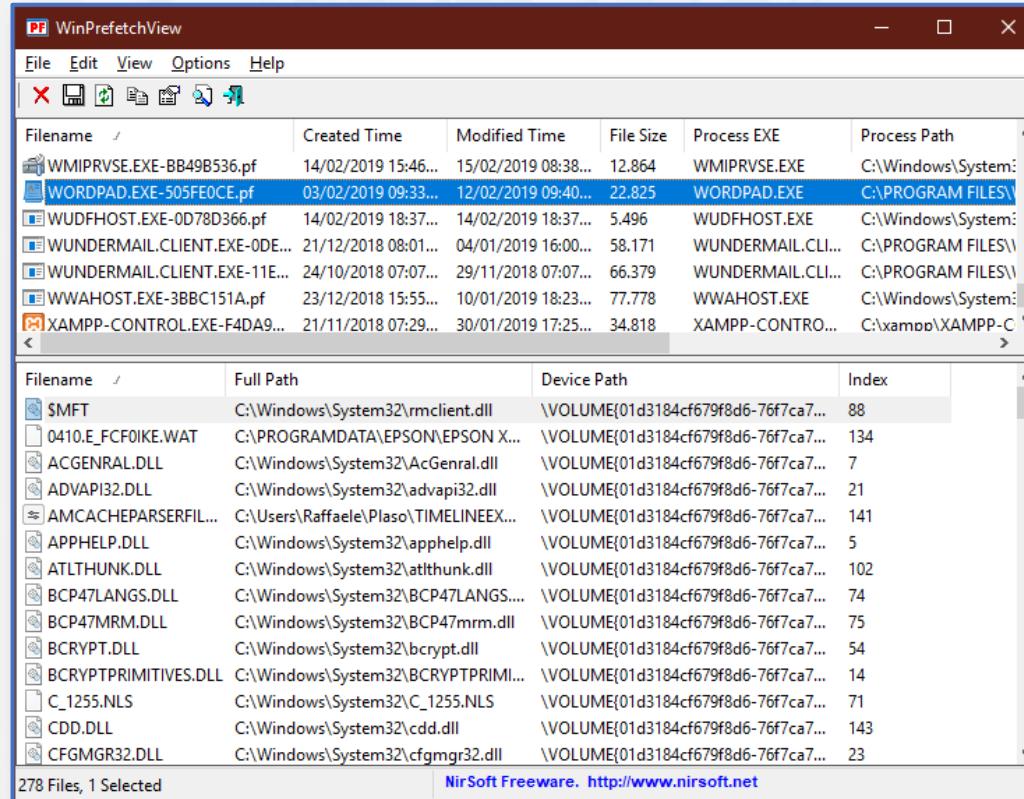
Il tool WinPrefetchView | Caratteristiche | 1/9

- Per l'analisi dei file di prefetch, approfondiremo il tool **WinPrefetchView**, sviluppato da NirSoft ed è gratuitamente scaricabile
- Permette di visualizzare tutti i file, contenuti nella cartella Prefetch di Windows
 - Per ciascun file di prefetch, permette di visualizzarne tutti i dettagli
- Di default, visualizza i file di prefetch del sistema in cui il tool è avviato
 - Tuttavia, tramite delle opportune opzioni a linea di comando, è possibile specificare anche una cartella specifica (o un file di prefetch specifico)
- Disponibile unicamente per sistemi Windows-based
- Ulteriori informazioni e maggiori dettagli:
 - https://www.nirsoft.net/utils/win_prefetch_view.html

La Cartella Prefetch

Il tool WinPrefetchView | 2/9

- *Interfaccia Utente di WinPrefetchView*



La Cartella Prefetch

Il tool WinPrefetchView | 2/9

- *Interfaccia Utente di WinPrefetchView*

The screenshot shows the WinPrefetchView application window. It has a menu bar with File, Edit, View, Options, Help, and a toolbar with icons for opening files, saving, and filtering. Below is a two-table view of prefetch data.

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path
WMIPRVSE.EXE-BB49B536.pf	14/02/2019 15:46...	15/02/2019 08:38...	12.864	WMIPRVSE.EXE	C:\Windows\System:
WORDPAD.EXE-505FE0CE.pf	03/02/2019 09:33...	12/02/2019 09:40...	22.825	WORDPAD.EXE	C:\PROGRAM FILES\
WUDFHOST.EXE-0D78D366.pf	14/02/2019 18:37...	14/02/2019 18:37...	5.496	WUDFHOST.EXE	C:\Windows\System:
WUNDERMAIL.CLIENT.EXE-0DE...	21/12/2018 08:01...	04/01/2019 16:00...	58.171	WUNDERMAIL.CLI...	C:\PROGRAM FILES\
WUNDERMAIL.CLIENT.EXE-11E...	24/10/2018 07:07...	29/11/2018 07:07...	66.379	WUNDERMAIL.CLI...	C:\PROGRAM FILES\
WWAHOST.EXE-3BBC151A.pf	23/12/2018 15:55...	10/01/2019 18:23...	77.778	WWAHOST.EXE	C:\Windows\System:
XAMPP-CONTROL.EXE-F4DA9...	21/11/2018 07:29...	30/01/2019 17:25...	34.818	XAMPP-CONTRO...	C:\xampp\xampp-C

Filename	Full Path	Device Path	Index
\$MFT	C:\Windows\System32\rmclient.dll	\VOLUME{01d3184cf679f8d6-76f7ca7...}	88
0410.E_FCF0IKE.WAT	C:\PROGRAMDATA\EPSON\EPSON X...	\VOLUME{01d3184cf679f8d6-76f7ca7...}	134
ACGENRAL.DLL	C:\Windows\System32\AcGenral.dll	\VOLUME{01d3184cf679f8d6-76f7ca7...}	7
ADVAPI32.DLL	C:\Windows\System32\advapi32.dll	\VOLUME{01d3184cf679f8d6-76f7ca7...}	21

OSSERVAZIONE

WinPrefetchView avvia automaticamente il reperimento di informazioni sui file di prefetch e dei relativi dettagli, all'interno del sistema in uso

La Cartella Prefetch

Il tool WinPrefetchView | 2/9

- *Interfaccia Utente di WinPrefetchView*

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path
WMIPRVSE.EXE-BB49B536(pf)	14/02/2019 15:46...	15/02/2019 08:38...	12.864	WMIPRVSE.EXE	C:\Windows\System...
WORDPAD.EXE-505FE0CE(pf)	03/02/2019 09:33...	12/02/2019 09:40...	22.825	WORDPAD.EXE	C:\PROGRAM FILES\...
WUDFHOST.EXE-0D78D366(pf)	14/02/2019 18:37...	14/02/2019 18:37...	5.496	WUDFHOST.EXE	C:\Windows\System...
WUNDERMAIL.CLIENT.EXE-0DE...	21/12/2018 08:01...	04/01/2019 16:00...	58.171	WUNDERMAIL.CLI...	C:\PROGRAM FILES\...
WUNDERMAIL.CLIENT.EXE-11E...	24/10/2018 07:07...	29/11/2018 07:07...	66.379	WUNDERMAIL.CLI...	C:\PROGRAM FILES\...
WWAHOST.EXE-3BBC151A(pf)	23/12/2018 15:55...	10/01/2019 18:23...	77.778	WWAHOST.EXE	C:\Windows\System...
XAMPP-CONTROL.EXE-F4DA9...	21/11/2018 07:29...	30/01/2019 17:25...	34.818	XAMPP-CONTRO...	C:\xampp\xampp-C...

Lista dei file di prefetch

278 Files

Numero di file di prefetch (in
questo caso, 278)

La Cartella Prefetch

Il tool WinPrefetchView | 2/9

- *Interfaccia Utente di WinPrefetchView*

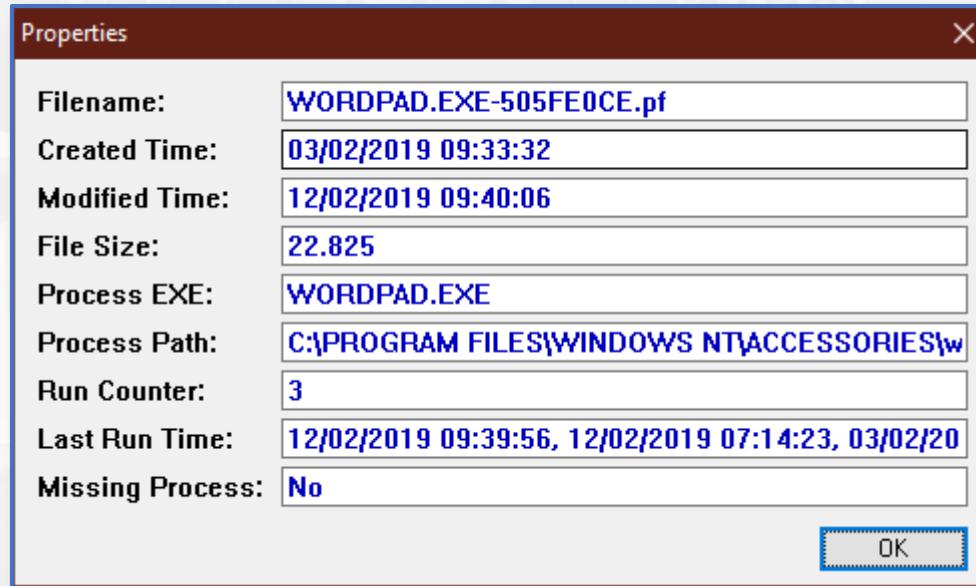
File utilizzati per l'avvio del programma, specificato dal file di prefetch selezionato (nella lista, evidenziata nella slide precedente)

Filename	Full Path	Device Path	Index
\$MFT	C:\Windows\System32\rmclient.dll	\VOLUME{01d3184cf679f8d6-76f7ca7...}	88
0410.E_FCF0IKE.WAT	C:\PROGRAMDATA\EPSON\EPSON X...	\VOLUME{01d3184cf679f8d6-76f7ca7...}	134
ACGENRAL.DLL	C:\Windows\System32\AcGeneral.dll	\VOLUME{01d3184cf679f8d6-76f7ca7...}	7
ADVAPI32.DLL	C:\Windows\System32\advapi32.dll	\VOLUME{01d3184cf679f8d6-76f7ca7...}	21
AMCACHEPARSERFIL...	C:\Users\Raffaele\Plaso\TIMELINEEX...	\VOLUME{01d3184cf679f8d6-76f7ca7...}	141
APPHELP.DLL	C:\Windows\System32\apphelp.dll	\VOLUME{01d3184cf679f8d6-76f7ca7...}	5
ATLTHUNK.DLL	C:\Windows\System32\atlthunk.dll	\VOLUME{01d3184cf679f8d6-76f7ca7...}	102
BCP47LANGS.DLL	C:\Windows\System32\BCP47LANGS...	\VOLUME{01d3184cf679f8d6-76f7ca7...}	74
BCP47MRM.DLL	C:\Windows\System32\BCP47mrm.dll	\VOLUME{01d3184cf679f8d6-76f7ca7...}	75
BCRYPT.DLL	C:\Windows\System32\bcrypt.dll	\VOLUME{01d3184cf679f8d6-76f7ca7...}	54
BCRYPTPRIMITIVES.DLL	C:\Windows\System32\BCRYPTPRIMI...	\VOLUME{01d3184cf679f8d6-76f7ca7...}	14
C_1255.NLS	C:\Windows\System32\C_1255.NLS	\VOLUME{01d3184cf679f8d6-76f7ca7...}	71
CDD.DLL	C:\Windows\System32\cdd.dll	\VOLUME{01d3184cf679f8d6-76f7ca7...}	143
CFGMGR32.DLL	C:\Windows\System32\cfgmgr32.dll	\VOLUME{01d3184cf679f8d6-76f7ca7...}	23

La Cartella Prefetch

Il tool WinPrefetchView | 3/9

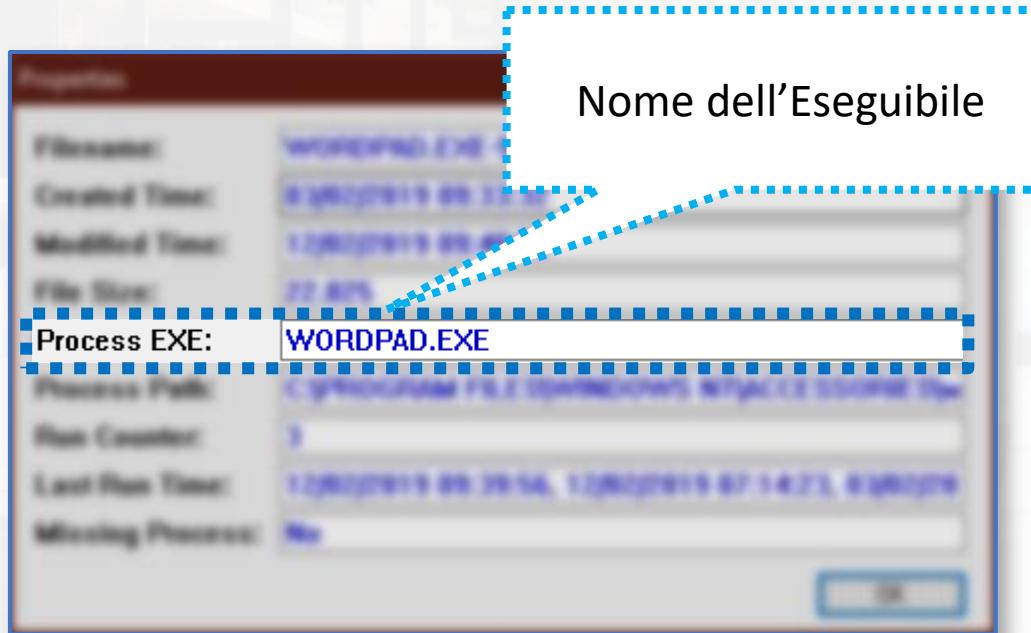
- *Proprietà di un File di Prefetch*



La Cartella Prefetch

Il tool WinPrefetchView | 3/9

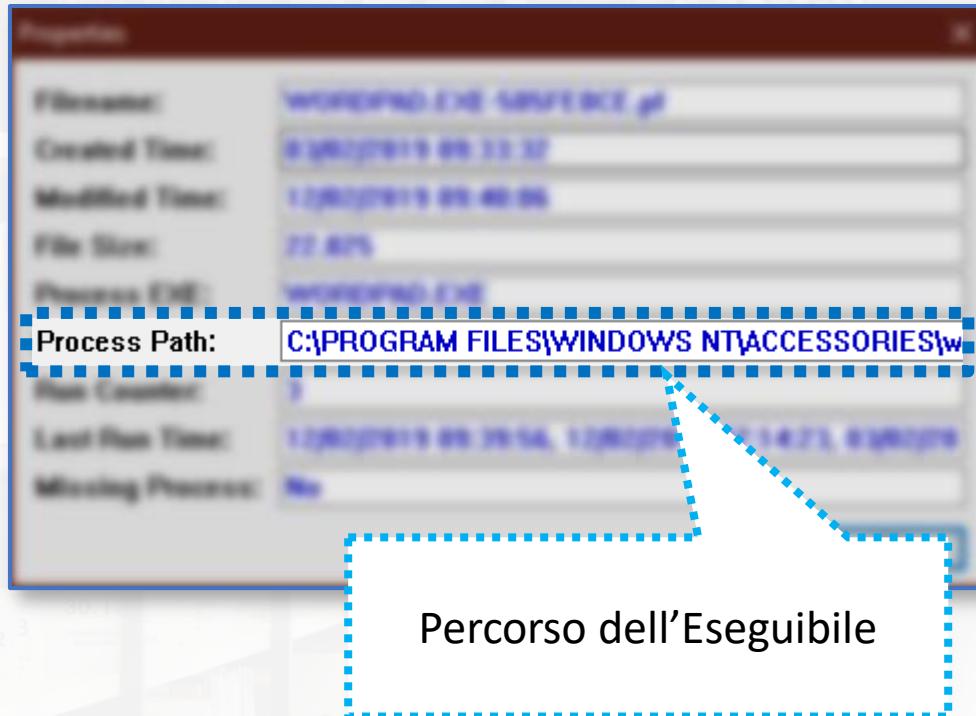
- Proprietà di un File di Prefetch



La Cartella Prefetch

Il tool WinPrefetchView | 3/9

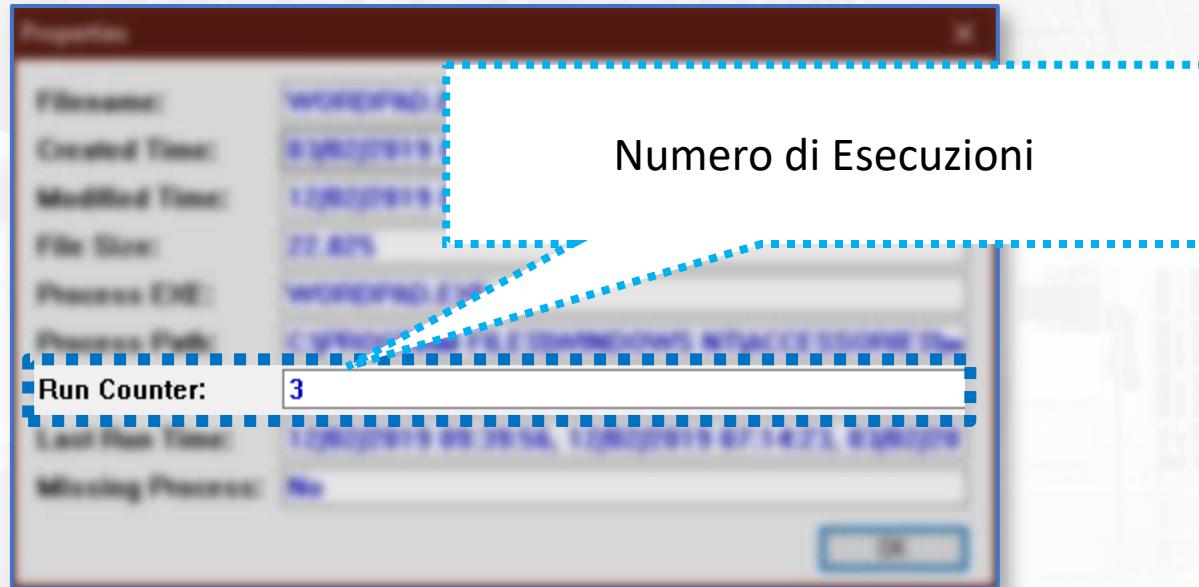
- Proprietà di un File di Prefetch



La Cartella Prefetch

Il tool WinPrefetchView | 3/9

- Proprietà di un File di Prefetch

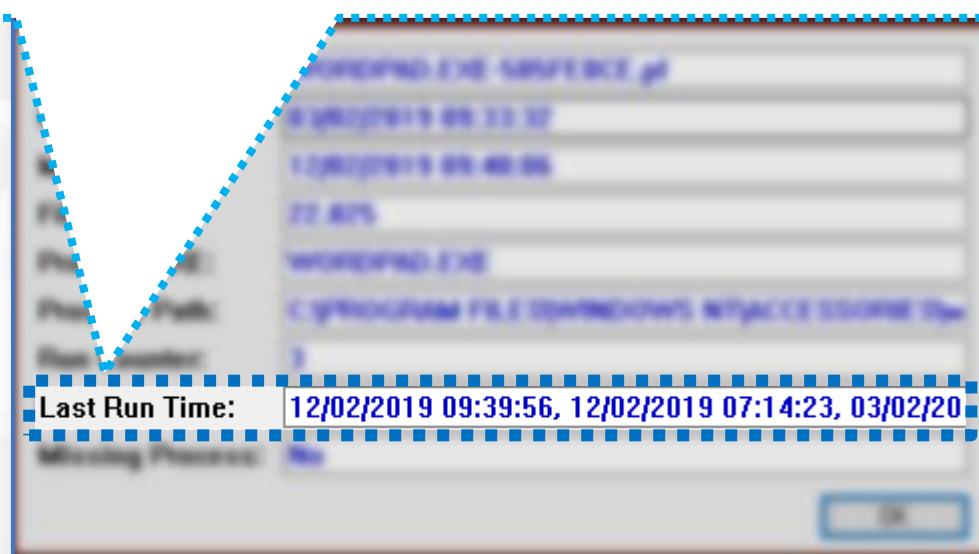


La Cartella Prefetch

Il tool WinPrefetchView | 3/9

- *Proprietà di un File di Prefetch*

Data e ora delle ultime esecuzioni (in questo caso, sono riportate data/ora delle ultime tre esecuzioni)



Attività Pianificate di Windows

To Do List:

~
~
~

Attività Pianificate di Windows

Caratteristiche e Importanza | 1/3

- All'interno del S.O., possono esservi installate diverse applicazioni, che necessitano di eseguire determinate **attività (tasks)**, in un preciso orario/una precisa data e/o con una determinata frequenza
 - *Esempi*
 - Verifica degli aggiornamenti di un software
 - Trasmissioni di dati ad un server
 - Backup di dati in un'apposita cartella
- Tali attività sono dette **attività pianificate (scheduled tasks)**
 - Sono memorizzate tipicamente nella seguente cartella: C:\Windows\System32\Tasks

Attività Pianificate di Windows

Caratteristiche e Importanza | 2/3

- Ciascuna attività pianificata è memorizzata in un file XML, il quale contiene diverse informazioni, fra cui:
 - Chi ha creato l'attività pianificata (autore)
 - Quale è la data e/o l'ora in cui l'attività verrà eseguita
 - Eventualmente, la frequenza con cui l'attività verrà ripetuta
 - *Esempi*
 - Una o più ripetizioni al giorno, una o più ripetizioni alla settimana, ecc.
 - Il percorso relativo all'eseguibile o al comando, che verrà eseguito dall'attività
- È importante notare che le attività pianificate possono anche essere definite dall'utente
 - Pertanto, è necessario considerare anche questo aspetto, nell'ambito dell'investigazione forense

Attività Pianificate di Windows

Caratteristiche e Importanza | 3/3

- *Esempio di possibili attività pianificate dall'utente*
 - Aprire quotidianamente il software Microsoft Word alle ore 10:00
 - Inviare una email alle ore 12:00 di un giorno specificato
 - Avviare l'esecuzione del backup alle 15:00, ogni venerdì

Attività Pianificate di Windows

Analisi delle Attività Pianificate | 1/15

- Analisi delle attività pianificate
 - *Live System*
 - *Dead System*



Attività Pianificate di Windows

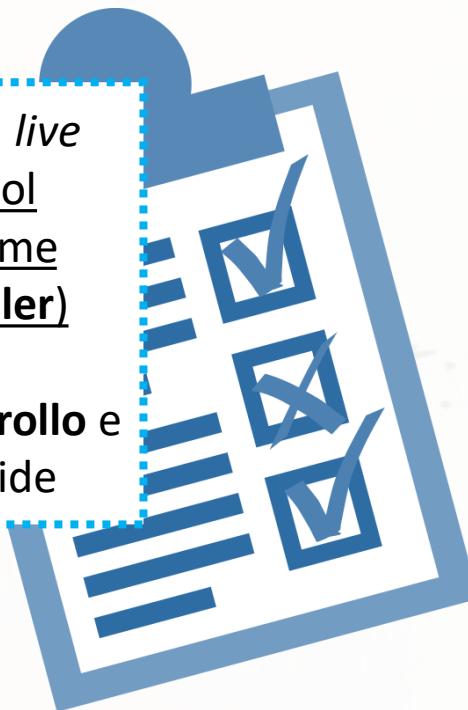
Analisi delle Attività Pianificate | 1/15

- Analisi delle attività pianificate

- Live System***
- Dead System***

L'analisi delle attività pianificate, in un *live system*, può avvenire mediante il tool (integrato in Windows), denotato come **Utilità di Pianificazione (Task Scheduler)**

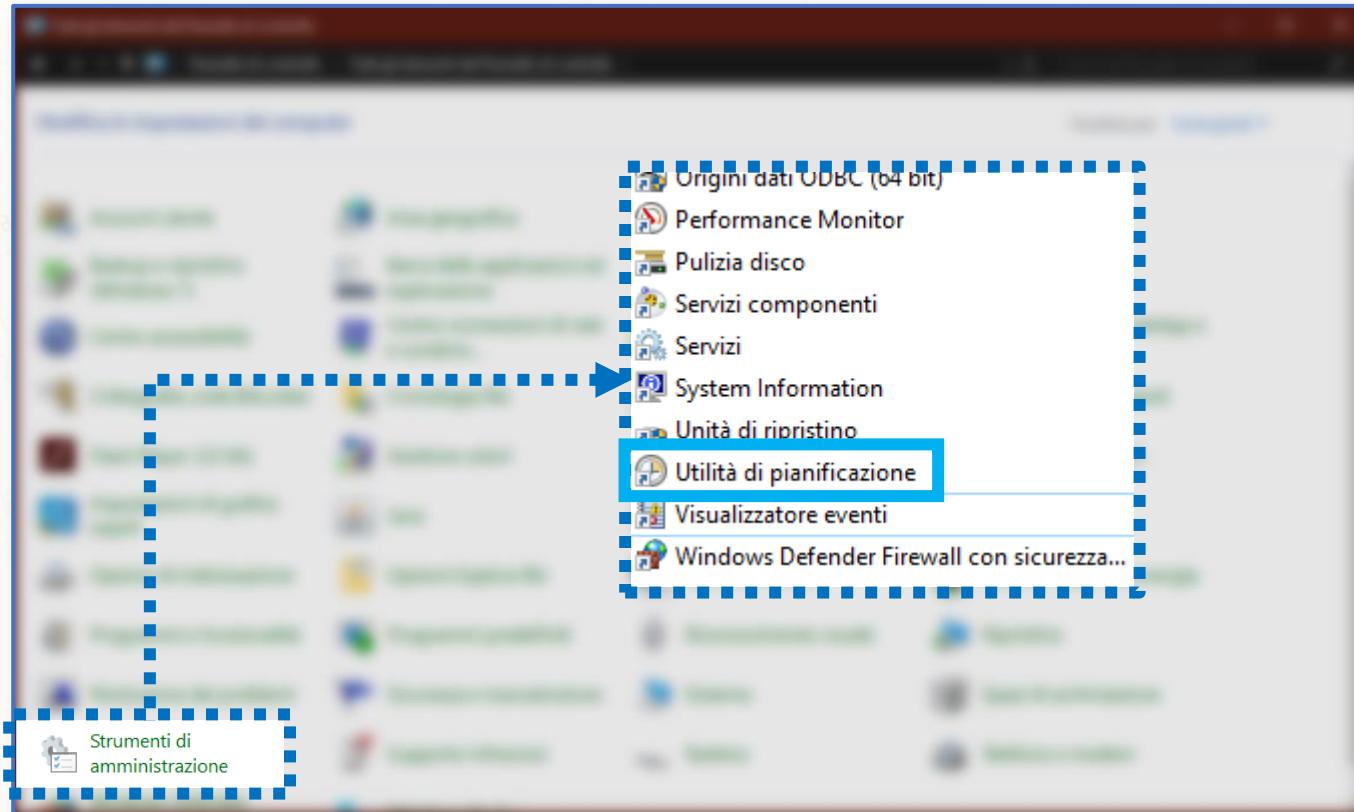
Il tool è accessibile dal **Pannello di Controllo** e verrà approfondito nelle prossime slide



Attività Pianificate di Windows

Analisi delle Attività Pianificate | 2/15

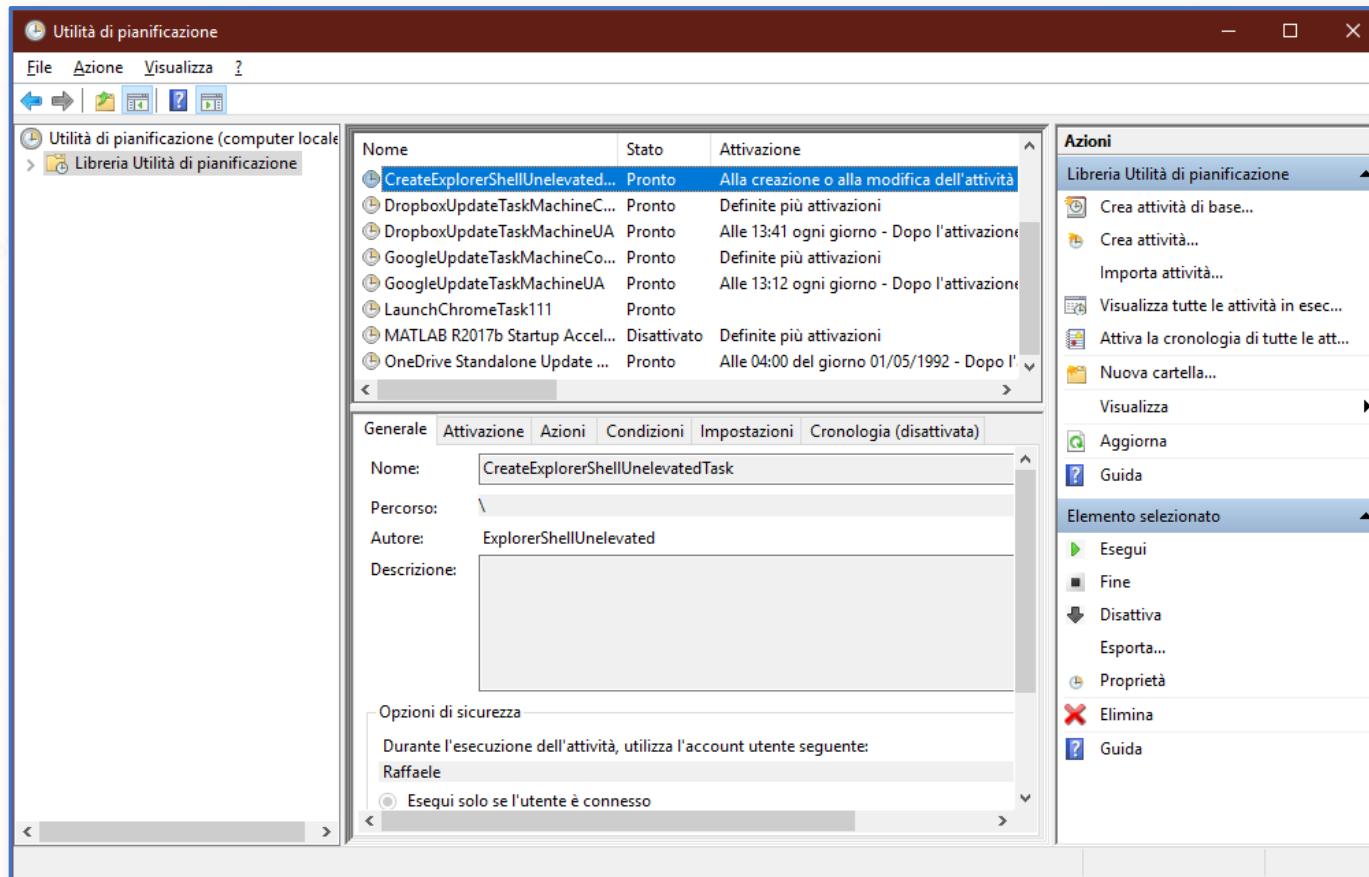
- Avvio del Tool dal Pannello di Controllo | Windows 10



Attività Pianificate di Windows

Analisi delle Attività Pianificate | 3/15

- *Interfaccia Utente del tool Utilità di Pianificazione | 1/6*



Attività Pianificate di Windows

Analisi delle Attività Pianificate | 3/15

- *Interfaccia utente*

Lista delle attività pianificate

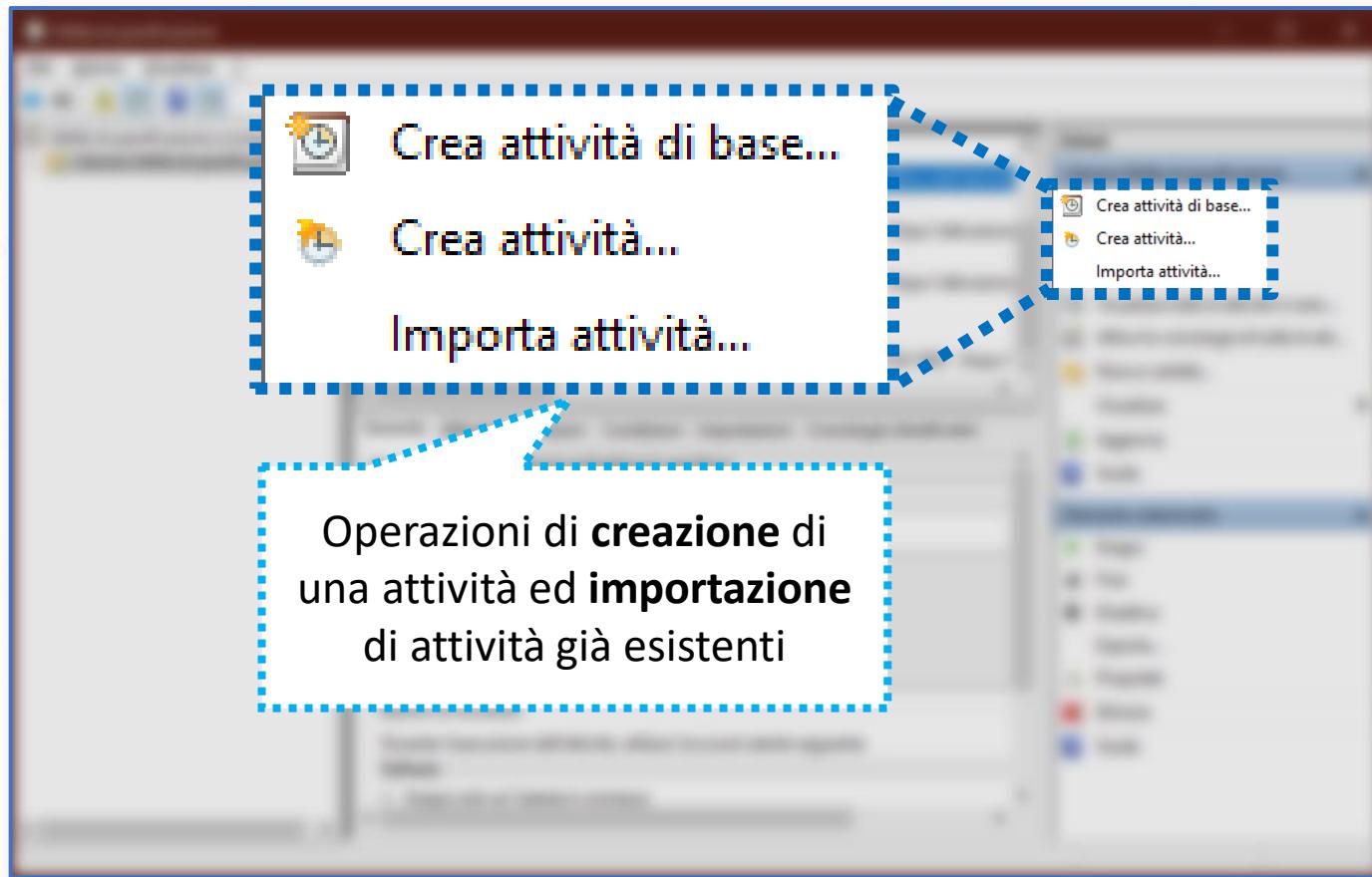
Attività Pianificate | 1/6

Nome	Status	Dettagli
CreateExplorerShellUnelevated...	Pronto	Alla creazione o alla modifica dell'attività
DropboxUpdateTaskMachineC...	Pronto	Definite più attivazioni
DropboxUpdateTaskMachineUA	Pronto	Alle 13:41 ogni giorno - Dopo l'attivazione
GoogleUpdateTaskMachineCo...	Pronto	Definite più attivazioni
GoogleUpdateTaskMachineUA	Pronto	Alle 13:12 ogni giorno - Dopo l'attivazione
LaunchChromeTask111	Pronto	
MATLAB R2017b Startup Accel...	Disattivato	Definite più attivazioni
OneDrive Standalone Update ...	Pronto	Alle 04:00 del giorno 01/05/1992 - Dopo l'

Attività Pianificate di Windows

Analisi delle Attività Pianificate | 3/15

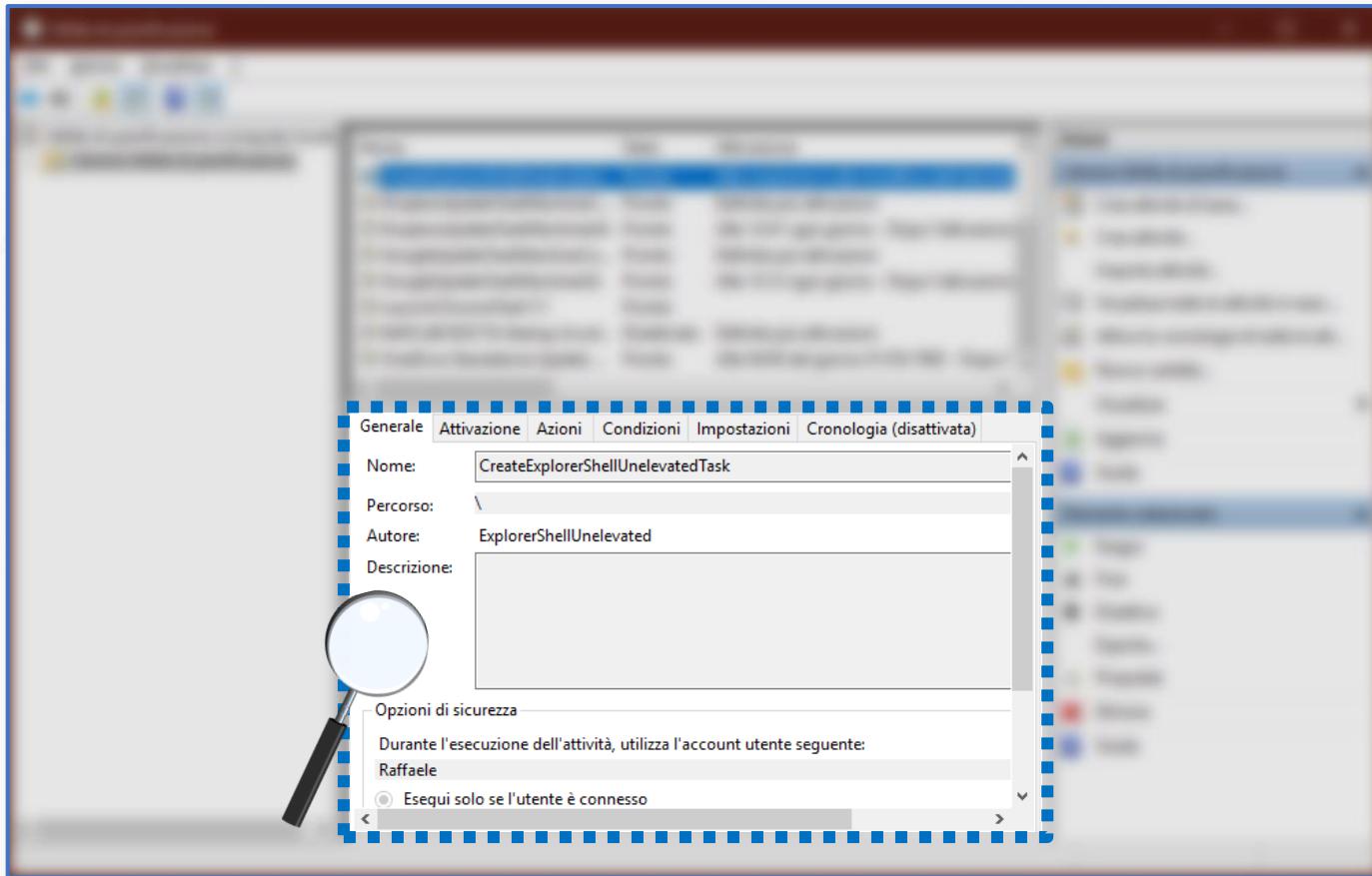
- *Interfaccia Utente del tool Utilità di Pianificazione | 1/6*



Attività Pianificate di Windows

Analisi delle Attività Pianificate | 3/15

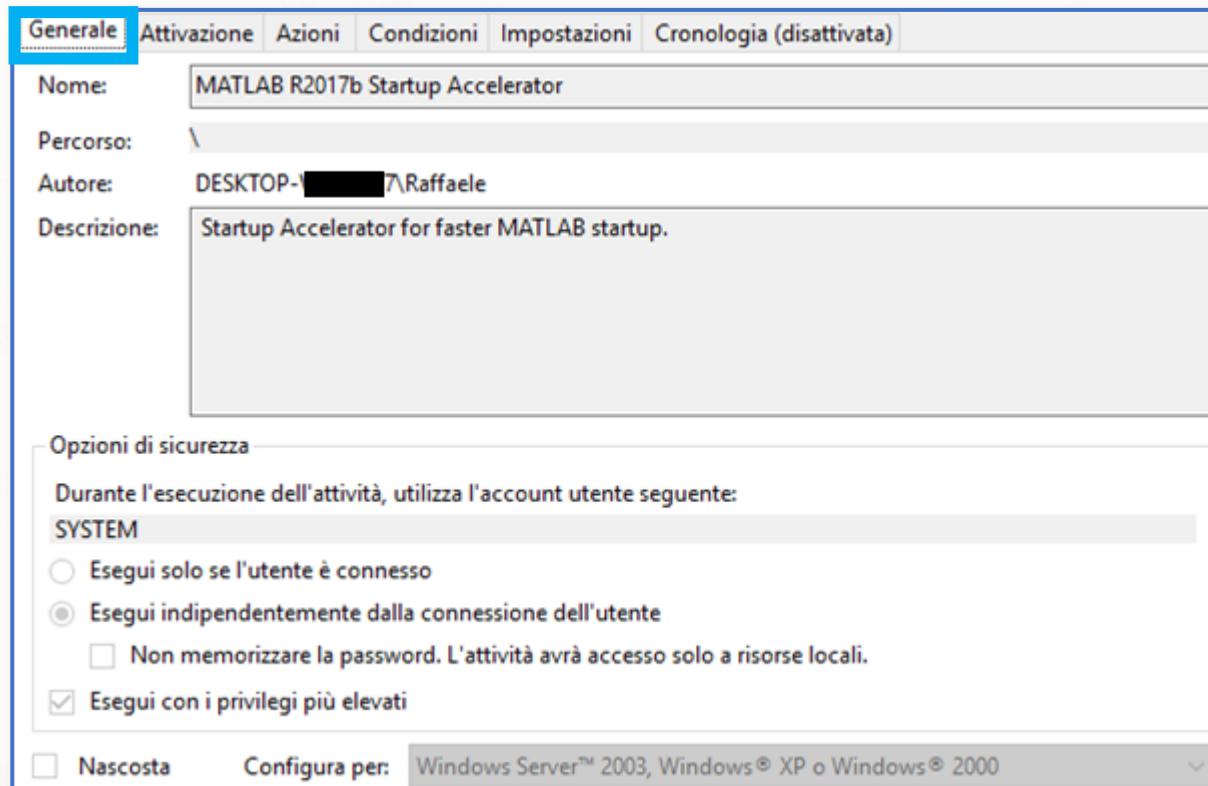
- *Interfaccia Utente del tool Utilità di Pianificazione | 1/6*



Attività Pianificate di Windows

Analisi delle Attività Pianificate | 4/15

- *Interfaccia Utente del tool Utilità di Pianificazione | 2/6*



Attività Pianificate di Windows

Analisi delle Attività Pianificate | 5/15

- *Interfaccia Utente del tool Utilità di Pianificazione | 3/6*

Generale Attivazione Azioni Condizioni Impostazioni Cronologia (disattivata)

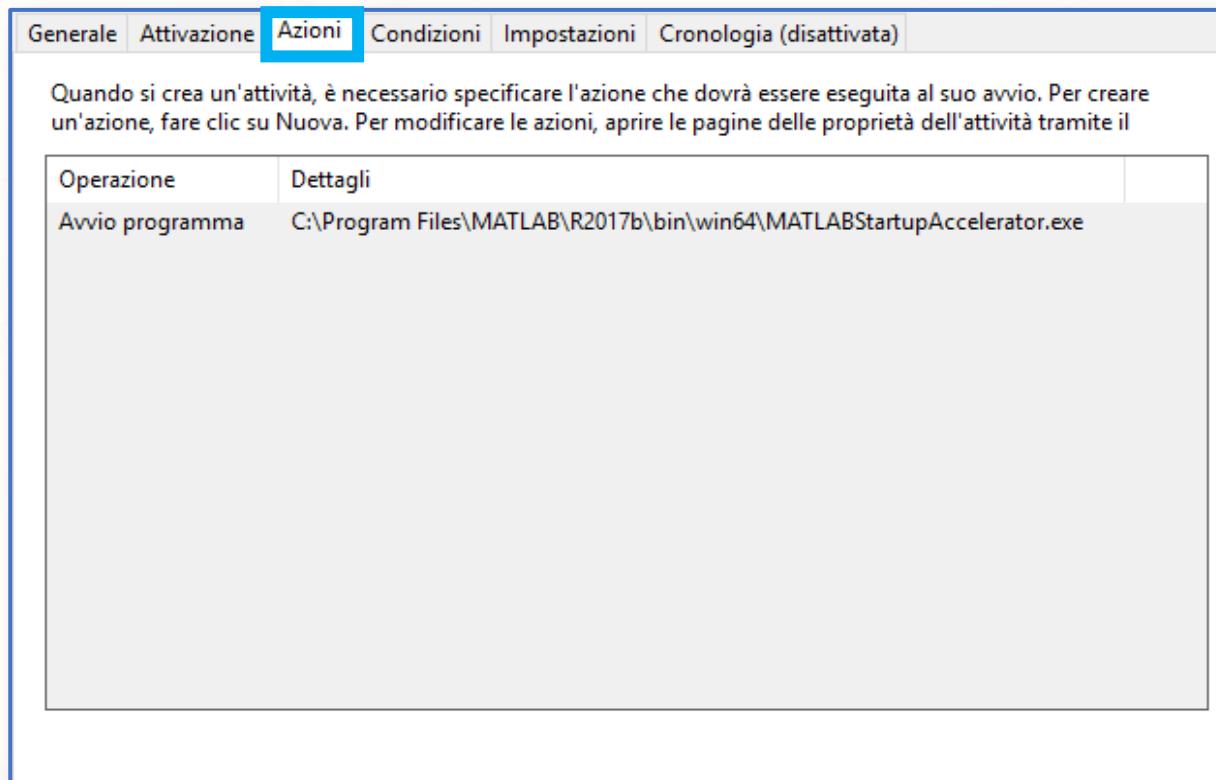
Quando si crea un'attività, è possibile specificare le condizioni che ne determineranno l'esecuzione. Per modificare tali condizioni, aprire le pagine delle proprietà dell'attività tramite il comando Proprietà.

Attivazione	Dettagli	Stato
All'accesso	All'accesso di qualsiasi utente	Attivato
Ogni giorno	Alle 08:04 ogni giorno	Attivato
Ogni giorno	Alle 13:04 ogni giorno	Attivato

Attività Pianificate di Windows

Analisi delle Attività Pianificate | 6/15

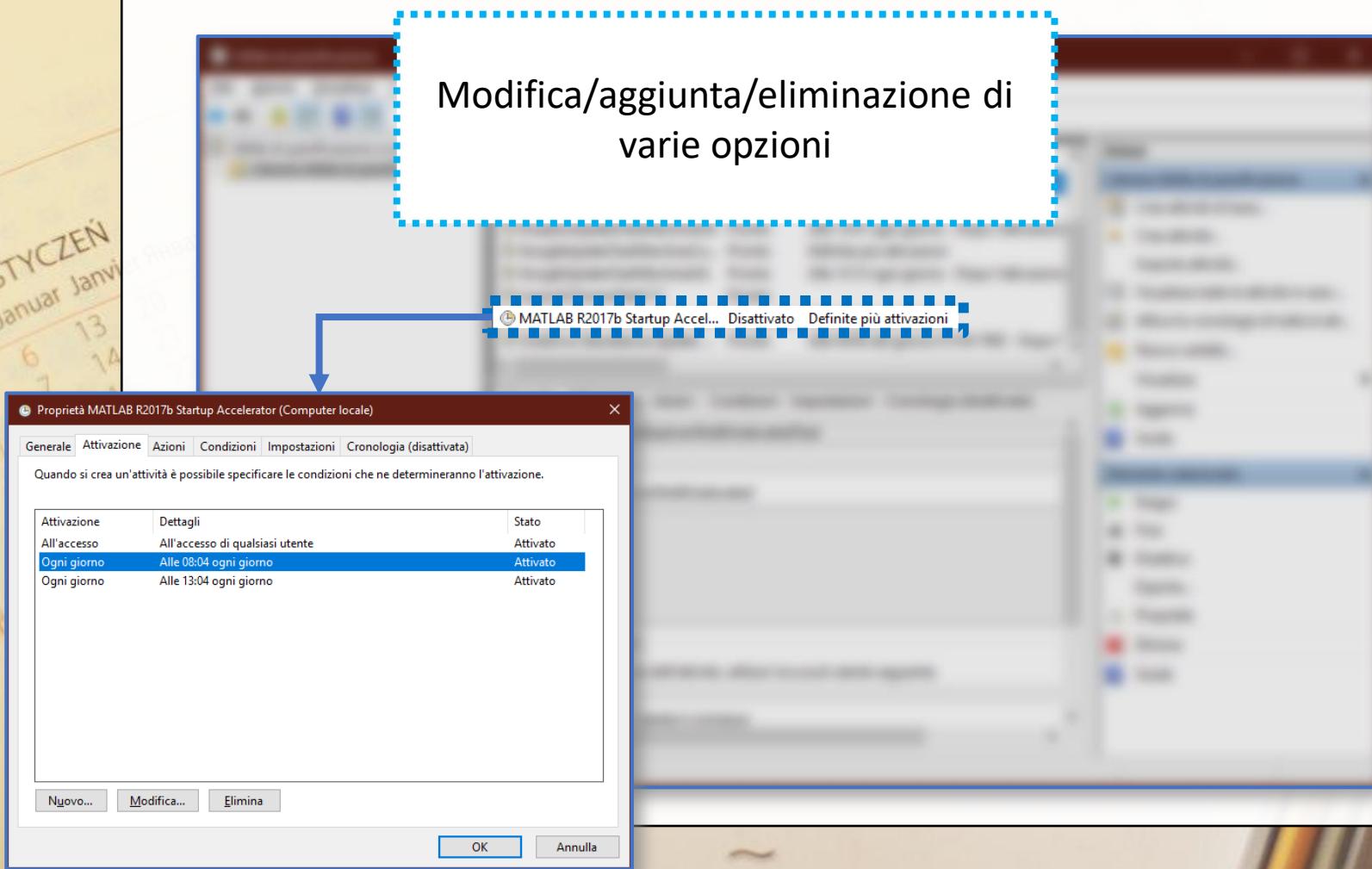
- *Interfaccia Utente del tool Utilità di Pianificazione | 4/6*



Attività Pianificate di Windows

Analisi delle Attività Pianificate | 7/15

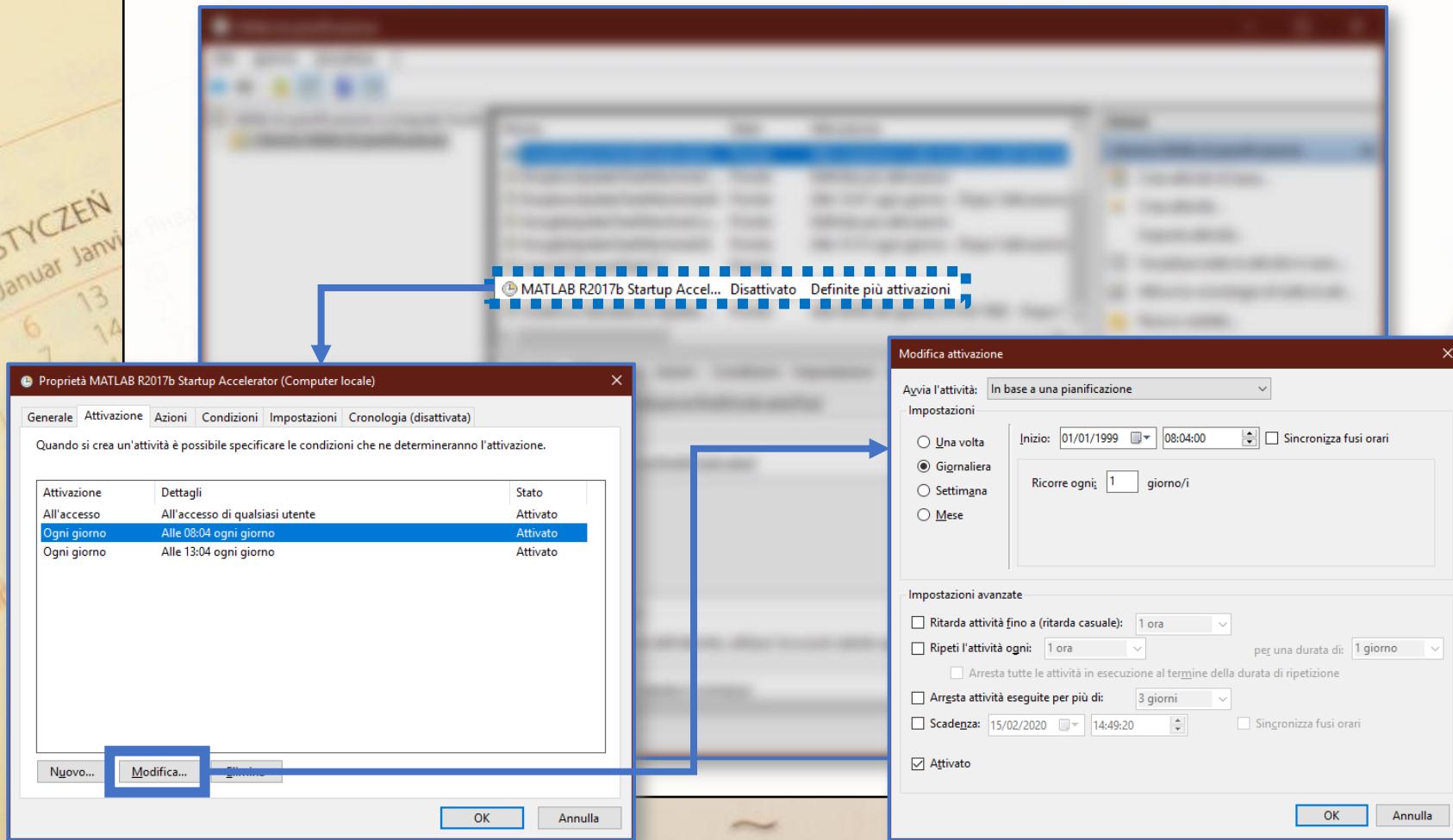
- *Interfaccia Utente del tool Utilità di Pianificazione | 5/6*



Attività Pianificate di Windows

Analisi delle Attività Pianificate | 8/15

- *Interfaccia Utente del tool Utilità di Pianificazione | 6/6*



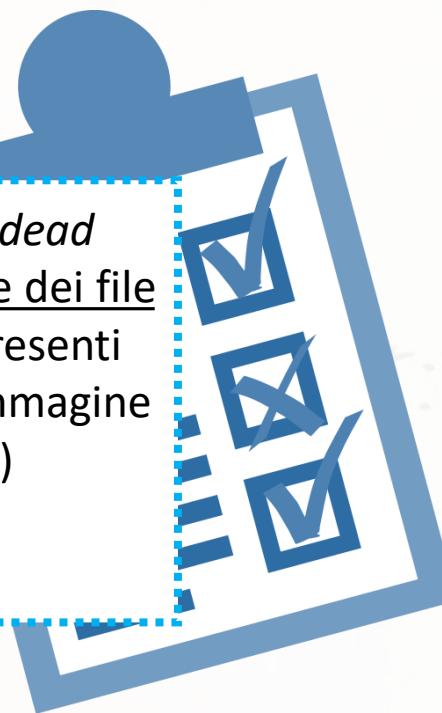
Attività Pianificate di Windows

Analisi delle Attività Pianificate | 9/15

- Analisi delle attività pianificate
 - *Live System*
 - **Dead System**

L'analisi delle attività pianificate, in un *dead system*, può avvenire mediante l'ispezione dei file XML, associati alle attività pianificate, presenti nella relativa cartella (accedendovi dall'immagine forense, acquisita dal dead system)

Esempio nelle prossime slide



Attività Pianificate di Windows

Analisi delle Attività Pianificate | 10/15

- Esempio File XML (GoogleUpdateTaskMachineUA) relativo ad una Attività Pianificata*

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Version>1.3.33.23</Version>
    <Description>Tiene aggiornato il software di Google. Se questa attività viene disabilitata o interrotta, il software di Google non verrà mantenuto aggiornato. Ciò non permetterà di risolvere eventuali problemi dovuti a vulnerabilità della protezione e alcune funzionalità potrebbero non essere eseguite correttamente. Questa attività viene disininstallata automaticamente quando non viene utilizzata da alcun software di Google.</Description>
    <URI>GoogleUpdateTaskMachineUA</URI>
  </RegistrationInfo>
  <Triggers>
    <CalendarTrigger>
      <StartBoundary>2018-12-20T13:12:35</StartBoundary>
      <Repetition>
        <Interval>PT1H</Interval>
        <Duration>PID</Duration>
      </Repetition>
      <ScheduleByDay>
        <DaysInterval>1</DaysInterval>
      </ScheduleByDay>
    </CalendarTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-18</UserId>
      <RunLevel>HighestAvailable</RunLevel>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
    <StartWhenAvailable>true</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <Enabled>true</Enabled>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Program Files (x86)\Google\Update\GoogleUpdate.exe</Command>
      <Arguments>/ua /installsource scheduler</Arguments>
    </Exec>
  </Actions>
</Task>
```

Contenuto del file GoogleUpdateTaskMachineUA

Attività Pianificate di Windows

Analisi delle Attività Pianificate | 11/15

- Esempio File XML (GoogleUpdateTaskMachineUA) relativo ad una Attività Pianificata*

```
<RegistrationInfo>
  <Version>1.3.33.23</Version>
  <Description>Tiene aggiornato il software di Google. Se questa attività viene disabilitata o interrotta, il software di Google non verrà mantenuto aggiornato. Ciò non permetterà di risolvere eventuali problemi dovuti a vulnerabilità della protezione e alcune funzionalità potrebbero non essere eseguite correttamente. Questa attività viene disinstallata automaticamente quando non viene utilizzata da alcun software di Google.</Description>
  <URI>\GoogleUpdateTaskMachineUA</URI>
</RegistrationInfo>
```



```
<RegistrationInfo>
  <Version>1.3.33.23</Version>
  <Description>Tiene aggiornato il software di Google. Se questa attività viene disabilitata o interrotta, il software di Google non verrà mantenuto aggiornato. Ciò non permetterà di risolvere eventuali problemi dovuti a vulnerabilità della protezione e alcune funzionalità potrebbero non essere eseguite correttamente. Questa attività viene disinstallata automaticamente quando non viene utilizzata da alcun software di Google.</Description>
  <URI>\GoogleUpdateTaskMachineUA</URI>
</RegistrationInfo>
```

Tag informativi, inclusa la descrizione dell'attività (evidenziata)

Nell'esempio, si tratta di un'attività pianificata per l'aggiornamento di software Google

Attività Pianificate di Windows

Analisi delle Attività Pianificate | 12/15

- Esempio File XML (GoogleUpdateTaskMachineUA) relativo ad una Attività Pianificata*



```
<Triggers>
  <CalendarTrigger>
    <StartBoundary>2018-12-20T13:12:35</StartBoundary>
    <Repetition>
      <Interval>PT1H</Interval>
      <Duration>P1D</Duration>
    </Repetition>
    <ScheduleByDay>
      <DaysInterval>1</DaysInterval>
    </ScheduleByDay>
  </CalendarTrigger>
</Triggers>
```

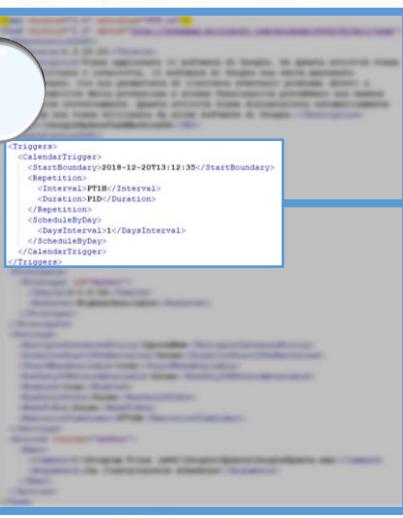
```
<Triggers>
  <CalendarTrigger>
    <StartBoundary>2018-12-20T13:12:35</StartBoundary>
    <Repetition>
      <Interval>PT1H</Interval>
      <Duration>P1D</Duration>
    </Repetition>
    <ScheduleByDay>
      <DaysInterval>1</DaysInterval>
    </ScheduleByDay>
  </CalendarTrigger>
</Triggers>
```

Informazioni sull'eventuale **ripetizione** dell'attività e sulla **schedulazione** della stessa

Attività Pianificate di Windows

Analisi delle Attività Pianificate | 12/15

- Esempio File XML (GoogleUpdateTaskMachineUA) relativo ad una Attività Pianificata*



```
<Triggers>
  <CalendarTrigger>
    <StartBoundary>2018-12-20T13:12:35</StartBoundary>
    <Repetition>
      <Interval>PT1H</Interval>
      <Duration>P1D</Duration>
    </Repetition>
    <ScheduleByDay>
      <DaysInterval>1</DaysInterval>
    </ScheduleByDay>
  </CalendarTrigger>
</Triggers>
```

Attività iniziata a partire dalle ore 13:12:35,
del 20/12/2018

Attività Pianificate di Windows

Analisi delle Attività Pianificate | 12/15

- Esempio File XML (GoogleUpdateTaskMachineUA) relativo ad una Attività Pianificata



```
<Triggers>
  <CalendarTrigger>
    <StartBoundary>2018-12-20T13:12:35</StartBoundary>
    <Repetition>
```

```
      <Interval>PT1H</Interval>
      <Duration>P1D</Duration>
    </Repetition>
    <ScheduleByDay>
      <DaysInterval>1</DaysInterval>
    </ScheduleByDay>
  </CalendarTrigger>
</Triggers>
```

Informazioni sull'eventuale **ripetizione** dell'attività, nell'arco di **un giorno**

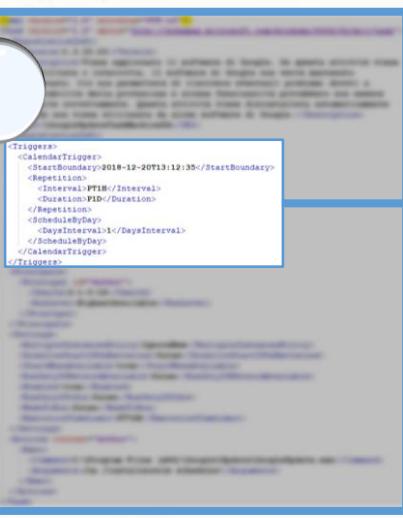
Nell'esempio, l'attività viene ripetuta ogni ora (tag *Interval*) per la durata di un giorno (tag *Duration*)

NOTA: I valori PT1H (valore tag *Interval*) e P1D (valore tag *Duration*) sono nel formato ISO 8601

Attività Pianificate di Windows

Analisi delle Attività Pianificate | 12/15

- Esempio File XML (GoogleUpdateTaskMachineUA) relativo ad una Attività Pianificata*



```
<Triggers>
  <CalendarTrigger>
    <StartBoundary>2018-12-20T13:12:35</StartBoundary>
    <Repetition>
      <Interval>PT1H</Interval>
      <Duration>P1D</Duration>
    </Repetition>
    <ScheduleByDay>
      <DaysInterval>1</DaysInterval>
    </ScheduleByDay>
  </CalendarTrigger>
</Triggers>
```

Informazioni sull'eventuale **schedulazione** dell'attività, nell'arco eventualmente di **più giorni**

Nell'esempio, l'attività viene ripetuta ogni giorno

Attività Pianificate di Windows

Analisi delle Attività Pianificate | 13/15

- Esempio File XML (GoogleUpdateTaskMachineUA) relativo ad una Attività Pianificata*

```
<Principals>
  <Principal id="Author">
    <UserId>S-1-5-18</UserId>
    <RunLevel>HighestAvailable</RunLevel>
  </Principal>
</Principals>
```

Tag informativi sull'**autore** dell'attività



```
<Principals>
  <Principal id="Author">
    <UserId>S-1-5-18</UserId>
    <RunLevel>HighestAvailable</RunLevel>
  </Principal>
</Principals>
```

Attività Pianificate di Windows

Analisi delle Attività Pianificate | 14/15

- Esempio File XML (GoogleUpdateTaskMachineUA) relativo ad una Attività Pianificata*

```
<Settings>
  <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
  <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
  <StartWhenAvailable>true</StartWhenAvailable>
  <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
  <Enabled>true</Enabled>
  <RunOnlyIfIdle>false</RunOnlyIfIdle>
  <WakeToRun>false</WakeToRun>
  <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
</Settings>
```

Tag relativi ad **impostazioni/settaggi** per l'esecuzione dell'attività



```
<Settings>
  <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
  <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
  <StartWhenAvailable>true</StartWhenAvailable>
  <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
  <Enabled>true</Enabled>
  <RunOnlyIfIdle>false</RunOnlyIfIdle>
  <WakeToRun>false</WakeToRun>
  <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
</Settings>
```

Attività Pianificate di Windows

Analisi delle Attività Pianificate | 14/15

- Esempio File XML (GoogleUpdateTaskMachineUA) relativo ad una Attività Pianificata*

```
<Settings>
  <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
  <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
  <StartWhenAvailable>true</StartWhenAvailable>
  <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
  <Enabled>true</Enabled>
  <RunOnlyIfIdle>false</RunOnlyIfIdle>
  <WakeToRun>false</WakeToRun>
  <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
</Settings>
```

Nell'esempio, l'attività pianificata è attiva (valore *true* del tag *Enabled*)



A screenshot of the Windows Task Scheduler interface. A specific task configuration window is open, showing various settings like trigger, action, and conditions. A magnifying glass icon is placed over this window, pointing towards the XML code below.

```
<Settings>
  <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
  <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
  <StartWhenAvailable>true</StartWhenAvailable>
  <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
  <Enabled>true</Enabled>
  <RunOnlyIfIdle>false</RunOnlyIfIdle>
  <WakeToRun>false</WakeToRun>
  <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
</Settings>
```

Attività Pianificate di Windows

Analisi delle Attività Pianificate | 15/15

- Esempio File XML (GoogleUpdateTaskMachineUA) relativo ad una Attività Pianificata*

```
<Actions Context="Author">
  <Exec>
    <Command>C:\Program Files (x86)\Google\Update\GoogleUpdate.exe</Command>
    <Arguments>/ua /installsource scheduler</Arguments>
  </Exec>
</Actions>
```

Informazioni in merito al **programma/comando** (tag *Command*) da eseguire, con gli eventuali **relativi argomenti** (tag *Arguments*)

Nell'esempio, il programma è GoogleUpdate.exe

```
<Actions Context="Author">
  <Exec>
    <Command>C:\Program Files (x86)\Google\Update\GoogleUpdate.exe</Command>
    <Arguments>/ua /installsource scheduler</Arguments>
  </Exec>
</Actions>
```