Università degli studi di Salerno
Facoltà di Scienze Matematiche Fisiche e Naturali

Corso di Laurea Magistrale in
Informatica

Windows Forensic Analysis: Data Remanence

Cinque Valerio 0522500098
Testorio Francesco 0522500075

Anno Accademico 2011-2012

Indice degli argomenti

INTRODUZIONE

Investigazioni Informatiche

L'utilizzo delle tecnologie in campo informatico e nella comunicazione digitale, ha portato al giorno d'oggi all'aumento del numero dei reati informatici, mostrando dunque una certa familiarità acquisita da parte dei delinquenti o criminali col mondo dell'informatica.
I reati in ambito informatico di cui siamo soggetti oggi, vanno dal cyber terrorismo alle truffe attraverso il mezzo Internet, senza dimenticare i reati già conosciuti di pedopornografia, spionaggio e manomissioni di apparecchiature informatiche.
In questo contesto le investigazioni informatiche svolgono un ruolo di primo piano, sia per fare rispettare la legalità attraverso il mezzo informatico, sia per ricercare le prove lasciate dall'autore di un crimine. Per investigazioni informatiche s'intendono una serie di tecniche e metodologie informatiche che devono essere applicate per eseguire l'analisi di un crimine o di una violazione alla sicurezza mediante un sistema informatico al fine di acquisire, conservare, analizzare e documentare delle prove da una Computer Crime Scene durante un'attività investigativa. Ogni reato informatico 'lascia' delle tracce che possono essere analizzate dagli investigatori al fine di formare la cosiddetta "prova digitale" o "digital evidence". Usando gli opportuni strumenti per l'indagine informatica è quasi sempre possibile risalire ad ogni documento elettronico creato, consultato e/o cancellato. In questo scenario, entra in gioco il Data Remanence (Persistenza dei dati nel sistema), ovvero i possibili residui dei dati che restano in un sistema anche dopo aver tentato di cancellarli.

La Digital Forensics

Con il termine forensics s'intende il processo dell'utilizzo di conoscenze scientifiche nella raccolta, analisi e presentazione di prove in tribunale.
Con il termine "Digital Forensics" s'intende definire un "processo" costituito dall'insieme di misure, di carattere legislativo, organizzativo e tecnologico, tese ad analizzare dati e/o informazioni trattati in formato digitale. Le misure tecnologiche in ambito "Digital Forensics" si riferiscono ad un insieme di procedure e di operazioni per la preservazione, l'identificazione, lo studio, la documentazione di sistemi digitali, al fine di evidenziare l'esistenza di prove durante un'attività investigativa.

Progetto

In questo scenario di Digital Forensics, il nostro progetto analizza il Sistema Operativo Microsoft Windows 7, mostrando le evidenze che possono essere generate, cancellate e modificate nei registri del sistema. Presentiamo prima una panoramica sulle caratteristiche del Sistema Operativo Microsoft Windows, tra cui le versioni, il File System, i registri e le proprietà nelle quali è possibile trovare delle evidenze di tipo digitale.
Mostriamo in seguito, con casi di studio, come trovare delle evidenze all'interno di Microsoft Windows 7, usando appositi strumenti ed inoltre analizzeremo il problema della Data Remanence (Persistenza dei dati nel sistema).

Capitolo 1

Digital Forensics e Microsoft Windows

Il sistema operativo Windows è tra i più popolari al mondo, nonostante le sue molteplici versioni. Proprio a causa di questa popolarità, chi opera delle indagini forensi su questo sistema, deve conoscere bene le caratteristiche associate ad ognuna di queste versioni, così come gli artefatti associati in modo da ottenere un'analisi migliore.
Per eseguire un'analisi forense su sistema Windows, è importante conoscere meccanismi quali il processo di avvio, creazione e cancellazione dei file.
Inoltre è utile capire come aggregare e correlare i dati su questo sistema, per capire ad esempio l'ora e la data del trasferimento di un file.

1.1 Versioni recenti di Microsoft Windows

Microsoft ha sviluppato il sistema operativo Windows, creando varie versioni che in pratica sono una l'evoluzione dell'altra. Descriviamo in questo paragrafo, in modo generale, le versioni di Windows più recenti.

Microsoft Windows XP

Il sistema operativo Windows XP è la più familiare delle versioni Windows, poiché dalla sua entrata in scena nel 2001 dove si presentava con tre edizioni per assecondare ogni tipologia di utente (Home, Media Center e Professional), ha saputo conquistare una grande maggioranza di clienti con una nuova interfaccia (per l'epoca) molto familiare. Esso veniva eseguito con File System FAT o NTFS (che verrà affrontato nel dettaglio in seguito) e presenta alcune caratteristiche molto utili per gli esaminatori forensi. Infatti, le evidenze delle azioni dell'utente sono registrate in alcuni settori che sono facili da visitare per investigatori digitali esperti, attraverso degli appositi tool e nei quali è possibile trovare le seguenti informazioni:

- Cronologia internet
- Event Log
- File di prefetch
- Thumbs.db

Oltre queste evidenze, che sono tra le più comuni, gli esaminatori forensi possono anche allargare il loro campo di ricerca andando a scovare altre caratteristiche che sono più complicate da analizzare, come:

- Punti di ripristino
- Registri di sistema
- Memoria
- Superamento della crittografia Windows per documenti e dati distrutti

Nonostante questo sistema sia stato superato da Windows Vista e Windows 7, Microsoft continuerà ad aggiornarlo fino al 2014 e ciò fa pensare proprio a quanto sia stato e sia ancora tuttora popolare questo sistema.

Microsoft Windows Vista e 7

Il sistema operativo Windows Vista, presenta simili caratteristiche di Windows 7 a livello di File System e registri. Per cui, quando parliamo di Windows Vista ci riferiamo anche a Windows 7, poiché hanno le stesse caratteristiche. Come per Windows XP, anche Windows Vista al suo esordio nel 2007, si presentava con multiple edizioni: Starter, Home Basic e Basic N, Home Premium, Business e Business N, Enterprise e infine Ultimate. Ognuna di esse ha delle proprie capacità e delle proprie caratteristiche, come ad esempio Vista Home, che permette agli utenti di eseguire back-up dei documenti, mentre Vista Enterprise permette la creazione di copie cloni dell'intero hard disk o di partizioni dell'hard disk per un recupero successivo. Analogamente a XP anche Vista utilizza un File System NTFS. Caratteristiche aggiuntive di Vista rispetto a XP sono ad esempio:

- La capacità di Windows Search (la ricerca in windows) di indicizzare la maggior parte dei file utente e le cartelle per aiutare gli utenti nella ricerca di file particolari.
- Il grande utilizzo di metadati.

Vista però, oltre a portare delle migliorie per gli utenti, comporta anche degli svantaggi per gli esaminatori forensi che avevano acquisito con XP una certa familiarità con alcune caratteristiche di Windows. In particolare, le differenze tra XP e Vista che portano delle difficoltà per gli investigatori digitali sono:

- Differenze di pathing tra XP e Vista (ad esempio: \Users\<*username*>\AppData\Local in Vista contro \Documents and Settings\<*username*>\Local Settings in XP)
- Differenze nella struttura dati Recycle Bin
- Codifica BitLocker (funzionalità di protezione dei dati)

1.2 Tracce dell'attività dell'utente

In questo paragrafo mostriamo alcune delle tracce che potrebbero essere lasciate dagli utenti sul sistema, in che modo è possibile recuperarle e in che modo possono interessare un esaminatore forense.

Metadati

I metadati contengono informazioni riguardanti altri dati.
Si classificano in:

- Metadati del File System
  - ✓ Esempio: le timestamp dei file che indicano quando una cartella o un file è stato copiato, spostato o scritto. In particolare, per l'indagine forense interessano quelle informazioni che mostrano l'attività dell'utente, come la creazione di un file, la modifica, l'ultimo accesso e la modifica del SIA (cioè la modifica della entry nel MFT).
- Metadati delle applicazioni
  - ✓ Esempio: l'intestazione di un documento Office. A differenza dei metadati del File System, i metadati delle applicazioni si trovano all'interno dei file a cui si riferiscono (come i file di Microsoft Office, file PDF e foto digitali). Queste informazioni, generalmente collocate o registrate con l'applicazione utilizzata per creare o lavorare con il file, possono essere preziose per l'investigatore.

Logging

Quando un utente ha accesso ad un computer lascia, inevitabilmente, tracce della sua attività:

- Effettuare il log in ed il log out nel sistema
  - ✓ Lascia tracce in alcune chiavi del registro di sistema e nel file NTUSER.DAT
- Windows Event Logging registra informazioni relative a:
  - ✓ Applicazioni
  - ✓ Sicurezza
  - ✓ Accesso alle risorse

Tracce lasciate dall'uso di applicazioni

Link Files (file di collegamento): i file di collegamento (estensione .LNK) sono semplicemente scorciatoie, che puntano ad un altro file o una cartella. Gli utenti a volte creano queste scorciatoie intenzionalmente per un comodo accesso a determinati elementi, ma più spesso Windows crea automaticamente i file di collegamento nel tentativo di aiutare l'utente e velocizzare le operazioni e memorizza questi file link su Desktop, Start Menu, o cartelle recenti.

Prefetch Files*:* i file prefetch (estensione .PF) sono un tipo di file specializzati, simile al file di collegamento, utilizzati dai sistemi operativi Windows XP/2k3/Vista/7 per accelerare il funzionamento dei file eseguibili. Ogni volta che viene avviata un'applicazione in Windows, dietro le quinte il sistema operativo crea un prefetch file contenente alcune informazioni sul programma avviato. In Windows XP e Vista, in particolare, l'applicazione di prefetch dati è utilizzata per eseguire le applicazioni in modo più efficiente nelle successive esecuzioni. In pratica i file di prefetch sono utilizzati per ottimizzare l'esecuzione dei processi frequenti. I file di prefetch sono memorizzati in una cartella denominata Prefetch situata nella cartella di sistema %SystemRoot%\Prefetch, normalmente C:\WINDOWS\Prefetch.

Programmi installati*:* I programmi installati su un sistema in esame spesso hanno una grande rilevanza sull'inchiesta. Le informazioni su questi programmi installati sono reperibili nella cartella C:\Program Files, che contiene i file e le cartelle create quando un'applicazione viene installata e viene spesso utilizzata come posizione dalla quale eseguire un programma (per esempio, C:\Program Files\Microsoft Office\Office12\winword.exe). Questa cartella è utile in quanto ci permette di definire quando un programma è stato installato (fornisce indicazioni sulle date dei file creati). Altre fonti di informazioni sui programmi installati, sono le cartelle di dati delle applicazioni che si trovano sotto ogni profilo utente, nelle seguenti locazioni:

- C:\Documents and Settings\<*user folder*>\Application Data (Windows XP).
- C:\Users\<*user folder*>\AppData (Windows Vista and 7).

Queste cartelle contengono dati specifici per i programmi installati dall'utente e potrebbero contenere residui di essi anche dopo averli disinstallati.

Processo di avvio

È una caratteristica di Windows importante per gli investigatori forensi poiché interrompendo il processo di avvio, è possibile visualizzare e documentare la configurazione CMOS (meglio nota come impostazione di Basic Input Output – BIOS, consiste in una serie d'istruzioni di base utili per un computer per inizializzare i suoi componenti hardware). Inoltre è utile per gli esaminatori forensi capire il funzionamento del processo di avvio per tre motivi:

- ✓ Dimostrare che nessun file utente creato in precedenza è stato modificato
- ✓ Determinare quale versione di windows è eseguita e quando è stata installata
- ✓ Rilevare che non ci siano segni di manomissione

Thumbnail cache

I file thumbnail, sono immagini in miniatura che forniscono un'anteprima del contenuto delle cartelle o di un file. In Windows XP, un file «thumbs.db» è presente in ogni cartella e contiene sia la miniatura del contenuto e sia il data-time stamp dei file visualizzati. In Windows Vista e 7, i file sono raggruppati in una cartella per ogni utente. Per gli esaminatori forensi le thumbnail sono utili

in quanto possono rimanere nel sistema anche dopo che l'effettivo oggetto, cui l'anteprima dell'immagine si riferisce, è stato eliminato.

File di stampa

Ulteriori informazioni per le indagini forensi derivano anche dai file di stampa.
I file di stampa, nel formato EMF (Enhanced Metafile), contengono la pagina da mandare in stampa. Vengono mantenuti solo se sorgono problemi durante la stampa.
Al prossimo riavvio, vengono automaticamente cancellati.

Cestino

Cancellare un file non corrisponde a metterlo nel cestino.
Il cestino è una cartella che ospita, oltre ai file inseriti in esso, due file particolari:

- «INFO2», in Windows XP, funge da indice e archivio di informazioni sui file inviati nel Cestino. Quando un file viene spostato nel Cestino, viene rinominato e il suo nome inizia con una "D" (presumibilmente per "deleted" - cancellato), seguito dalla lettera di unità in cui il file precedentemente risiedeva, un numero incrementato, e l'estensione del file originale del file (per esempio, Dc3.doc). Anche se il nome del file viene modificato, i dati di posizione fisica sul disco, le sue dimensioni e il codice sono immutati, e il file può essere ancora aperto o visualizzato con poca fatica. Ogni file spostato nel Cestino ha il suo record nel file INFO2, con ogni record di 800 byte di lunghezza. Questi record INFO2 dei file contengono informazioni importanti che gli esaminatori possono interpretare e utilizzare nelle loro indagini.
- Due file che iniziano per «$R» e «$I», in Vista e 7. Il Cestino in Vista e 7 opera in modo diverso da quello dei suoi cugini in precedenza. In Vista (e 7), la cartella Cestino è stata rinominata $Recycle.Bin e (al contrario di Windows 2k/XP/2k3) una sottocartella Cestino viene creata per un utente la prima volta che si logga (esegue l'accesso al sistema), a prescindere dal fatto che sia stato cancellato o meno qualcosa. Un'altra differenza è che il file INFO2 è stato sostituito da un processo che utilizza due file di corrispondenza per ogni file inviato al Cestino. Quando un file viene inviato al Recycle Bin (cestino) Vista, viene rinominato con uno pseudo nome del file che inizia con $R e termina con l'estensione originale del file; questo File $R contiene il contenuto originale del file. Insieme al file $R, un altro file (il cui nome inizia con $I e nominato ad essere complementare al file $R) viene creato e contiene la data del file e il tempo di eliminazione (file di offset 16; 8 byte) e il percorso del file al momento della cancellazione (file di offset 24; lunghezza variabile, in Unicode).

Questi file mantengono informazioni relative ai file inseriti.

Connessioni di dispositivi esterni

Ogni qual volta un dispositivo esterno come ad esempio una pendrive USB, viene collegata al computer, Windows registra delle tracce nel registro di sistema. Queste informazioni possono essere molto utili per capire se l'utente ad esempio ha del materiale che non risiede sul disco fisso del computer ma su supporti rimovibili.

File di paging e cattura live della memoria

Per migliorare le performance del sistema, Windows aggiunge alla memoria fisica, la memoria virtuale.
Mentre UNIX sfrutta una vera e propria partizione, Windows realizza la memoria virtuale attraverso il file «Pagefile.sys».
Il contenuto di tale file può spesso rivelarsi una vera miniera di informazioni per gli investigatori, in quanto può contenere ad esempio degli eseguibili decompressi, password in chiaro ed altro ancora. Il contenuto della memoria fisica (RAM) può essere letto attraverso appositi tool e come per i file di paging, può rivelarsi ricco di informazioni.

Punti di ripristino

Un altro "contenitore" implicito di informazioni per gli investigatori forensi, è il punto di ripristino presente dalle versioni Windows Xp in poi. Infatti Windows utilizza i punti di ripristino per consentire di riportare ad un preciso stato temporale il sistema. Un punto di ripristino è costituito da una copia di backup dei file di sistema e delle applicazioni.

1.3 Cancellazione e distruzione dei dati

Un altro punto di interesse di Windows è la cancellazione e la distruzione dei dati: attraverso quali procedure è possibile effettuare queste operazioni e quali tracce lascino queste operazioni, sono le caratteristiche principali che interessano l'investigatore forense. Di seguito vedremo quali sono le operazioni che possono portare alla cancellazione e alla distruzione dei file.

Wiping

Per poter affermare di aver cancellato definitivamente un file, non basta utilizzare i tradizionali strumenti messi a disposizione del sistema operativo.
Un file può risultare nel File System come cancellato ma, i suoi dati, finché non sovrascritti, possono ancora essere recuperati.
L'attività di wiping consiste nel forzare la sovrascrittura. Un tool di wiping è un programma e, in quanto tale, può lasciare una traccia.

Deframmentazione

La deframmentazione è un'altra possibilità di cancellazione definitiva.
Questa provvede ad avvicinare i blocchi che costituiscono i frammenti dei file nel disco, in modo da ottimizzare letture e scritture. L'attività di deframmentazione causa una sovrascrittura parziale di blocchi.

1.4 Internet e attività di comunicazione

Altra particolare attenzione nelle indagini forensi, meritano le possibili tracce lasciate dall'utente durante la navigazione Internet. Come vedremo, sono molto di interesse i browser con le loro funzionalità e la chat di Windows.

Browser

Un browser fornisce diverse tracce dell'attività di un utente:

- Cookie
  - ✓ Mantengono informazioni relative a una sessione aperta con un web server
- Internet history
  - ✓ Mantiene una ricca cronologia delle URL visitate dell'utente
- Web cache
  - ✓ Contiene i file scaricati durante la visita delle pagine web

Windows Chat

Sono molte le informazioni derivabili da un programma di messaggistica istantanea per Windows:

- Cronologia conversazioni
- File scambiati
- Lista contatti

Capitolo 2

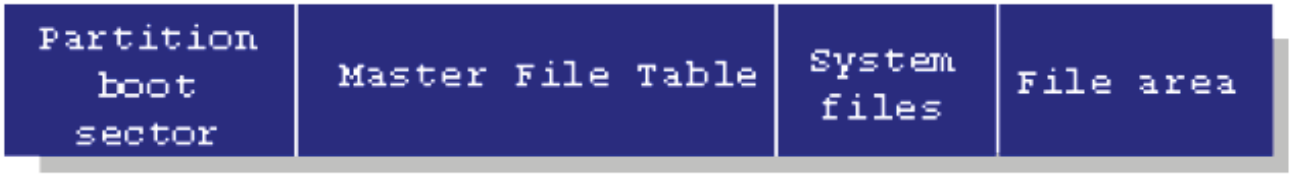
Il File System di Windows

Il File System di "default" nei sistemi operativi da Windows NT in poi è NTFS.
Sfortunatamente non sono mai state pubblicate delle specifiche da parte di Microsoft. Tutto ciò che si sa su questo File System è grazie al reverse engineering, cioè il lavoro di gruppi che hanno pubblicato quello che credono essere il funzionamento dell'NTFS.

2.1 NTFS (New Technology File System)

Il File System NTFS è l'alternativa al vecchio File System, utilizzato sempre nei sistemi operativi Windows, FAT32 che è stato utilizzato fino a Windows XP. Questo vecchio File System teneva traccia delle aree del disco disponibili e di quelle già usate dai file e dalle directory. Il numero 32 sta ad indicare il numero di bit allocati per numerare i cluster (raggruppamento logico di settori contigui in un disco rigido) del disco. NTFS Utilizza una struttura dati chiamata MFT – Master File Table e delle entries (voci all'interno della tabella) chiamate attributi indice invece di una tabella di allocazione file (FAT).

Questo File System può essere visto come diviso in:



Ogni cosa in NTFS è un file e ogni cosa in un file è un attributo e abbiamo dunque due conseguenze:

- Anche le informazioni di sistema vengono archiviate in file e quindi possono trovarsi in qualsiasi parte del volume
- Qualunque cosa, dal nome del file ai dati che contiene, sono attributi del file stesso.

Descrizione dei file all'interno di NTFS

Nome File	$ MFT Record	Funzione Generale
$MFT	0	MFT stessa
$MFTMirr	1	Usato per recuperabilità del sistema
$LogFile	2	Usato per recuperabilità del sistema
$Volume	3	Contiene informazioni sul volume formattato
$AttrDef	4	Elenca gli attributi supportati dal volume formattato
$Bitmap	6	Tracce di uso di cluster sul volume
$Boot	7	Sottolinea il settore di avvio del volume sul disco
$BadClus	8	Tiene traccia della posizione dei cluster danneggiati sul disco
$Secure	9	In Windows 2000 e successivi, memorizza descrittori di sicurezza

Di seguito andremo a vedere nel dettaglio alcuni dei file del File System NTFS elencati nella tabella precedente e in particolare, vedremo la loro funzionalità e in che modo possono interessare gli esaminatori forensi.

$MFT

Gli esaminatori forensi reputano essenziale la conoscenza di MFT, in quanto consente di determinare quali siano gli strumenti forensi appropriati, necessari all'analisi sul sistema.
L'MFT è organizzata in una serie di record, ognuno con un suo numero (identificativo del file).
Ogni record ha una lunghezza standard di 1024 byte, così che risulta facile trovare l'entry di un particolare file nel MFT. Infatti basta moltiplicare il numero di record del file per 1024 e poi procedere verso un certo *File Offset* (FO) all'interno del file $MFT. Questo FO rappresenta il primo byte del record MFT del file.
In Windows NT e 2000, i record MFT iniziano con il byte `sequence FILE*`, mentre nelle altre versioni come Vista e 7 iniziano con `FILE0`.

$LogFile

Il $Logfile viene utilizzato dal File System come una sorta di log delle transazioni e viene utilizzato per garantire stabilità al sistema e per permettere il ripristino in caso di errori catastrofici. In pratica vengono memorizzate le operazioni come complete e incomplete a seconda se debbano essere rifatte o annullate. Il $LogFile contiene riferimenti ai record MFT e buffer di indici (essenzialmente cartella con le entry in NTFS). I record MFT (che mostrano l'intestazione del record, informazioni standard su attributi e attributi di filename) possono essere individuati all'interno del $LogFile attraverso le stringhe di intestazione FILE* o FILE0.

Anche gli indici di buffer possono essere individuati attraverso la stringa di intestazione INDX. Inoltre, all'interno del $LogFile è possibile trovare anche le stringhe di intestazione per i file di collegamento, che permettono di recuperare delle informazioni relative ad un file o ad una cartella che è stata definitivamente cancellata.

$Volume

Il file $Volume è un altro file interno al NTFS, contiene solo attributi ed è presente nella MFT. In pratica contiene attributi come il nome del volume (l'etichetta).

Data Access Control

NTFS è più sicuro di FAT, come dimostra il fatto che è presente una Access Control List (ACL) che disciplina l'accesso in lettura, scrittura ed esecuzione dei file e delle cartelle di Windows.
Ci sono descrittori di sicurezza memorizzati nel file $Secure, che specificano informazioni di proprietà ed accesso ai file.

Flussi di file

NTFS memorizza le informazioni contenute nei file o delle cartelle all'interno della Master File Table permettendo la creazione di più di un attributo dati per ogni singolo file. In questo scenario, abbiamo dunque un flusso di dati principale che tradizionalmente è considerato come il contenuto del file ed in più, può essere affiancato da uno o più flussi di dati alternativi. Questi flussi di dati alternativi detti ADS (Alternate Data Streams), in origine vennero creati da Microsoft per permettere una sorta di compatibilità tra il sistema Windows e il sistema Macintosh.
ADS può essere utilizzato però, non solo per mantenere informazioni su alcuni registri, ma anche per nascondere dati. Un file mantenuto nell'ADS di un altro file, non ha un'icona propria e non viene visualizzato dall'utente di Windows, ma tuttavia quest'ultimo può comunque eseguire il file direttamente dall'ADS senza il bisogno di estrarlo dalla posizione nascosta. Come esempio riportiamo molte semplici stringhe di linee di comando, utilizzate per inserire un file (un eseguibile, in questo caso) nel ADS di un altro file ed eseguire il file segreto da quella posizione. Il risultato di questa operazione è l'esecuzione di rootkit.exe, anche se il file rootkit.exe originale è stato eliminato in Windows Explorer.

```
type rootkit.exe > c:\windows\notepad.exe:rootkit.exe
start c:\windows\notepad.exe:rootkit.exe
```

Per questo motivo i file dannosi (come questo rootkit segreto inserito in un ADS da un hacker) sono ovviamente di interesse per un esaminatore.

Compressione dei dati

Il File System NTFS di Windows fornisce agli utenti la possibilità di comprimere i dati sul disco, in modo da risparmiare spazio. Quando i file, cartelle o addirittura interi volumi NTFS sono compressi, Windows sostituisce i dati ridondanti con un segnaposto che occupa meno spazio. La decompressione viene poi gestita "a volo" dal sistema operativo, quando una particolare porzione di dati è accessibile da parte dell'utente. Oggetti dati che sono stati compressi portano un attributo di "C" (e sono spesso visti in blu) quando vengono visualizzati in Windows Explorer.
NTFS usa anche gli Sparse File: in pratica sono file salva spazio, cioè viene allocato sullo spazio disco solo la porzione di dati del file richiesta dall'applicazione, mentre quella che non è richiesta viene memorizzata in uno spazio non allocato. Quando il file viene letto, le porzioni di codice del file specificato vengono lette da un'applicazione, e le porzioni non specificate sono semplicemente sostituite con degli zeri in memoria. Questo processo permette di allocare meno spazio sul disco per file molto grandi, conservando quindi le risorse di memorizzazione. Nell'analisi forense, attraverso degli strumenti precisi e analizzando i dischi, questi sparse file vengono facilmente distinti dagli altri file, comprendendo così che c'è stata una compressione di dati su disco.

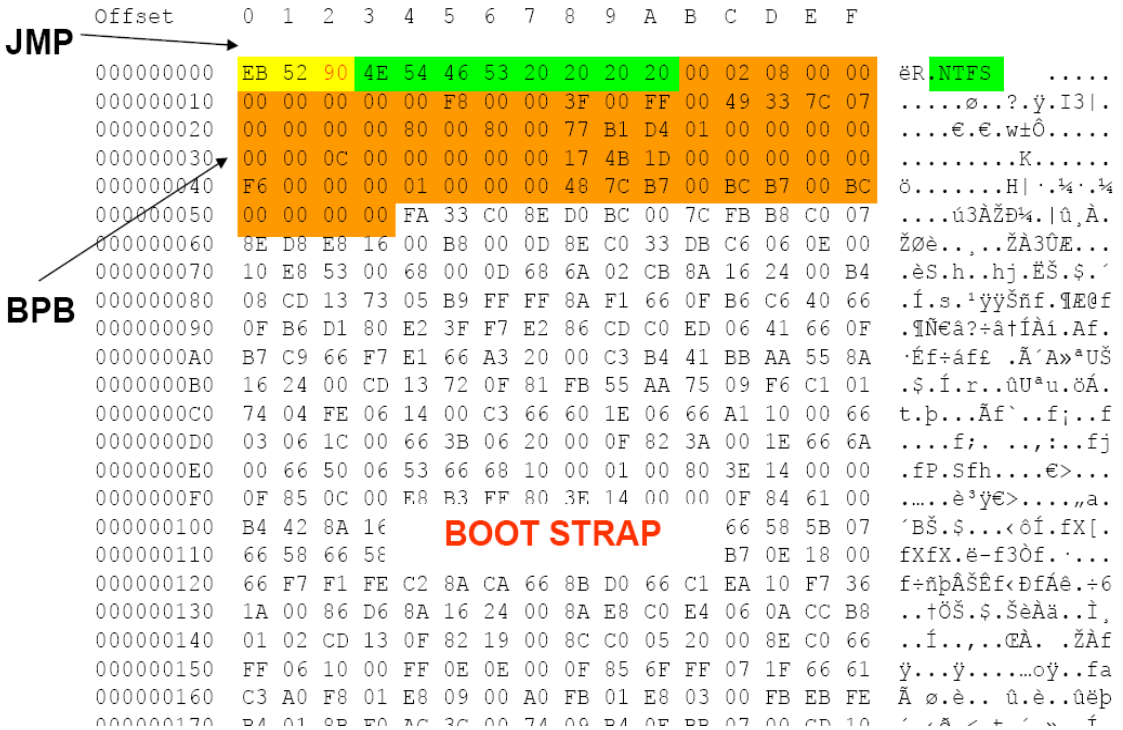
Reparse Point

Essenzialmente sono file o cartelle che fungono da link, ma contengono informazioni aggiuntive su oggetti e posizioni ai quali puntano. Queste informazioni permettono al File System di trattare i dati in modi differenti.
Questi Reparse Point sono utilizzati come:

- hard link (un file con più nomi)
- symbolic link (file per file)
- punti di giunzione (cartella per cartella)
- punti di mount (cartella di volume)

Partition Boot Sector

È un file ma è l'unico che ha una posizione fissa nel volume: il settore 0.
Il boot sector è una regione di spazio di un supporto magnetico o di una partizione. Ogni partizione ha, infatti un boot sector, che viene caricato ed eseguito durante il processo di Boot Strap del pc. Al suo interno, contiene un piccolo programma che carica il sistema operativo in memoria e trasferisce il controllo della macchina ad esso.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000000000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ëR.NTFS .....
000000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	49	33	7C	07	.....ø..?.ÿ.I3|.
000000020	00	00	00	00	80	00	80	00	77	B1	D4	01	00	00	00	00	....€.€.w±Ô.....
000000030	00	00	0C	00	00	00	00	00	17	4B	1D	00	00	00	00	00	.........K.....
000000040	F6	00	00	00	01	00	00	00	48	7C	B7	00	BC	B7	00	BC	ö.......H|·.¼·.¼
000000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	B8	C0	07	....ú3ÀŽÐ¼.|û¸À.
000000060	8E	D8	E8	16	00	B8	00	0D	8E	C0	33	DB	C6	06	0E	00	ŽØè..¸..ŽÀ3ÛÆ...
000000070	10	E8	53	00	68	00	0D	68	6A	02	CB	8A	16	24	00	B4	.èS.h..hj.ËŠ.$.´
000000080	08	CD	13	73	05	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	.Í.s.¹ÿÿŠñf.¶Æ@f
000000090	0F	B6	D1	80	E2	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	.¶Ñ€â?÷â†ÍÀí.Af.
0000000A0	B7	C9	66	F7	E1	66	A3	20	00	C3	B4	41	BB	AA	55	8A	·Éf÷áf£ .Ã´A»ªUŠ
0000000B0	16	24	00	CD	13	72	0F	81	FB	55	AA	75	09	F6	C1	01	.$.Í.r..ûUªu.öÁ.
0000000C0	74	04	FE	06	14	00	C3	66	60	1E	06	66	A1	10	00	66	t.þ...Ãf`..f¡..f
0000000D0	03	06	1C	00	66	3B	06	20	00	0F	82	3A	00	1E	66	6A	....f;. ..‚:..fj
0000000E0	00	66	50	06	53	66	68	10	00	01	00	80	3E	14	00	00	.fP.Sfh....€>...
0000000F0	0F	85	0C	00	E8	B3	FF	80	3E	14	00	00	0F	84	61	00	.…..è³ÿ€>....„a.
000000100	B4	42	8A	16									66	58	5B	07	´BŠ.$...‹ôÍ.fX[.
000000110	66	58	66	58									B7	0E	18	00	fXfX.ë-f3Òf.·...
000000120	66	F7	F1	FE	C2	8A	CA	66	8B	D0	66	C1	EA	10	F7	36	f÷ñþÂŠÊf‹ÐfÁê.÷6
000000130	1A	00	86	D6	8A	16	24	00	8A	E8	C0	E4	06	0A	CC	B8	..†ÖŠ.$.ŠèÀä..Ì¸
000000140	01	02	CD	13	0F	82	19	00	8C	C0	05	20	00	8E	C0	66	..Í..‚..ŒÀ. .ŽÀf
000000150	FF	06	10	00	FF	0E	0E	00	0F	85	6F	FF	07	1F	66	61	ÿ...ÿ.....…oÿ..fa
000000160	C3	A0	F8	01	E8	09	00	A0	FB	01	E8	03	00	FB	EB	FE	Ã ø.è.. û.è..ûëþ
000000170	B4	01	8B	F0	AC	3C	00	74	09	B4	0E	BB	07	00	CD	10	´.‹ð¬<.t.´.»..Í.

JMP = Salta istruzione. Questa istruzione verrà eseguita e salterà oltre il resto dell'intestazione (non-eseguibile) se la partizione è avviabile
BPB = BIOS Parameter Block. Il suo inizio è dato da BMP, Bytes per settore, il cui valore è solitamente 512.
Boot Strap = insieme delle operazioni che vengono eseguite durante la fase di avvio del computer: dall'accensione fino al caricamento vero e proprio del sistema operativo .

2.2 Master File Table (MFT) di NTFS

In questo paragrafo illustriamo la MFT del File System NTFS, ovvero andremo a mostrare alcuni file che fanno parte della MFT, individuandone anche attributi e punti di interesse per gli esaminatori forensi.

$MFT record base

MFT è la master file table di NTFS, ha una propria struttura dati e può essere analizzata sfruttando appositi tool, oppure anche a mano. Ad esempio analizzando due byte localizzati nel record ad offset 22 è possibile conoscere lo status del file.

Flag	Significato
00 00	File cancellato
01 00	File allocato
02 00	Directory cancellata
03 00	Directory allocata

Il record MFT è composto anche di altri tipi di attributi che hanno una specifica funzione e struttura. Ogni attributo possiede un proprio header (intestazione) che identifica il tipo di attributo e la taglia.

Gli attributi si dividono in:

- residenti (esistono all'interno di un dato record MFT);
- non residenti (esistono al di fuori del record, posizionati sul disco e solo referenziati nel record).

Standard Information Attribute (SIA)

SIA è un attributo residente identificato nel record dalla sequenza esadecimale \x10\x00\x00\x00. Da questo attributo deriva il data-time per i file o cartelle visualizzato e interpretato da Windows e da determinati tool forensi. Inizia all'offset 24 all'interno dello stream degli attributi (ad esempio i 23 byte dopo \x10) e nei successivi 32 byte ci sono informazioni riguardanti la creazione dei file, l'ultima modifica, l'entry del MFT modificato e l'ultimo accesso al data-file nel formato FILETIME.

Filename Attribute (FNA)

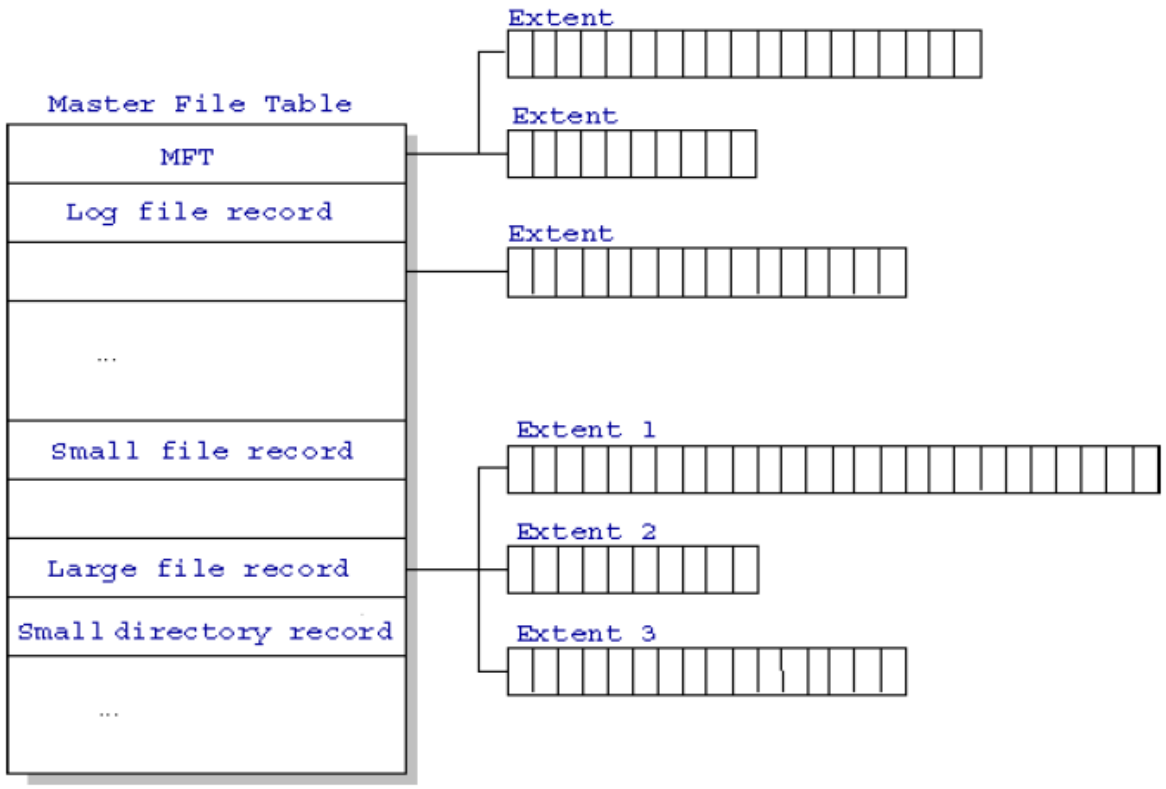
FNA è un attributo residente identificato nel record dalla sequenza esadecimale \x30\x00\x00\x00. Tra i dati contenuti nell'attributo per un particolare file ci sono referenze alla sua cartella genitore, alla taglia logica e fisica, al suo file name Unicode, e un set di quattro 64-bit data-time come per SIA.
Inizia dall'offset 32 e nei successivi 32 byte ci sono informazioni riguardanti la creazione dei file, l'ultima modifica, l'entry del MFT modificato, l'ultimo accesso al data-file con ogni campo da 8 byte.

A differenza di SIA, per cui data e tempo sono aggiornati ogni volta che l'utente accede o modifica il file, in FNA data e tempo sono settati quando il file referenziato è creato sul volume e generalmente non è aggiornato tramite l'uso normale del sistema.

Data attribute

Gli attributi di un record MFT sono molto importanti per un esaminatore, perché contengono o il dato attuale se il dato è residente oppure un puntatore su dove il dato risiede sul disco.
Un attributo residente contiene il dato attuale del file referenziato dal record MFT e questo succede quando il dato è di piccola taglia (massimo 600 byte) come un piccolo file di testo o un cookie. Se invece il file è di grandi dimensioni, l'MFT contiene una lista di cluster assegnati al file.

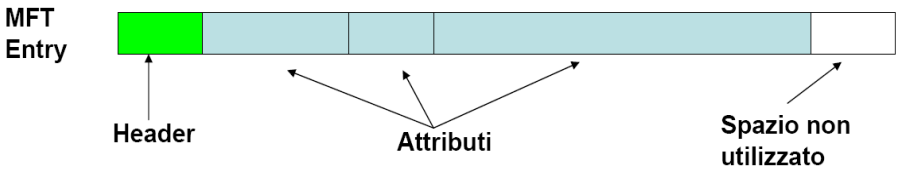
MFT



MFT contiene le informazioni su tutti i file e le directory. Ogni file o directory ha almeno una "riga"nella tabella. Ogni riga è in genere (cioè in tutti i sistemi operativi Microsoft) formata da 1024 byte, ma la sua dimensione esatta è definita nel boot sector.

Anche MFT è un file per cui contiene una riga (la prima), per riferirsi a se stesso. L'implementazione di NTFS per Microsoft prevede di partire con un MFT il più piccolo possibile ed ingrandirlo solo quando è necessario. Il boot sector specifica dove inizia l'MFT ma solo leggendo questa riga è possibile determinare dove "continua".

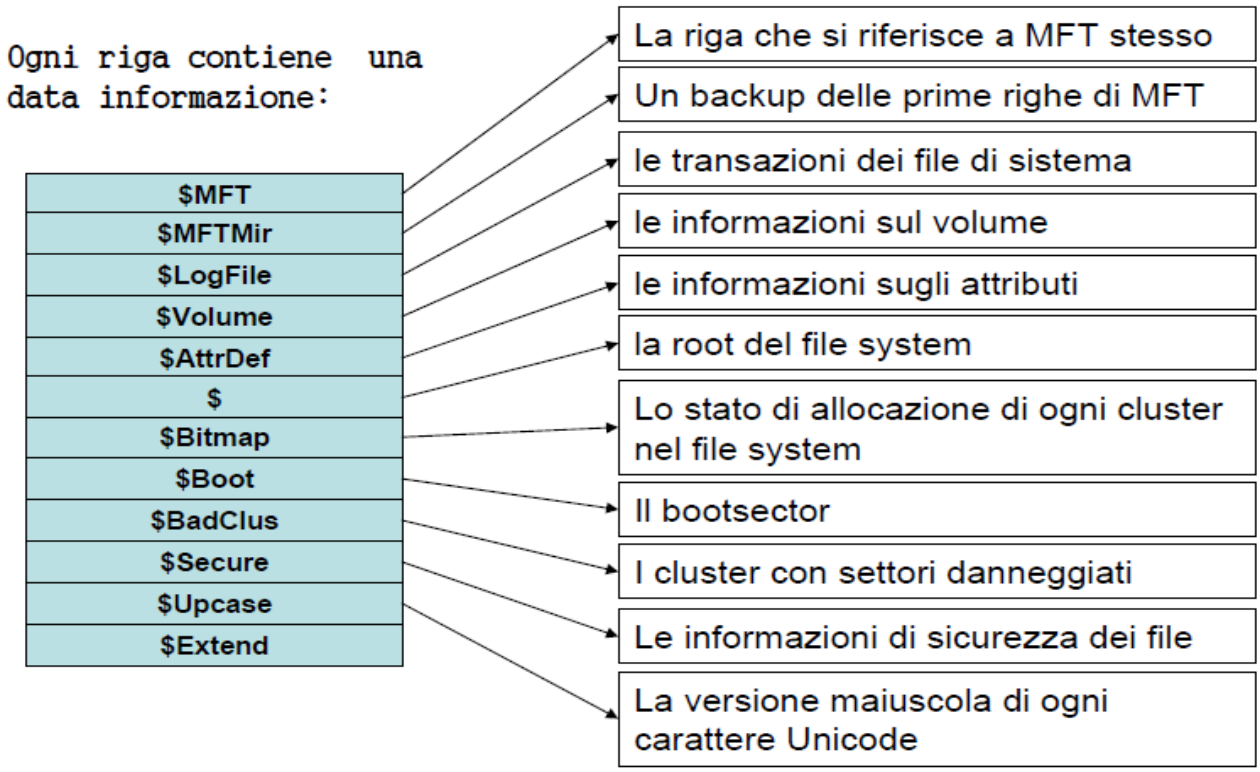
MFT entry



Ogni MFT Entry inizia con la sigla standard "FILE", oppure "BAAD" in caso di problemi.
Sono presenti inoltre dei campi flag che identificano che l'entry è usato e se è una directory.
Se per gli attributi di un file non sono sufficienti 1024 byte possono essere usate più righe. In questi casi la riga principale è chiamata "base entry" e ogni riga figlia contiene l'indirizzo della riga base all'interno di uno dei propri campi fissi.

File System Metadata Files

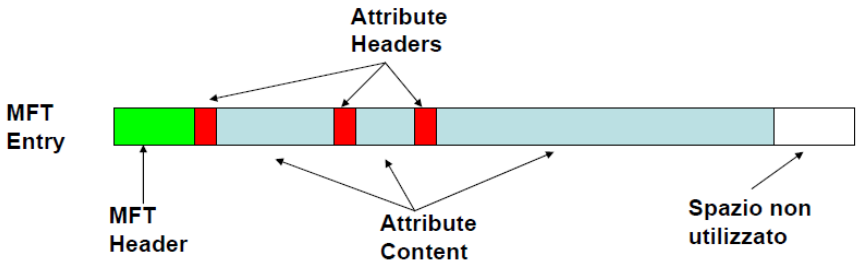
Poiché tutto in NTFS è considerato un file ci devono essere dei file contenenti le informazioni di sistema. Microsoft riserva le prime 16 righe a questi file di sistema ed i loro nomi iniziano tutti per $ e la prima lettera è maiuscola.



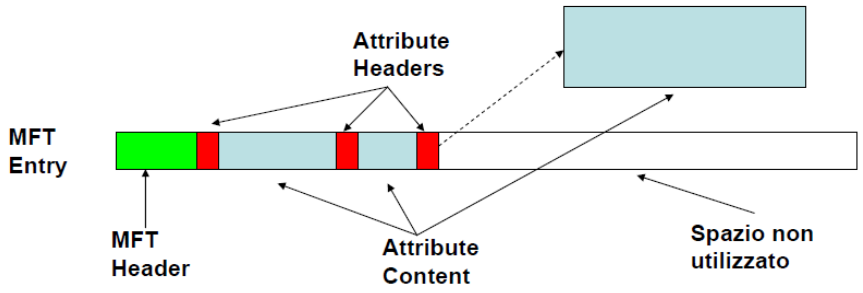
Attributi

Ogni entry può contenere attributi di vario tipo, ognuno con la sua diversa struttura ed ognuno di essi è formato da due parti: un'*intestazione generica* e standard per tutti gli attributi e un *contenuto specifico* per ogni attributo.

Attributi nelle MFT entry



L'intestazione (Header) specifica il tipo di attributo, la sua dimensione e il suo nome. Il contenuto (content) di un attributo può avere ogni formato e dimensione.
NTFS definisce 2 "luoghi" dove un attributo può essere memorizzato e in questi casi l'attributo prende il nome di *resident* o *non-resident*.



Un attributo *resident* è contenuto completamente nell'entry. Un attributo *non-resident* è contenuto in un cluster esterno il cui indirizzo è contenuto nell'header. I **cluster** sono insiemi di settori consecutivi il cui numero è una potenza di 2.

Tipi di attributi standard

16	$STANDARD_INFORMATION	Ultimo accesso, tempo di creazione e di modifica, proprietario e security ID
32	$ATTRIBUTE_LIST	Lista degli altri attributi
48	$FILE_NAME	Nome del file e i tempi di creazione modifica e ultimo accesso
64	$VOLUME_VERSION	Informazioni sul volume (esiste solo nella versione 1.2, Windows NT)
64	$OBJECT_ID	Un identificativo univoco a 16-byte (ver. 3.0+)
80	$SECURITY_DESCRIPTOR	Il controllo di accesso
96	$VOLUME_NAME	Nome del volume
112	$VOLUME_INFORMATION	FileSystem versione e altri flag
128	$DATA	Il contenuto del file
144	$INDEX_ROOT	Il nodo radice di un albero di indici
160	$INDEX_ALLOCATION	I nodi dell'albero
176	$BITMAP	Una mappa di bit per $MFT e per gli indici
192	$SYMBOLIC_LINK	Informazioni sui link software

- Ogni entry MFT ha come attributi almeno $FILE_NAME e $STANDARD_INFORMATION. Entrambi questi attributi sono sempre residenti.
- Ogni file ha un attributo $DATA
- Ogni directory ha un attributo $INDEX_ROOT, se la directory è grande vengono usati anche $INDEX_ALLOCATION e $BITMAP
- Lo stato di allocazione dei cluster è definita dentro $BITMAP il cui campo $DATA contiene una sequenza di bit corrispondenti ognuno al relativo cluster; se il bit vale 0 il cluster non è allocato, se vale 1 è allocato.

Base MFT Entries

Un file può avere 65536 attributi per cui può essere stipato in più entry e quando questo accade, l'entry "originaria" prende il nome di base MFT entry e l'entry "non-base" mantiene l'indirizzo della base entry in uno dei suoi campi. Inoltre le Non-Base entry non hanno un attributo $FILE_NAME e nemmeno $STANDARD_INFORMATION.

Sparse Attribute

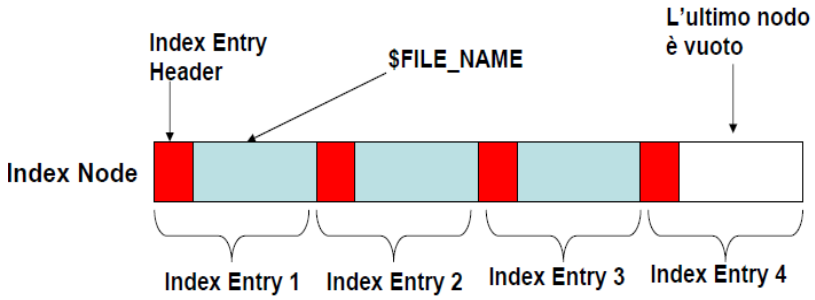
NTFS può risparmiare spazio su disco salvando parte dei $DATA non residenti come "sparse", in questo caso un cluster che contiene solo 0 non viene scritto sul disco. Una "sparse run" contiene solo la dimensione in cluster ma non l'inizio e contiene inoltre un flag per identificarsi come sparse.

Compressed Attribute

NTFS permette di memorizzare l'attributo data non-residente in maniera compressa a livello di File System. L'informazione sul fatto che quel file è compresso si trova sia in $STANDARD_INFORMATION che in $FILE_NAME. Prima di comprimere un attributo i dati vengono spezzati in "compression unit".
Possono presentarsi 3 casi per ogni unità:

- Tutti i cluster sono zero.
- L'unità compressa non contiene meno cluster dell'originale.
- L'unità compressa contiene meno dati dell'originale. In questo caso l'unità compressa viene memorizzata e viene aggiunto uno "sparse run" per rendere la lunghezza del file uguale alla lunghezza originaria.

Indici



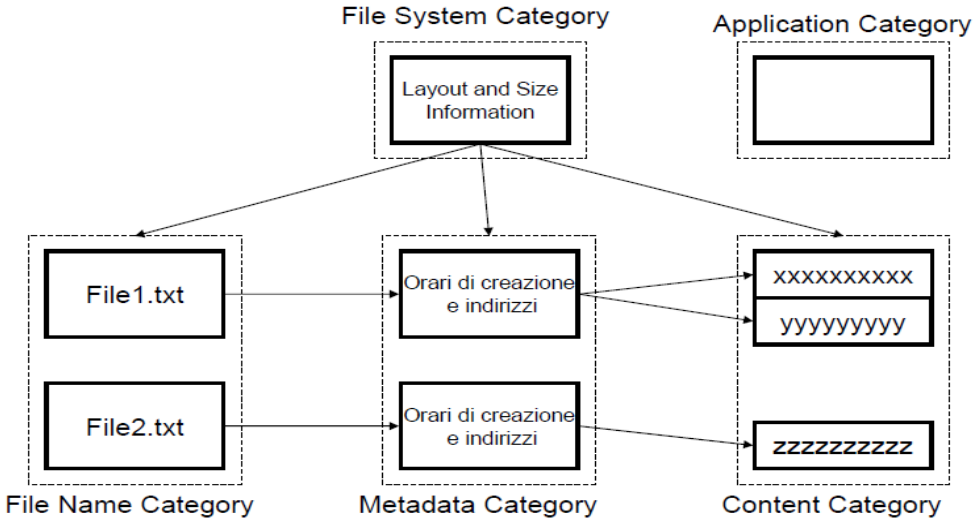
NTFS utilizza delle strutture indicizzate in vari casi. Il caso più comune è quello di una directory contenente attributi $FILE_NAME.
Gli indici in NTFS vengono memorizzati in due tipi di attributi:
$INDEX_ROOT –sempre residente.
$INDEX_ALLOCATION –non residente e può contenere più index record.

Eliminazione file in NTFS

Quando un file viene eliminato dall'NTFS il sistema esegue diverse operazioni, ma nell'ambito forense, i comportamenti che interessano gli esaminatori forensi sono:

- L'entry del file eliminato viene rimossa dall'indice del genitore e i metadati della cartella genitore sono aggiornati. È possibile anche che i metadati siano aggiornati quando si vuole andare a cancellare un file, per esempio cliccando col tasto destro sul file.
- I due byte a partire dall'offset 22 passano da allocato (\x01\x00) a non allocato (\x00\x00).
- Le posizioni appropriate in $Bitmap (entry che indica lo stato di allocazione di ogni cluster nel File System) sono modificate per mostrare che sia lo spazio occupato dal record MFT che lo spazio precedentemente occupato dal file stesso è ora non allocato e pronto per il riutilizzo.

2.3 Categorie di NTFS



Suddivisione in categorie del File System Windows

Come si vede dalla figura, il File System di Windows viene suddiviso in quattro categorie, ognuna con file e attributi diversi. Di seguito andremo ad esplorare ogni singola categoria, analizzandone file e attributi appartenenti.

File System Category

Vediamo in dettaglio quali sono i file che fanno parte della categoria File System e quali sono i loro attributi. La categoria File System contiene informazioni di layout e dimensioni dei settori del disco in analisi.

$MFT

Attributi:
$STANDARD_INFORMATION →Ultimo accesso, tempo di creazione e di modifica, proprietario e security ID.
$FILE_NAME →Nome del file e i tempi di creazione modifica e ultimo accesso.
$DATA → contiene la lista dei cluster su cui si trova MFT.

$MFTMirr

Funge da copia di $MFT, nel caso in cui non si possa disporre di $MFT viene usato $MFTMirr. Come una copia esatta, ha gli stessi attributi di $MFT.

$Boot

Attributi:
$STANDARD_INFORMATION →Ultimo accesso, tempo di creazione e di modifica, proprietario e security ID.
$FILE_NAME →Nome del file e i tempi di creazione modifica e ultimo accesso.

$SECURITY_DESCRIPTOR →controllo di accesso
$DATA →contenuto del file

In particolare, $Boot contiene la dimensione dei cluster, il numero di settori del File System ecc.

$Volume

Attributi:
$STANDARD_INFORMATION → ultimo accesso, tempo di creazione e di modifica, proprietario e security ID.
$FILE_NAME → nome del file e i tempi di creazione modifica e ultimo accesso.
$OBJECT_ID → identificativo univoco a 16-byte (ver. 3.0+)
$SECURITY_DESCRIPTOR → controllo di accesso
$VOLUME_NAME → nome del volume
$VOLUME_INFORMATION → versione File System e altri flag
$DATA → contenuto del file

$AttrDef

Attributi:
$STANDARD_INFORMATION → ultimo accesso, tempo di creazione e di modifica, proprietario e security ID.
$FILE_NAME → nome del file e i tempi di creazione modifica e ultimo accesso.
$SECURITY_DESCRIPTOR → controllo di accesso
$DATA → contenuto del file
$AttrDef→ contiene il nome e il type ID di ogni attributo. In questo modo è possibile definire dei nuovi attributi.

Considerazioni che possono interessare l'analisi forense

Nella categoria "File System" non dovrebbero esserci dati utente, ma in teoria è possibile inserire dei dati in settori non utilizzati dalle specifiche NTFS ed ecco quindi perché anche questa parte può interessare l'indagine forense.

Content Category

Siccome non tutti i dati di NTFS sono contenuti nelle entry MFT, ma alcuni sono allocati su cluster esterni, in questa categoria andremo a vedere quali sono i file ed i loro attributi presenti in questi cluster esterni.

Cluster

- I cluster sono insiemi di settori consecutivi il cui numero è una potenza di 2.
- Se la dimensione del volume non è multipla della dimensione del cluster, Microsoft esclude gli ultimi settori.

$Bitmap

Lo stato di allocazione dei cluster è definito dentro $Bitmap il cui campo $Data contiene una sequenza di bit corrispondenti ognuno al relativo cluster; se il bit vale 0 il cluster non è allocato, se vale 1 è allocato.
Attributi:
$STANDARD_INFORMATION
$FILE_NAME
$DATA

$BadClus

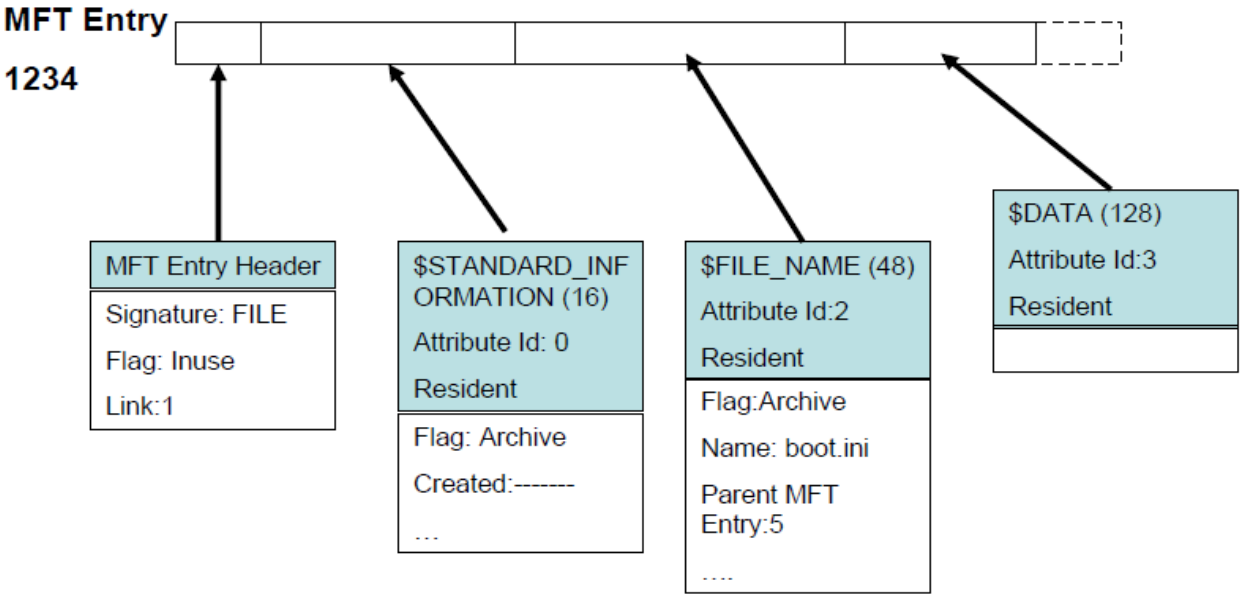
L'attributo $Data (chamato $Bad) è un file sparse e tiene traccia dei cluster danneggiati del File System. La dimensione riportata da $Bad è equivalente alla dimensione del File System, ma non ha cluster assegnati (si aggiungono quando ne viene trovato uno danneggiato).
Attributi:
$STANDARD_INFORMATION
$FILE_NAME
$DATA
$DATA → con NOME: $Bad e non residente.

Considerazioni che possono interessare l'analisi forense

In alcuni casi possono esserci settori non "clusterizzati" alla fine del volume e questi possono contenere dei dati nascosti.
In effetti è possibile segnare come "Bad" dei settori in cui nascondere dei dati, ma è molto rischioso poiché l'hd potrebbe rimappare i settori che vede come danneggiati con settori "di scorta"; recuperare questi settori è difficile e dipende molto dalle specifiche del disco.

Metadata Category

Include i dati che descrivono file e cartelle. Tutti i Metadata sono inclusi negli attributi



$STANDARD_INFORMATION

Esiste in tutti i file e le cartelle e contiene i metadata principali.
Contenuto:

- 4 Date a 64bit (in nanosecondi dal 1/1/1601)
- Creation Time
- Modified Time
- MFT Modified Time
- Accessed Time
- Flag per le proprietà generali del file
- Dalla versione 3.0+ sono stati aggiunti 4 nuovi campi per gestire la sicurezza

$FILE_NAME

Ogni file o directory ha un attributo $FILE_NAME al proprio interno e un attributo $FILE_NAME che lo riguarda nell'indice della sua directory parent.
Contenuto:

- Il nome del file codificato in UTF-16 Unicode (il nome deve appartenere ad uno specifico name space)
- Il riferimento alla directory parent
- 4 Date come in $STANDARD_INFORMATION
- La dimensione del file
- Un flag per indicare alcune caratteristiche del file o della directory

$DATA

Si possono trovare anche più attributi $Data in un file, il primo è senza nome mentre gli altri devono averne uno.
Questi $DATA in più sono molto comodi per aggiungere informazioni nascoste, dato che è possibile farlo anche da prompt (ATTENZIONE: se il file viene copiato su un File System diverso l'informazione si perde):
C:/> echo "Hello"> file.txt : foo

$ATTRIBUTE_LIST

Viene usato per quelle entry che richiedono più attributi di quanti ne entrino nell'entry stessa.
Contenuto:
Contiene la lista di tutti gli attributi escluso se stesso, ogni nodo della lista contiene il "type id" dell'attributo e l'entry MFT dove si trova l'attributo.

$SECURITY_DESCRIPTOR

E'utilizzato solo con Windows NT mentre con la versione 3.0 la sicurezza viene passata al file $Secure, poiché molti file hanno la stessa impostazione di sicurezza è più conveniente inserire il tutto in un solo file.

Contenuto: ogni file contiene un identificatore Security ID utilizzato come indice in **$Secure** dove si trova il corretto descrittore.

$Secure

Contiene due indici $SDH e $SII e un attributo $DATA ($SDS) che contiene il descrittore.
$SII è ordinato in base ai Security ID dei singoli file.
$SDH è un Hash del descrittore che permette di non avere due descrittori uguali.

Considerazioni che possono interessare l'analisi forense

- Ogni entry può avere più $DATA
- Si può usare la parte inutilizzata di un'entry per nascondere dati, con il rischio che questi vengano cancellati.
- E'possibile risalire a nome e path di file cancellati.
- La presenza di dati non residenti o di attributi sparsi su più entry complica un pò le cose.

File Name Category

Ci serve per collegare un file ad un nome.
Come abbiamo visto NTFS usa gli indici per memorizzare i nomi dei file nelle cartelle, per questo ci serviranno attributi quali $INDEX_ROOT e $INDEX_ALLOCATION

Directory

Ogni directory ha un'entry in MFT con un flag che la identifica come tale.
Un campo index in una directory contiene un riferimento all'indirizzo del file e un (o più) attributo $FILE_NAME.
Agli attributi $INDEX_ROOT, $INDEX_ALLOCATION, $BITMAP è assegnato il nome $I30.
Ogni volta che si effettua la modifica di un nome questi campi vengono riorganizzati questo può portare alla presenza di campi non validi in zone non allocate ma che contengono informazioni sul file.

Root Directory

La Root Directory di NTFS è sempre allocata come entry 5 in MFT con nome ".", tutti i file di sistema si trovano nella root.

Link

NTFS permette di avere file con più nomi utilizzando gli hard link. Questi devono appartenere allo stesso volume del file principale e ne viene tenuta traccia nell'header dell'entry.

- Un file con hard link non può essere cancellato.
- Da NTFS 3.0+ è possibile linkare anche file esterni al volume (anche remoti) tramite reparse point.
- I Reparse point hanno dei flag che li distinguono e uno speciale attributo $REPARSE_POINT che contiene le informazioni sul target.
- NTFS ne tiene traccia in /$Extend/$Reparse.

Object identifiers

NTFS 3.0+ permette di indirizzare un file o una directory anche attraverso un identificativo univoco a 128 bit assegnato ad ogni oggetto dal S.O.
Un file o una directory a cui viene assegnato un ID ha un attributo $OBJECT_ID, che contiene l'ID e alcune informazioni su dove l'oggetto è stato creato.
/$Extend/$ObjectID è un indice contenente un nodo per ogni object ID assegnato contenente il riferimento all'oggetto stesso.

Considerazioni che possono interessare l'analisi forense

In NTFS a causa della riallocazione dei nomi, un file name non allocato può essere fuorviante poiché non è detto che appartenga ad un file cancellato.
L'allocazione del file name di un file cancellato può essere molto utile, per cui per trovare un file cancellato possiamo analizzare le entry MFT e gli spazi non allocati di una directory index.

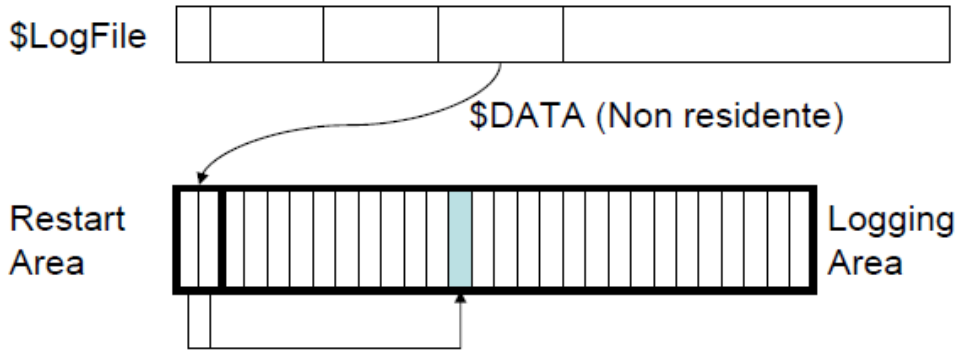
Application Category

NTFS permette un'elevata integrazione con caratteristiche richieste a livello di applicazione, che non sono direttamente necessarie per il File System.
La più importante è:

Logging –File System Journaling

Logging –File System Journaling

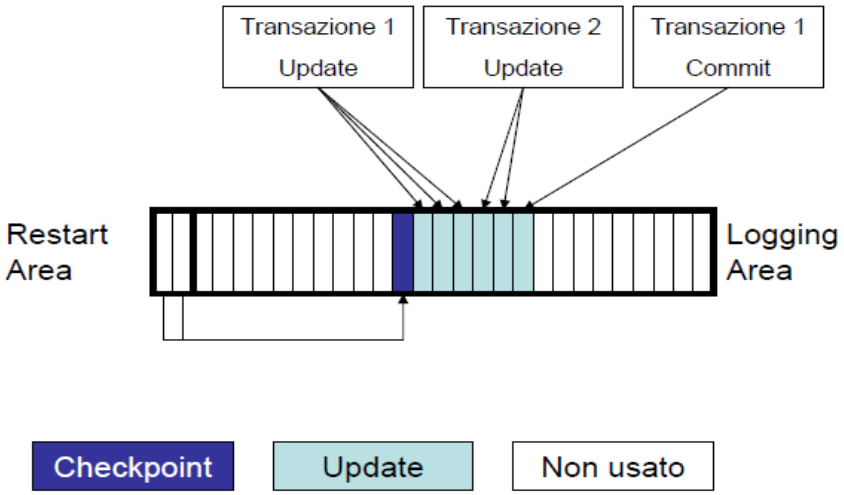
Per aumentare l'affidabilità del File System, Microsoft aggiunge il concetto di journal a NTFS, in questo modo diventa più facile recuperare il sistema in caso di crash.
Il log $LogFile ha due sezioni "restart" e "logging".



L'area "restart" contiene due copie di una struttura dati che indica al sistema operativo quale transazione deve essere esaminata puntando all'area "logging".
Quest'area "logging" contiene una serie di record e ogni record contiene un logical sequence number (LSN) di 64 bit. Inoltre la struttura dell'area è "ciclica".

Microsoft descrive 2 possibili tipi di record:

- **Update** che descrive la transazione prima che avvenga, oltre a LSN contiene due campi principali: l'operazione da eseguire, e come fare l' "undo" dell'operazione. Eseguita l'operazione viene aggiunto un altro record update chiamato commit che indica che la transazione è eseguita.
- **Checkpoint** che indica da quale parte del log il sistema operativo deve partire per verificare il File System, Windows ne crea uno ogni 5 secondi e ne memorizza l'LSN nella restart area.



Change Journal

Il "change journal" è un file di log che tiene traccia di quando un file è modificato memorizzando le informazioni in /$Extend/$UserJrnl che contiene due attributi $DATA:

- Il primo chiamato $Max che contiene informazioni di base.
- Il secondo chiamato $J che contiene il log memorizzato in record di varie dimensioni.

Ogni record contiene il nome del file, la data di modifica e il tipo di modifica ed ha un Update Sequence Number (USN) a 64-bit.

Capitolo 3

Registry di Microsoft Windows e Data Remanence

Il Registro di Windows è una delle componenti essenziali degli attuali sistemi operativi Microsoft Windows ed è utile anche per verificare la problematica del Data Remanence, cioè la rappresentazione dei dati residui che restano anche dopo che sono stati fatti tentativi per rimuovere o cancellare dati. Infatti i sistemi operativi come Windows forniscono un sistema per cui un file non viene eliminato immediatamente quando l'utente ne richiede l'azione. Al contrario, il file viene spostato in una sorta di contenitore, per consentire all'utente di ripristinare facilmente un errore. Quindi attraverso il Registry di Windows verifichiamo se dopo l'eliminazione di un dato, esso è stato realmente eliminato o se è possibile ritrovarlo.
Il Registro di sistema di Windows esegue due attività critiche per il sistema operativo Windows: la prima è che funge da repository (deposito, una sorta di database per i dati) per le impostazioni del sistema operativo Windows e le applicazioni che sono installate sul sistema. La seconda è che funge da database della configurazione di tutto l'hardware installato. Il Registro di sistema è definito come segue:
Un database gerarchico centralizzato utilizzato in Microsoft Windows 98, Windows CE, Windows NT, utilizzato per memorizzare le informazioni necessarie a configurare il sistema per uno o più utenti, applicazioni e dispositivi hardware.
In questo lavoro sono discussi diversi elementi del Registro di Windows che potrebbero essere preziosi per un investigatore forense. In primo luogo è stata analizzata la struttura del Registro di Windows, così che vengono discussi elementi all'interno del registro di Windows che potrebbero essere di valore probatorio.

3.1 Registry di Windows sotto la lente d'ingrandimento

Il Registro di sistema contiene informazioni a cui il sistema operativo fa continuamente riferimento mentre viene utilizzato:

- profili utenti
- applicazioni installate
- impostazioni delle finestre
- proprietà per cartelle e icone delle applicazioni
- ecc…

Il sistema operativo Windows organizza il Registro logicamente in una serie di chiavi di root (radice) ed esistono strumenti come l'editor del Registro di Windows, che può essere utilizzato per visualizzare la struttura logica del Registro stesso.

Chiavi di root

Il sistema operativo Windows organizza il Registro logicamente in una serie di chiavi di root (radice) una in ogni file binario detto hive ed esistono strumenti come l'editor del Registro di Windows, che può essere utilizzato per visualizzare la struttura logica del Registro stesso.

Ci sono cinque chiavi di root logiche nel Registro di Windows, che sono:
1. HKEY_CLASSES_ROOT.
2. HKEY_CURRENT_USER.
3. HKEY_LOCAL_MACHINE.
4. HKEY_USERS.
5. HKEY_CURRENT_CONFIG.

HKEY_CLASSES_ROOT

È responsabile dei tipi di file e delle loro estensioni e come Windows deve gestire le varie tipologie di file, come aprirli e come stamparli. Inoltre sono presenti la definizione delle classi e le impostazioni di base dell'interfaccia utente.

HKEY_CURRENT_USER

È responsabile delle informazioni e della configurazione dell'utente Windows corrente, come il suo desktop, le impostazioni del tema e dei colori e le altre voci specifiche delle impostazioni utente. Vi è configurato anche le connessioni di rete e delle periferiche sempre per l'utente corrente.

HKEY_LOCAL_MACHINE

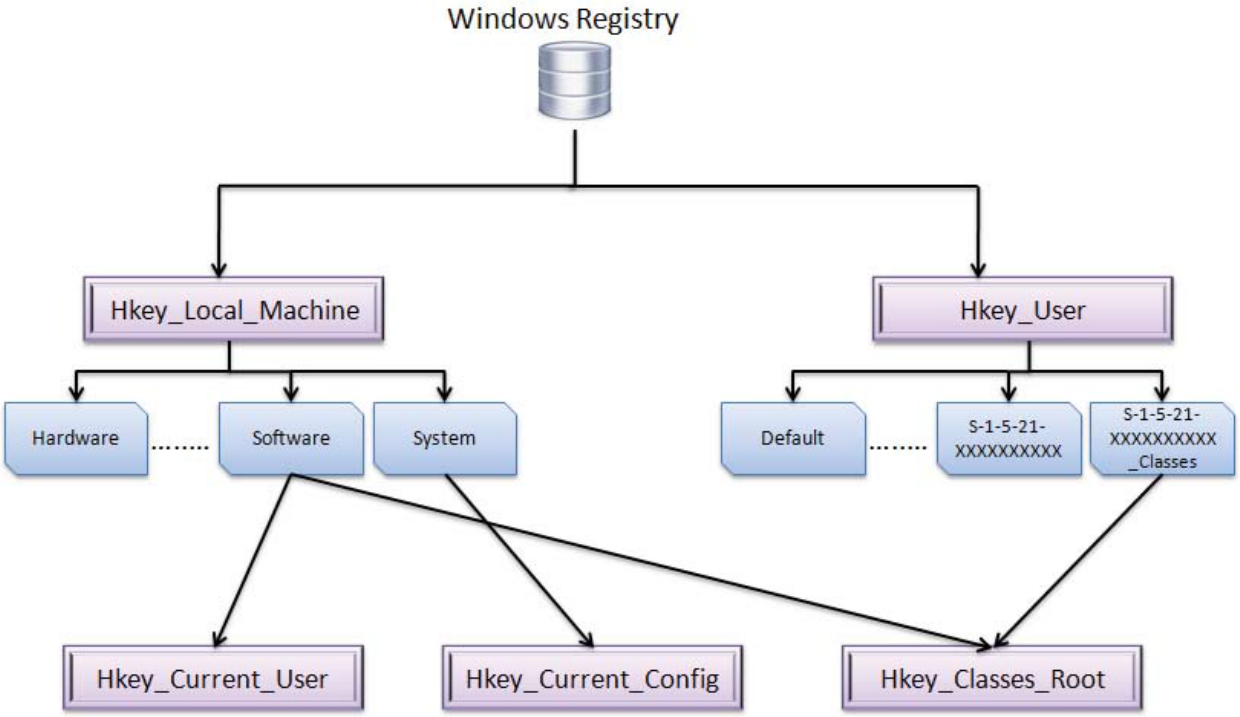
È responsabile di tutta la configurazione hardware della macchina e del sistema operativo, quindi informazioni sull'hardware quali la tastiera, il monitor, le stampanti. Oltre all'hardware vi sono configurate le voci per il software, quindi il software installato, i driver ed i servizi di Windows.

HKEY_USERS

Così come l'hive HKEY_CURRENT_USER contiene le informazioni sull'utente corrente, questo contiene le informazioni su tutti gli utenti definiti in Windows sui loro profili ed impostazioni.

HKEY_CURRENT_CONFIG

È responsabile delle informazioni e della configurazione hardware corrente.



In realtà sono solo due le chiavi che sono root: HKEY_LOCAL_MACHINE e HKEY_USERS. Queste due chiavi principali sono memorizzate sul disco rigido del sistema e non sono dati volatili in memoria principale. Le altre chiavi radici sono sottoinsiemi di queste due chiavi.

Ogni chiave del registro di sistema può contenere a sua volta delle sottochiavi e inoltre, chiavi e sottochiavi possiedono a loro volta, uno o più valori che determinano le impostazioni per il sistema che la chiave rappresenta.

I file hive sono stati modificati di volta in volta nelle varie versioni di Windows. Le modifiche sono state apportate perché ogni nuovo sistema operativo Windows ha nuove funzionalità. La seguente figura mostra le variazioni di file hive del Registro in diverse versioni del Sistema operativo Windows:

- In Windows 95 e Windows 98 il registro è memorizzato nei file USER.DAT e SYSTEM.DAT, posizionati nella cartella d'installazione di Windows (tipicamente `C:\WINDOWS`). Inoltre in Windows 98 sono stati introdotti anche i criteri di gruppo che permettono di ridurre o inibire l'accesso a specifiche chiavi del registro (Policy.pol).
- In Windows NT e nei sistemi operativi da esso derivati (2000, XP e Server 2003) il registro è composto da alcuni file posizionati in `%SystemRoot%\System32\Config` (tutti senza estensione): SAM, SECURITY, SOFTWARE, SYSTEM, DEFAULT. Inoltre, nella cartella di ogni profilo utente, è memorizzata una versione personalizzata di questi file: NTUSER.DAT. In XP troviamo anche USRCLASS.DAT (usato anche nelle versioni successive) che contiene delle impostazioni per applicazioni di ogni utente, che non possono essere copiate su altre macchine, se l'utente accede ad esse con un solo account.
- In Windows Vista e 7 il registro è composto, come in XP, da alcuni file posizionati in `%SystemRoot%\System32\Config` (tutti senza estensione): SAM, SECURITY, SOFTWARE, SYSTEM, DEFAULT, COMPONENTS, USRCLASS.DAT (l'unico con estensione). In più c'è BCD che contiene i dati di configurazione di avvio.

*Ci sono tre o più file hive che hanno nome NTUSER.DAT. Il primo è legato all'account dei servizi di rete, il secondo all'account dei servizi locali e il terzo all'account utente (ogni account utente ha i suoi file hive NTUSER.DAT).

Si dispone di una serie di file di supporto contenenti copie di backup dei relativi dati.

- I file di supporto per tutti gli hive, tranne che per HKEY_CURRENT_USER, si trovano nella cartella %SystemRoot%\System32\Config
- I file di supporto per HKEY_CURRENT_USER si trovano nella cartella %SystemRoot%\Profiles\nome_utente.
- Le estensioni dei nomi dei file in queste cartelle indicano il tipo di dati in essi contenuto.

Valori utilizzabili nel Registro di sistema

I valori ed i tipi per le chiavi del registro possono essere differenti.

REG_SZ

Indica un **valore stringa**, cioè composto da caratteri alfanumerici. Molto usato all'interno del registro per specificare nomi, settaggi e descrizioni delle impostazioni e dei programmi.

REG_MULTI_SZ

Indica un **valore multistringa**, cioè composto da più stringhe su più linee. Questi valori si possono modificare ma non creare.

REG_EXPAND_SZ

Indica un **valore stringa espandibile**, ovvero una variabile stringa usata per indicare path e percorsi di file e directory.

REG_BINARY

Indica un **valore binario**, ovvero costituito da due soli possibili valori, 0 e 1. Rappresentano spesso impostazioni hardware e software e sono di sovente convertiti nel corrispondente valore esadecimale.

REG_DWORD

Indica un **valore numerico (a 32 o 64 bit)**, usato per attivare o disattivare determinate impostazioni, ad esempio una chiave con valore 1 risulta attiva mentre con lo 0 è disattiva, anche se può prendere altri valori viene spesso usato come tipo booleano per indicare un valore attivo/disattivo.

3.2 Analisi forense dei registri di Windows 7

In questa parte del nostro lavoro, illustriamo con degli screenshot come si presenta il Registry di Windows. In particolare analizziamo il sistema attraverso le chiavi di registro principali e poi effettuiamo un'analisi più profonda andando ad analizzare le chiavi del Registry che riguardano i programmi di start up, le reti e i dispositivi connessi.

Analisi del sistema

Il registro di Windows contiene una grande quantità di informazioni sul sistema, come le impostazioni e la configurazione del sistema. C'è un certo numero di questi valori che sarebbero di interesse per un investigatore forense.

In primo luogo, il nome del computer è disponibile nella seguente chiave del Registro di sistema: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\NomeComputer

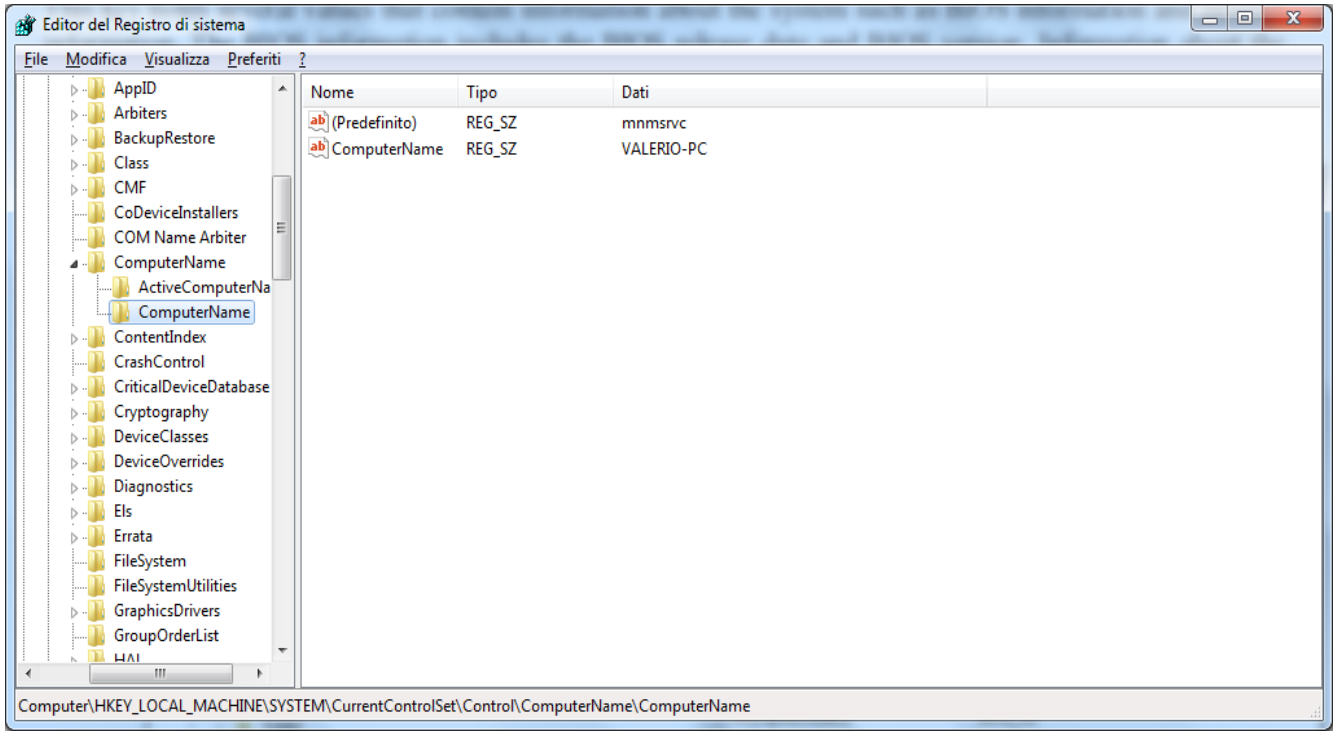


Figura 3.1 Chiave contenente il nome del computer

La sottochiave del registro che contiene le informazioni di sistema ha il seguente percorso: HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS
Questa chiave contiene diversi valori che contengono informazioni sul sistema, come le informazioni sul BIOS e le informazioni del prodotto. Le informazioni del BIOS includono la data di rilascio del BIOS e la versione del BIOS. Le informazioni sul BIOS includono il nome del prodotto del sistema e il product name. La Figura 3.2 mostra la sottochiave del registro che contiene le informazioni di sistema.

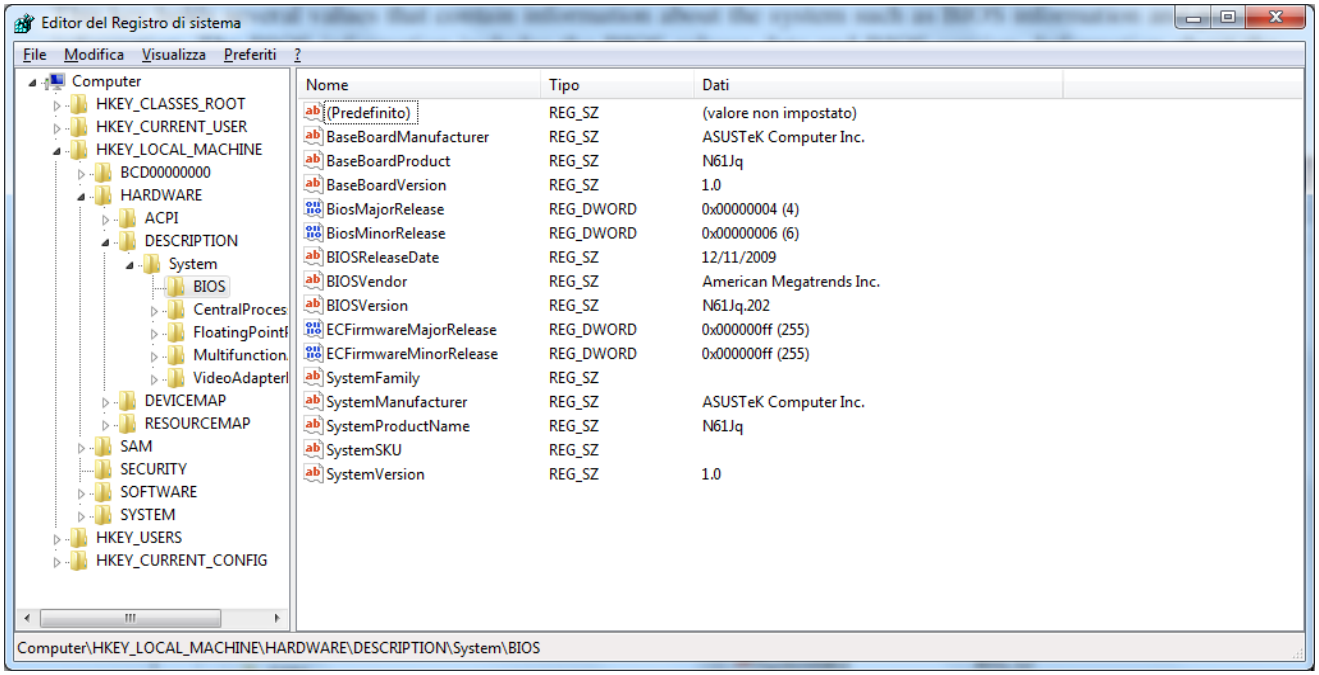


Figura 3.2 Sottochiave di registro contenente informazioni di sistema

Le informazioni sui processori del sistema sono memorizzate nelle seguenti chiavi del Registro di sistema:
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0

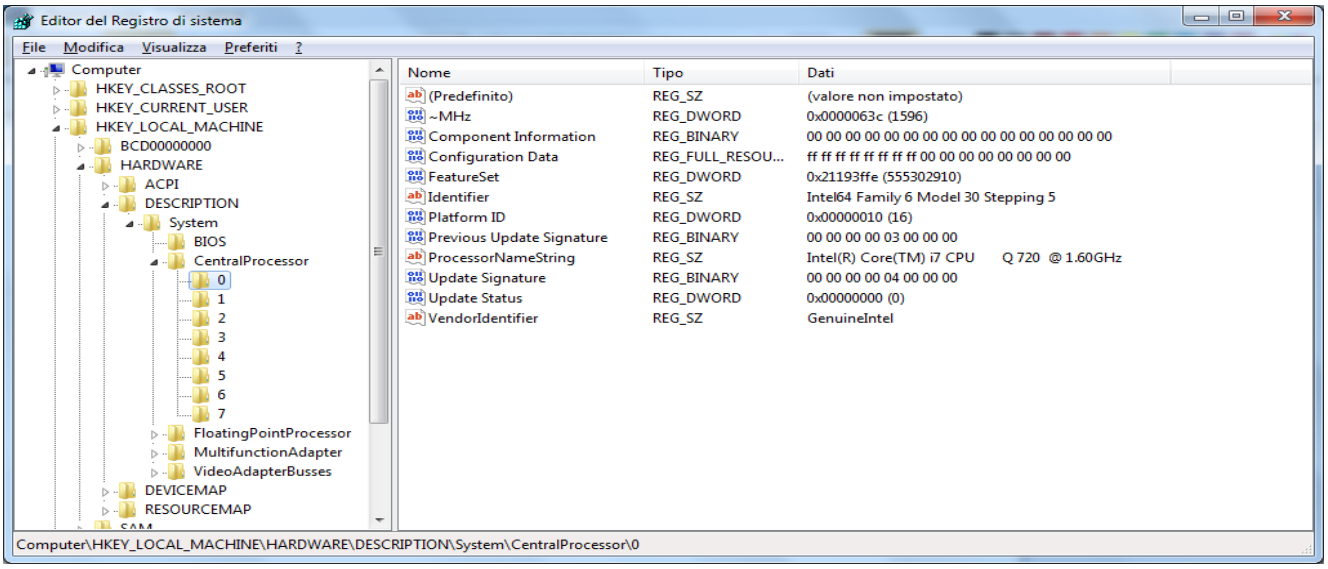


Figura 3.3 Chiavi contenenti informazioni sui processori del sistema

HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\…
Queste informazioni includono il nome del processore, la sua velocità e il codice identificativo del venditore come mostrato nella Figura 3.3.

C’è una serie di elementi di informazione circa gli account utente che è memorizzata nel registro di sistema. Per esempio un elenco degli account utente, l’ora dell'ultimo login di ogni account, se esso richiede una password, se si tratta di un account attivato o disattivato e il metodo utilizzato per l'hash (metodo per crittografare) della password dell'account utente. Tutte queste informazioni sono contenute nella seguente chiave di registro: HKEY_LOCAL_MACHINE\SAM\Domains\Account\Users

Per accedere alle informazioni di questo registro abbiamo utilizzato il software AcessData Registry Viewer in demo mode.
La figura 3.4 mostra i dettagli di un account Amministratore così com’è visualizzato in AcessData Registry Viewer.

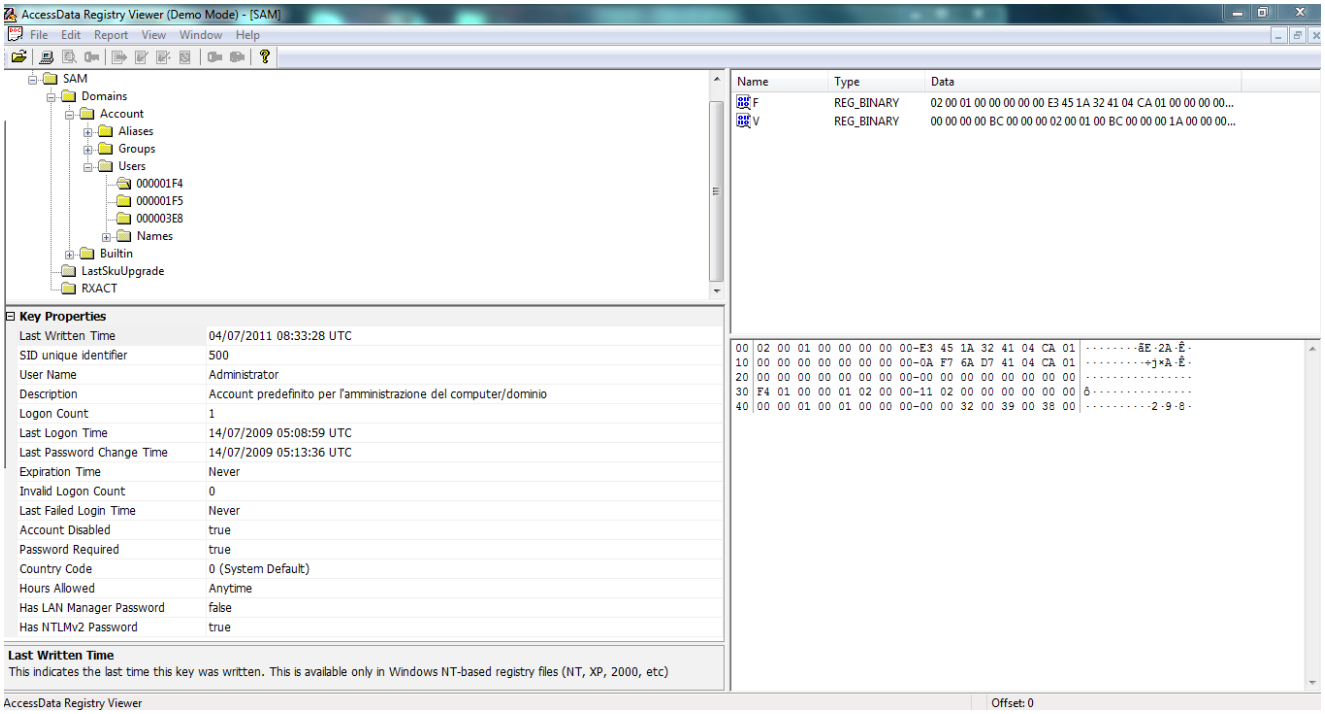


Figura 3.4 Schermata del software AcessData Registry Viewer che mostra i dettagli dell’account Amministratore

Le proprietà di questo tipo di chiave sono:

- **Last written Time:** questa indica l'ultima volta che questa chiave è stata scritta. È disponibile solo nei registri Windows NT-based (NT, XP, 2000, ecc).
- **SID unique identifier:** questa è l'unica porzione identificativa di SID che identifica l'utente sulla macchina.
- **User Name:** è l'user name dell'utente con questo SID.
- **Description:** descrizione dell'utente.
- **Logon Count:** numero di logon che l'utente ha effettuato. Si ferma al numero 65535.
- **Last Logon Time:** indica l'ultima volta che l'utente con questo SID ha effettuato il logon correttamente su questa macchina.
- **Last Password Change Time:** ultima volta che la password è stata cambiata.
- **Expiration Time:** indica quando la password dell'utente scade.
- **Invalid Logon Count:** numero di logon tentati senza successo dall'ultimo logon corretto.
- **Last Failed Login Time:** ultimo login fallito.
- **Account Disabled:** è settato a "true" se l'account è stato disabilitato.
- **Password Required:** è settato a "true" se è necessaria una password per effettuare il logon.
- **Country Code:** codice del paese dell'utente.
- **Hours Allowed:** ore in cui l'utente ha i permessi per effettuare il logon.
- **Has LAN Manager Password:** è settato a "true" se l'utente ha un valore della password hash del LAN Manager.
- **Has NTLMv2 Password:** è settato a "true" se l'utente ha un valore della password hash del NTLMv2.

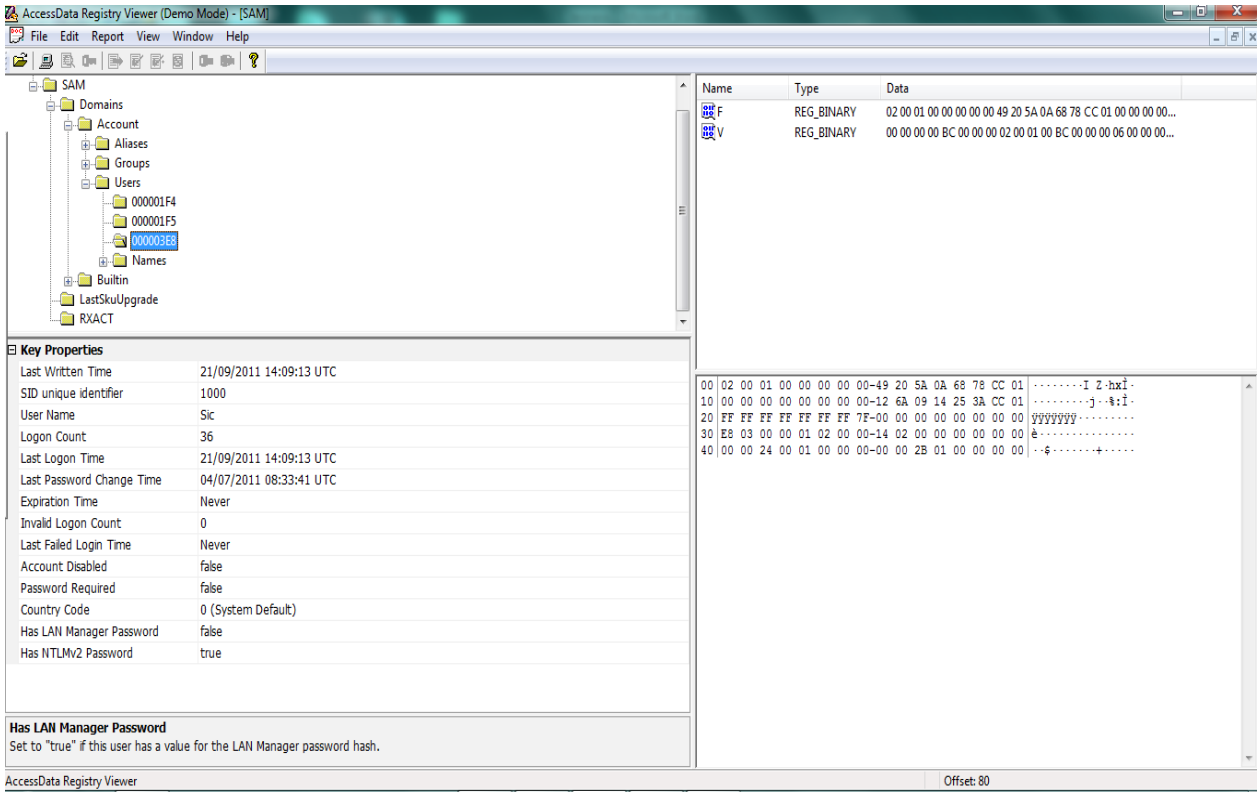


Figura 3.5 Esempio di proprietà di una chiave in AcessData Registry Viewer

Inoltre i nomi degli account utente sono elencati nella seguente chiave di registro: HKEY_LOCAL_MACHINE\SAM\Domains\Account\Users\Names

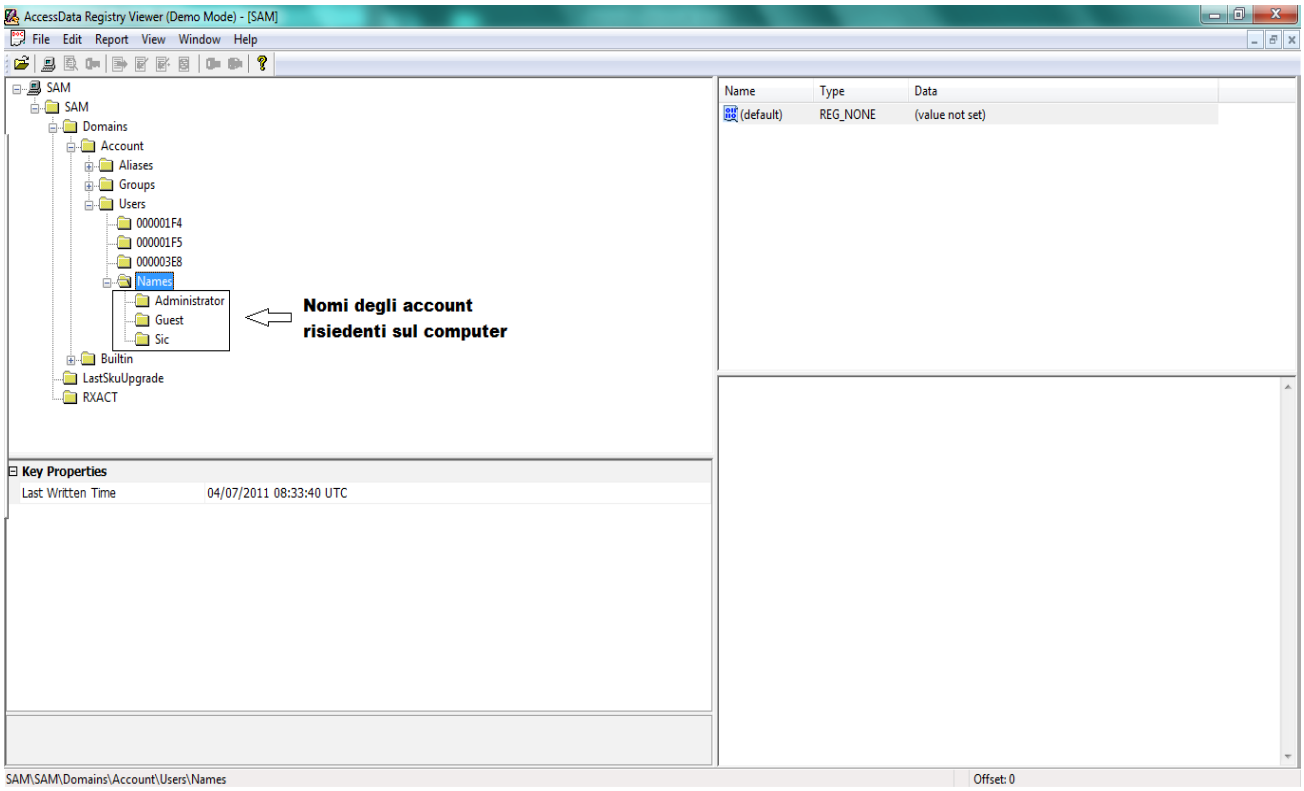


Figura 3.6 mostra i nomi degli account utente visualizzati tramite AcessData Registry Viewer.

Altra informazione importante, che può interessare un investigatore forense e che è prelevabile dai registri, è quella riguardante l'ultimo shutdown (arresto del sistema) del sistema. Questa informazione è memorizzata nel valore ShutdownTime nella seguente chiave di registro: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Windows

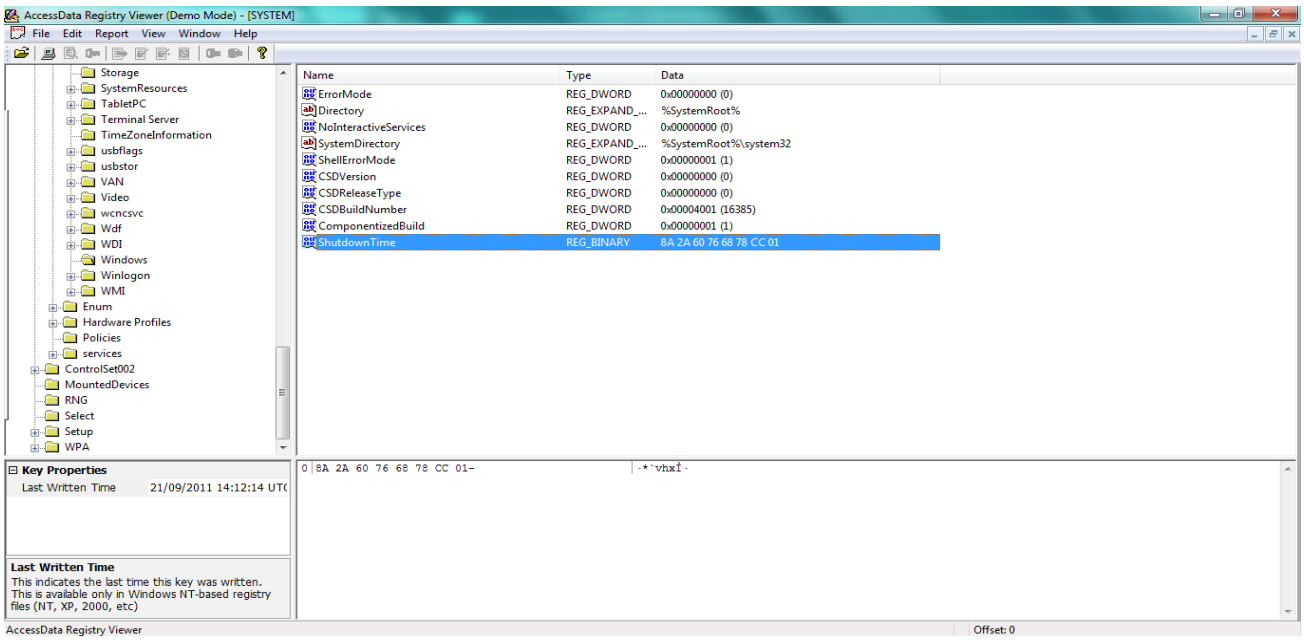


Figura 3.7 valore ShutdownTime tramite AcessData Registry Viewer

Programmi Startup

In Figura 3.8 vengono mostrate le informazioni sui programmi in startup del sistema risiedenti nella chiave:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

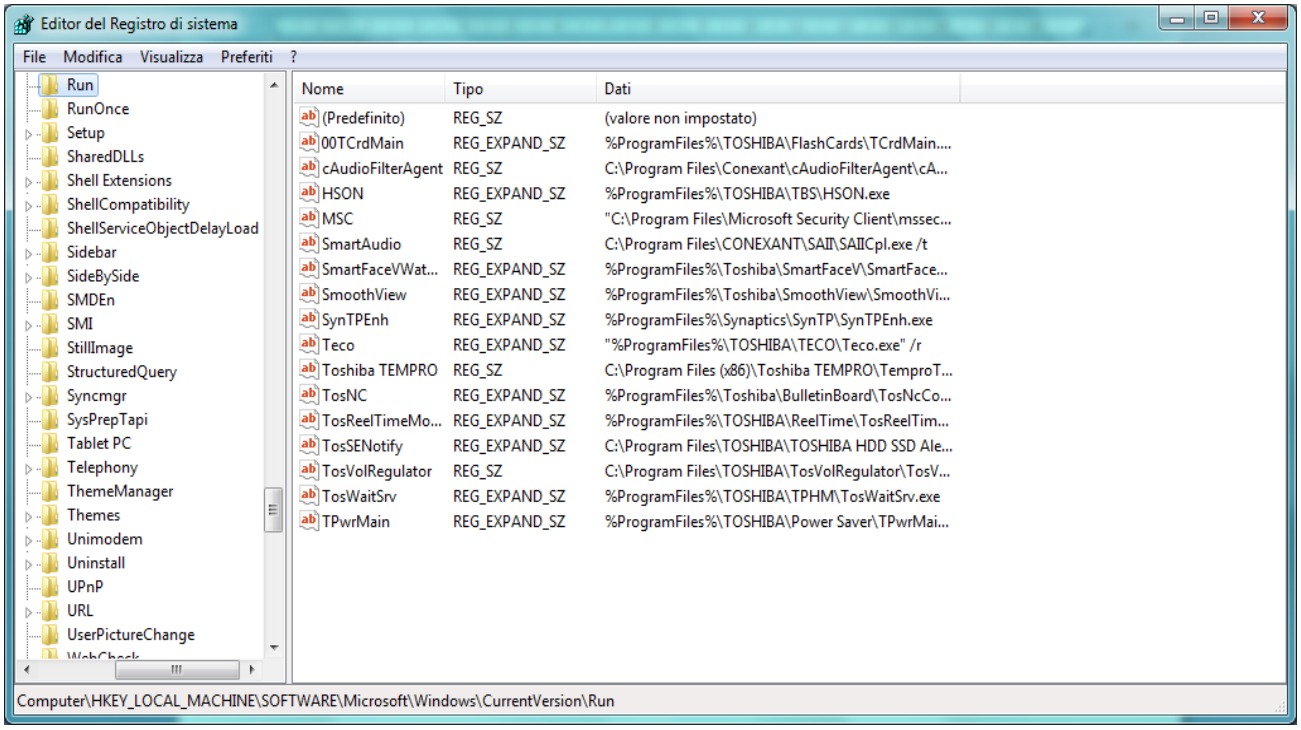


Figura 3.8 Informazioni sui programmi in startup del sistema

Reti Intranet

La lista delle reti intranet cui il computer è stato connesso è memorizzata in:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache\Intranet

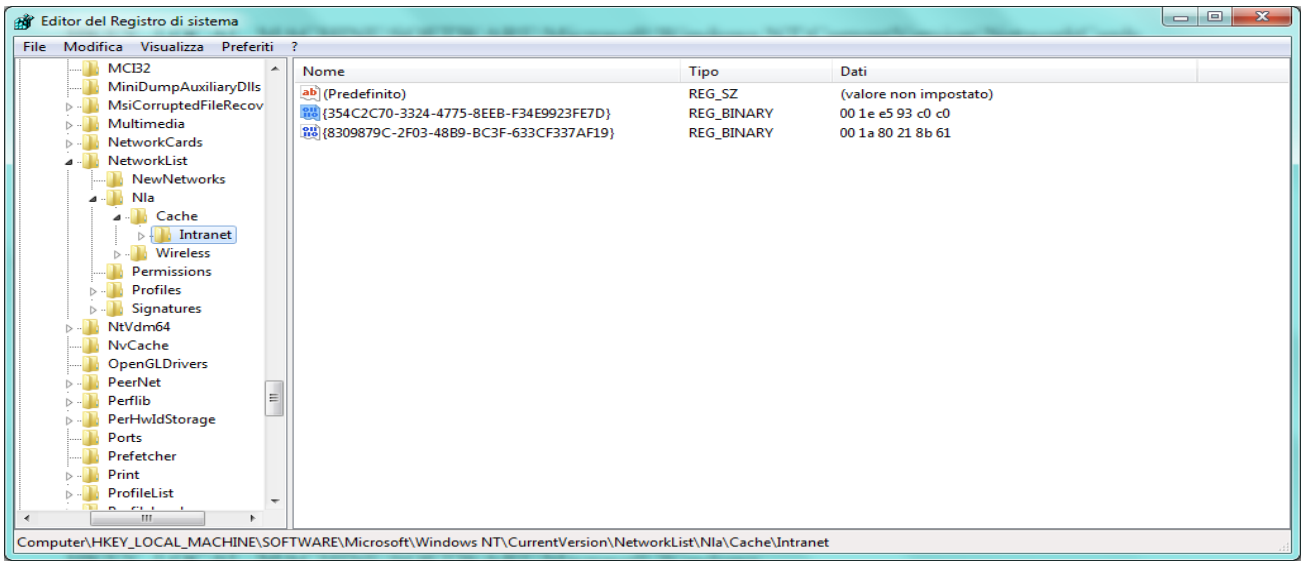


Figura 3.9 Lista delle reti intranet cui il computer è stato connesso

Reti Wireless

Per ogni rete wireless cui il computer si è connesso, gli identificatori sono memorizzati in: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\NetworkList\Nla\Wireless

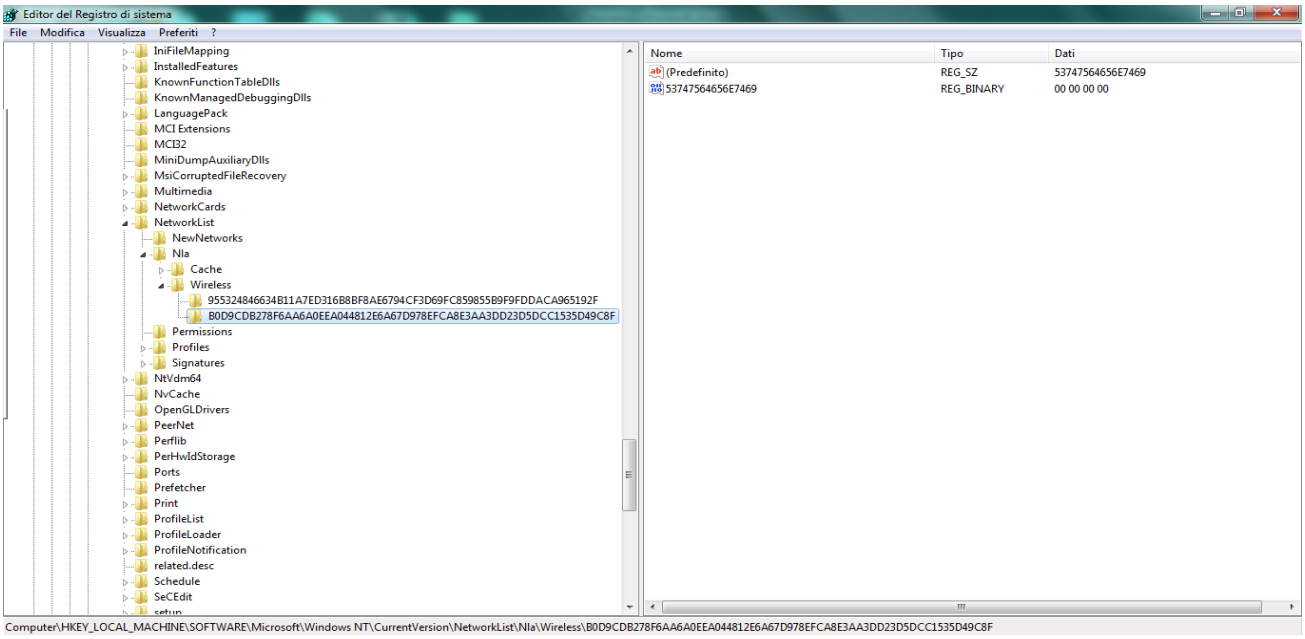


Figura 3.10 Reti wireless cui il computer è connesso.

Questa chiave è solo un elenco di identificatori per ciascuna delle reti wireless cui il sistema è stato collegato. Ulteriori informazioni su ciascuna di queste reti wireless come ad esempio l'indirizzo MAC del gateway predefinito, il suffisso DNS e SSID si possono trovare anche all'interno del Registro di sistema. Questo può essere fatto collegando l'identificatore della chiave precedente alla seguente chiave di registro di Windows come illustrato nella figura 3.11. Questa chiave ha una grande quantità di informazioni sulle reti in generale e non solo sulle reti wireless. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

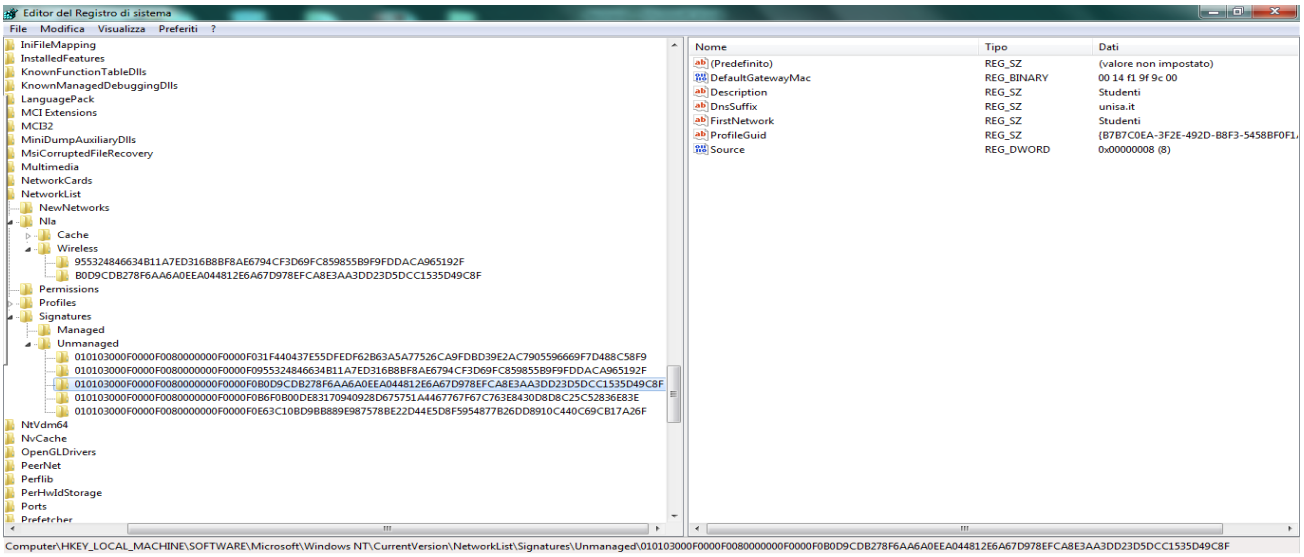


Figura 3.11 Informazioni più dettagliate sulle reti wireless cui il computer è collegato

Inoltre, il registro di Windows contiene informazioni importanti per l'investigatore forense sulle reti Wireless. Queste informazioni includono la data di creazione e ultima data di connessione. Essi sono memorizzati nella seguente sotto chiave di registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{Wireless - Identifier}

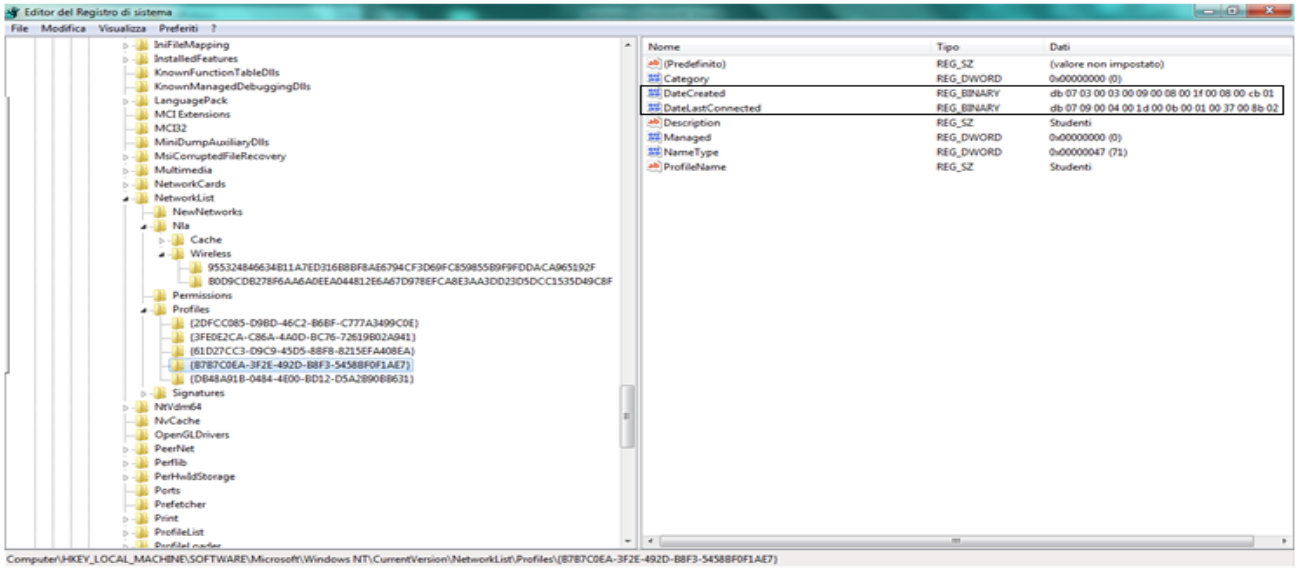


Figura 3.12 Data di creazione e data di ultima connessione di una rete wireless

Il tipo di questi valori è un tipo di dati binario. Quello che segue è una spiegazione di come visualizzare questi valori come data e ora normale.

DB 07	09 00	04 00	1D 00	0B 00	01 00	37 00	8B 02
07 DB	00 09	00 04	00 1D	00 0B	00 01	00 37	02 8B
Anno	Mese	Giorno	Giorno n.	Ora	Minuti	Secondi	
2011	Settembre	Giovedì	29	11	1	37	

1. La lunghezza del valore è di 16 byte.
2. Il valore è memorizzato utilizzando Little Indian, convertire in Big Indian.
3. Anno = 07DB = 2010.
4. Mese = 0009 = Settembre.
5. Giorno = 0004 = Giovedì.
6. Giorno a numero = 001D = 29.
7. Ora = 000B = 11.
8. Minuti = 0001 = 1.
9. Secondi = 0037= 37.

Quindi la data e l'ora corrispondenti all'ultima connessione alla rete wireless sono:
giovedì 29 settembre 2011 ore 11:01:37

Analisi dei dispositivi connessi

In questa parte vedremo quali sono le chiavi associate ai dispositivi esterni collegati ad un computer come ad esempio stampanti e dispositivi usb.

Stampanti

C'è una serie di chiavi all'interno del registro che contengono informazioni sui driver di stampa che esistono nel sistema. Uno di queste chiavi è la seguente:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Print\Printers

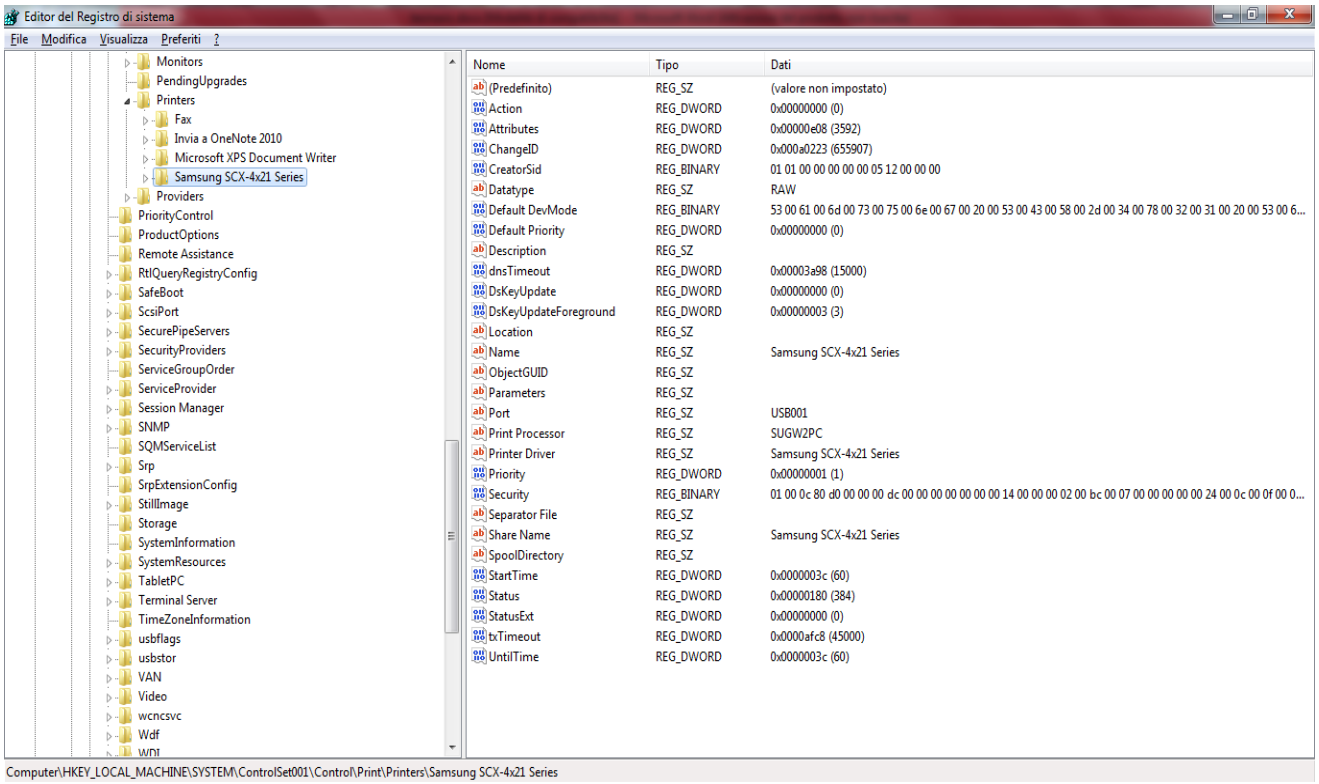


Figura 3.13 Esempio di chiave che contiene informazioni sui driver della stampante che esistono nel sistema

Questa chiave elenca i driver della stampante che esistono nel sistema. L'investigatore può ottenere ulteriori informazioni su ciascun driver della stampante accedendo alla sottochiave PrinterDriverData.

Dispositivi Usb

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

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR

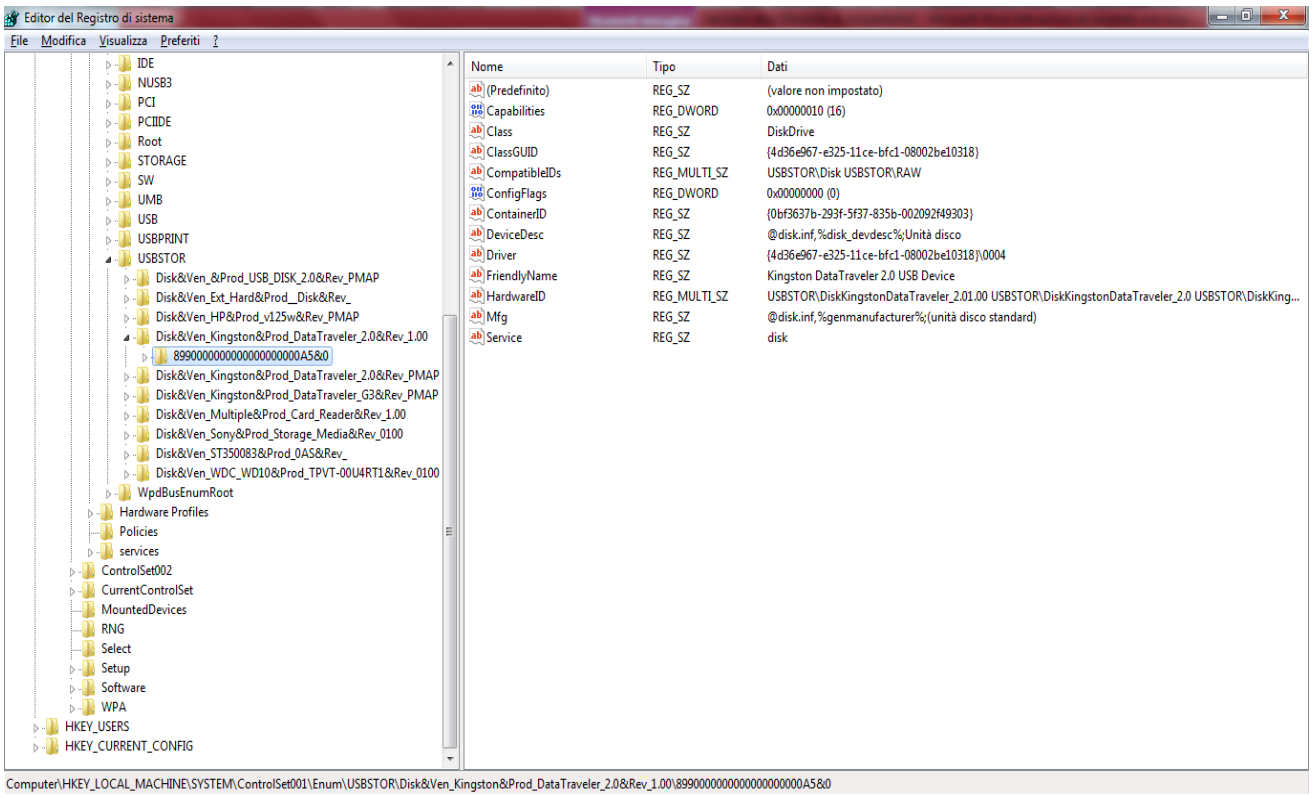


Figura 3.14 Chiave contenente informazioni sulla periferica usb collegata al sistema

Cronologia per file

La lista di cronologia mette in luce l'attività più recente eseguita sul sistema. Per esempio se sono state recentemente visitate le pagine web o se sono stati aperti dei file word. Ci sono diverse sottochiavi nel Registro di sistema che mostrano l'attività recente degli utenti del sistema.
Un esempio può essere conoscere, in base all'estensione, i file che sono stati aperti dall'utente e queste informazioni risiedono nella sottochiave:

HKEY_USERS\S-1-5-21-[UserIdentifier]\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.estensione

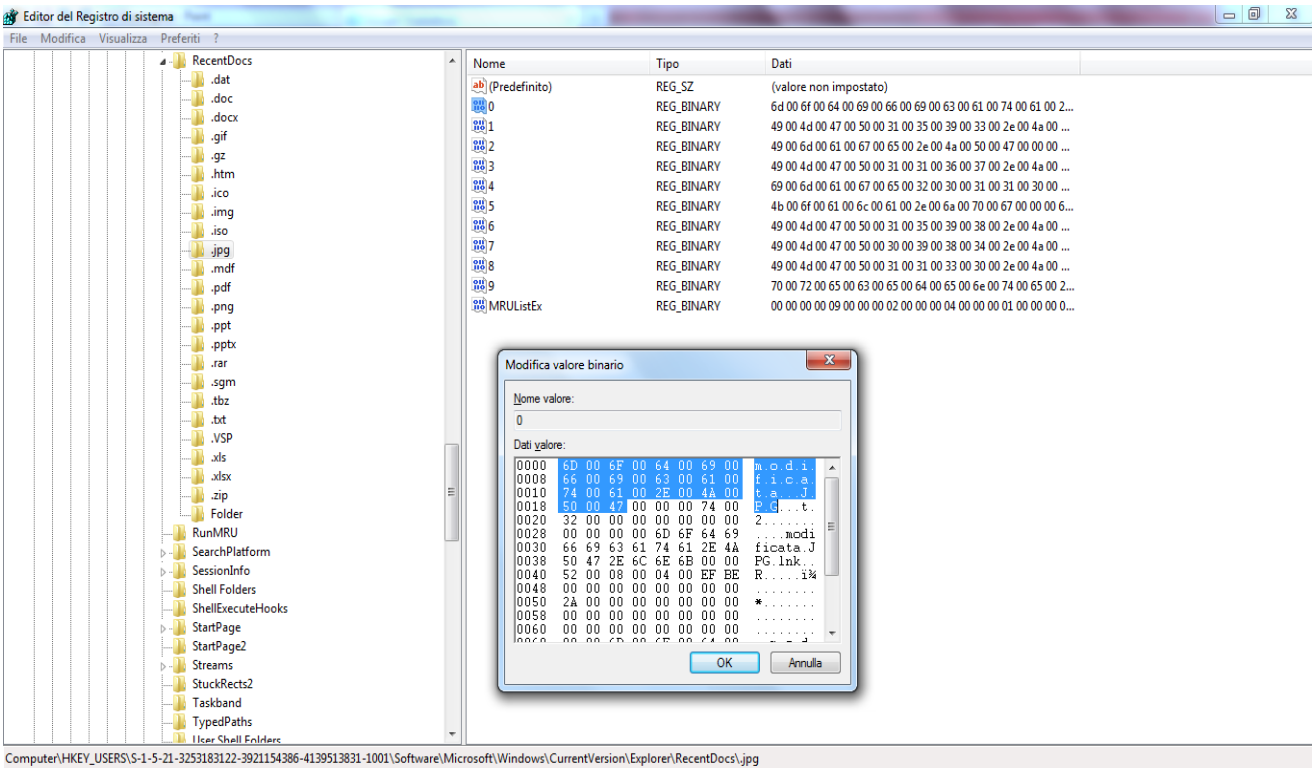


Figura 3.15 Esempio di informazioni sull'estensione .jpg . Mostra che è stato aperto il file modificata.jpg

Altro esempio potrebbe essere conoscere i documenti office aperti. Queste informazioni si trovano in:
HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Office \14.0\Programma*\File MRU

*Per programma si intende uno dei programmi del pacchetto Office (Word, Excel, PowerPoint, ecc).

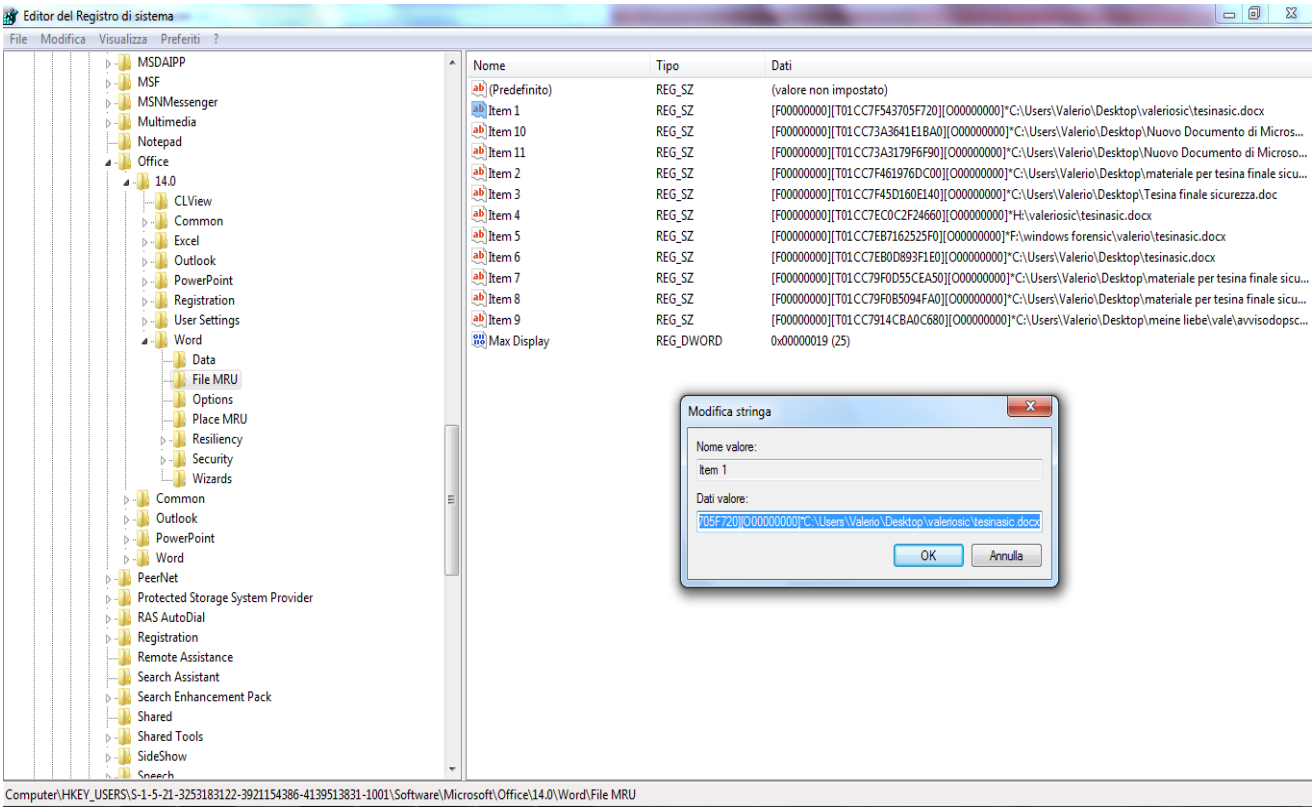


Figura 3.16 Nell'esempio si evince che è stato aperto l'elemento tesinasic.docx.

Valore dell’analisi dei registri in Windows.

L’analisi dei sistemi fornisce all’investigatore forense preziose informazioni sul sistema. Evidenzia un quadro sulle capacità di calcolo della macchina sospetta, come il nome del processore, velocità del processore, la famiglia di sistema, nome del sistema e la versione del sistema. Oltre a questo, l'investigatore forense farà un’indagine dei nomi, le identità o nickname di persone che stavano usando la macchina sospetta in base al nome del computer e un elenco di account utente. Inoltre, l’estrazione dell’ora di ultimo arresto fornirà informazioni riguardanti l'ultima volta che la macchina sospetta è stata utilizzata e questo ad esempio, può indicare che la macchina non è legata ad un determinato crimine.
L’analisi delle applicazioni fornisce utili informazioni sulle applicazioni che sono istallate sulla macchina sospetta. L’investigatore forense dovrebbe controllare i programmi di startup perché tra essi potrebbero esserci dei “malicious programs”, ovvero dei programmi creati appositamente per gestire la macchina sospetta e quindi il sistema può essere stato mandato in esecuzione da terzi piuttosto che dall’utente della macchina in esame. Per esempio, se la macchina sospetta è stata utilizzata per inviare attacchi DOS, l’utente del sistema potrebbe non essere il criminale che ha avviato l’attacco, ma potrebbe essere stato eseguito da un criminale che controlla la macchina dell’utente in remoto.

L’analisi di rete darà all'investigatore forense una panoramica delle attività di rete che sono state eseguite dalla macchina sospetta. Dall'elenco delle schede di rete, si possono identificare tutte le schede che sono state utilizzate dal sistema e se queste sono parte integrante del computer o collegate esternamente al sistema. Inoltre, si ottiene una lista delle intranet cui la macchina sospetta era collegata. Si possono ottenere informazioni preziose sulle reti wireless cui il sistema si è collegato, inclusi i nomi dei profili di eventuali reti wireless, la data di creazione e l'ultima data di connessione.

L'analisi dei dispositivi collegati darà le informazioni all’investigatore forense sui dispositivi che sono stati collegati al sistema. A tal proposito vi sono due categorie di dispositivi collegati: stampanti e periferiche USB. La lista di stampanti e le loro informazioni, come il nome del modello e la data di installazione sono preziose informazioni e potrebbero essere considerate come potenziali prove digitali. Per esempio in un crimine contro la contraffazione, i criminali usano normalmente le stampanti ad alta qualità per la produzione di una carta di credito simile all’originale. Inoltre, è importante conoscere quali dispositivi USB sono collegati al sistema e informazioni come ID del prodotto e numero di serie, specialmente nel caso del furto di dati da un computer.

Conoscendo i file di tipo immagine come quelli con estensione jpg e GIF si è in grado di fornire una potenziale prova digitale nei crimini come la pedofilia. Nei crimini come il furto di identità, la contraffazione e il terrorismo, il criminale può memorizzare le informazioni della carta di credito che è stata utilizzata per trasferire denaro, in un file .txt o in un file word che possono essere recuperati dall’elenco della cronologia dei file recentemente utilizzati.

3.3 Casi di studio su Registry di Windows 7

Nel primo caso di studio, usando dapprima l'editor di registro RegEdit di Windows 7, creiamo una sottochiave con un proprio valore, la modifichiamo e la cancelliamo per poi vedere tramite l'editor esadecimale WinHex, se sull'hard disk è rimasta qualche traccia del valore precedente dopo l'esecuzione di queste due operazioni.
Nel secondo caso di studio, usando due tool di MiniPe, una live cd di Windows Xp, mostriamo come è possibile visualizzare, creare e modificare sottochiavi e valori nel Registry di Windows 7.

3.3.1 Creare, modificare e cancellare le chiavi del Registro di Sistema

Le chiavi ed i suoi valori possono essere creati, modificati o cancellati tramite l'Editor del Registro di Sistema, richiamabile digitando "regedit" dal box esegui.
Per aggiungere una chiave di registro, basta selezionare la chiave genitore e dal menu scegliere Modifica->Nuovo->Chiave, oppure con la chiave selezionata premere il tasto destro del mouse e scegliere Nuovo->Chiave. A questo punto si creerà una sottocartella (nella parte sinistra dell'editor) alla quale assegnare il nome per la nuova chiave creata.
Per modificare invece il valore di una chiave di registro, bisogna selezionarla (sul lato destro dell'editor) e col tasto destro del mouse scegliere modifica, immettere il nuovo valore e confermare con Ok.

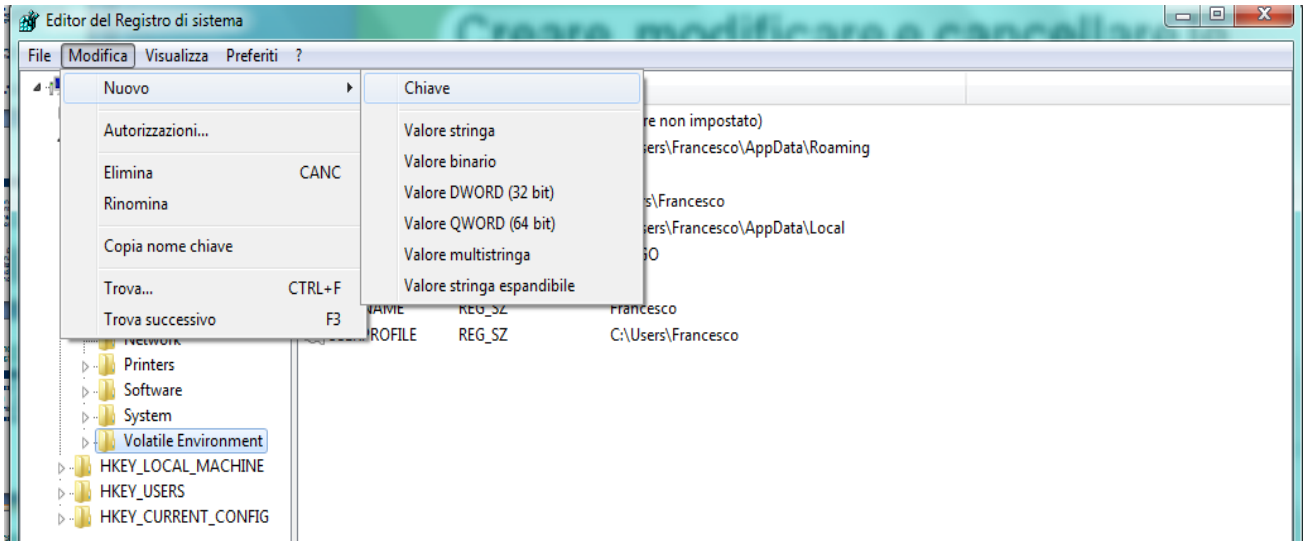


Figura 3.17 Prima schermata dell'editor di registro

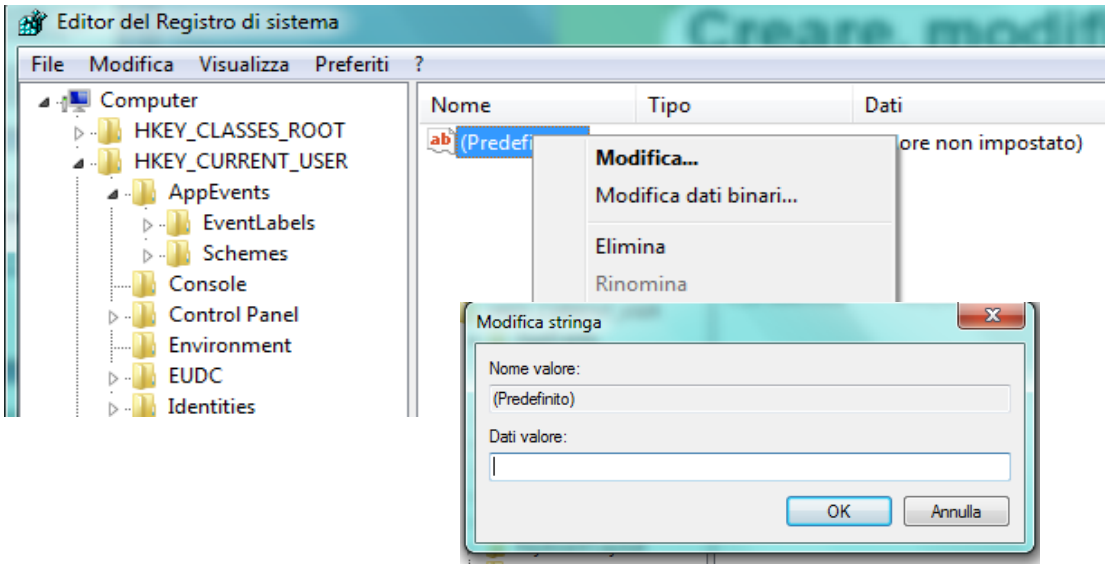


Figura 3.18 Modifica del valore di una chiave di registro

Per cancellare una chiave basta selezionarla ed eliminarla premendo canc o la voce Elimina dall'apposito menù contestuale richiamato con il tasto destro del mouse.
Alcune delle modifiche apportate alle chiavi, hanno un effetto immediato sulle impostazioni del sistema, per altre invece è necessario riavviare il sistema. Infine sempre dal menu modifica è possibile richiamare la funzione "Trova" (Ctrl+F) per la ricerca delle chiavi, una funzione molto utile per districarsi tra le migliaia di voci presenti nel registro di sistema. Dalla funzione Trova basta inoltre premere F3 per spostarsi al valore successivo.

3.3.2 WinHex

WinHex è un editor esadecimale shareware di file, dischi e ram di proprietà X-Ways Software Technology AG, per i sistemi operativi Windows, abbastanza facile da utilizzare ma riservato comunque a persone con una certa competenza.

Con questo programma è possibile fare:

- Editor disco (logico & fisico; supporta le FAT12, FAT16, FAT32, NTFS e CDFS)
- Editor RAM (vuol dire modificare altri processi di memoria virtuale)
- Interprete Dati, con il riconoscimento di 19 tipi di dati
- Modifica struttura dati usando maschere
- Concatenamento, divisione, unione, analisi e comparazione dei file
- Funzione di ricerca e sostituzione flessibile
- Automazione della modifica dei file
- Annullamento e copia dei meccanismi per i file e i dischi
- Cancellazione irreversibile dati confidenziali
- Importazione di ogni formato di appunti
- Conversione formati: Binario, Hex ASCII, Intel-Hex e Motorola-S

Nel nostro caso di studio è stata usata la versione 16.0

Passi del caso di studio

È stata creata con l'ausilio di RegEdit una sottochiave con nome "chiave1" nella chiave HKEY_CURRENT_CONFIG, gli è stato assegnato un valore con nome "val1" e come dati valore, un pattern noto "qazqazqazqazqazqazqaz". Come mostrato in figura 3.19

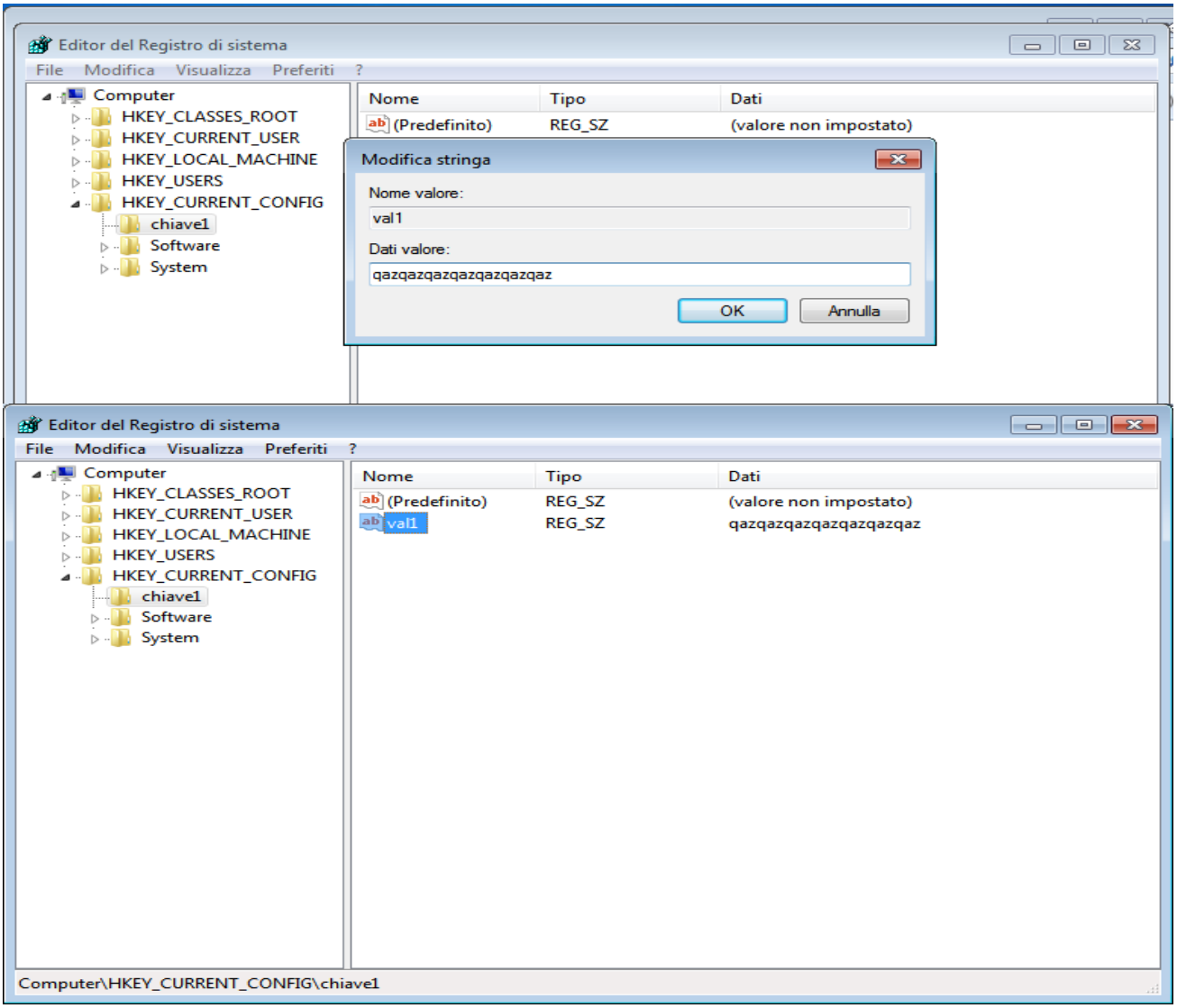


Figura 3.19 creazione di "chiave1" con nome valore "val1".

Vediamo ora le schermate principali di WinHex e come è possibile utilizzare la funzione di ricerca nell'intero hard disk per un determinato valore:
Selezioniamo *Apri unità disco* nel menù *Strumenti* e scegliamo l'unità disco da analizzare, in questo caso (C:).

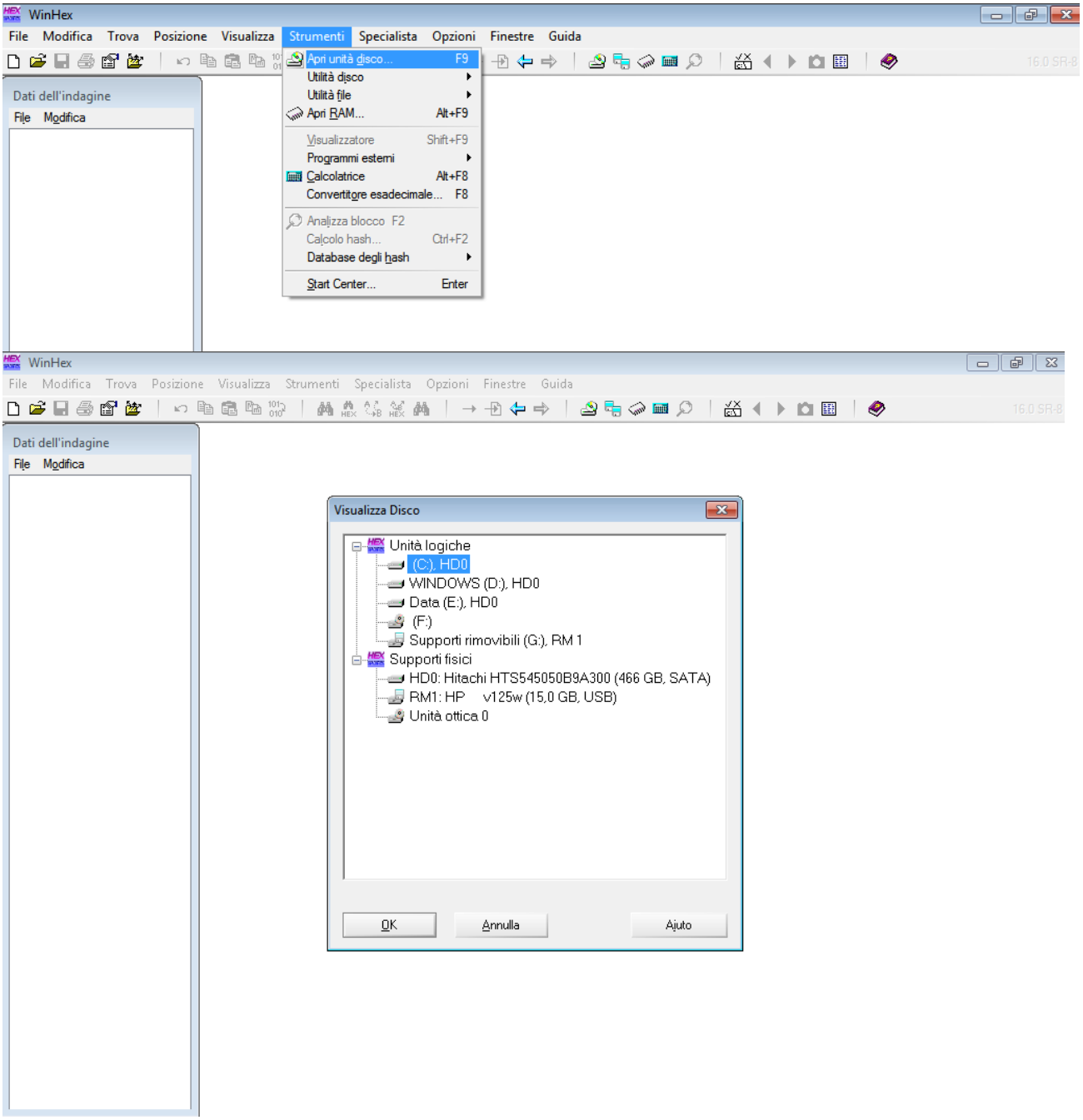


Figura 3.20 Selezione dell'unità disco in WinHex

Una volta scelta l'unità disco, WinHex ci mostra il contenuto di ogni settore in valore esadecimale e la relativa decodifica in caratteri di testo. Come vedremo in seguito, tutto ciò ci servirà a localizzare i relativi settori di residenza di ogni informazione ricercata.

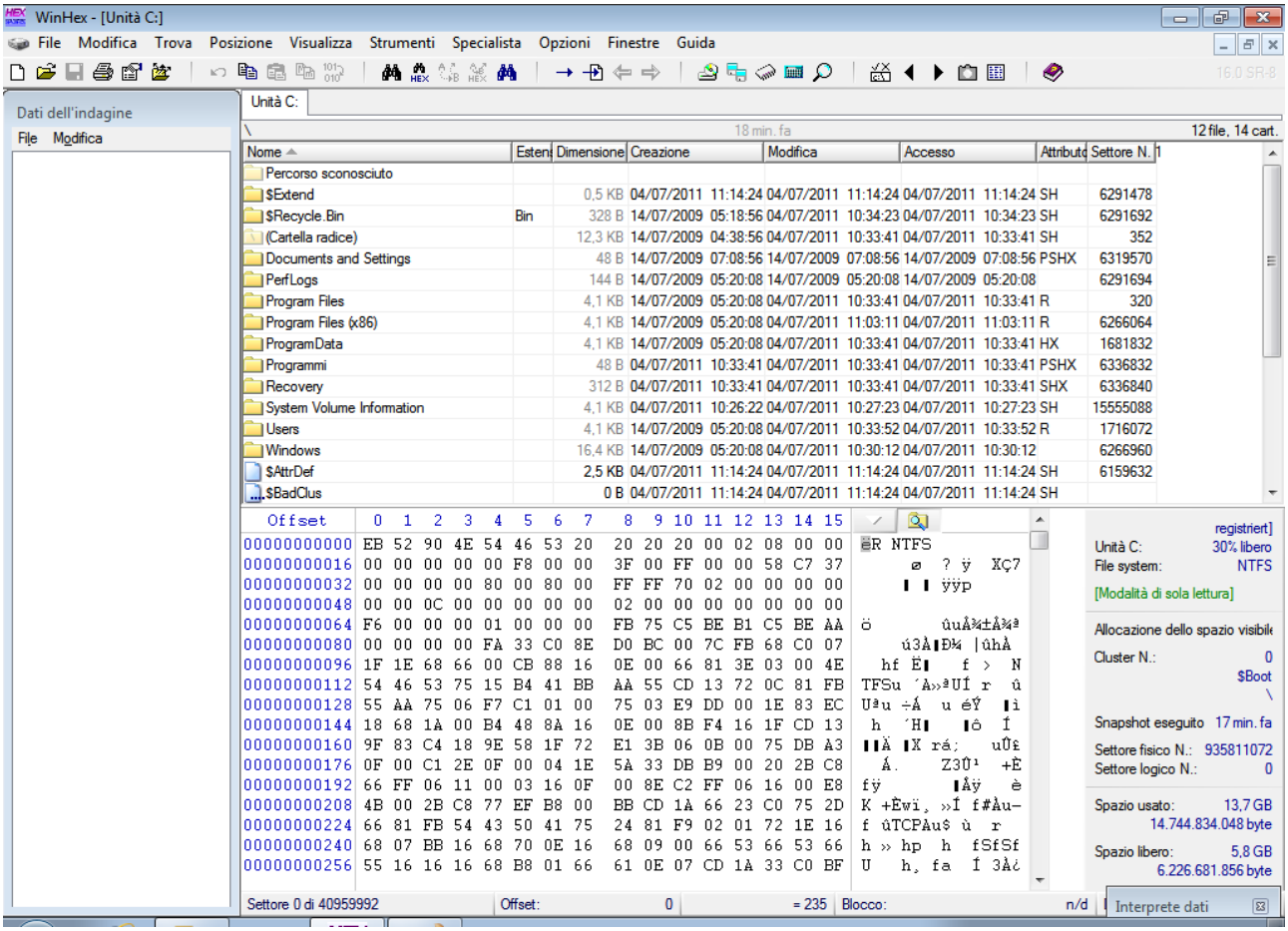


Figura 3.21 Contenuto del disco in esadecimale e relativa decodifica in caratteri.

Di seguito è mostrata la ricerca del valore della sottochiave creata, selezionando l'opzione *Caratteri speciali* con valore "?". Il carattere "?" usato nella ricerca è un metacarattere (o carattere wildcard), che può essere sostituito da qualsiasi altro carattere in una stringa. Nel nostro caso, serve a permettere la riuscita della ricerca anche se i caratteri che compongono la stringa non sono successivi l'uno all'altro, cioè se tra un carattere e l'altro della stringa è presente un carattere differente da quelli che la compongono.

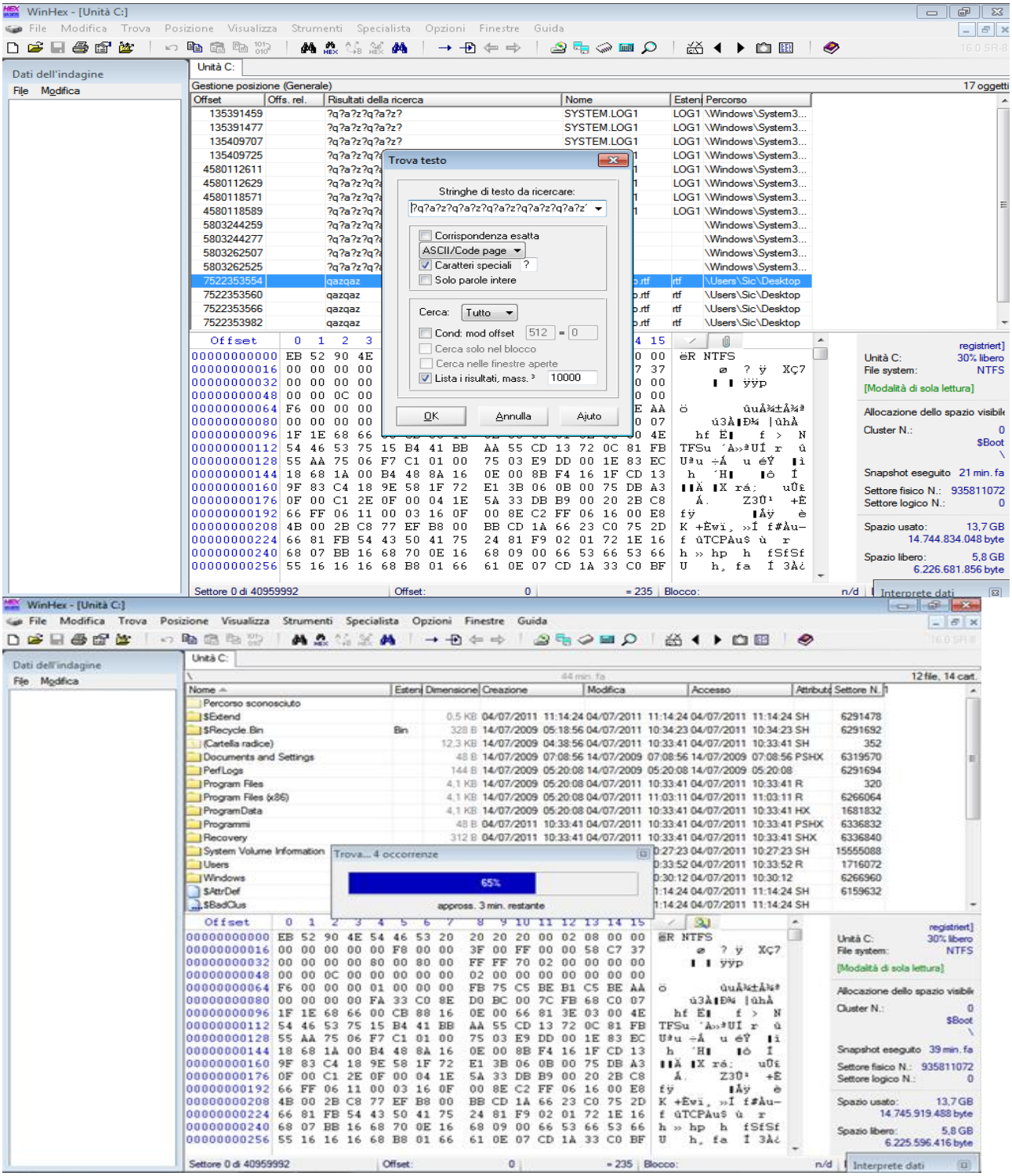


Figura 3.22 Scrittura del valore da ricercare nel campo testo dell'opzione trova e susseguente ricerca delle occorrenze

Vediamo di seguito dove, nel nostro disco e in quale file, risiede la chiave e il valore associato.

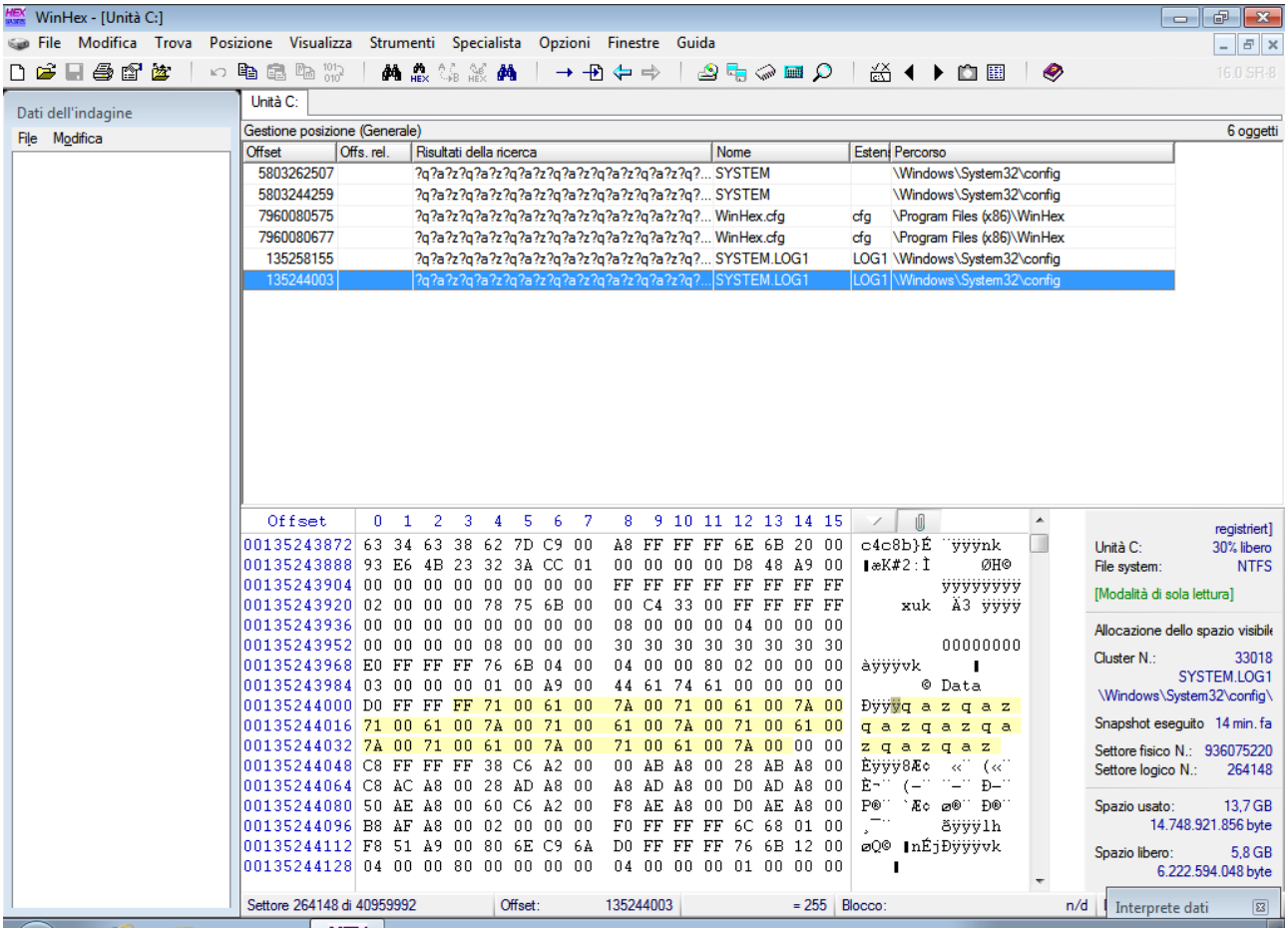


Figura 3.23 Path della chiave con il valore ricercato

L'informazione risiede nel file \Windows\System32\config\SYSTEM. Nei settori a partire dall'offset *259, risiede solo il pattern noto scelto per il determinato valore val1 della sottochiave chiave1, mentre partendo dall'offset *464 viene mostrato anche il nome della sottochiave "chiave1" e il nome valore di quest'ultima "val1", compreso il pattern noto a partire dal settore con offset *507. Il sistema effettua periodicamente delle copie di sicurezza delle parti modificate del registro, creando file con estensione .LOG1 (SYSTEM.LOG1 se ci riferiamo al log del file SYSTEM) che mantengono, finché non sovrascritti, determinate informazioni. Come si vede in figura dall'offset selezionato *003 fino al settore con offset *045, vi è una copia di backup dell'informazione contenuta dai settori a partire dall'offset *259.
Il file WinHex.cfg mantiene in memoria le ricerche effettuate da WinHex, quindi non è utile al nostro scopo.

3.3.3 Modifica e cancellazione chiave

Modifichiamo ora il valore di val1 con il pattern più breve "trrtrrtrrtrr" sempre con RegEdit e controlliamo dove sono state inserite le modifiche e se risiedono tracce del vecchio valore.

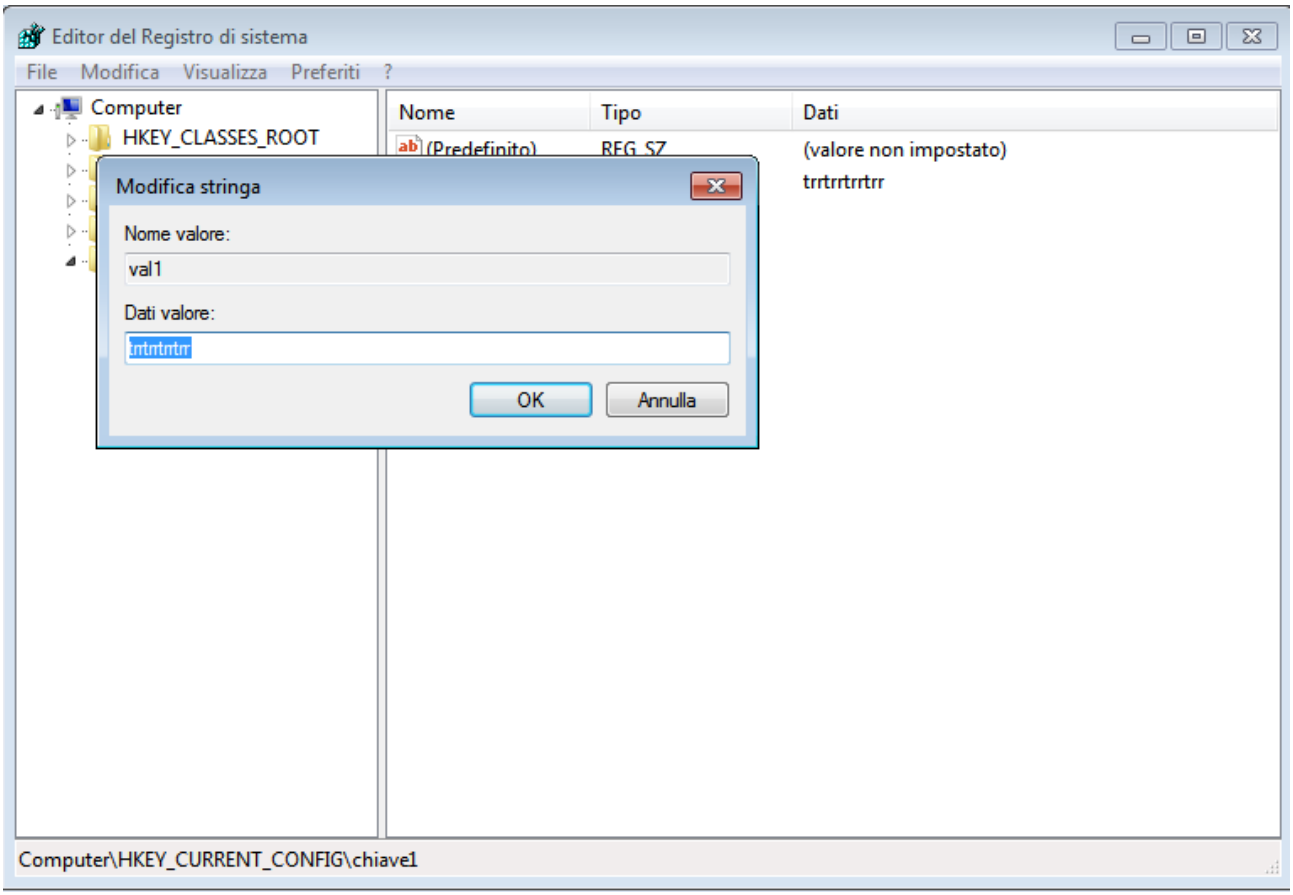


Figura 3.24 Modifica di dati valore di "val1" con l'uso di RegEdit

La figura 3.25, fa notare che avendo sostituito il nuovo pattern noto “trrtrrtrrtrr” di lunghezza minore al valore precedente, sfruttando la ricerca precedentemente effettuata mostrata in figura 3.23, una parte di esso ancora sussiste. Il valore quindi non è stato riscritto completamente, ma una traccia anche se parziale, può essere già trovata.

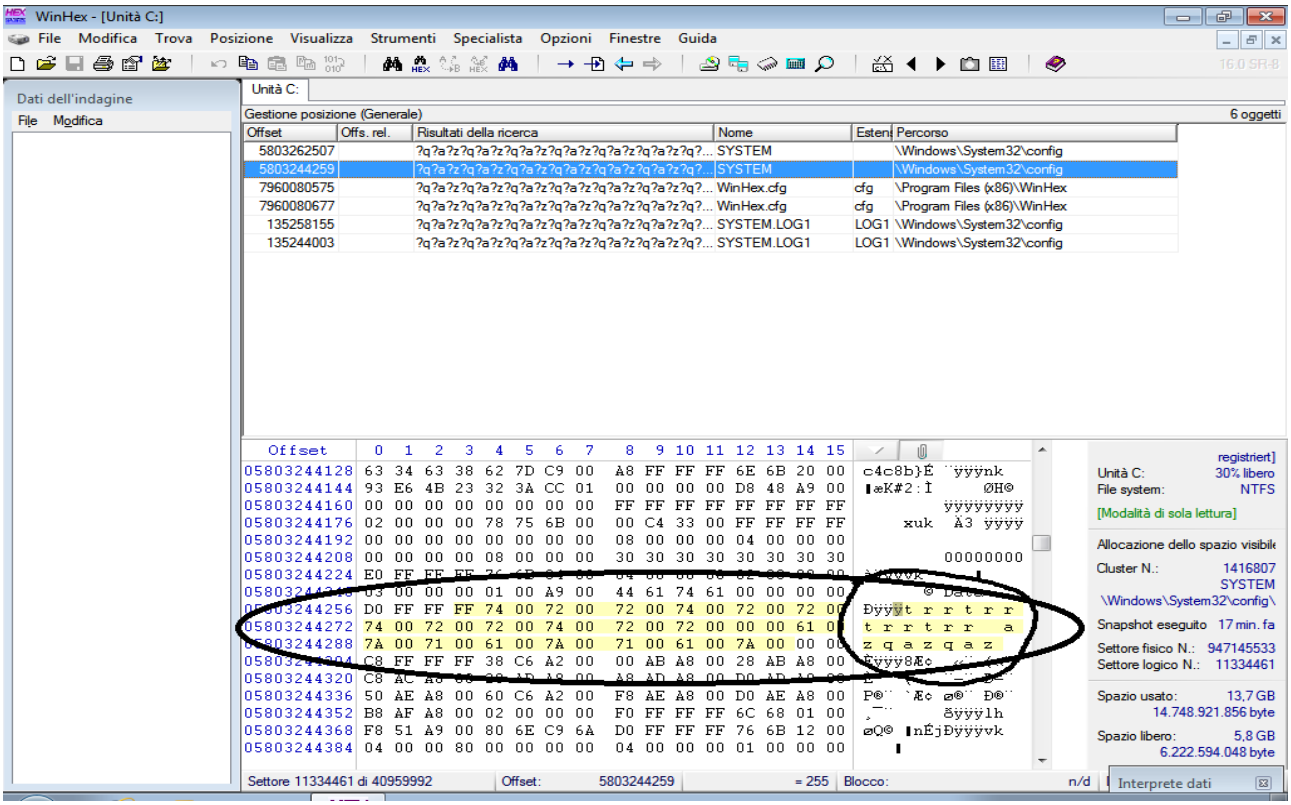


Figura 3.25 In evidenza le tracce ritrovate dopo la modifica del valore di val1

In questa immagine che rappresenta una nuova ricerca del vecchio valore, possiamo notare che anche se il valore è stato riscritto tramite RegEdit, può essere ancora trovato a partire dal settore con offset *507, lasciando quindi una traccia completa.

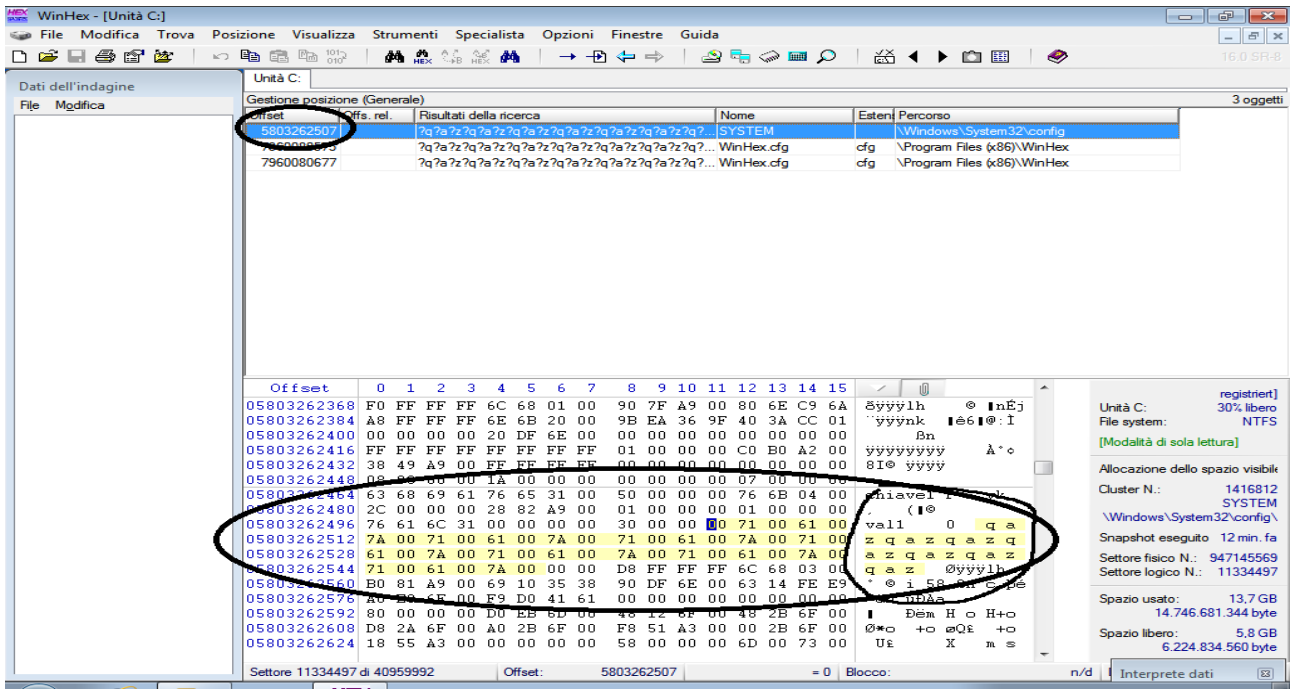


Figura 3.26 Ricerca del vecchio valore della chiave

Successivamente riavviamo Windows 7 ed effettuiamo una nuova ricerca per il vecchio valore "qazqazqazqazqazqazqaz". Come si vede dalla prossima figura, sono stati creati anche due log del file di nome SYSTEM che quindi copiano la traccia.

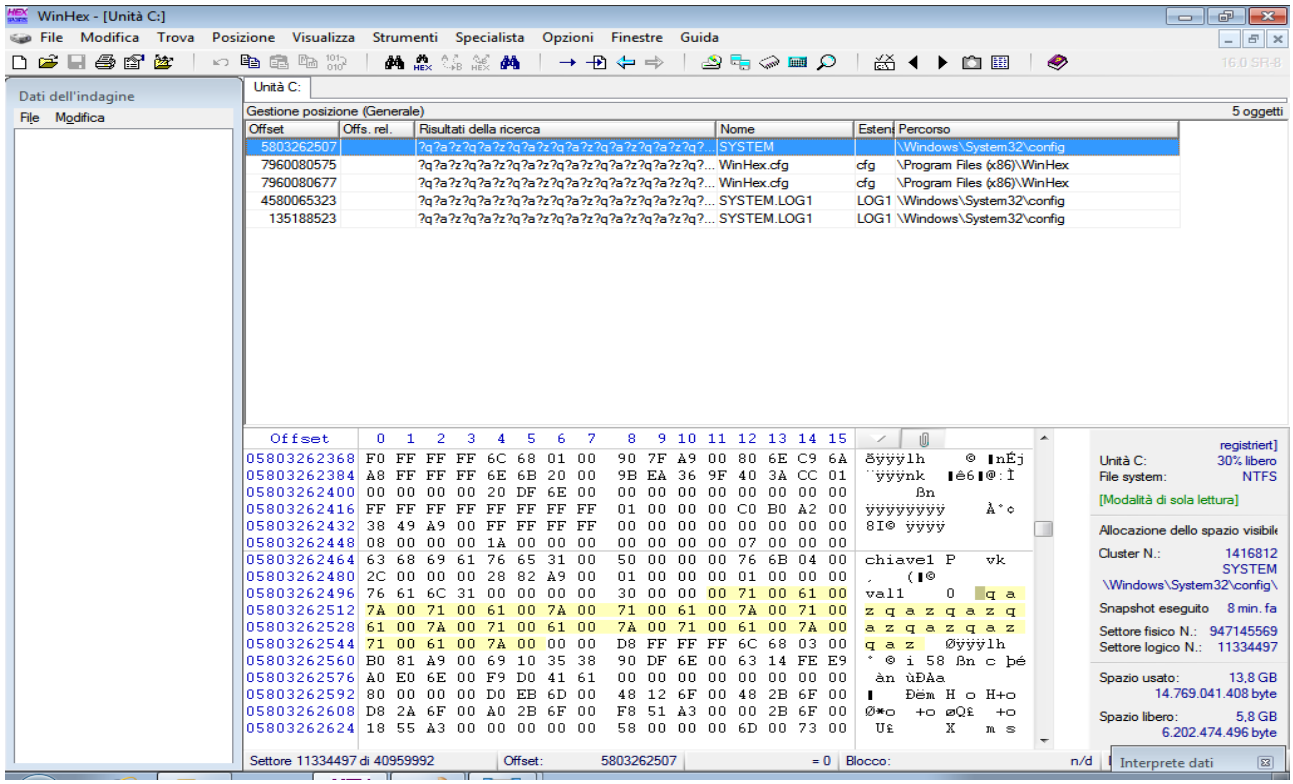


Figura 3.27 Due log del file SYSTEM

Successivamente abbiamo modificato di nuovo il valore rimpiazzandolo con il pattern “ciaociaociao”.
In seguito abbiamo istallato un driver per la periferica Wireless, e siamo venuti a conoscenza, come si evince dalla prossima figura, del fatto che i settori a partire dall’offset *507 in cui risiedevano le informazioni relative al vecchio pattern “qazqazqazqazqazqazqaz”, erano stati sovrascritti totalmente mostrando solo come piccola traccia, la stringa “chiave1” che era il nome della sottochiave.

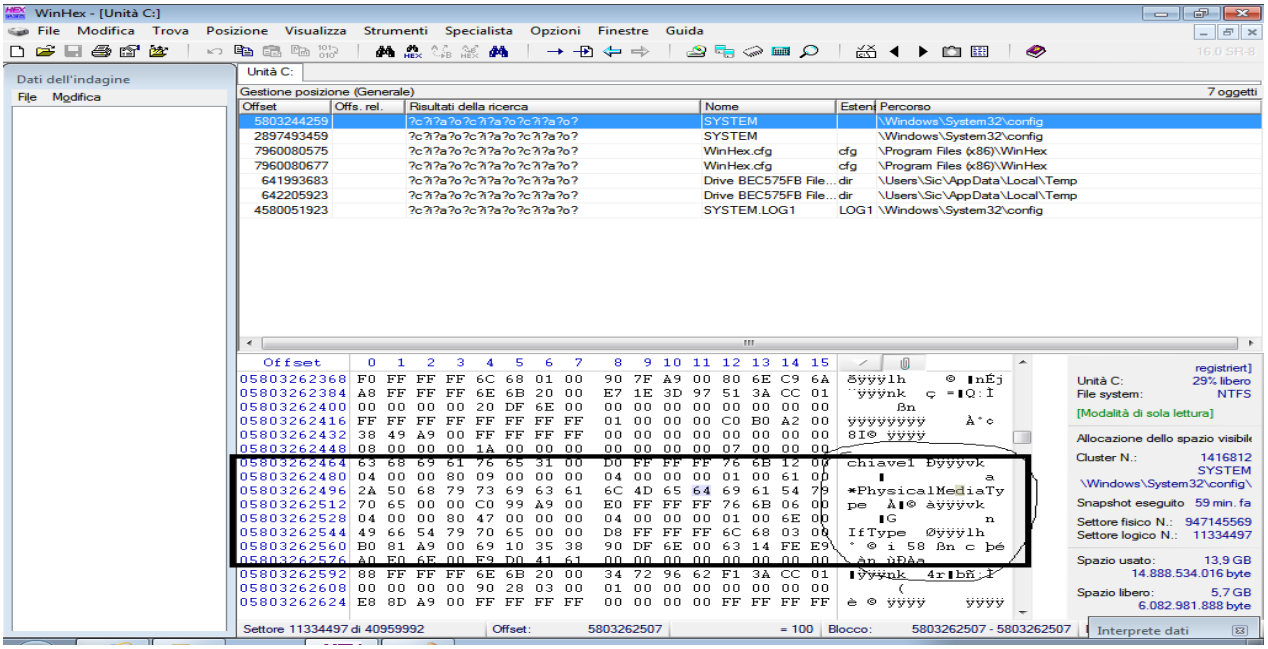


Figura 3.28 Settori a partire dall’offset *507 dopo l’installazione di una periferica Wireless

In una nuova ricerca del valore “ciaociaociao” abbiamo notato una sua occorrenza nel driver Driver BEC575FB Files.dir nella cartella \Users\nome dell’user utilizzatore\AppData\Local\Temp.

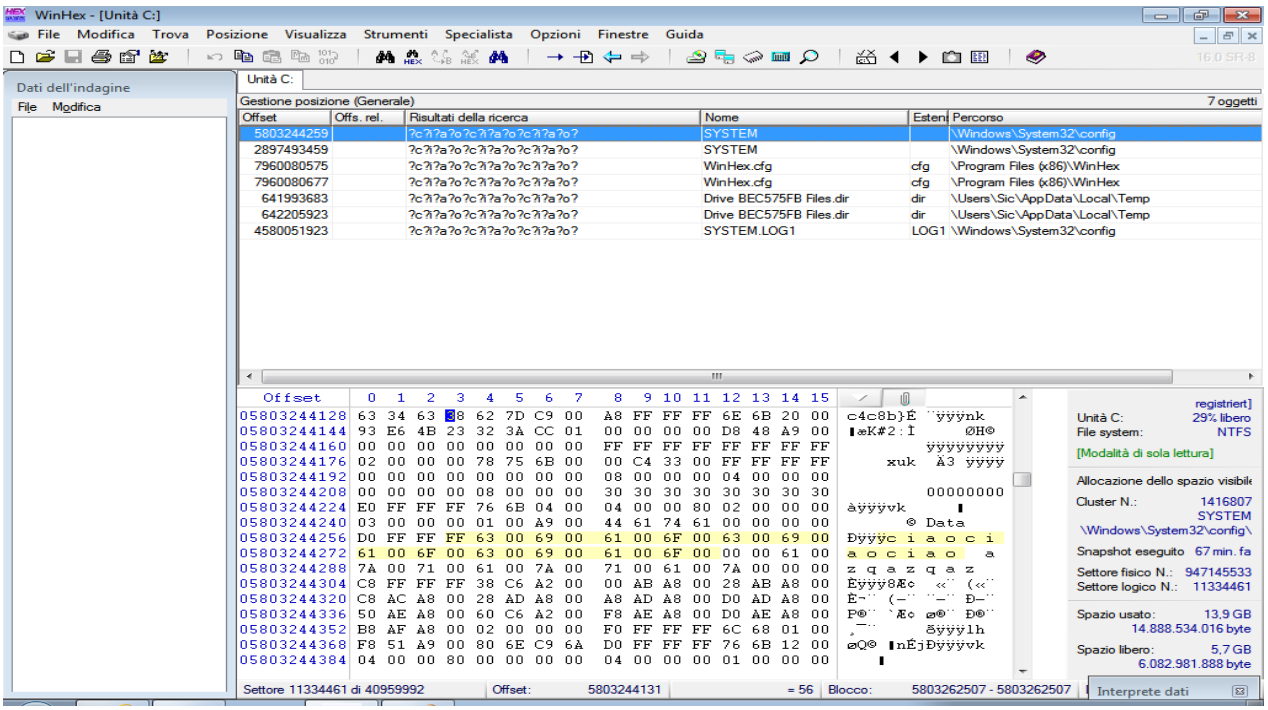


Figura 3.29 Esito della ricerca del valore “ciaociaociao”

Eseguiamo la cancellazione, attraverso il comando *Elimina* di RegEdit, dell'intera sottochiave con il relativo valore e riavviamo il Sistema Operativo. Come si evince dalla figura sottostante, le tracce persistono in settori ora non utilizzati, denotati dal nome *Spazio libero*, che potranno essere sovrascritti dal sistema successivamente, cancellando ogni traccia.

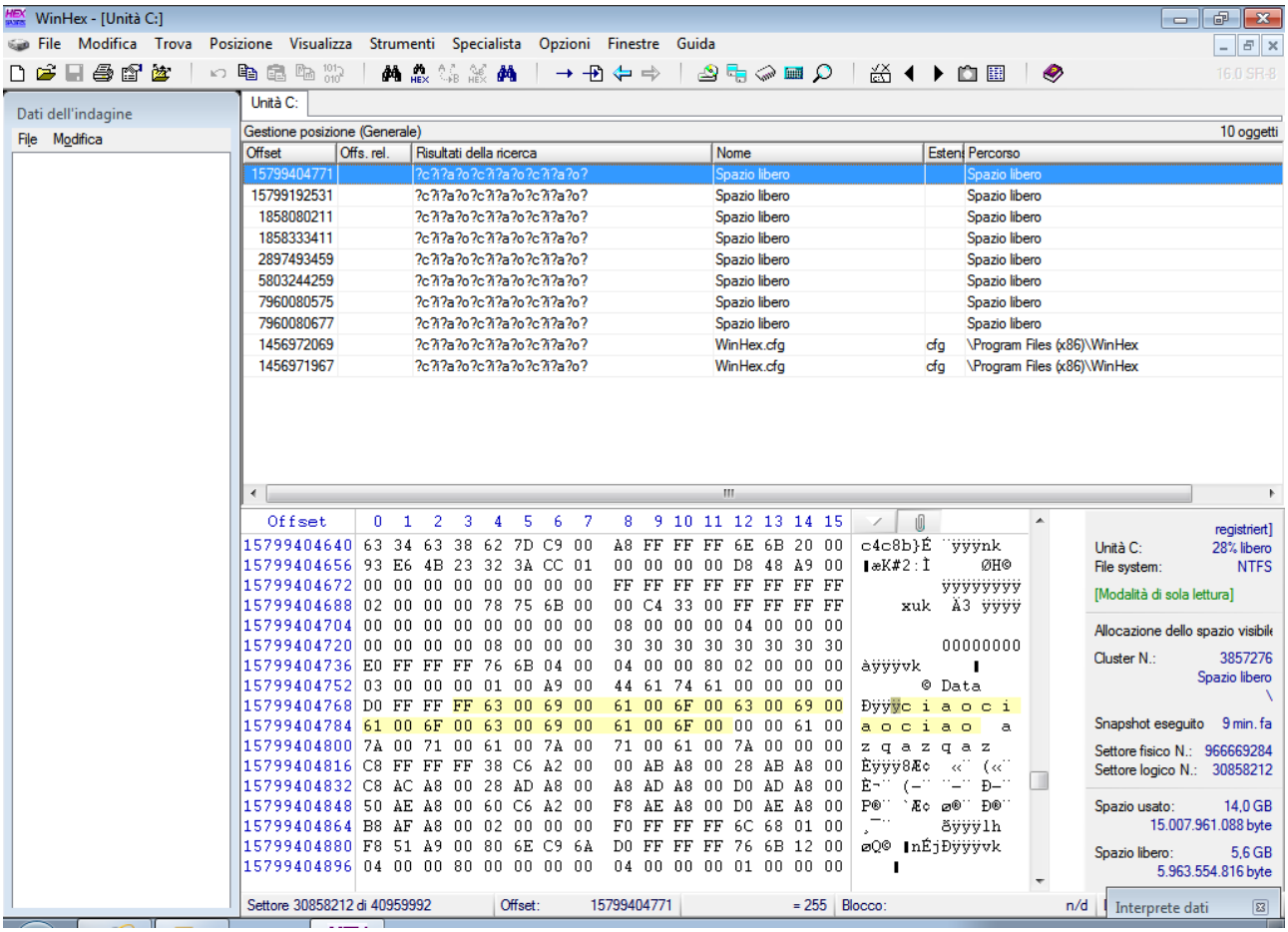


Figura 3.30 Tracce della chiave cancellata in altri settori inutilizzati

Abbiamo creato successivamente una nuova sottochiave e un valore ad essa associata, assegnandogli il pattern noto “ertertertert”.
Dopo il riavvio del computer abbiamo avviato la ricerca tramite WinHex delle tracce del pattern all’interno del disco restituendo i risultati mostrati nella figura 3.31.

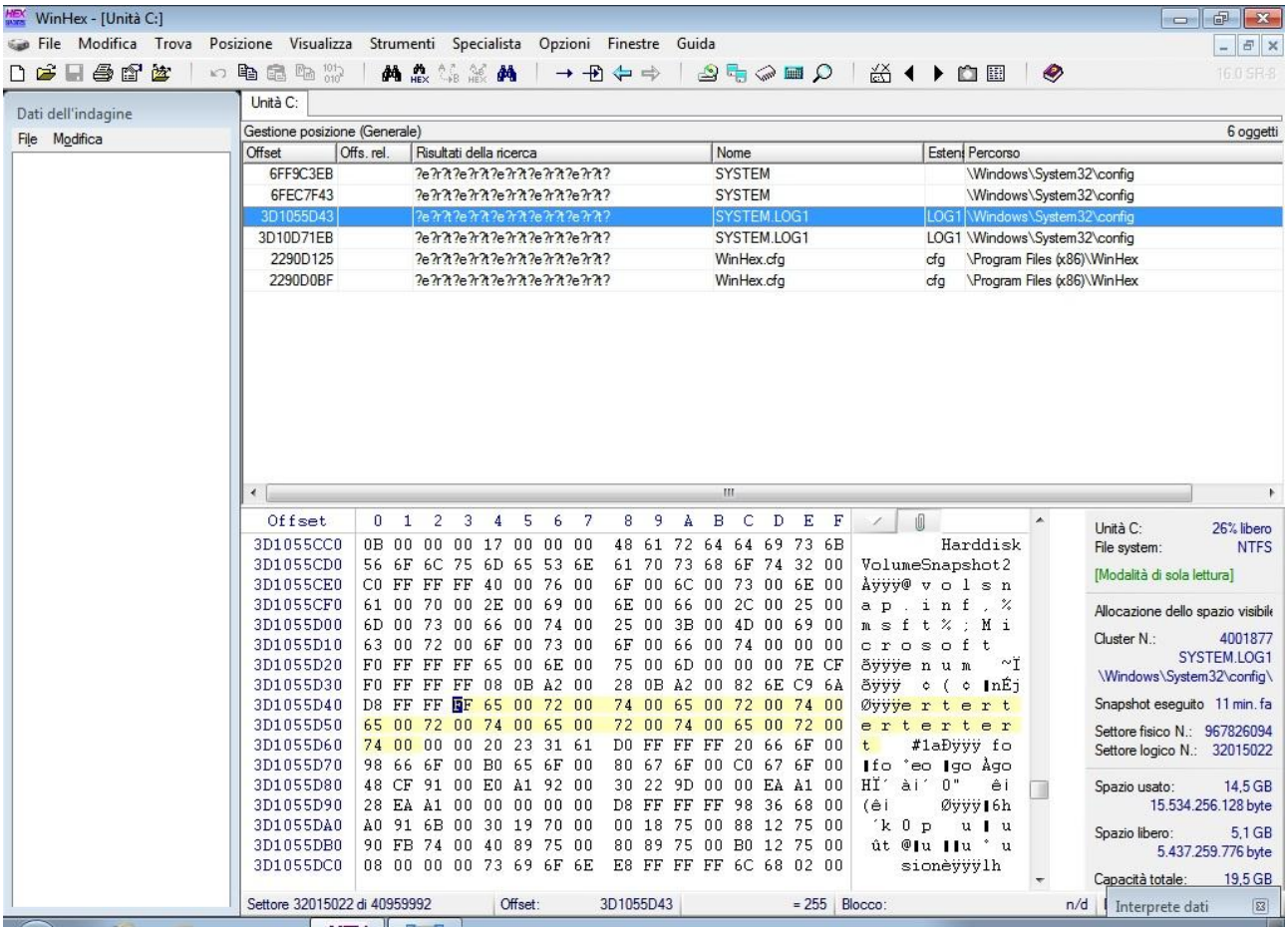


Figura 3.31 Risultati della ricerca del pattern noto “ertertertertert”

In seguito ad un ulteriore riavvio, abbiamo effettuato una nuova ricerca del pattern noto. Si nota dalla figura 3.32, che entrambi i file di log precedenti sono stati sovrascritti, come si evince dai settori evidenziati, nei quali risiedeva la traccia mostrata in figura 3.31. Il sistema però ha creato due altri file di log.

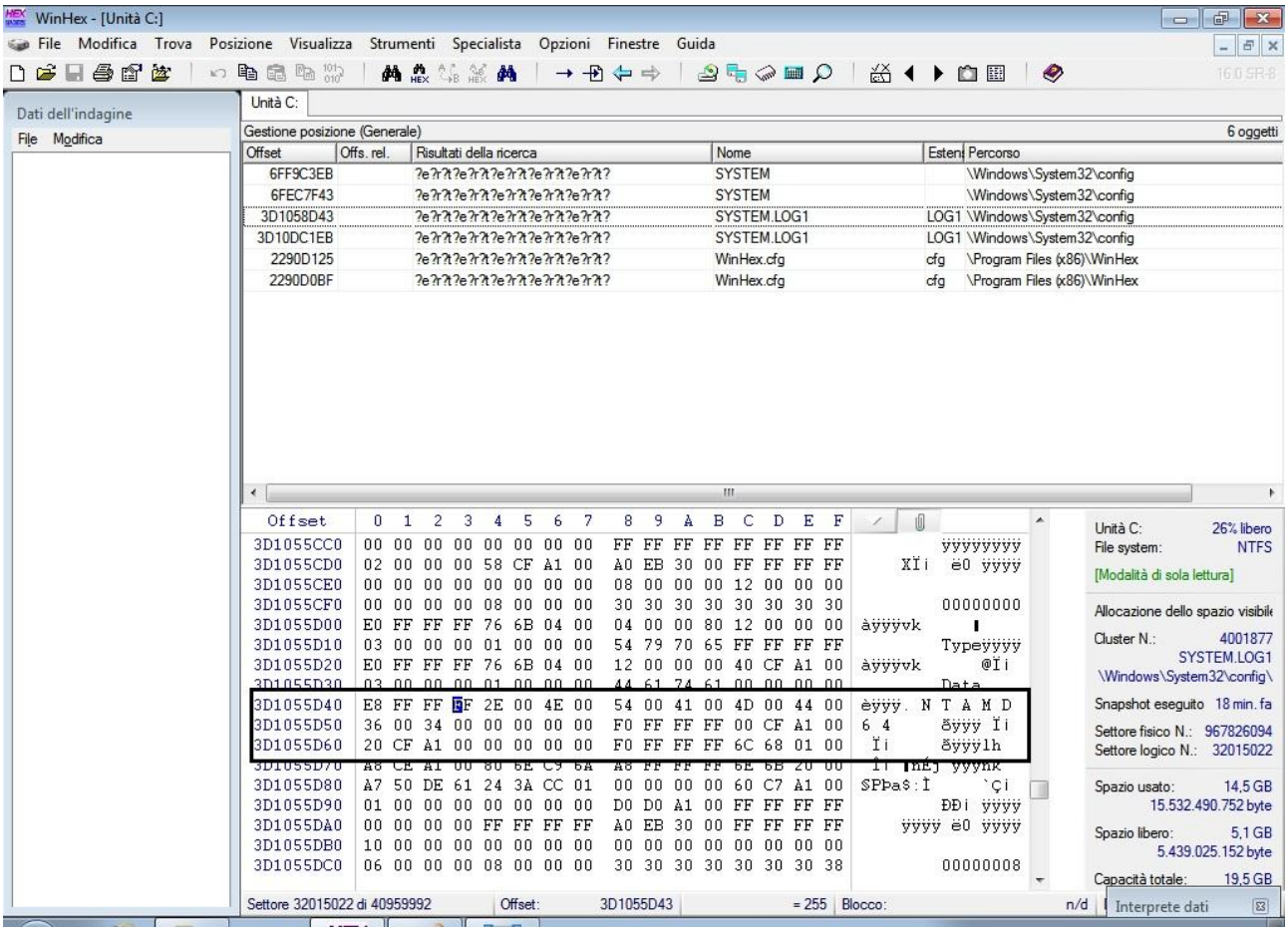


Figura 3.32 Settori sovrascritti nei quali risiedeva la vecchia informazione

Successivamente abbiamo cancellato l'intera sottochiave e riavviato il computer. Abbiamo avviato la ricerca e alcune informazioni sono state trovate, ma ci siamo poi accorti che, nel prosieguo della ricerca, il sistema operativo le aveva sovrascritte, infatti analizzando i settori restituiti dalla ricerca, essi risultano sprovvisti del pattern ricercato.

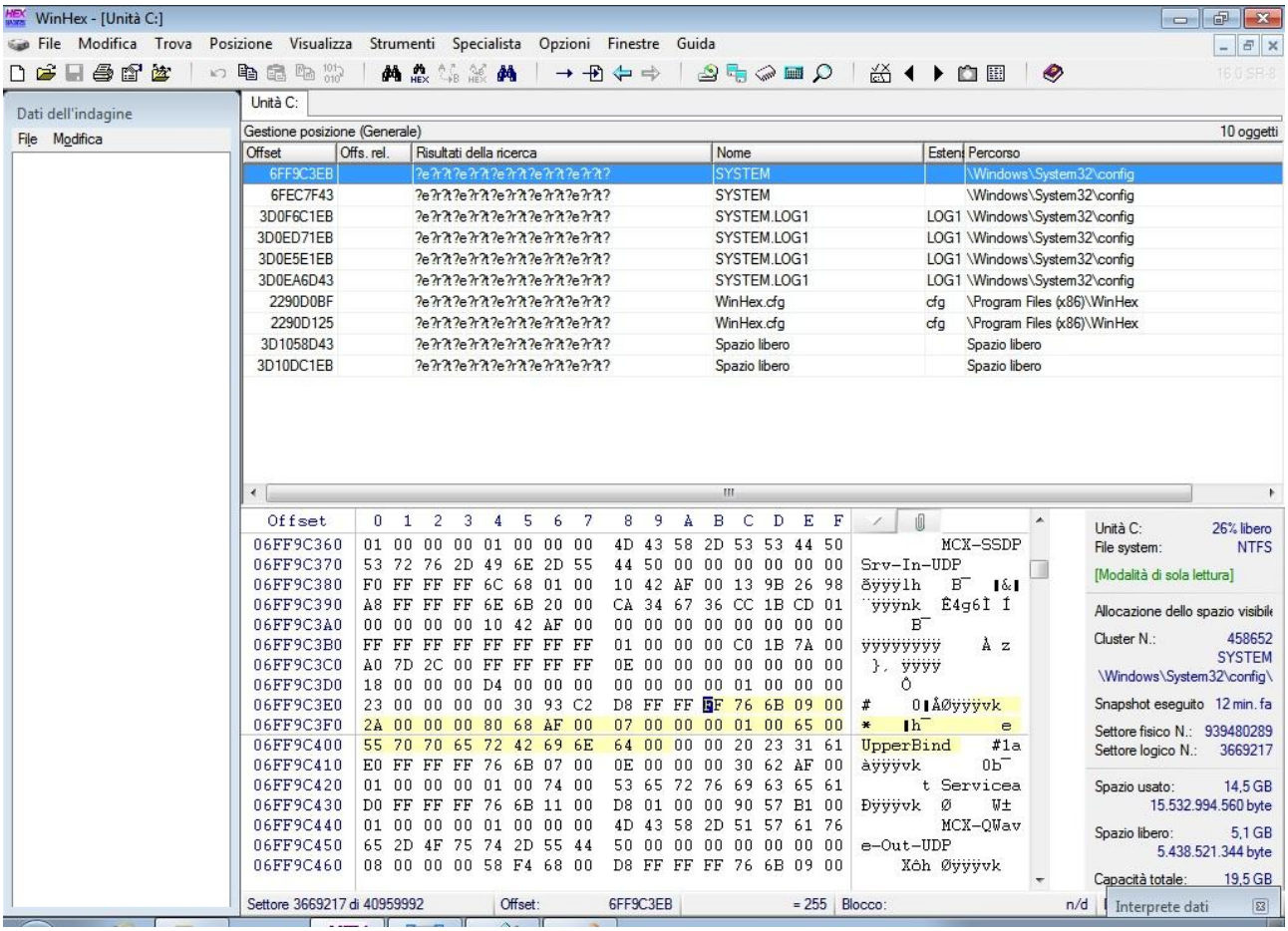


Figura 3.33 Nuova ricerca dopo la cancellazione della sottochiave

Per essere sicuri che realmente il sistema avesse sovrascritto il tutto, abbiamo effettuato nuovamente la ricerca del pattern noto e come si evince dalla figura 3.34, non sono state più trovate tracce.

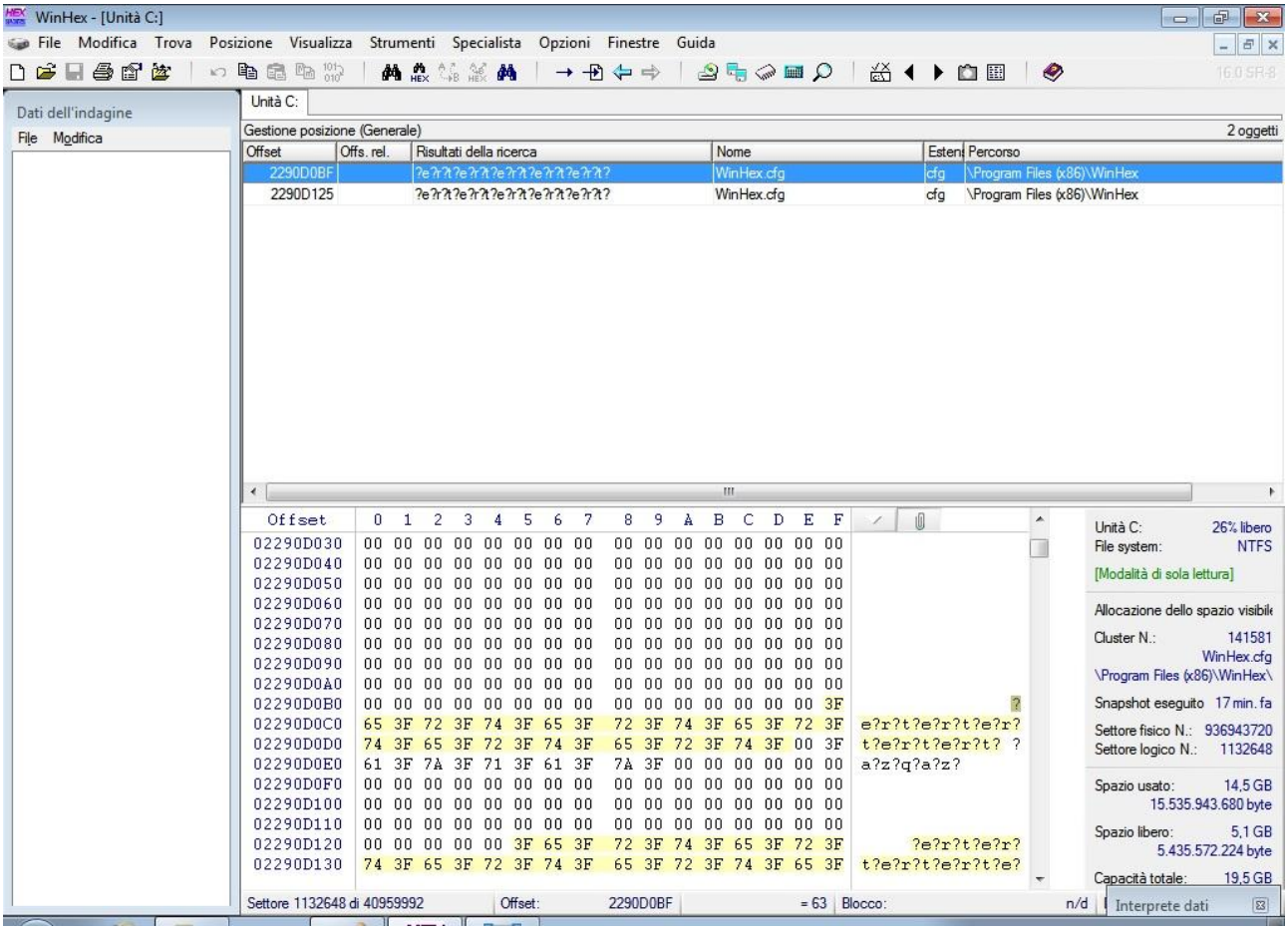


Figura 3.34 Ricerca del pattern noto e nessuna traccia trovata

Da questo caso di studio si evince che rimangono tracce dei valori anche precedentemente modificati e eliminati, però dopo l'uso normale del pc è possibile eliminare le tracce, anche con l'istallazione di un semplice driver di sistema.

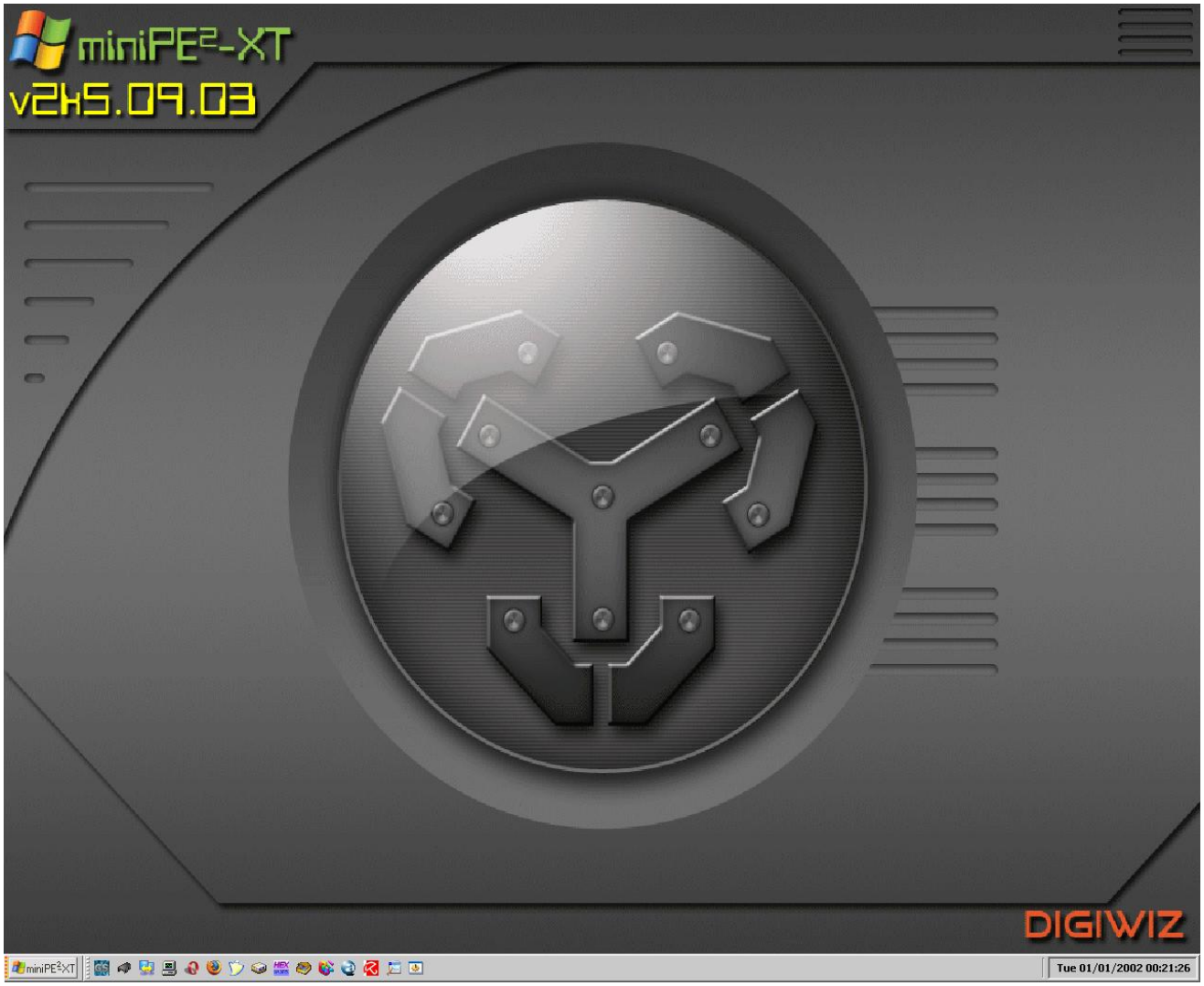
3.3.4 Utilizzo di MiniPe

Mostriamo ora un altro caso di studio, effettuato sul Registry di Windows 7 usando una versione live di Windows Xp, MiniPe, che fornisce dei tool per la manipolazione del registro di sistema e per la sua analisi.

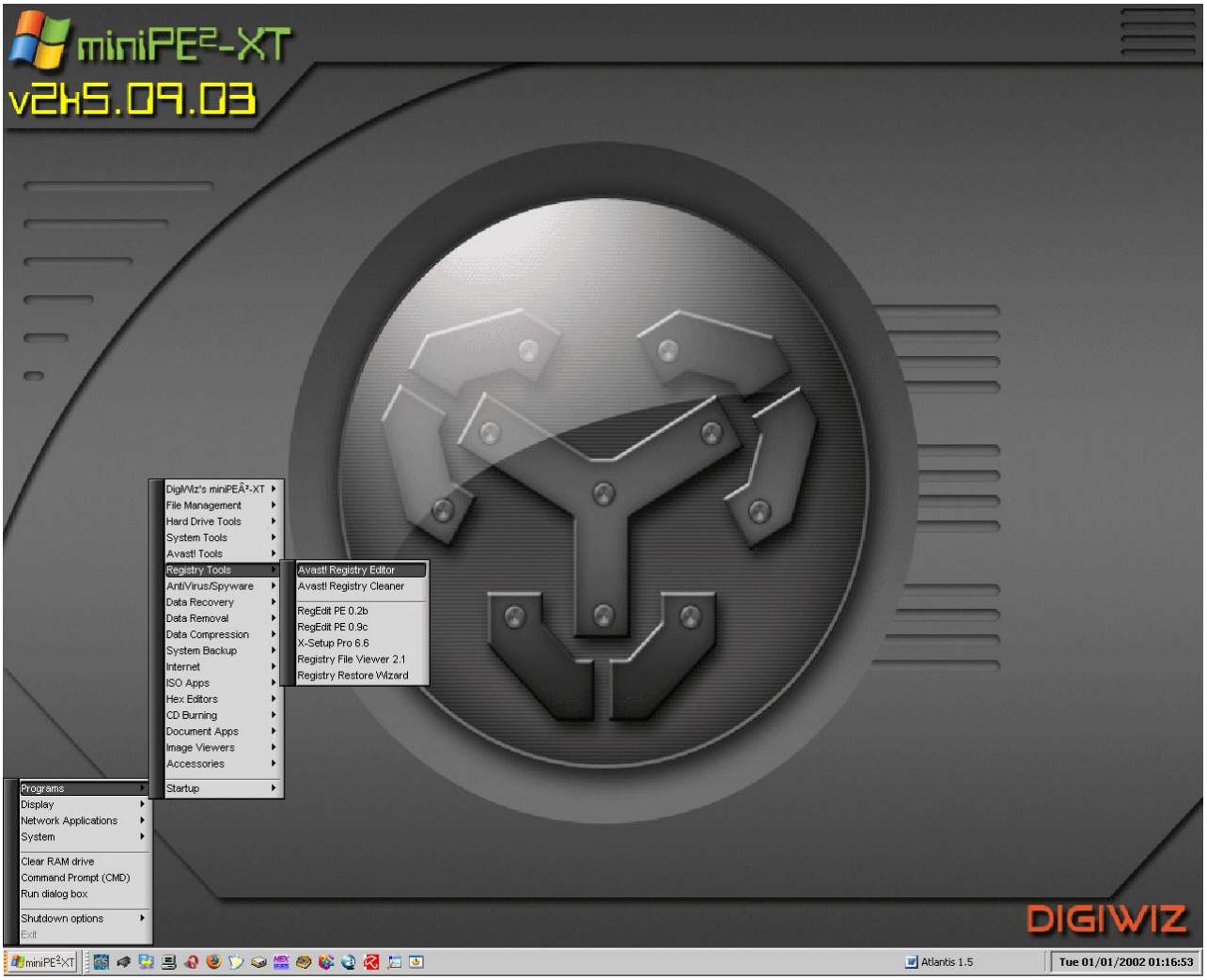
MiniPe

MiniPe è una live cd modificata del sistema operativo Windows XP che possiede una moltitudine di funzionalità e tool di ogni genere tra cui quelli necessari per modificare da remoto i registri del nostro Windows 7.
Per questo esperimento è stata usata la versione del 2009: miniPE^2-XT v2k5.09.03.
Nella figura sottostante vediamo la schermata iniziale del nostro cd live MiniPe.

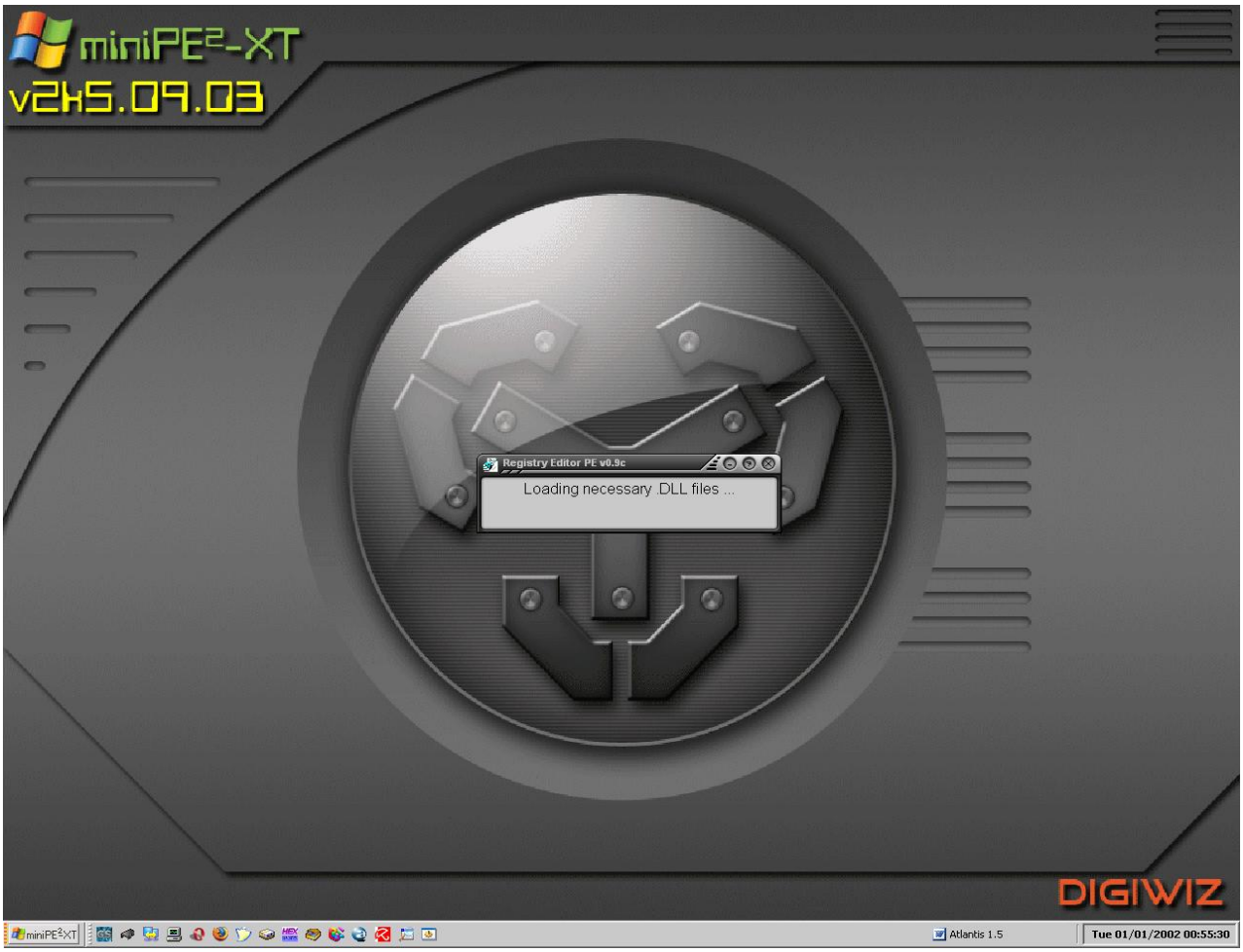
Verranno mostrati i passi per visualizzare, modificare e creare chiavi e valori tramite questo live cd da remoto.



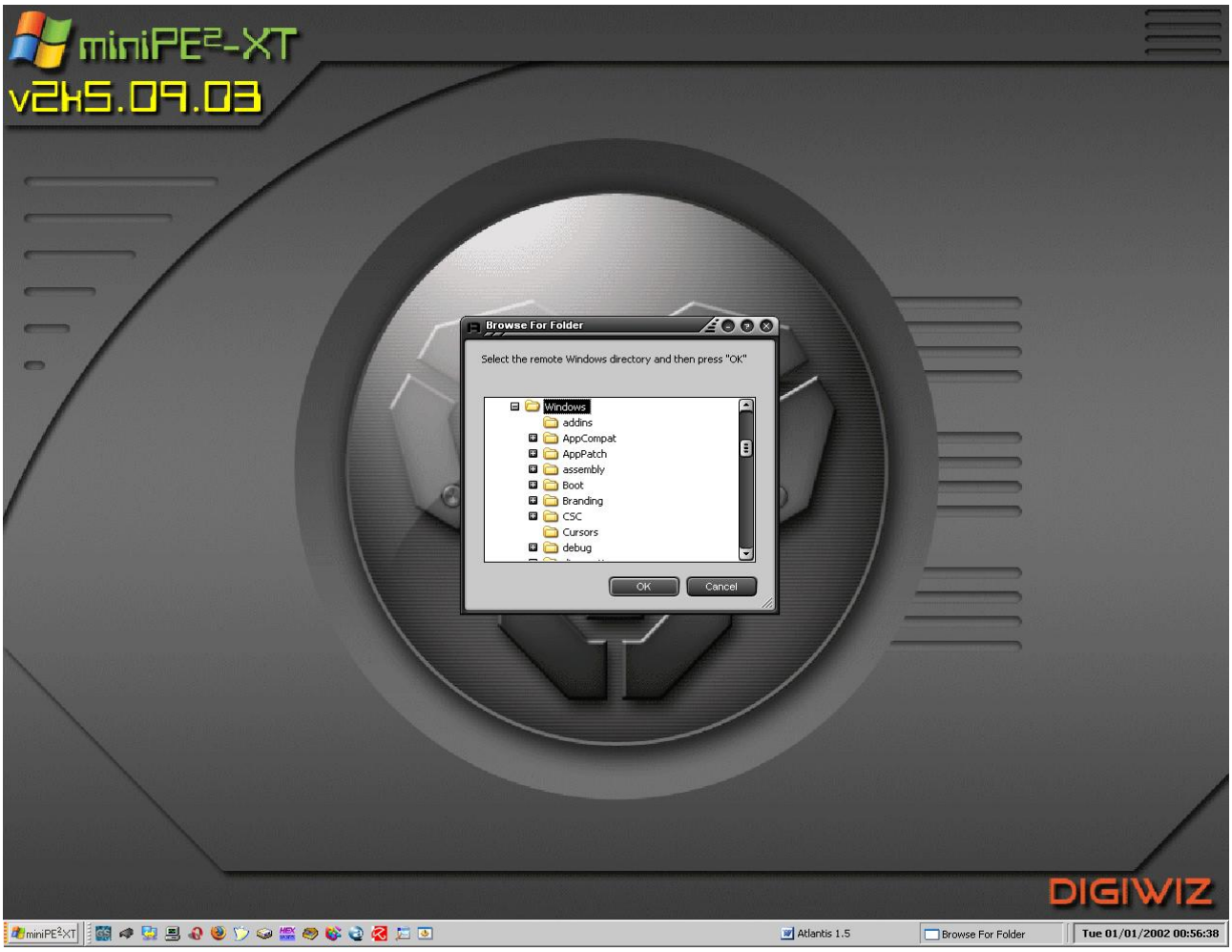
Per il nostro esperimento abbiamo utilizzato due tool compresi in MiniPe. Il primo è ***RegEdit PE 0.9C.***



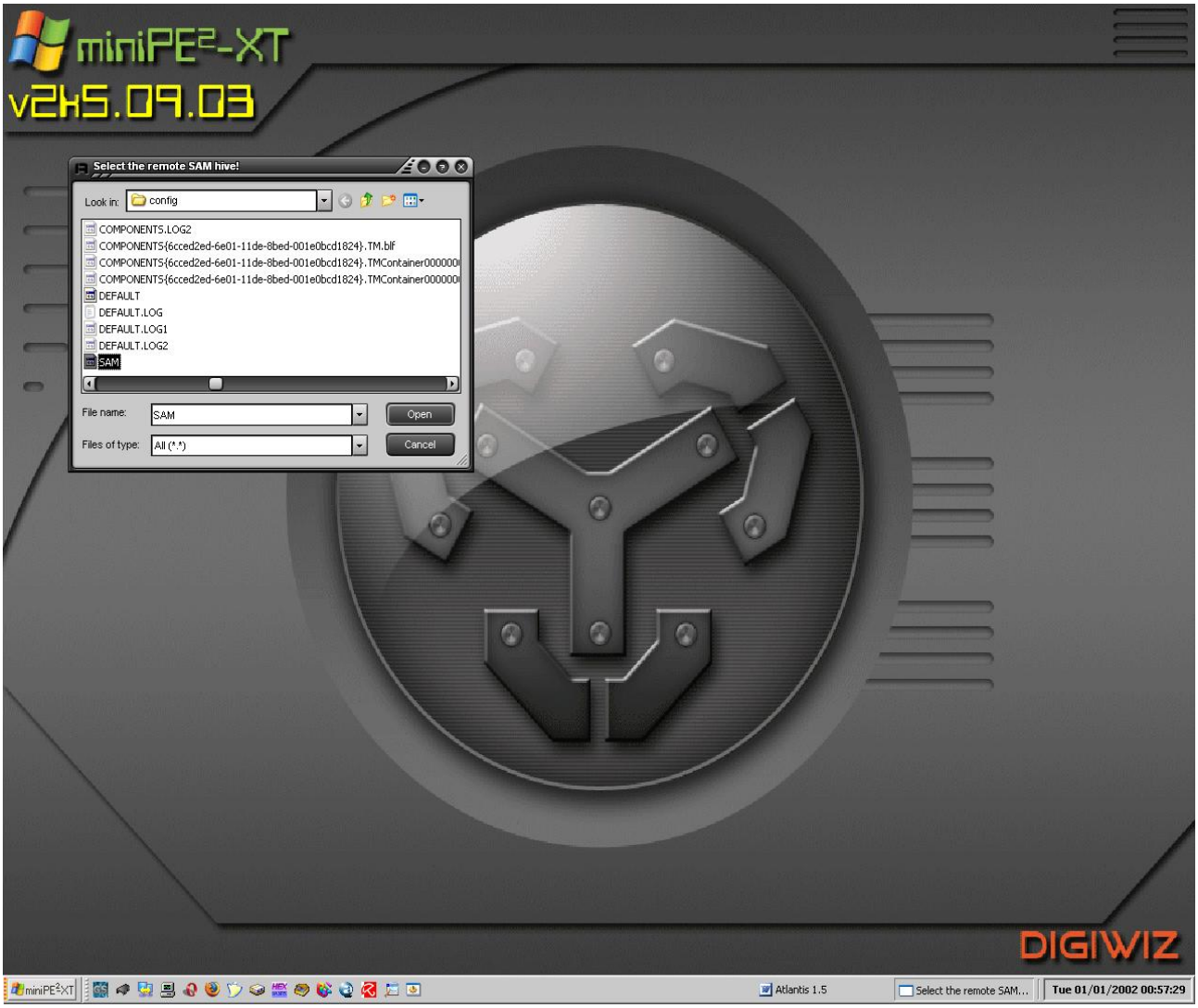
Il programma appena avviato comincia a caricare i file .DLL necessari.



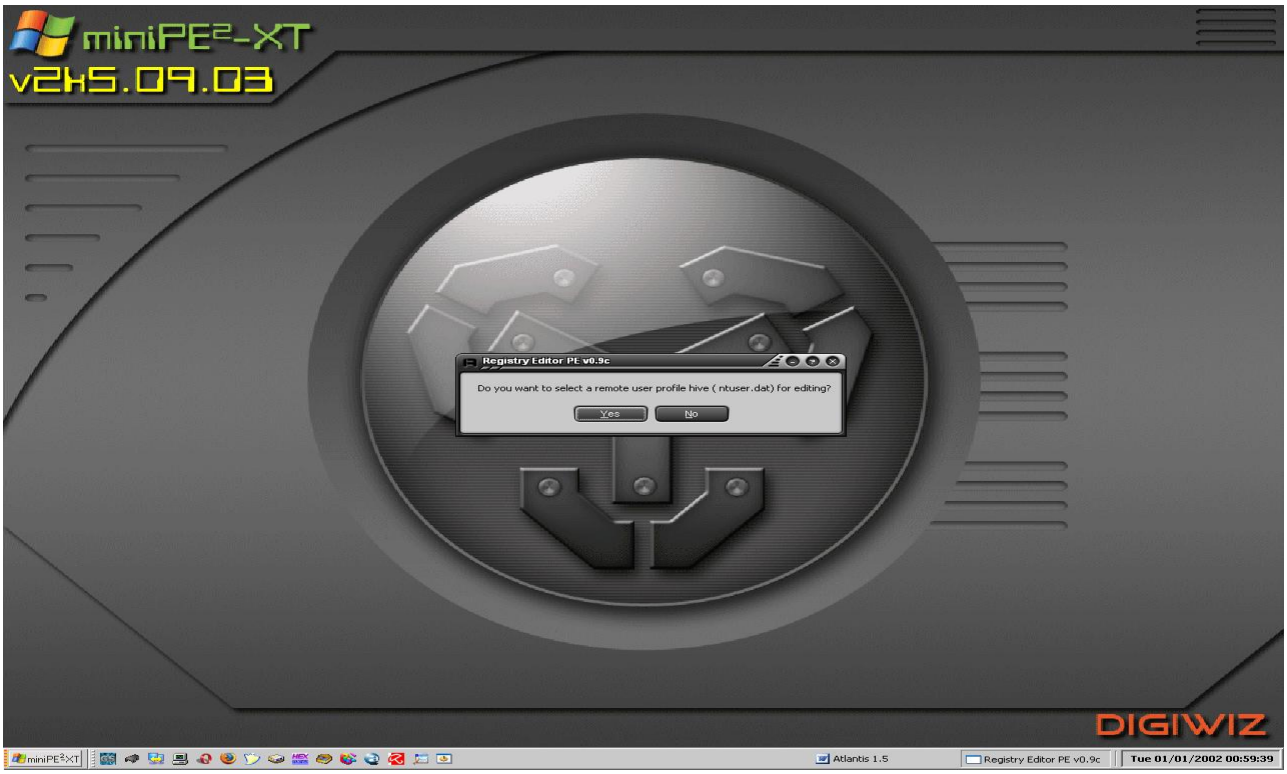
Il programma ci fa selezionare la cartella “Windows”, dalla partizione in cui è istallato il sistema operativo, per cominciare a prelevare i file di registro necessari per aprire l’intero Registro di Sistema di Windows 7.

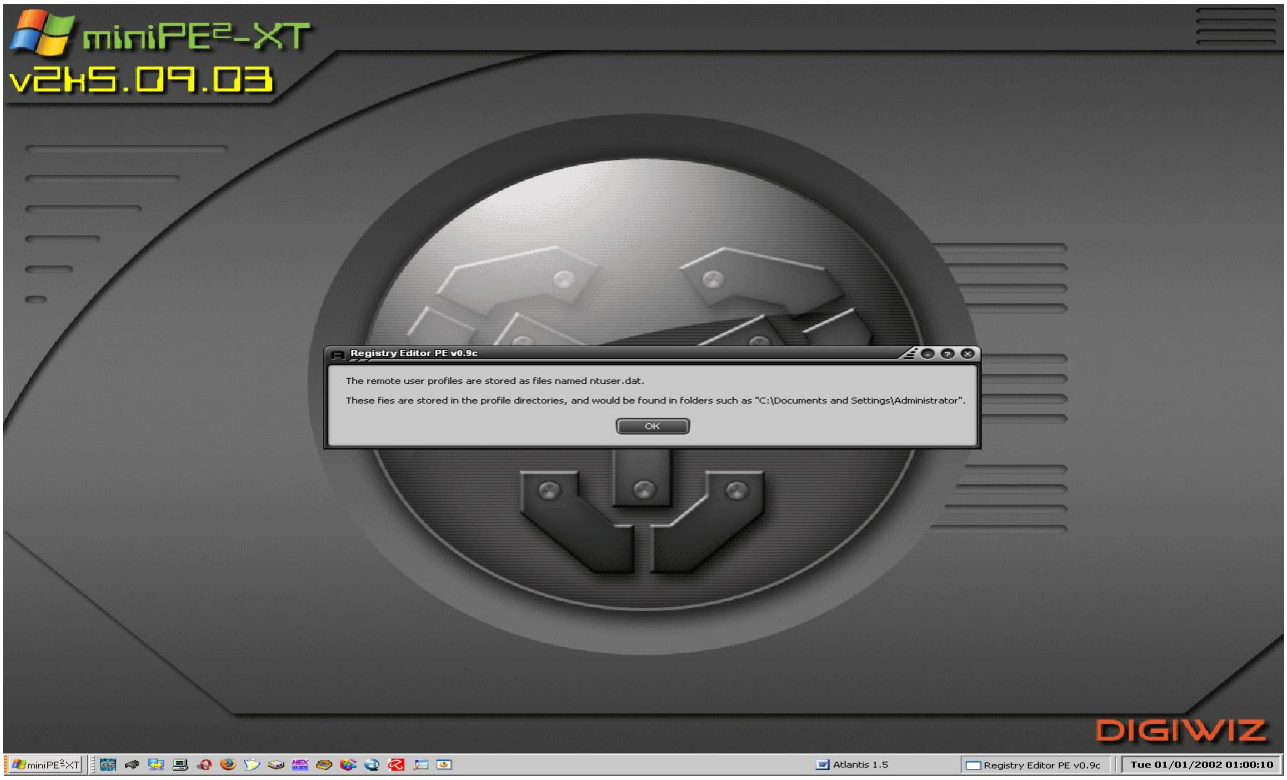


Selezioniamo i file SAM, SECURITY, SOFTWARE e SYSTEM da cui caricare il Registro di Sistema.

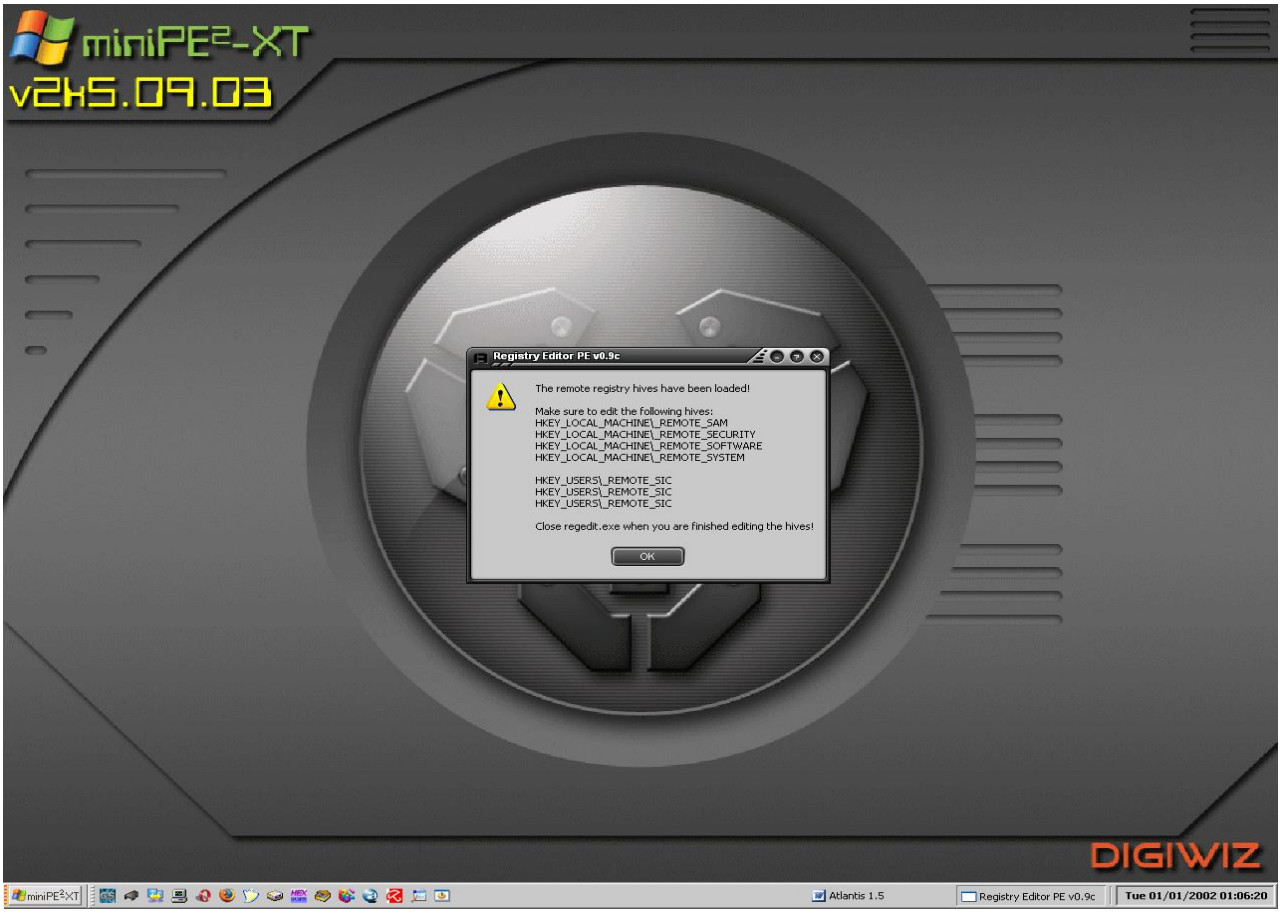


Scegliamo un nostro profilo remoto già esistente ntuser.dat utilizzabile per l'editing.

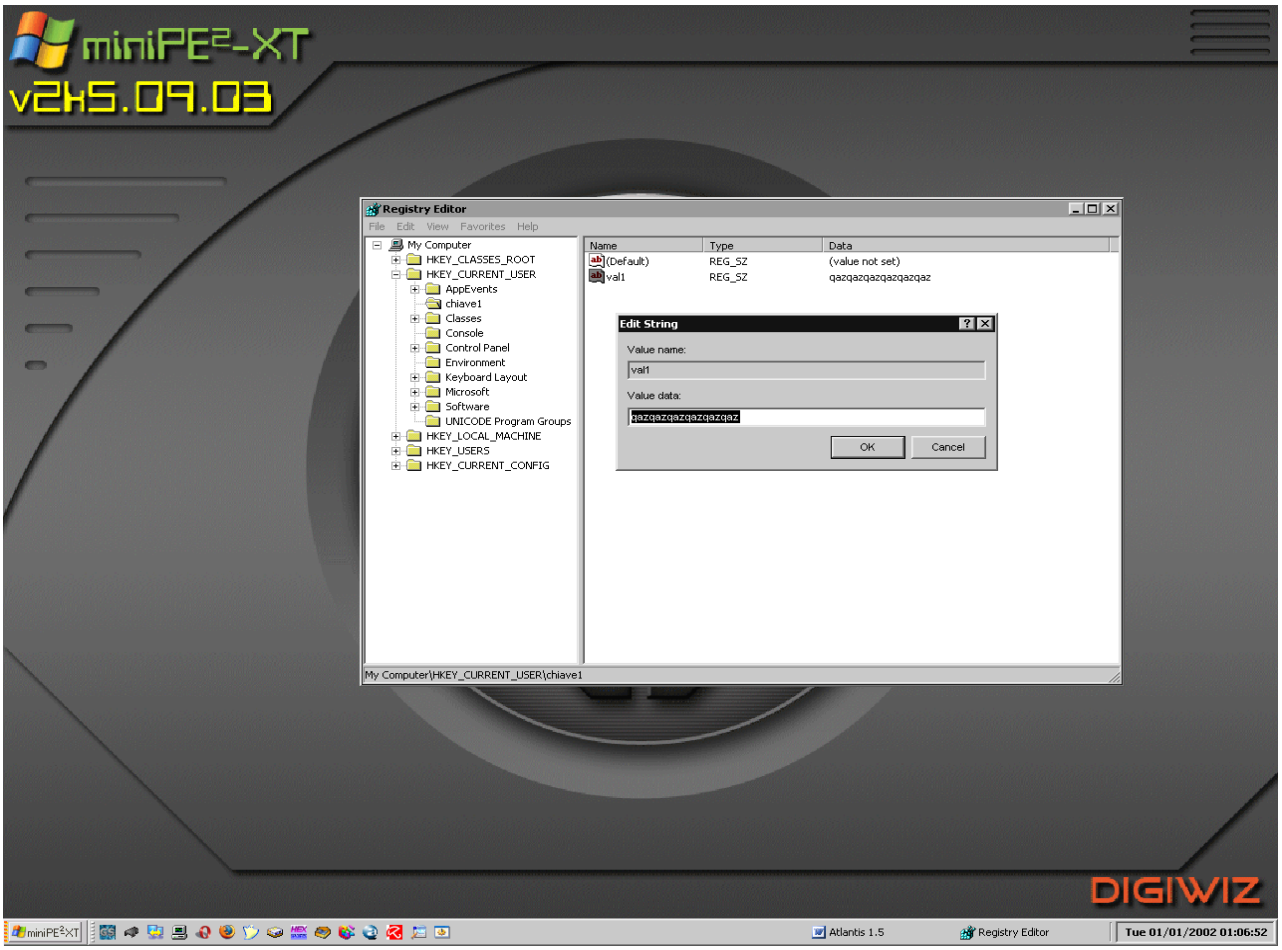




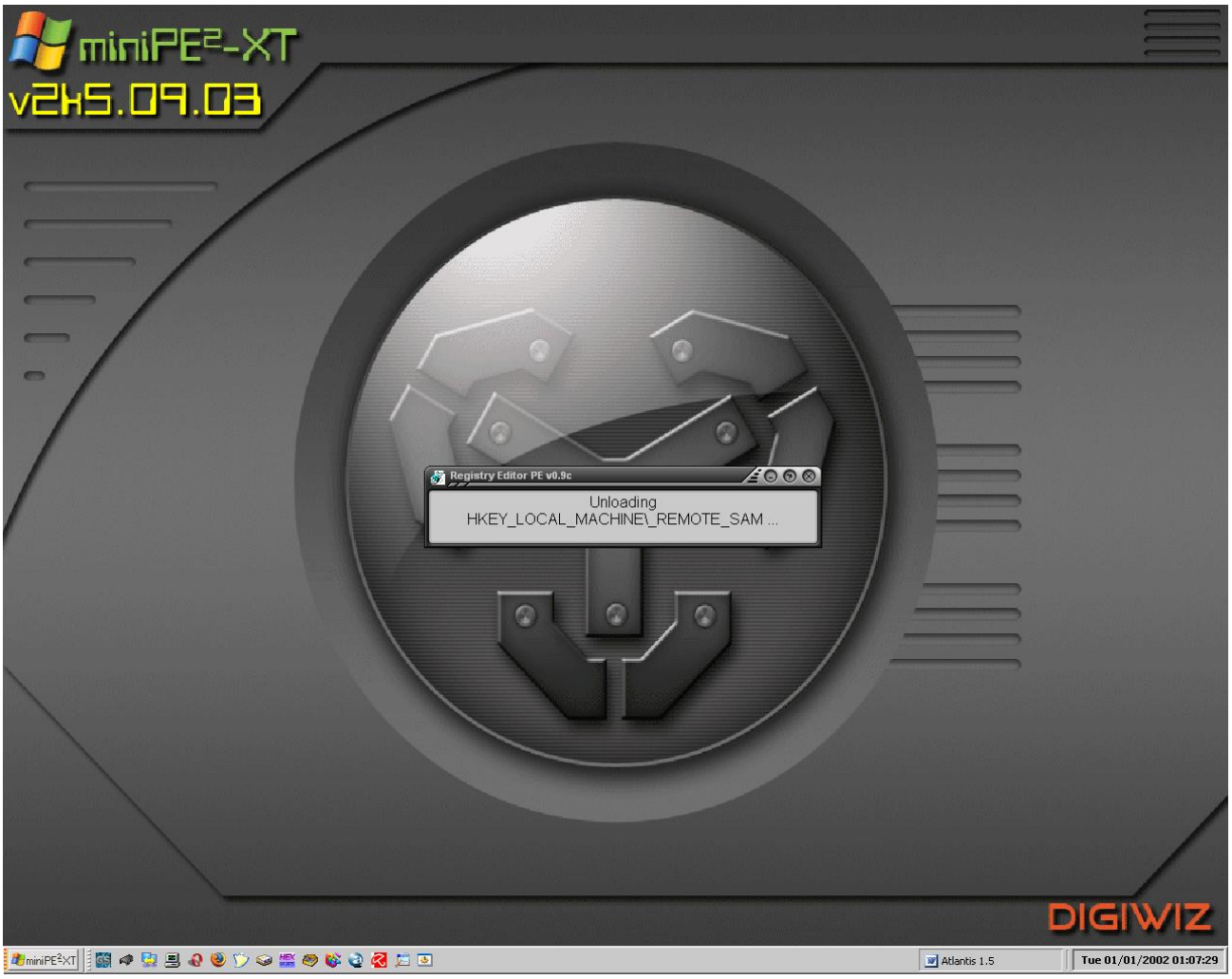
Nella schermata sottostante è visualizzato il form che indica che il registro remoto di Windows 7 è stato caricato con successo.



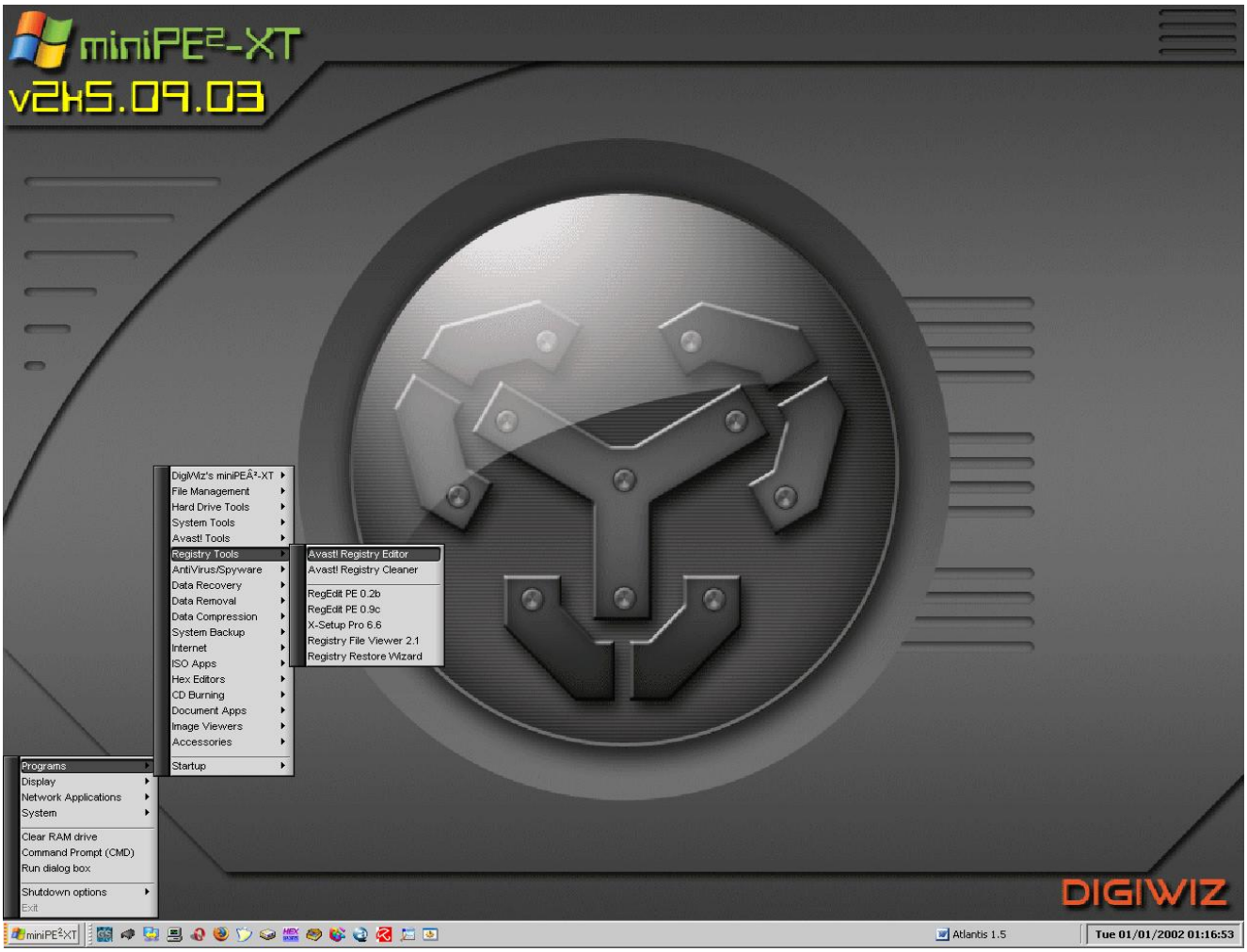
Si riesce senza problemi a modificare o a creare una chiave di registro come si evince nella schermata sottostante, in cui è mostrata la creazione di una sottochiave “chiave1” con un proprio valore che ha nome “val1” e dati valore “qazqazqazqazqazqaz”.



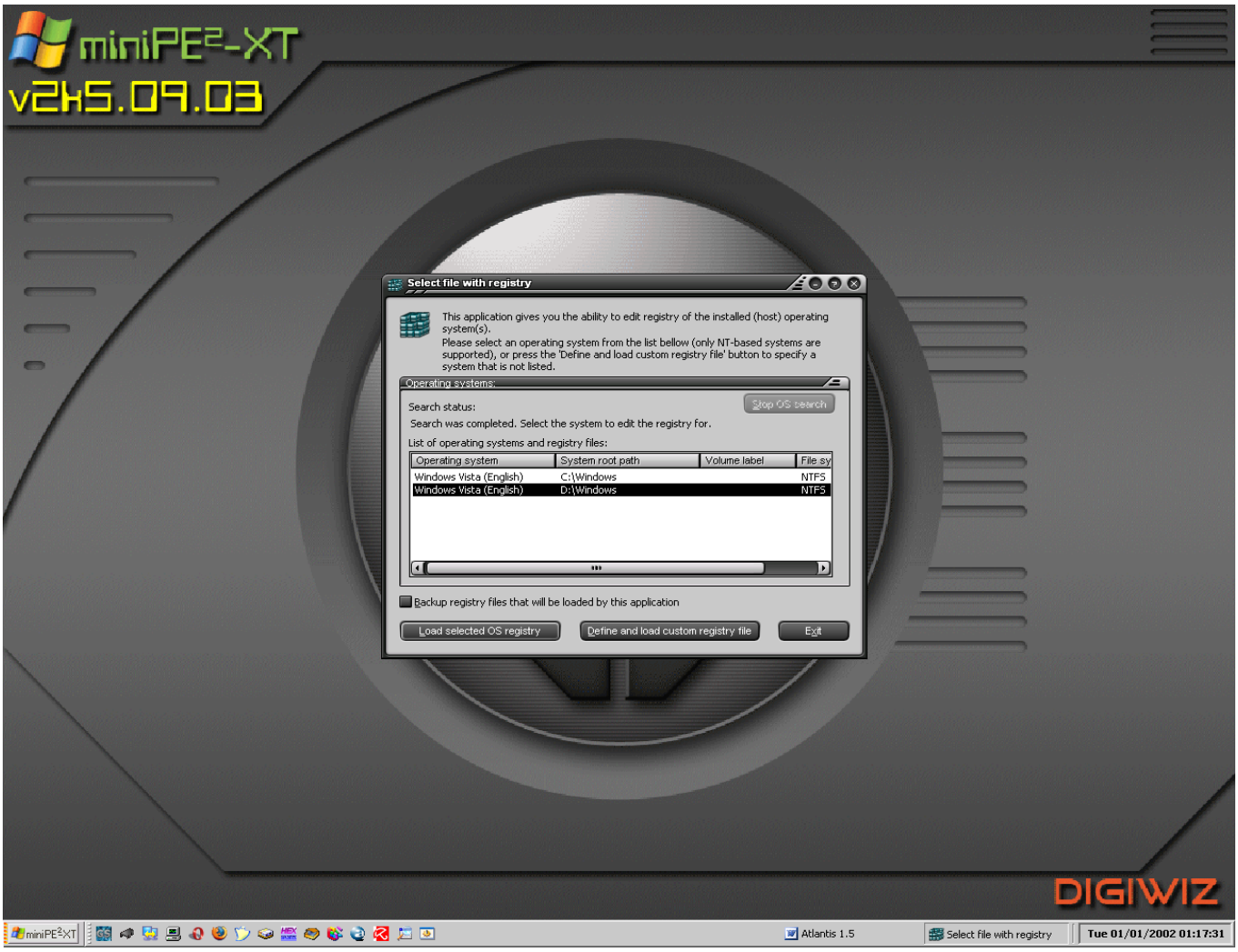
Alla fine, quando il programma viene chiuso, i file precedentemente allocati vengono deallocati.



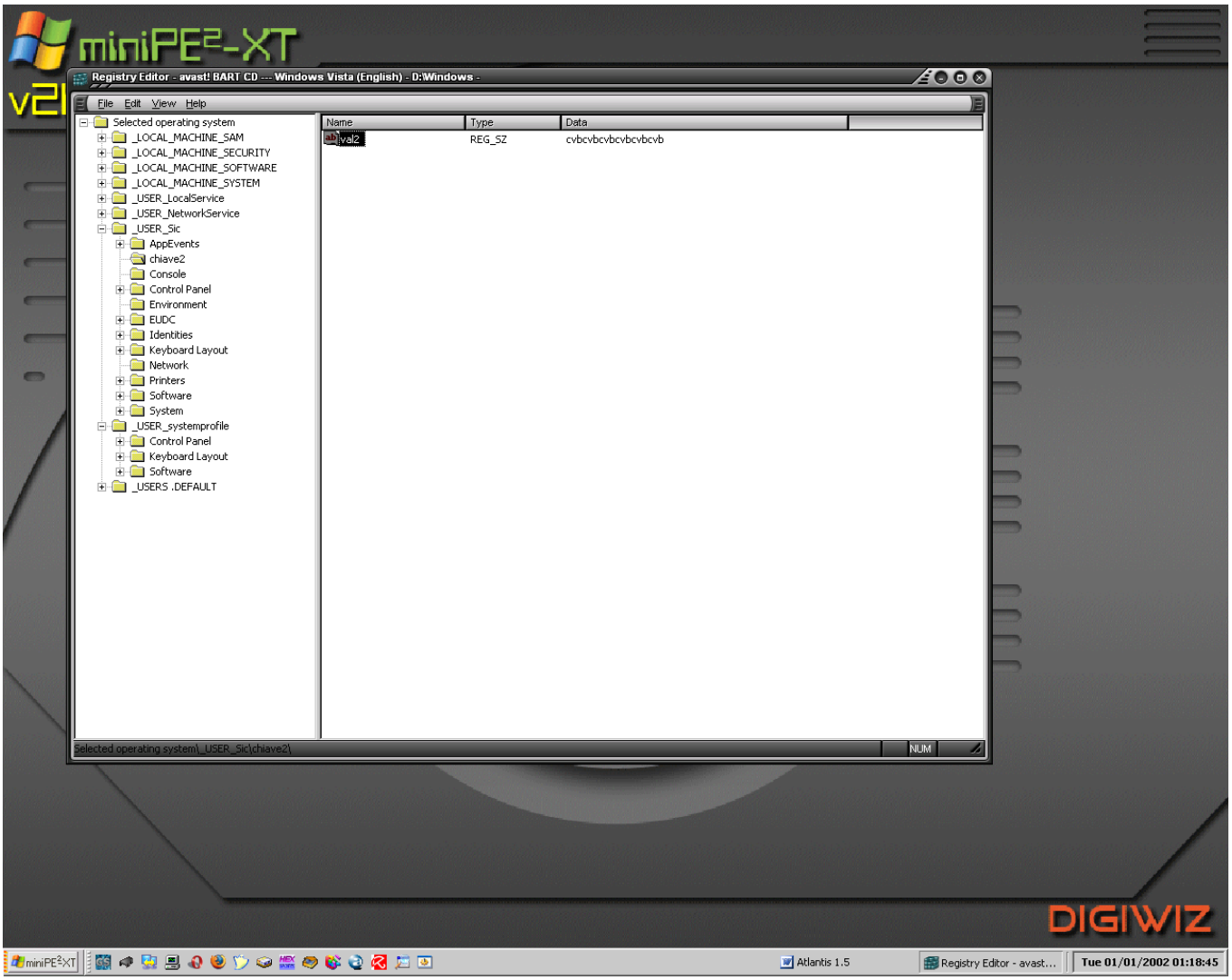
Il secondo tool di editor di registri che mostriamo è: ***Avast Registry Editor***.



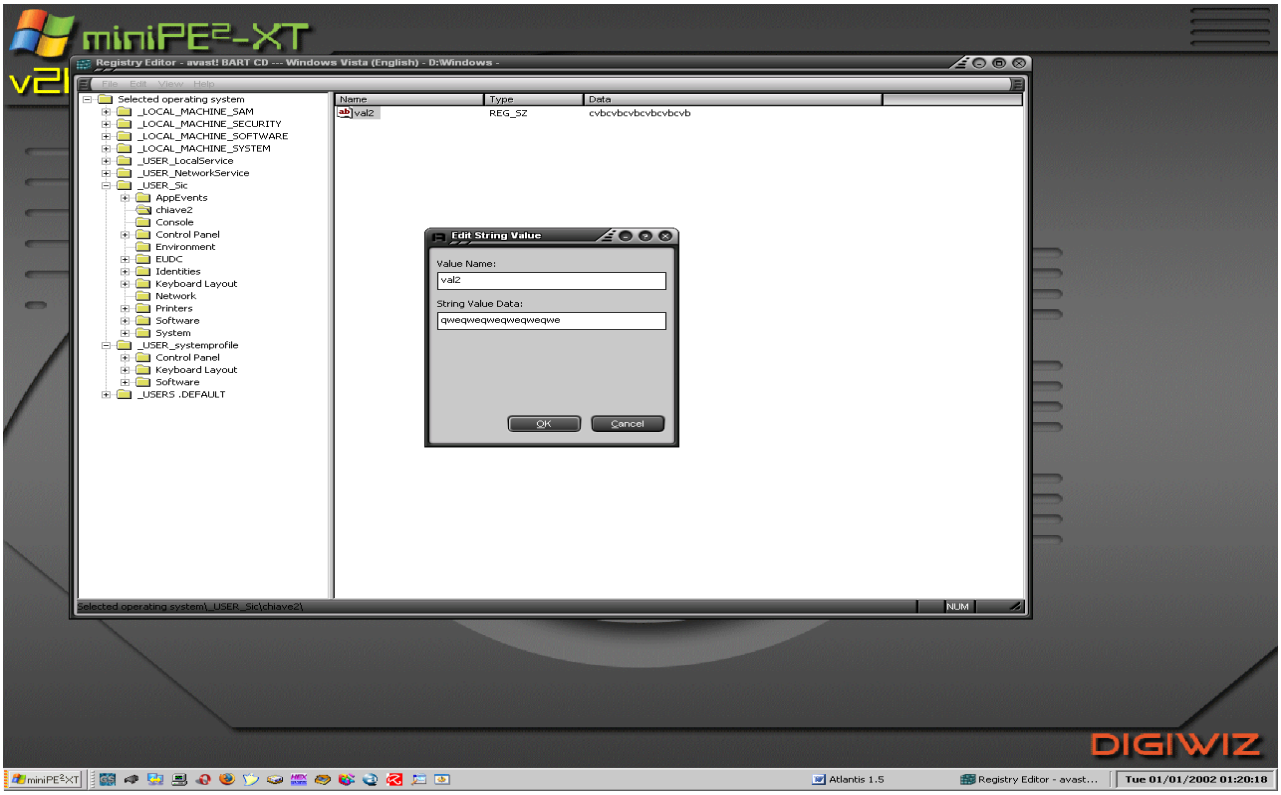
Il programma fa scegliere la partizione desiderata dove risiede il sistema operativo di cui visualizzare i registri.
Vediamo che il software identifica il nostro sistema operativo come Windows Vista, perché nel 2009 Windows 7 non era ancora stato rilasciato. Sostanzialmente non ci sono molte modifiche tra Windows Vista e 7, per cui le operazioni possono ritenersi valide anche per Windows 7.

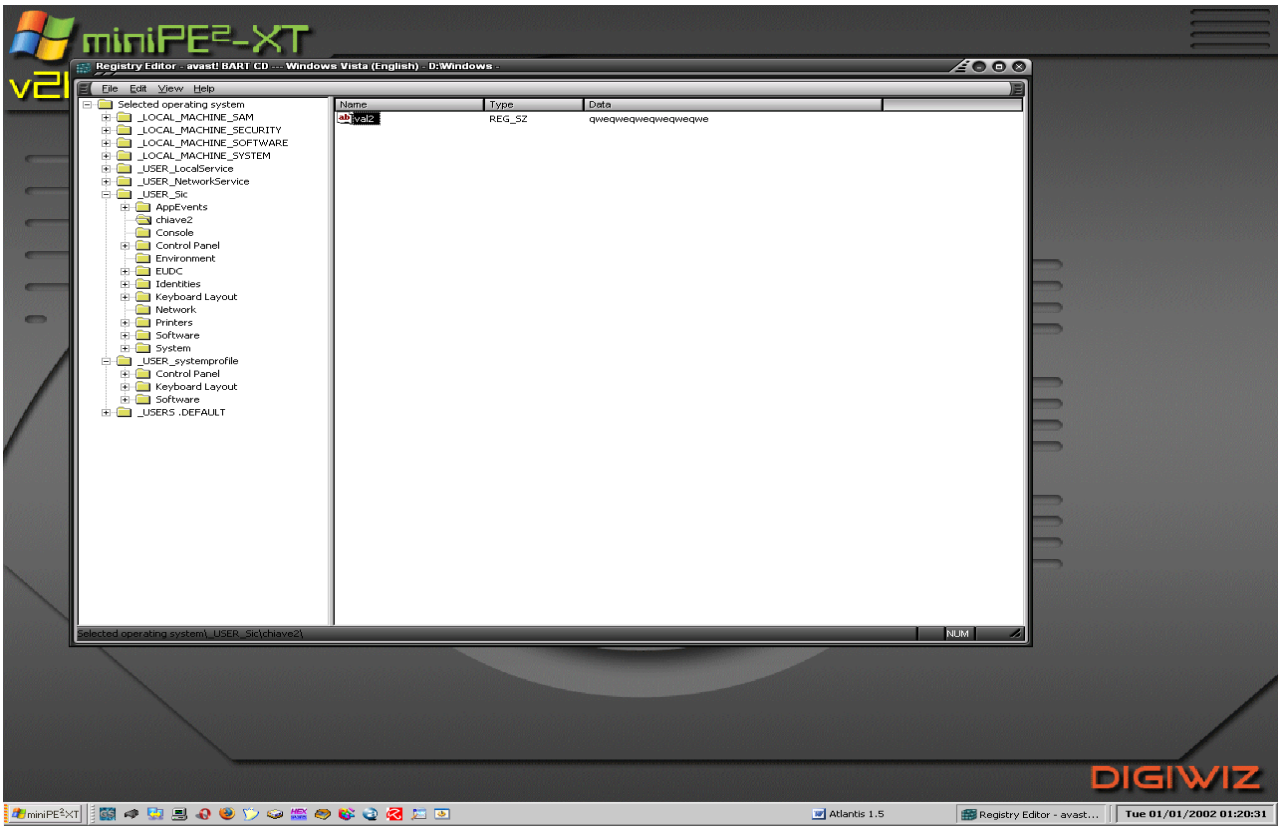


Nella schermata sottostante viene mostrato che il programma ha aperto correttamente il Registro di Sistema. Inoltre è possibile visualizzare anche la chiave e valore creati direttamente sul RegEdit di Windows 7.

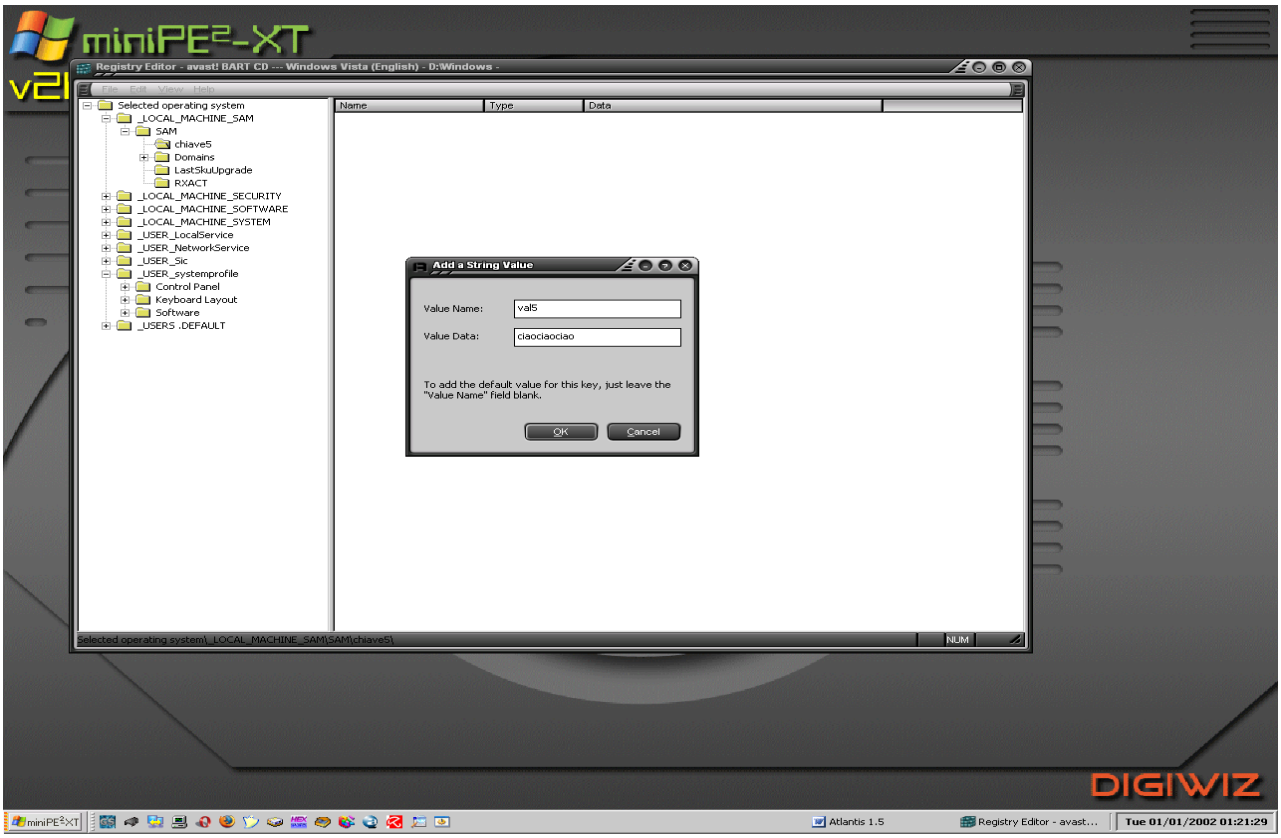


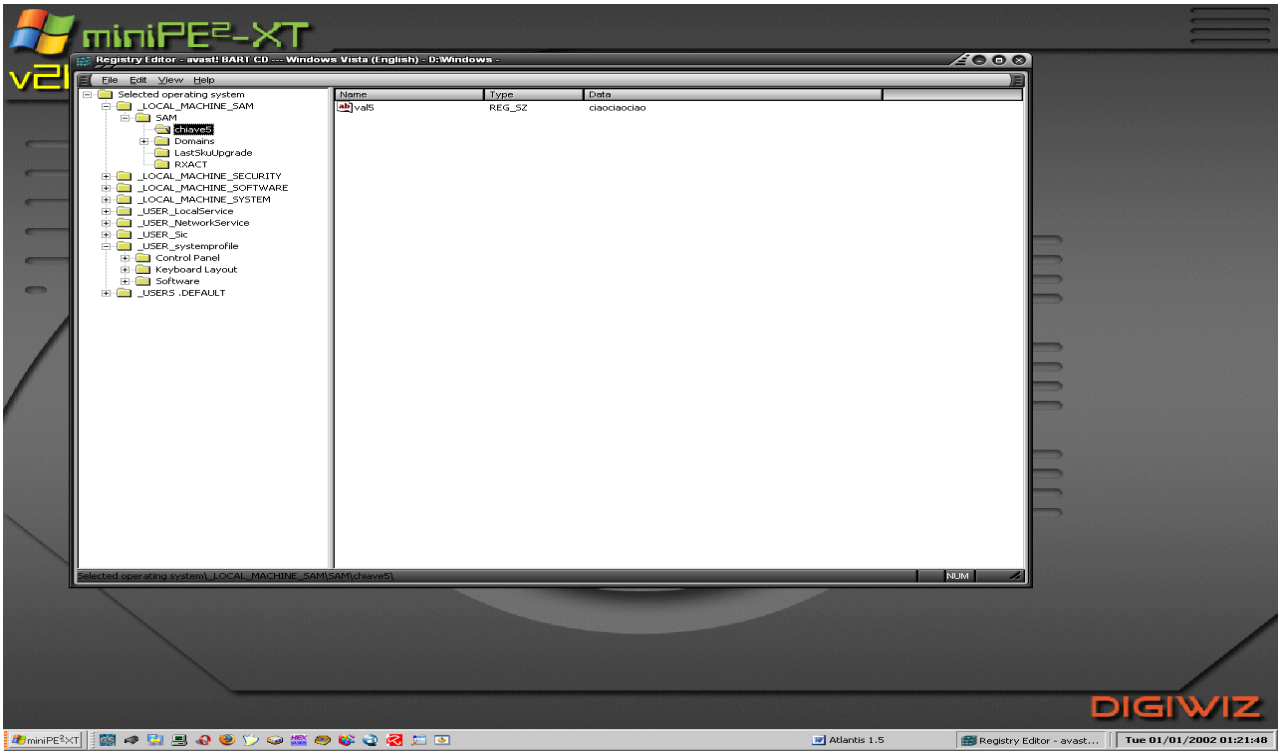
Viene modificato il valore di “val2” della sottochiave “chiave2” da “cvbcvbcvbcvbcvbcvb” a “qweqweqweqweqweqwe”.



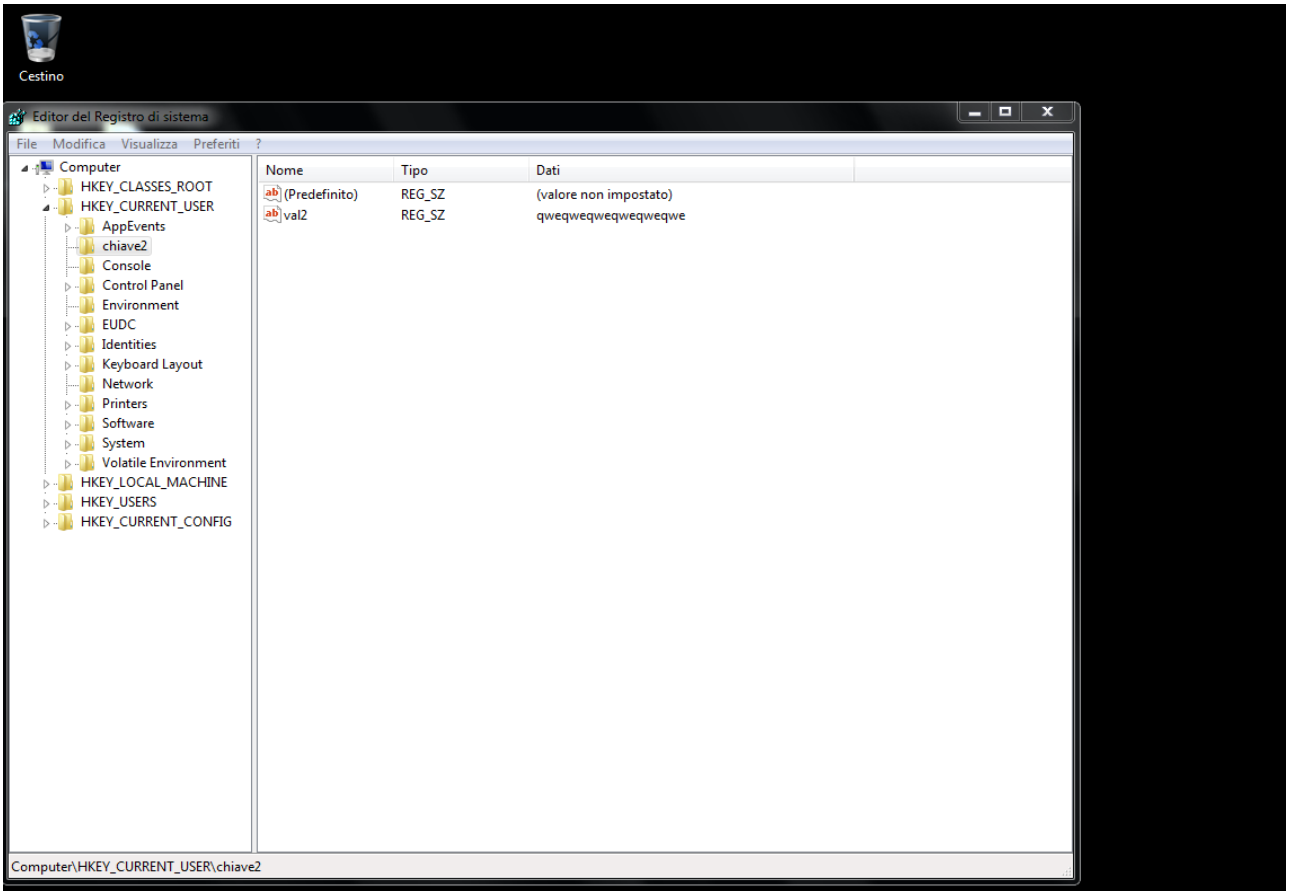


È possibile anche creare nuove chiavi come evidenziato nelle schermate sottostanti, in cui è mostrata la creazione di una sottochiave “chiave5” con nome valore “val5” e dati valore “ciaociaociao” in “SAM”.





Successivamente viene mostrato la schermata di RegEdit di Windows 7 dopo la modifica della sottochiave “chiave2” tramite Avast Registry Editor, come mostrato in figura:



Conclusioni

Nonostante il File System NTFS e il Registry di Windows, siano ancora dei territori non del tutto esplorati in campo di Digital Forensics, abbiamo mostrato quali possono essere gli strumenti utili da utilizzare per ispezionare il Sistema Operativo più conosciuto ed utilizzato al mondo e in quali punti, sia del File System e sia del Registry, andare ad usarli per scovare tracce di interesse forense. Da tutto questo lavoro comunque viene messo in evidenza l'interessante verità di un sistema operativo non del tutto trasparente e che comunque lascia spazio alla possibilità di nascondere le tracce e di contro, l'importante certezza che ciò che l'utente crede di aver eliminato definitivamente è solo apparenza, perché infatti con gli strumenti giusti e delle buone conoscenze di fondo, è possibile recuperare dati che sembravano invece cancellati da tempo. Comunque sia, è pur sempre importante per un investigatore forense conoscere a fondo il mondo dei sistemi operativi Windows, così che in qualsiasi momento e nelle sedi competenti, sia possibile poter mettere al servizio della verità delle armi importanti.

Bibliografia

I. Casey, E. *Handbook of Digital Forensics and Investigation.* Cap. 5 *Windows Forensic Analysis*. 2010 Elsevier Academic.

II. Farmer Derrick J., *A Forensic Analysis of the Windows Registry*. Champlain College (Vermont). 2007 http://eptuners.com/forensics/contents/examination.htm.

III. Khawla.A.Alghafli, Andrew Jones, Thomas Anthony Martins. *Forensic Analysis of the Windows 7 Registry*. Australian Digital Forensics Conference, Security Research Centre Conferences. 2010 Edith Cowan University Reserch Online