



Sistemi operativi Windows

Corso di Informatica Forense - OIG
Facoltà di Giurisprudenza
Università degli studi di Bologna

dr. Stefano Fratepietro

m@il: fratepietro@cirsfid.unibo.it
skype: stefano.fratepietro



CIRSFID



stevlab.net

Contenuti

- Storia di Microsoft Windows
- Introduzione al File System
- Principali caratteristiche
- Principali locazioni di dati

Storia I

- La prima versione di Microsoft Windows fu la versione 1.0 rilasciata nel 1985; essa non era un vero e proprio sistema operativo ma un programma lanciato da console DOS che rappresentava una serie di comandi in modalità grafica
 - **Mancava completamente il supporto per le reti di computer Windows e di altri sistemi operativi**
 - **Il sistema era mono utenza**
 - **Concetti di sicurezza inesistenti**

Storia II

- Dal 1992 Microsoft sviluppò il supporto per le reti informatiche anche per i sistemi desktop, così nacquero:
- Windows 3.1
 - Windows 3.11
 - Ancora sistema mono utente
 - Possibilità di utilizzare una rete IP
 - Primi concetti di sicurezza applicati ad un sistema casalingo



Storia IV

Arrivo di Windows 2000 nel 1999

- Fu introdotto con successo sia nel mercato dei server che delle workstation
- Primo sistema operativo Microsoft compatibile con le allora nuove architetture a 32 bit
- Adozione di NTFS anche per i sistemi user
- Windows 2000 adottava una serie di caratteristiche, in particolare l'interfaccia utente da Windows 98, che lo resero abbastanza user-friendly e molto più stabile
- Introduzione del primo Windows Update
- Introduzione di Active Directory



Storia V

Arrivo di Windows Xp nel 2001

- Sviluppato sulle basi di Windows 2000
- Migliorato il supporto hardware, soprattutto per periferiche multimediali e di dispositivi di memorie di massa
- Migliorata la stabilità
- Obbligo di utilizzo di NTFS
- Supporto per sistemi multi processore
- Disponibile una versione anche per architetture a 64bit



Storia VI

Arrivo di Windows Vista nel 2006

- Sviluppato con codice ex novo
(dicono loro)
- Nuova versione del file system NTFS
- Nuovo boot loader
- Nessun cambiamento sostanziale per la struttura ad albero delle directory che è rimasta invariata



Contenuti

- Storia di Microsoft Windows
- **Introduzione al File System**
- Principali caratteristiche
- Principali locazioni di dati



File system I

- In informatica, un file system è un meccanismo con il quale i file sono immagazzinati e organizzati su un dispositivo di archiviazione, come un hard disk o un CDROM
- Formalmente, un file system è l'insieme dei tipi di dati astratti necessari per la memorizzazione, l'organizzazione gerarchica, la manipolazione, la navigazione, l'accesso e la lettura dei dati



File system II

- I file system generalmente usano dispositivi di archiviazione che offrono l'accesso ad un array di blocchi di dimensione fissa, generalmente in settori di 512 byte l'uno
- Il file system è responsabile dell'organizzazione di questi settori e tiene traccia di quali settori appartengono a quali file, e quali invece non sono utilizzati



Tipi di File System I

- Amiga FileSystems - OFS, FFS1 e 2, International, PFS, SFS usati su Amiga
- BFS (Beos File System) - file system nativo di BeOS
- DFS , ADFS - file system della Acorn
- EFS (IRIX) - un vecchio file system a blocchi usato su IRIX
- Ext2 - Extended File System 2, diffuso su sistemi GNU/Linux
- Ext3 - Extended File System 3, diffuso su sistemi GNU/Linux (ext2+journaling)
- FAT - Usato su DOS, Microsoft Windows e su molti dispositivi dedicati, dispone di tabelle a 12 e 16 bit
- FAT32 - versione con tabelle a 32 bit di FAT
- FFS - Fast File System, usato in vecchi sistemi BSD
- HFS - Hierarchal File System, usato su vecchie versioni di Mac OS
- HFS+ - Hierarchal File System Plus, usato sulle versioni recenti di Mac OS e su Mac OS X



Tipi di File System II

- HPFS - High Performance File System, usato su OS/2
- ISO 9660 - Usato su dischi CD-ROM e DVD-ROM (anche con estensioni Rock Ridge e Joliet)
- JFS - Journaling File System, disponibile su sistemi GNU/Linux, OS/2, e AIX
- LFS - Log-structured File System
- Minix - Usato su sistemi Minix
- NTFS - New Technology File System. Usato su sistemi basati su Windows NT
- ReiserFS - File system journaling diffuso su sistemi GNU/Linux
- UDF - File system a pacchetti usato su supporti WORM/RW, CD-RW e DVD
- UFS - Unix File System, usato su vecchi sistemi BSD
- UFS2 - Unix File System, usato su nuovi sistemi BSD
- UMSDOS - File system FAT esteso con permessi e metadata, usato su GNU/Linux
- XFS - Usato su sistemi IRIX
- ZFS - Creato dalla Sun



Network File System

- AFS (Andrew File System)
- AppleShare
- CIFS (conosciuto anche come SMB o Samba)
- Coda
- GFS
- InterMezzo
- Lustre
- NFS



Caratteristiche generali

Dal punto di vista dell'utente un file system è composto da due elementi:

- File: collezione di informazioni correlate composte da
 - Nome: Stringa di caratteri che identifica un file nel file system
 - Tipo: Associazione di un file ad un software per la sua lettura/utilizzo (non in tutti i sistemi operativi)
 - Locazione e dimensioni: Dimensioni e posizionamento del file all'interno del file system
 - Data ed ora: Informazioni relative alla data della creazione del file e alla sua ultima modifica
- Directory: un insieme di informazioni per organizzare e fornire informazioni su file che compongono il file system (**armadio di file**)



Caratteristiche generali

Generalmente il file system è composto da:

- Superblock: Contiene informazioni sul tipo di file system
- Tabelle per la gestione dello spazio libero
- Tabelle per la gestione dello spazio occupato (non su tutti i File System)
- Root directory: Directory radice del file system (/)
- File e directory

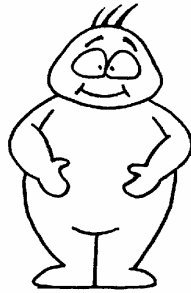


Tipi diversi di file

- MS-Dos: Massimo 8 caratteri per il nome del file e massimo 3 per l'estensione
- Windows 9x e derivati da tecnologia NT: Nomi ed estensioni di lunghezza fino a 255 + 3 caratteri con associazione dell'estensione del file al relativo software che permette la lettura/esecuzione del file
- Linux, Unix e Mac OS X: Nomi di lunghezza variabile, manca completamente il concetto di estensione del file.



File System FAT

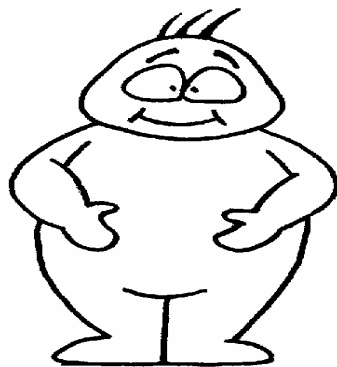


Caratteristiche FAT

- Gli elementi della FAT sono di lunghezza fissa, pari a 16 bit, non è possibile indirizzare più di 65535 cluster e poiché un cluster non può essere maggiore di 32768 byte, il file system ha un limite massimo superiore di 2 Gbyte per la dimensione della partizione.
 - FAT: File Allocation Table - Tabella di allocazione dei blocchi
 - Root directory: La directory di livello gerarchico più elevato
 - Sotto directory: Le directory di livello inferiore alla radice
 - Clusters: blocchi che contengono i dati dei file



File System FAT 32



Caratteristiche FAT32

- Per superare i limiti sulla dimensione dei volumi imposta dal FAT16, Microsoft decise di creare un nuovo FAT chiamato FAT32, con cluster da 32 bit, anche se in realtà ne vengono utilizzati solo 28
- In teoria questo dovrebbe permettere 268.435.438 (228) cluster, cioè una dimensione totale dell'ordine dei 2 terabyte
- In realtà a causa delle limitazioni all'interno del sistema operativo, non è permesso al FAT di superare i 4.177.920 (224) cluster, riducendo la dimensione massima a 124.55 gigabyte
- Le utilities di formattazione e partizionamento di Windows 2000 e XP hanno un limite di 32 GB per le partizioni FAT32, ma è un limite arbitrario

Tutto questo prima della sp2 di XP e sp4 di 2000, allo stato attuale non dovrebbe essere cambiato nulla



File System NTFS

- I nomi dei file e delle cartelle possono essere lunghi fino a 255 caratteri e possono contenere caratteri di tutte le lingue del mondo grazie alla codifica Unicode
- La dimensione dei volumi e il massimo numero di file sono "praticamente" illimitati; la dimensione del volume può raggiungere al massimo i 256 Terabytes(232 clusters - 1), il numero limite di files è invece di circa 4,3 miliardi (232 - 1)
- La dimensione massima di un singolo file è di 16 Terabytes, contro i 4 GigaBytes di FAT e FAT32
- Supportati gli hard link



File System NTFS

- Affidabilità - NTFS è un sistema transazionale, questo vuol dire che se un'operazione è interrotta a metà (ad esempio per un blackout) viene persa solo quell'operazione ma non è compromessa l'integrità del file system
- Permessi e Controllo d'Accesso - a ciascun file o cartella è possibile assegnare dei diritti di accesso (lettura, scrittura, modifica, cancellazione e altri)



Struttura logica I

- L'albero "generico" del file system FAT di una partizione, ad esempio c:/ (dove la lettera C sta per il nome della partizione), è composto da una root directory "/" dove sono contenute tutti i file e le directory del sistema
- I file "vitali" del sistema operativo sono contenuti nella cartella Windows di default
- I file dei software installati generalmente sono contenuti nella directory Programmi (Program Files)
- **Documenti e file utente sono contenuti nella cartella "Documents and settings" (solo nelle versioni sviluppate con tecnologia NT)**



Struttura logica II

- In "Documents and settings" si trovano tutti i profili utente racchiusi in cartelle nominate con il nome utente dell'account di appartenenza
- All'interno dei profili utente vi sono le sottocartelle dei profili locali del Desktop e dei software utilizzati dall'account

"Documents and settings è generalmente un buon contenitore di file dove trovare elementi rilevanti per le indagini"



Contenuti

- Storia di Microsoft Windows
- Introduzione al File System
- **Principali caratteristiche**
- Principali locazioni di dati

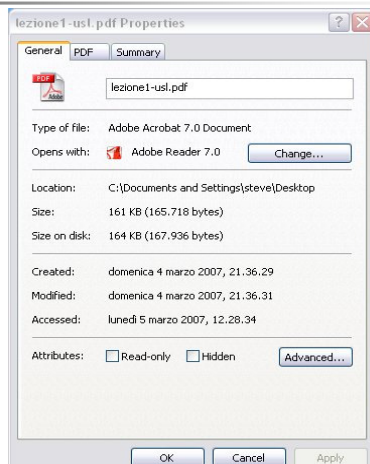


Precisazioni

- Nel caso di un computer non collegato ad un dominio Windows, tutte le informazioni risiedono localmente
- Nel caso di un computer collegato ad un dominio Windows, alcune informazioni "potrebbero" risiedere sul server Active Directory
 - Potrebbero perché dipende sempre dalla configurazione che è stata data al sistema



Proprietà di un file



Alternate Data Stream I

- **Solo su NTFS**, le informazioni su file e cartelle sono memorizzate in una tabella chiamata **Master File table (MFT)**. In questa regione del disco ogni file è identificato da una collezione di oggetti chiamati attributi; tra questi troviamo, per esempio, il nome assegnato al file, la data di creazione e, ovviamente, i dati che ne rappresentano il contenuto
- NTFS permette la creazione di più di un attributo dati per ogni singolo file. Il flusso dati principale, quello che tradizionalmente consideriamo il contenuto del file, può quindi essere affiancato da uno o più **flussi dati alternativi**.
- possiamo paragonare gli ADS agli allegati di un messaggio di posta elettronica in cui il flusso dati principale rappresenta il corpo dell'email.



Alternate Data Stream II

- Microsoft implementò ADS in NTFS per consentire a Windows NT di poter operare come file-server per i sistemi Macintosh basati sul filesystem HFS
- Il filesystem di Apple infatti memorizza dati supplementari relativi al file, quali icone e altri metadati, in una struttura separata simile ad un ADS; In questo modo i sistemi Mac potevano operare in modo trasparente sui dati presenti sul server NT
- Con Windows 2000 l'uso degli stream alternativi si è esteso tant'è che, per ogni documento, ora è possibile memorizzare informazioni aggiuntive quali titolo, oggetto, autore, parole chiave ecc. attraverso la scheda Riepilogo presente nelle Proprietà del relativo file. Queste meta-informazioni vengono salvate in appositi ADS di sistema



Alternate Data Stream III

Si elencano alcune caratteristiche degli ADS che possono permetterne un utilizzo "ambiguo":

- Sono virtualmente invisibili per l'utente e per i programmi che non li supportano
- La dimensione del file visualizzata dal sistema è sempre e solo quella del flusso principale
- Possono essere allegati a file ma anche a cartelle
- Possono contenere qualsiasi tipo di dato: un semplice testo, una immagine ma anche script e codice eseguibile
- È possibile l'esecuzione diretta di un ADS eseguibile incapsulato in un semplice file di testo
- Nessun limite in dimensione viene posta ai flussi alternativi
- L'unico effetto visibile in seguito all'aggiunta o alla modifica di un ADS è il cambiamento della data del file



Contenuti

- Storia di Microsoft Windows
- Introduzione al File System
- Principali caratteristiche
- **Principali locazioni di dati**



Allocazioni standard I

- c:\Windows\ (file del sistema operativo)
- c:\Windows\System32\Config (file del registro di Windows)
- c:\Windows\System32\Config\SysEvent.Evt (log eventi sistema)
- c:\Windows\System32\Config\AppEvent.Evt (log eventi programmi)
- c:\Windows\System32\Config\SecEvent.Evt (log di eventi "bloccati" per motivi di sicurezza)

