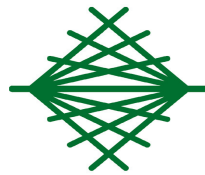


Sistemi operativi e file system

Dr. Stefano Fratepietro
stefano@yourside.it



LABORATORI
GUGLIELMO
MARCONI

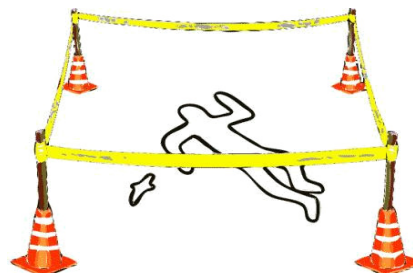
smau 2007

 **yourside**
SOLUZIONI INFORMATICHE AL TUO FIANCO

Contenuti



- Sistemi operativi
 - Microsoft Windows
 - Linux
 - Mac OS X
- File system
 - Windows
 - Linux
 - Mac
 - Iso9660





Organizzazione della giornata

- Quattro ore teoriche con approfondimenti introduttivi tecnico forensi
- Quattro ore pratiche di attività informatico forense in laboratorio

Fate domande!



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 III

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 IV

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 V

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



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

Generalmente un 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

- 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 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



File system NTFS I

- 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 II

- 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

- 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"

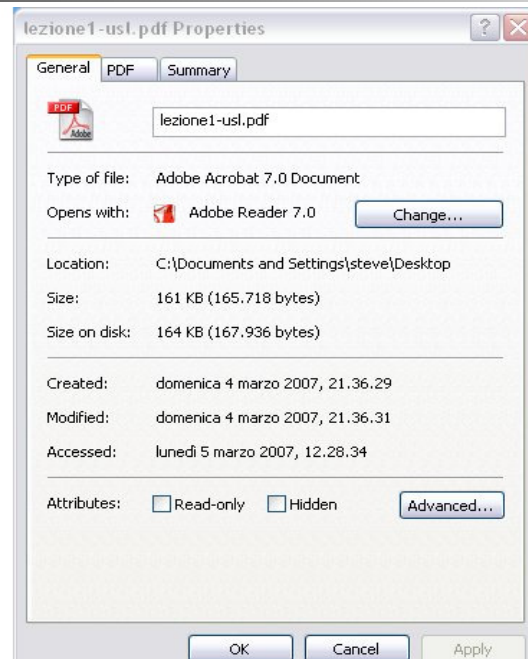


Precisazioni

- 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 in Windows



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 tantè 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

Allocazione dati standard



- 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)

Allocazioni standard II



- c:\Document and Settings (profili utente)
- c:\Programmi (file dei programmi installati mediante l'utilizzo di un installer)
- c:\Document and Settings\nomeutente\ (tutti i file e directory relativi a configurazioni, documenti, desktop, cache di programmi ecc. di un utente)
- c:\Programmi\Mozilla Firefox\nomeprofilo (profilo, cache e tutti i dati inerenti all'utente appartenente al profilo)



Linux – storia I

- Linux nasce nel 1991 da un' idea di Linus Torvalds
- Linux non è altro che un kernel "unix-like" creato da zero
- Nel 1994, con la presentazione "al mondo" della versione 1.0, nascono Red Hat e Suse, aziende leader nel settore delle distribuzioni commerciali
- Nel 1996 viene rilasciata la versione 2.0 con notevoli passi avanti in termini di prestazioni e supporti hardware



Linux – storia II

- Nel 1999 viene rilasciata la versione 2.2
- Nel 2001 viene rilasciata la versione 2.4 con notevoli passi avanti in termini di prestazioni e supporti hardware
- Nel 2005 viene rilasciata la versione 2.6, prima versione del kernel con supporti e miglioramenti per l'utilizzo del sistema lato utente



Distribuzioni I

- Una distribuzione Linux è una distribuzione software che include un kernel Linux e un insieme variabile di altri strumenti e applicazioni software, siano esse freeware, open source o commerciali.
- Le distribuzioni sono distribuite gratuitamente (Licenza GPL)
- Esistono distribuzioni a pagamento, in questo caso non si paga il software ma servizi correlati alla distribuzione fornita



Distribuzioni II

- Ogni distribuzione mira a raggiungere determinati obiettivi e a soddisfare una parte delle esigenze informatiche
 - Distribuzioni lato user
(Ubuntu, Mandrake)
 - Distribuzioni lato server
(Debian, Suse, Red Hat)
 - Distribuzioni ibride
(Knoppix, Gentoo)



Distribuzioni III

- Non esiste uno standard nell'organizzazione delle directory
- Può capitare che a seconda della distribuzione possa cambiare la locazione dei file e delle directory di configurazione e o addirittura il nome con cui esse sono chiamate



Distribuzioni IV

Esempio: file di configurazione della rete

- in Debian è in `/etc/network/interfaces`
- in Red Hat è in `/etc/sysconfig/network`



Live cd Linux I

- Un Live CD è un CD-ROM (anche dvd) contenente un sistema operativo in grado di essere avviato ed eseguito senza doverlo installare su un hard disk
- Si utilizza per scopi dimostrativi, didattici o **per avere a disposizione un sistema operativo completo da usare su un computer altrui**



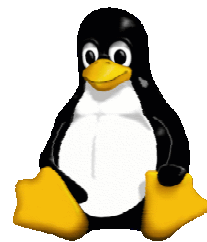
Live cd Linux II

- Tutti i dati vengono caricati nella memoria volatile (RAM) del sistema dove vengono eseguite tutte le operazioni ove vi è necessità di memorizzare dati
- Le unità di memoria non volatile (hard disk, dispositivi esterni di memoria) non vengono per alcun motivo alterate a meno che non vi sia la volontà dell'utente



File system Linux I

- I sistemi Unix oriented (Linux, BSD e similari) hanno a disposizione un'ampia gamma di tipi di file system da poter utilizzare indipendentemente dal tipo di distribuzione usata, unica limitazione consiste nelle versioni di kernel obsolete.
- In alcuni casi è possibile l'utilizzo di file system sviluppati per altri sistemi operativi
(ad esempio Windows)



File system Linux II

- Nei sistemi Unix un inode è una struttura dati sul file system che archivia le informazioni base dei file, delle cartelle o di qualsiasi altro oggetto. Le informazioni includono:
 - la dimensione del file e la sua locazione fisica (se risiede su un dispositivo a blocchi come, ad es., un hard disk)
 - il proprietario e il gruppo di appartenenza
 - le informazioni temporali di creazione, modifica e ultimo accesso



File system III

- Ogni inode ha associato un numero univoco all'interno del dispositivo e ogni file presente è identificato come un link hardware all'inode tramite il suo numero
- Il sistema operativo, quando un programma cerca di accedere ad un file tramite un nome (es. documento.txt), cerca l'inode corrispondente e recupera tutte le informazioni sopra descritte per operare correttamente con il file



File system Linux IV

Principali caratteristiche di un file system Linux sono:

- superblock: contiene informazioni sulla partizione come il numero di blocchi complessivo, il numero di inode, il numero di blocchi liberi, un'indicazione di quando è avvenuta l'ultima verifica della struttura, etc. L'informazione contenuta nel superblock è così importante che viene duplicata in varie zone del disco in modo che possa più facilmente essere recuperata in caso di errore



File system Linux V

- block bitmap: tabella in cui ad ogni bit è associato un blocco di dati. Lo stato del bit indica se il relativo blocco è libero o allocato ad un file
- inode bitmap: tabella in cui ciascun bit è associato ad un "inode". Lo stato del bit indica se il corrispondente inode è libero o in uso



File system Linux VI

- Ogni dispositivo a blocchi formattato, viene visto come una raccolta di inode, ciascuno con un numero che lo individua all'interno di quel dispositivo.

Ogni inode contiene:

- Tipo del file: File, directory ecc...



File system Linux VII

- Codice gruppo proprietario (group), numero che individua un gruppo di utenti, lo si trova in /etc/group
- Permessi rwx per l'user, gruppo e altri: illustrano se un processo appartenente a quell'user o a quel gruppo che può leggere/scrivere/eseguire il file
- Data di ultimo accesso all'inode, modifica dell'inode, modifica del file



Principali caratteristiche I

- architetture a 32 e 64 bit
- multi piattaforma: supporto per architetture diverse da quelle x86
- multitasking: più programmi funzionano contemporaneamente
- multiuser: più utenti nella stessa macchina contemporaneamente
- protezione della memoria tra processi, in modo che un programma non possa mandare in crash l'intero sistema

Principali caratteristiche II



- memoria virtuale con paginazione su disco: in una partizione separata o in un file del filesystem o in entrambi, con la possibilità di aggiungere nuove aree durante il funzionamento (sono chiamate aree di swap)
- demand loads eecutables: Linux legge dal disco solo le parti di un programma che sono attualmente usate
- console virtuali multiple: sessioni di login indipendenti attraverso la console, scambiabili premendo una combinazione di tasti dedicati
- supporto per quasi tutti i file system

Principali caratteristiche III



- Un programma in esecuzione si chiama processo
- Un processo ha uno user-id e un group-id che sono quelli dell'utente che lo ha lanciato e un process-id (pid) univoco
- Ogni file e directory hanno uno user-id, un group-id (che sono quelli del loro proprietario) e un insieme di diritti
- I diritti di un file/directory regolano indipendentemente la possibilità per i processi di leggere, scrivere e eseguire/consultare il file/directory in base all'uguaglianza o meno degli user-id e dei group-id del processo e del file

Assegnazione dei permessi



- I permessi vengono identificati nel seguente modo:
 - lettura definito dal flag r che tradotto in numero assume il valore 4
 - scrittura definito dal flag w che tradotto in numero assume il valore 2
 - esecuzione definito dal flag x che tradotto in numero assume il valore 1
 - nessun permesso che tradotto in numero assume il valore 0

Esempio: `chmod 755 nomefile`

- 7 -> lettura scrittura esecuzione al proprietario
- 5 -> lettura esecuzione al gruppo
- 5 -> lettura esecuzione agli altri utenti

Gestione delle memorie di massa I



- All'interno della directory `/dev` sono presenti diversi file speciali chiamati file di device che si comportano in modo diverso dai file normali
- Questo tipo di file sono un'interfaccia per i driver (che fanno parte del kernel Linux) che si occupano del reale accesso all'hardware

Gestione delle memorie di massa II



- null: rende nullo un output
- zero: device virtuale con tutti i bit settati a zero
- fd0: Primo lettore di dischetti
- fd1: Secondo lettore di dischetti
- hda: Disco fisso o lettore CD IDE presente sulla prima porta IDE (Master)
- hdb: Disco fisso o lettore CD IDE presente sulla prima porta IDE (Slave)
- hdc: Disco fisso o lettore CD IDE presente sulla seconda porta IDE (Master)
- hdd: Disco fisso o lettore CD IDE presente sulla seconda porta IDE (Slave)

Gestione delle memorie di massa III



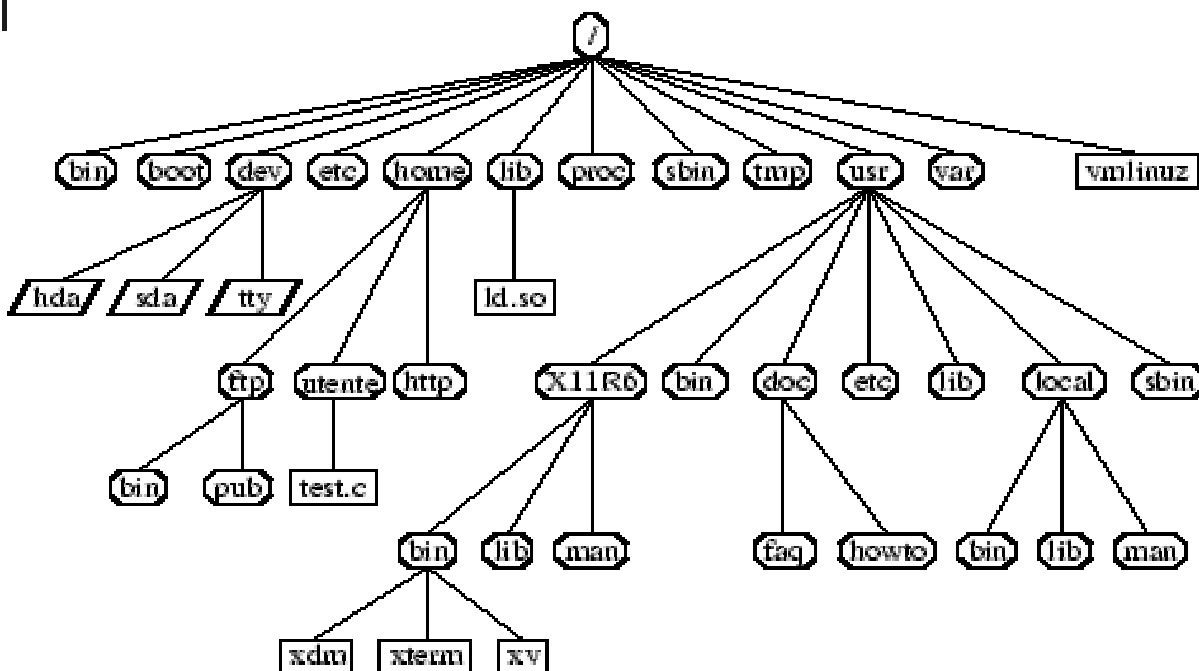
- hda1: Prima partizione del primo disco fisso IDE
- hdd15: Quindicesima partizione del quarto disco fisso IDE
- sda: Il disco fisso SCSI con l'ID SCSI più basso (p.e. 0)
- sdb: Il disco fisso SCSI con l'ID SCSI successivo (p.e. 1)
- sdc: Il disco fisso SCSI con l'ID SCSI ulteriore (p.e. 2)
- sda1: Prima partizione del primo disco fisso SCSI
- sdd10: Decima partizione del primo disco fisso SCSI
- sr0: Il lettore CD SCSI con l'ID SCSI più basso
- sr1: Il lettore CD SCSI con l'ID SCSI successivo
- ttyS0: Porta seriale 0, COM1 sotto MS-DOS
- ttyS1: Porta seriale 1, COM2 sotto MS-DOS



Principali locazioni dati I

- /: radice del sistema
- /bin: programmi "di base" del sistema (mkdir ad esempio è qui)
- /home: profili utente e tutti i file dei profili dei software
- /lib: librerie di sistema
- /media: usato per gestire le periferiche esterne in automatico
- /proc: informazioni dettagliate sul sistema in tempo reale
- /usr: librerie, eseguibili e documentazione
- /var: log, file di lavoro del sistema
- /sbin: file essenziali per permettere l'avvio e il recupero del sistema
- /etc: file di configurazione del sistema - *.conf

Struttura ad albero del FS





Bibliografia

- <http://www.cs.unibo.it/~sacerdot/>
- Slides del corso di Informatica Forense, *Dr. Stefano Fratepietro – steve.yourside.it*