Operacijski sustavi

Iako većina korisnika danas koristi operacijski sustav Windows, nikako se ne smiju zaboraviti druge opcije, prvenstveno Linux i Mac OS. Istražitelj mora znati kako koji sustav radi, gdje pohranjuje podatke i što se sve može izvući s njega. Operacijski sustav se ponaša kao redatelj i tumač između korisnika i softvera i hardvera na računalu. Različiti operacijski sustavi drugačije funkcioniraju i istražitelj će koristiti drugačije metode i alate za pojedini OS.

Različite opcije

- **Windows**
  Najčešće korištene inačice su Windows XP, Vista i 7 (izvor).

- **Unix/Linux**
  Neke od različitih inačica Unixa su BSD, HP-UX, SCO, IBX AIX, Sun Solaris i Digital.
  Među najpopularnijim distribucijama Linuxa su Mandrake, SuSE, Caldera, MkLinux, Debian, Slackware i Red Hat.

- **Macintosh**
  Najnedavnija inačica MAC OS-a, OS X, je bazirana na Unix BSD operacijskom sustavu.

- **Ostali**
  - DOS (eng. *Disk Operating System*)
    Prvi operacijski sustav korišten na najranijim IBM-ovim osobnim ralčunalima. Microsoftova verzija je bila najčešća i zvala se MS-DOS. IBM je isto imao svoju inačicu koja se zvala PC-DOS. DOS nema grafičko sučelje ni miša nego se sve odvija putem komandne linije.
  - Linspire
    Ranije poznat kao Lindows, potpun operacijski sustav. Vrti Windows aplikacije na Linuxu.
  - OS/2
    Ranih 90-ih, IBM i Microsoft su se bili udružili da naprave OS/2 s nadama da će napraviti revoluciju osobnih računala zamjenjujući DOS. No razvoj je trajao duže od očekivanog i Microsoft je u međuvremenu napustio IBM. IBM i dalje razvija OS/2.
  - BeOS
    Operacijski sustav od tvrtke Be, Inc. Zauzima manje mjesta od drugih modernih operacijskih sustava, no i dalje ima pristupačno grafičko sučelje. Brz je i vrlo stabilan. Na većini računala je potrebno manje od 15 sekundi za podizanje sustava.

Filesystems

Datotečni sustav je način na koji OS organizira, upravlja i pristupa datotekama pomoću logičkih struktura (tablica sadržaja) na tvrdom disku (hard drive).

Tvrdi disk na kojem je OS instaliran se dijeli na komade koji se zovu klasteri (eng. *clusters*) ili alokacijske jedinice (ili blokovi u slučaju Linuxa). Svaki klaster sadrži određeni broj sektora. Sektori se nalaze na particiji na disku. Bez dodatnih struktura, svaka particija bi bila jedan veliki komad podataka. OS koristi mapovnu strukturu (eng. *directory structure*) kojom podacima dodjeljuje imena i

upravlja slobodnim prostorom prilikom stvaranja novih datoteka. Ta struktura i metoda organiziranja particije se zove datotečni sustav. Različiti operacijski sustavi imaju različite potrebe i stoga različite datotečne sustave. Konfiguracija u kojoj je više tipova sustava instalirano na tvrdom disku se zove *dual-boot* ili *multi-boot*.

Wikipedia: Pregled svih datotečnih sustava

Windows filesystems

FAT

FAT (eng. *File Allocation Table*) je jedan od najčešćih datotečnih sustava. Korištena još od vremena DOS-a. Tablica je pohranjena na početku particije. Da bi se zaštitila particija, pohranjene su 2 kopije tablice. Ova struktura nije pretjerano organizirana - datotekama se dodjeljuje prva slobodna lokacija na disku.

VFAT

VFAT (eng. *Virtual FAT*) je napredna verzija FAT sustava, još se naziva i FAT32. Koriste ga Windows 95 i noviji. Omogućava podacima da imaju duža imena nego prije te koristi manje alokacijske jedinice na disku nego FAT.

NTFS

NTFS (eng. *New Technology File System*) je razvijen za potrebe WIndows NT i novijih verzija Windowsa. Ranije verzije ga ne mogu koristiti. NTFS organizira datoteke u mape koje se zatim sortiraju. Također, vodi se evidencija o transakcijama datotečnog sustava što NTFS čini obnovljivim (eng. *recoverable*) sustavom.

Unix/Linux filesystems

Unix datotečni sustavi su organizirani kao hijerarhija mapa s početkom u mapi `root` koja je predstavljena kosom crtom (/). Unix gleda na sve diskove i vanjske uređaje kao dio istog datotečnog sustava. Tako će npr. *floppy* disketa biti u `/mnt/floppy`, a CD-ROM u `/cdrom`.

HPFS

HPFS (eng. *High Performance File System*) je dizajniran za OS/2 operacijski sustav. Organizira mape kao FAT, no koristi *super block* koji sadrži pokazivač na `root` te rezervni blok za popravljanje loših sektora.

ext2/ext3/ext4

Second/Third/Fourth Extended Filesystems su datotečni sustavi bazirani na stanju. To znači da sustav održava stanje svih otvorenih datoteka u memoriji. Od ext3 sustav počinje držati dnevnike i kontrolne točke koji pomažu oporavku sustava nakon neispravnog gašenja računala.

NFS

NFS (eng. *Network FIle System*) je razvijen od Sun Microsystems 1980-ih kao način kreiranja datotečnog sustava na klijentu bez diskova. NFS pruža udaljeni pristup dijeljenim datotečnim sustavima na mreži. Osnovna svrha NFS-a je mogućnost mountanja mapa na drugim računalima - na taj način im se može pristupiti kao da su na lokalnom računalu.

BFS

BFS (eng. *BeOS File Systems*) je dizajniran za BeOS operacijski sustav. Ima mogućnost pristupanja drugim sustavima kao što su FAT, FAT16, VFAT i HPFS particije. Moguća je podrška i FAT32 i NTFS particijama uz određene dodatke (eng. *drivers*).