debug.com - Survival Guide

Debug adalah suatu program kecil yang telah ada sejak DOS versi 3.0 dikeluarkan. Sampai sekarangpun program Debug tetap disertakan pada saat anda menginstall MS Windows. Program ini digunakan untuk melihat isi suatu blok memori (view), mengubahnya (edit), dan menjalankan (run) instruksi-instruksi yang ada di blok tersebut.

Cara menggunakan
Jika anda ada di lingkungan Windows, klik 'Start' dan kemudian pilih 'Run'. Dari window 'Run' ketikkan 'Debug' dan klik 'OK'.
Jika anda ada di lingkungan DOS, pindahlah ke subdirectory yang berisi instruksi-instruksi DOS. Jika Windows terinstall, pindahlah ke C:\Windows\Command, dan kemudian ketik 'Debug' dan tekan tombol 'Enter'.
Salah satu dari kedua cara tersebut akan memanggil program Debug dengan menampilkan cursor berbentuk strip (-) seperti di bawah ini.

```
C:\>Debug
-
```

Disini Debug menanti perintah dari kita.
Perintah yang dapat dijalankannya:
a : add, yang berarti kita akan mengubah isi dari blok memori (dimulai dari alamat 0100)
d : dump, yang berarti kita ingin melihat isi dari blok memori (128 bytes ditampilkan)
t : trace, yang berarti kita akan menjalankan instruksi-instruksi yang ada di blok memori (dimulai dari alamat 0100) instrucsion-by-instruction (1 't' menjalankan 1 instruksi)

contoh

```
C:\WINDOWS>debug
-a
1073:0100 mov ax,1234
1073:0103 mov bx,5678
1073:0106 push ax
1073:0107 push bx
1073:0108 pop ax
1073:0109 pop bx
1073:010A
-t

AX=1234  BX=0000  CX=0000  DX=0000  SP=FFEE  BP=0000  SI=0000  DI=0000
DS=1073  ES=1073  SS=1073  CS=1073  IP=0103   NV UP EI PL NZ NA PO NC
1073:0103 BB7856       MOV     BX,5678
-t

AX=1234  BX=5678  CX=0000  DX=0000  SP=FFEE  BP=0000  SI=0000  DI=0000
DS=1073  ES=1073  SS=1073  CS=1073  IP=0106   NV UP EI PL NZ NA PO NC
1073:0106 50           PUSH    AX
-t
```

```
AX=1234  BX=5678  CX=0000  DX=0000  SP=FFEC  BP=0000  SI=0000  DI=0000
DS=1073  ES=1073  SS=1073  CS=1073  IP=0107   NV UP EI PL NZ NA PO NC
1073:0107 53          PUSH    BX
-t

AX=1234  BX=5678  CX=0000  DX=0000  SP=FFEA  BP=0000  SI=0000  DI=0000
DS=1073  ES=1073  SS=1073  CS=1073  IP=0108   NV UP EI PL NZ NA PO NC
1073:0108 58          POP     AX
-t

AX=5678  BX=5678  CX=0000  DX=0000  SP=FFEC  BP=0000  SI=0000  DI=0000
DS=1073  ES=1073  SS=1073  CS=1073  IP=0109   NV UP EI PL NZ NA PO NC
1073:0109 5B          POP     BX
-t

AX=5678  BX=1234  CX=0000  DX=0000  SP=FFEE  BP=0000  SI=0000  DI=0000
DS=1073  ES=1073  SS=1073  CS=1073  IP=010A   NV UP EI PL NZ NA PO NC
1073:010A AA          STOSB
-q

C:\WINDOWS>_
```

keterangan :
AX,BX,CX,DX : register data (register serba guna)
SP (Stack Pointer) : register alamat yg berisi alamat dari data di tumpukan (stack)
perhatikan bagaimana SP berubah u/ instruksi PUSH dan POP
IP (Instruction Pointer) : register alamat yg berisi alamat dari instruksi
yg AKAN dilaksanakan (bukan yg sedang dilaksanakan)
perhatikan bagaimana IP berubah untuk setiap instruksi dgn besar perubahan
yg berbeda-beda (Intel menggunakan Variable Length Instruction)

perhatikan bahwa u/ setiap instruksi ada alamatnya dgn format :
1073:0100 (awal dari program) dimana "1073" adalah alamat segment yg digunakan dan merupakan isi dari register CS (Code Segment), dan "0100" adalah alamat offset yg merupakan isi dari register IP.
Sehingga formatnya = CS:IP
dimana CS+IP = alamat absolut dari instruksi tsb.