I Manuali di Giobe2000

TUTORIAL ASSEMBLER

Nuovo Ambiente Assembler

1.
Prima di partire devi sapere che ...

Studio Tecnico ing. **Giorgio Ober** contatto@giobe2000.it

Questa ***Monografia*** può differire in parte dalla versione *on-line*
soggetta a probabili aggiornamenti e integrazioni.

Verifica sempre le eventuali novità direttamente sul Sito

Prima di partire devi sapere che ...

Da molto tempo questo magico sito è un punto di riferimento (uno dei pochi *in italiano*) per lo studio e la programmazione in **Assembly**; lo *stile* della prosa, l'affidabilità dei contenuti e la *ricca e robusta dotazione* di esempi *originali* (sorgenti ASM) rende piuttosto improbabile ogni tentativo di *appropriazione indebita*.

Se stai leggendo queste righe vuol dire che hai deciso di imparare questa *nobile arte*, ma **prima di decidere** se è il caso di affrontare questa avventura su queste pagine **ho il dovere** di avvisarti di una cosa di importanza fondamentale, per sgombrare i dubbi sulle tue aspettative ed evitare di farti perdere tempo: **LEGGI CON ATTENZIONE LE PROSSIME CONSIDERAZONI**.

E' **importante sottolineare fin d'ora** che, per una scelta didattica ben precisa, il mio sito si occupa (per ora) della **programmazione Assembly di Base**.

L'**Assembly** che imparerai è l'unico che ti consente di capire il *funzionamento della CPU* e di far pratica con l'utilizzo diretto dei suoi *registri* e delle *periferiche* (tastiera, monitor, dischi, porte di I/O, ecc.) da essa controllate; sebbene sia didatticamente conveniente riferirsi al *set d'istruzioni* e all'*architettura* del patriarca a **16** bit (**8086**) con questo **Assembly** sarà possibile programmare anche i processori a **32** bit della famiglia **80x86** attualmente ancora presenti in molti dei nostri PC.

Di sicuro questo **Assembly** è l'ideale *per imparare* le tecniche e i segreti della programmazione ***a basso livello*** e *per consentire* l'intervento diretto, in modo immediato e veloce, su ogni oggetto presente sulla scheda madre e sui dispositivi che con essa danno forma al tuo computer (sistemi operativi permettendolo..).

Per consentire di trarre vantaggio da questo presupposto l'**Assembly** chi ti offro coinvolgerà le *primitive* e le *strutture* del **DOS** (un sistema operativo a **16** bit, come *Windows 3.x*): sebbene la cosa possa sembrare anacronistica questa scelta (aggiunta alla possibilità di fruire delle *primitive* del **BIOS**) è del tutto legittima (straordinariamente efficace e relativamente semplice da apprendere) e, soprattutto, garantita e supportata anche da **Windows** (un sistema operativo a **32** bit) fin dalle prime apparizioni (*Windows 9x* e *Windows ME*) in virtù della presenza della ***Virtual DOS Machine*** (**VDM**).

Ogni volta che si fa partire un ***eseguibile** a **16** bit* (come quelli che noi progetteremo in ogni dettaglio) oppure se si esegue l'*interprete dei comandi* **COMMAND** o **CMD**, la *macchina virtuale DOS* creerà un ambiente (*shell Dos*) nel quale esso girerà esattamente come se fosse ospitato da un *reale* sistema operativo *DOS*, *emulandone* le caratteristiche. Questo vale anche

per *Windows 2000*, *Windows XP* e *Windows Vista32*, sotto i quali si potrà godere in pieno della struttura offerta dal mio **Nuovo Ambiente Assembler** e collaudare ogni progetto proposto dal mio sito nella sezione dedicata all'**Assembly**, pur, talvolta, con qualche artificio (*device driver*) per superare la loro arrogante ingerenza sull'accesso diretto alla memoria o ai dispositivi di Input/Output.

Con le versioni recenti (per esempio *Windows XP**64*** e *Windows Vista**64***) il **Nuovo Ambiente Assembler** invece ***non funzionerà più***: questi sistemi operativi, destinati alle nuove architetture a **64** bit, non includono più la NT**VDM** e quindi nessuna applicazione MS-DOS (o Windows a 16-bit) potrà essere eseguita.

Ai possessori di queste versioni che desiderano comunque fruire dei miei servizi rimangono comunque almeno 2 vie alternative:

- partizionare il proprio disco fisso e dedicare una partizione anche a *Windows XP* (e/o addirittura a *Windows ME*)
- installare un ***emulatore***, come ***DOSBox*** (gratuito e molto efficiente) o come ***Microsoft Virtual PC*** o altro.., e imparare ad utilizzarlo

MA se desideri ***creare*** applicazioni di "***tipo Windows***" (come quelle che vedi *girare* sul tuo monitor) o se ti vuoi dedicare al ***Reversing*** di questi eseguibili (se non addirittura cimentarti con ***Cracking*** o in attività ***Hacking***), **qui stai perdendo il tuo tempo !!!**

Per poter realizzare applicativi di questo tipo devi utilizzare l'**Assembly Win32**, un potente linguaggio di programmazione strutturato come uno *ad alto livello*, in grado di sfruttare a pieno le potenzialità indiscusse di *Windows a 32 bit* rappresentate da una grandissima collezione di potenti ed efficienti ***funzioni***, dette **API** (**A**pplication **P**rogramming **I**nterface), in parte integrate dentro lo stesso Windows, del tutto diverse da quelle, pur importanti, del povero *DOS*.

Le **API** sono raccolte in particolari ***librerie*** *collegate dinamicamente al programma*, dette appunto **DLL** (**D**ynamic **L**inked **L**ibraries), a loro volta disponibili in notevole quantità e, all'occasione, anche progettabili e personalizzabili; il loro utilizzo garantisce ai tuoi lavori anche una **GUI** (**G**raphic **U**ser **I**nterface, *Interfaccia Grafica Utente*) del tutto simile a quelle disponibili in ogni applicativo *Windows* (e assolutamente impensabile in ambiente *DOS*).

Basta *CPU*, basta *registri*, basta *hardware*, basta *funzioni DOS* o *BIOS*, basta chiamate di *interrupt* (`INT`) *software*!! Solo ***oggetti*** pronti, preconfezionati, funzionali, immediatamente disponibili.
Basta *pane e salame* e *marzemino* .. E' tempo di *caviale* e *champagne*!!

Con l'**Assembly Win32** potrai realizzare progetti *vendibili* ed *esteticamente gradevoli*, praticamente senza fatica, disponendo di *tecniche di gestione* della memoria e dell'hardware *trasparenti* (questo fatto è la sua potenza ma anche il suo limite, da certi punti di vista...) e *potenti*.

In conclusione ci sono 2 tipi di **Assembly**: sono due pianeti completamente diversi: il primo dà il *senso del potere* e *del creatore*, mentre il secondo è un *lavoro da ragioniere*, dignitoso ma freddo, efficiente e opportunista.

- l'**Assembly di base** si basa sulla programmazione ***DOS***/***BIOS***, decisamente più creativa e formante di quella ***Win32***, e consente un **rapporto diretto con l'hardware** del computer, a partire da quello del processore; **ma** in questo ambiente ogni *oggetto* (finestra, menu, ecc.) e ogni problema (lettura tastiera, scrittura a video, trattamento dei dati, ecc.) deve essere creato da zero e l'aspetto dell'*interfaccia utente* sarà sempre piuttosto spartano, in *Modo Testo* (cioè con i tipici caratteri 80x25 in una *finestra DOS*) o in *Grafica limitata* alle basse risoluzioni (con qualche eccezione ..).
- l'**Assembly Win32** si basa sulla programmazione ***Windows32bit***, di certo più performante e gratificante, almeno dal punto di vista estetico: **tutto è pronto** per essere utilizzato con il massimo profitto in un ambiente grafico di altissima risoluzione; basta solo la determinazione di imparare il modo migliore per organizzare le strutture disponibili (che sono tante!!) e non è necessario sapere *come funziona* il computer: se per te questo è irrilevante e sei uno che *bada al sodo* questa è la tua via!!

A mio modestissimo avviso, **non è comunque ragionevole** arrivare al *secondo* senza essere passati per il *primo*; l'esperienza con l'**Assembly di base** è fondamentale per conoscere con tranquillità gli strumenti necessari e per farsi la mentalità logica indispensabile per affrontare con autonomia gli ambienti più complessi di **Win32**.

L'evoluzione da **Assembly di base** a **Assembly Win32** è un passo naturale e scontato che i miei amati lettori provvedono a compiere quando *si sono fatti le ossa* e sentono che quello che hanno letto fino a ieri non basta più; da quel momento non hanno più bisogno del *Maestro* e sono in grado di compiere da soli i passi necessari.

Potrà capitarti (come è capitato a me) di sentire qualche borioso benpensante che *raglia al cielo* il suo disprezzo per la *mia* credibilità e per il *nostro* lavoro, pontificandone l'inutilità e giudicandolo vecchio e superato dal tempo. Arrogarsi la presunzione di essere detentore della verità è cosa ahimè frequente, ai giorni nostri: è un diritto legittimo, ma molto spesso succede che questa gente ***vive di luce riflessa***, essendo priva del carisma, della sensibilità e della competenza necessaria per essere ***faro*** per qualcuno.

Non farti dunque intimorire e **fai una scelta *ponderata* e *serena***; del resto gli argomenti trattati sono gli stessi pianificati nei corsi di *Architettura dei Calcolatori* di molti Atenei (con buona pace dei benpensanti ...) e non di rado ho potuto godere del generoso apprezzamento sia dei docenti che degli studenti di questi e di altri corsi.

Se decidi di imbarcarti sul *mio battello* basta cliccare sulla *freccia a destra* (qui sotto) o tornare alla pagina principale e scegliere una delle voci dell'*elenco*: di certo quello che troverai nel mio sito non ha prezzo: è il frutto di una ***esperienza*** *consumata sul campo* e *verificata* con il piacere della conquista e dell'avventura.