

Ensamblador en DOS, Linux y Windows

© Francisco Charde Ojeda

Agradecimientos

Introducción

- Ensamblador y procesadores
- Ensamblador y sistemas
- Objetivos de este libro

1. Herramientas necesarias

Editores

- DOS

- Windows

- Linux

Ensambladores

- MASM

- NASM

- Otros ensambladores

- RAD y ensamblador

Enlazadores

Depuradores

Otras herramientas

Resumen

2. Nuestro primer programa

Esqueleto de un programa mínimo

Programas COM en DOS

- El código

- Ensamblado y enlace

Programas EXE en DOS

- Versión MASM

- Versión NASM

- Ensamblado y enlace

Programas Linux

- El código

- Ensamblado y enlace

Programas Windows

- El código

- Ensamblado y enlace

Resumen

3. Bases de numeración

Sistemas de numeración informáticos

Cálculo del valor de una cifra

Conversión entre bases de numeración

- Conversión a la base decimal desde cualquier base

- Conversión a cualquier base desde la base decimal

Operar con números binarios

- Bits, nibbles y bytes

- Números con signo

Operar con números hexadecimales

- De binario a hexadecimal y viceversa

- Números negativos en hexadecimal

Números en base ocho

Identificación de la base de un número
Resumen

4. Ejecución de un programa

- Formatos de archivo ejecutable
 - Ejecutables en DOS
 - Ejecutables en Linux
 - Ejecutables en Windows
 - Detalles sobre formatos de archivo
- Preparación del programa por parte del sistema
 - Recuperación de la cabecera del ejecutable
 - Asignación de bloques de memoria
 - Creación de un proceso
- Configuración de registros
 - Segmentos de código, datos y pila
 - El puntero de instrucción
 - Base y puntero de la pila
 - Acceso a los datos
- Arquitectura del procesador
 - Esquema de bloques
- Resumen

5. Registros y memoria

- Unidades de información
 - Palabras y dobles palabras
 - Múltiplos del byte
- Capacidad de direccionamiento
 - Registros de segmento
 - Párrafos y segmentos
 - Modelos de memoria
- Registros de uso general
- Asignación de valores
 - Valores inmediatos
 - Asignación entre registros
 - Lectura de datos de la memoria
 - Escritura de datos en la memoria
- Definición de datos en el programa
 - Campos simples
 - Conjuntos de campos
 - Referencias al segmento de datos
- Un ejemplo
- Resumen

6. Depuración

- Puesta en marcha del depurador
 - Nombres de archivos DOS
 - Apertura desde DEBUG
- Análisis del programa
 - Direcciones, instrucciones y código máquina
 - Traducción de etiquetas
 - Examen del contenido de datos
 - Estado inicial de los registros
- Ejecución paso a paso
 - Depuración de rutinas y BIOS
 - Ejecución hasta un cierto punto
- Alteración del curso del programa
 - Modificar el contenido de un registro
 - Cambiar los datos en memoria
 - Ensamblar nuevas instrucciones

Otras posibilidades de DEBUG
Resumen

7. Operaciones aritméticas

- Suma de dos números
 - Desbordamiento y acarreo
 - Suma con acarreo
 - Sumas de 32 bits con registros de 16
- Restar un número de otro
- Multiplicar dos números
- Dividir un número entre otro
- Incrementos y reducciones
- Aritmética BCD
 - Números BCD empaquetados y sin empaquetar
 - Suma de números BCD
 - Otras operaciones con números BCD
- Negativos, palabras y dobles palabras
- Uso de la unidad de punto flotante
 - Registros de la FPU
 - Tipos de datos
 - Introducción de datos en la FPU
 - Ejecución de operaciones
 - Recuperación de datos de la FPU
 - Un sencillo ejemplo
- Resumen

8. Condicionales

- El registro de indicadores
 - Obtención y restauración del registro de indicadores
- Comparación de valores
 - Igualdad y desigualdad
 - Menor y mayor que
- Instrucciones de manipulación de bits
 - Activación de bits individuales
 - Desactivación de bits individuales
 - Otras operaciones lógicas
 - Comprobación de bits individuales
 - Rotación y desplazamiento de bits
- Resumen

9. Bucles

- Bucles con saltos condicionales
- Instrucciones para implementar bucles
- Casos concretos
 - Bucles con condición compuesta
 - Bucles anidados
 - Transferencia de datos
- Resumen

10. Estructuración del código

- Procedimientos
 - Llamada a un procedimiento
 - Retorno de un procedimiento
 - Salvaguarda de los registros
 - Transferencia de parámetros
 - Una rutina de espera
 - Instrucciones de E/S
 - Comunicación con el reloj del sistema
 - Código de la rutina
 - Un ejemplo de uso

Macros

- Macros simples
- Expansión de la macro
- Macros complejas

Archivos de macros y procedimientos

Resumen

11. Manipulación de secuencias de bytes

- Orígenes, destinos e incrementos
 - Recuperación y almacenamiento de datos
 - Conversión de binario a decimal
 - Almacenamiento de valores
 - Repetición automática de la operación
 - Transferencia de una secuencia de datos
 - Búsqueda de un dato
 - Comparación de cadenas
- ### Resumen

12. La BIOS

- ¿Qué es la BIOS?
 - El mecanismo de interrupciones
 - El área de parámetros de la BIOS
 - Acceso a variables de la BIOS
 - Servicios de la BIOS
 - Acceso al adaptador de vídeo
 - Lectura del teclado
 - Configuración del sistema
 - Memoria disponible
 - Acceso a unidades de disco
 - Puertos serie y paralelo
 - Fecha y hora
 - Interrupciones hardware
 - Excepciones
 - Manipulación de los vectores de interrupción
- ### Resumen

13. Servicios de vídeo

- Detección del tipo de adaptador
 - Modos de visualización
 - Obtener y modificar el modo de visualización
 - Servicios para trabajar con texto
 - Posición y aspecto del cursor
 - Caracteres y atributos
 - Cambio de la página activa
 - Desplazamiento del texto
 - Servicios para trabajar con gráficos
 - Escritura y lectura de puntos
 - El color en adaptadores CGA
 - El color en adaptadores EGA
 - El color en adaptadores VGA
 - Lectura de los registros del DAC
 - Modificación de los registros del DAC
 - Efectos de color
- ### Resumen

14. Servicios de teclado

- Recuperación de teclas pulsadas
 - Teclados estándar
 - Teclados extendidos
- Estado de teclas muertas y de doble estado

Obtención de cadenas de caracteres
Resumen

15. Acceso a la impresora

Iniciación y estado de la impresora
Envío de información a la impresora
Puertos mejorados de impresora
Resumen

16. Configuración del equipo

Lectura de la memoria CMOS
 Datos contenidos en la CMOS
 Visualización de parámetros de la CMOS
Servicios extendidos de la BIOS
Resumen

17. Interrupciones DOS

Interrupciones y versiones de DOS
Funciones de la interrupción 21h
 Entrada y salida por la consola
 Comunicación serie y paralelo
 Fecha y hora
 Gestión de vectores
 Finalización y ejecución de programas
 Gestión de memoria
Un programa que ejecuta otros
Resumen

18. Tratamiento de archivos

Apertura y creación de archivos
 Creación de un nuevo archivo
 Creación de archivos temporales
 Apertura y cierre de archivos
Lectura y escritura de datos
 Guardar y restaurar pantallas
Borrado, renombrado y otras operaciones con archivos
Unidades y directorios
 La unidad por defecto
 El directorio actual
 Creación y borrado de directorios
 Archivos existentes en un directorio
UDisk
Resumen

19. Acceso a sectores de disco

Servicios del DOS
 Unidades de más de 32 Mb
 Unidades de más de 2 Gb
Servicios de la BIOS
Copia de discos
Resumen

20. Memoria expandida y extendida en DOS

Bits, direccionamiento y modos de operación
Memoria expandida
Memoria extendida
 Memoria alta
 Memoria superior
 Memoria extendida
La especificación XMS

El gestor XMS
Asignación de EMB
Transferencia de datos
Resumen

- 21. Programas residentes en DOS
 - Aplicación y problemática
 - Tipos de código residente
 - Limitaciones del código residente
 - Métodos para dejar código residente en memoria
 - Longitud del código residente
 - Activación del código
 - Asignación de un vector de interrupción
 - Ocupación en memoria
 - Fiabilidad del método
 - La interrupción múltiple
 - Engancharse a la interrupción múltiple
 - Un primer ejemplo
 - Cómo evitar la reinstalación
 - Facilitar la desinstalación
 - Restauración de los vectores
 - Liberar la memoria
 - Tercera versión de INT2F
 - A vueltas con la pila y el PSP
 - Una pila para la parte residente
 - Cambio del PSP activo
 - Estado del DOS y la BIOS
 - La reentrada y el DOS
 - Los indicadores InDOS y ErrorMode
 - La interrupción 28h
 - Estructura del programa residente
 - Los servicios de entrada y salida de caracteres
 - Las interrupciones BIOS
 - Tiempo de interrupción de un residente
 - Estado de otros elementos del sistema
 - Intercambio de la DTA
 - Gestión de errores críticos
 - Respuesta del controlador de error crítico
 - Otros aspectos a tener en cuenta
 - División por cero
 - Tratamiento de excepciones
 - Tratamiento de Control-C y Control-Inter
 - Inhibición del tratamiento de Control-C
 - Inhibición del tratamiento de Control-Inter
 - Otros aspectos a tener en cuenta
 - Acceso a la pantalla
 - Salvaguarda del contenido de la pantalla
 - Estado del teclado
 - Estado del ratón
 - Activación por teclado
 - Interceptar la interrupción de teclado
 - Control del teclado a bajo nivel
 - Códigos de teclado
 - Combinaciones de teclas
 - Bytes de estado del teclado
 - Esquema general de un programa residente
 - Instalación
 - Desinstalación
 - Supervisión
 - Gestor de INT 9h

- Gestor de INT 1Ch
- Gestor de INT 28h
- Gestor de INT 10h e INT 13h
- Activación
- Otros factores a tener en cuenta
- Una tabla de códigos ASCII residente
 - La instalación
 - Petición de activación
 - Estado de la BIOS
 - La activación
 - Mostrar la tabla de códigos ASCII
 - Otros gestores de interrupción
 - Procedimientos adicionales
 - Funcionamiento del programa
- Aplicaciones residentes y Windows
 - Residentes globales y locales
 - Problemas de un residente global
 - Iniciación de Windows
 - Funcionamiento bajo Windows
 - A vueltas con las VM
 - Copias individuales de datos
 - Secciones críticas
 - Ejecución de programas Windows
- Resumen

22. Servicios de Windows

- Herramientas necesarias
 - Inclusión de definiciones y bibliotecas
 - Ensamblado y enlace
 - Invocación a funciones Windows
- Estructura básica de una aplicación Windows
 - La clase de ventana
 - Creación de ventanas
 - Proceso de mensajes
 - El programa completo
- Uso de controles
 - Añadir un control a una ventana
 - Botones
 - Envío de mensajes a ventanas
 - Un ejemplo
 - Textos
 - Otros controles
- Dibujar en la ventana
- Resumen

23. Servicios de Linux

- Herramientas necesarias
- Servicios del núcleo de Linux
 - Devolución del control al sistema
 - Entrada y salida por consola
 - Macros de ayuda
 - Trabajo con archivos
 - Apertura y creación de archivos
 - El puntero de lectura/escritura
 - Constantes y macros
 - Acceso a la memoria de pantalla
 - Dispositivos vcs y vcsa
 - Guardar el contenido de la pantalla en un archivo
 - Manipulación del contenido de la pantalla
 - Acceso a discos

- La biblioteca de funciones de Linux
 - Entrega de parámetros
 - Servicios disponibles
- Resumen

24. 32 bits en DOS

- El modo protegido
 - Registros de control del procesador
 - Modificación de los registros de control
 - Segmentos y selectores
 - Descriptores de segmentos
 - Tipos de segmentos
 - Tablas de descriptores
 - De vuelta a los selectores de segmento
 - Direccionamiento en modo protegido
 - Entrada y salida del modo protegido
 - Preparación de la GDT
 - Cálculo de direcciones físicas
 - Núcleo del programa
 - Interrupciones en modo protegido
- DPMI
 - Anfitriones DPMI
 - Cientes DPMI
 - Detectar la presencia de un anfitrión DPMI
 - Activación del modo protegido
 - Servicios DPMI
 - Un ejemplo
- Extensores DOS
- Resumen

25. Recursos de interés

A. Contenido del CD-ROM

Índice alfabético