

Indice general

Prefacio	XV
----------------	----

CAPITULO 1

El DOS no documentado: la locura continúa	1
"Codificación cruel" y acuerdos vinculantes	3
WINDOWS y DR DOS	6
Rivalidad entre sistemas y armas del delito	8
El código de detección AARD de Windows	9
Una batería de test	11
Un portero gratuito	16
¿Realmente tiene alguna importancia el código de la versión beta?	18
Y, ¿entonces?	19
La respuesta de Microsoft	20
Documentar versus vincular	21
Windows de Microsoft utiliza el DOS no documentado	22
WIN.COM recorre la SFT	25
BlockDev y la función INT 2Fh AH=13h	26
El DOSMGR: la conexión de Windows con el DOS no documentado	26
CON CON CON CON CON	29
La llamada del DOSMGR sin documentar a la API	30
Implementación de las funciones del DOSMGR	36
Parcheando al DOS	39
El DOS conoce a Windows	41
El DOSMGR y el SDA	42
El DOSMGR y el indicador InDos	43
Ajustes de SYSTEM.INI y el DOS no documentado	44
KRNL386 engorda a la SFT	45
KRNL386 y el PSP	45
El DOS no documentado y la guerra de las utilidades	47
SmartDrive no documentado	48
DoubleSpace sin documentar	49
EMM386.EXE no documentado	51
Microsoft Anti-Virus	53
¿Sin problemas?	55

27-01-97.

January '97 -- Compaq. R-16238

DOS documentado	58
¿Por qué dejar la funcionalidad sin documentar?	61
Documentación y monopolio	63
Miedo al DOS no documentado	66
¿No estamos portándonos mal?	68

CAPITULO 2

Programación con DOS documentado y sin documentar: comparación	71
Empleo de las funciones documentadas del DOS	73
Llamadas al DOS desde el lenguaje ensamblador	74
Llamadas al DOS desde C	75
int86()	76
Ensamblador en línea	76
Seudo-variables de registro	78
Funciones de biblioteca del DOS	79
Llamadas al DOS desde Turbo Pascal	79
Llamadas al DOS desde BASIC	80
Utilización del DOS no documentado	82
Desensamblando el DOS	82
Utilización de la lista de interrupciones	84
Nada de números mágicos	86
Llamadas al DOS no documentado desde el lenguaje ensamblador	88
Versionitis del DOS	90
Acceso a SysVars	91
Llamadas al DOS no documentado desde C	92
Qué, ¿sin estructuras?	95
Llamadas al DOS no documentado desde Turbo Pascal	99
Llamadas al DOS no documentado desde BASIC	103
¿Cuándo no hay que utilizar las características sin documentar?	104
Verificación del DOS no documentado	105
Haciendo modificaciones	106
Un caso especial importante: la Red Novell	114
Conexión al DOS: envoltorios de aplicaciones	116
Dentro del modo protegido	121

CAPITULO 3

El DOS no documentado frente a Windows	123
Llamada al DOS no documentado desde Windows	125
¡En realidad, no funciona!	131
El temido fallo de protección general (GP)	134
Un shell DPMI	138
Prueba del DOS no documentado desde programas DPMISH	143
Las extensiones del DOS de Windows	146
Dentro de la extensión del DOS del DOSMGR	149
Cómo maneja el DOSMGR las llamadas al DOS no documentado	153
Creación de la XLAT del usuario	157

Programación DPMI	157
Ocultación de la DPMI	160
Readaptación de SFTWALK	168
Parte interna del servidor DPMI del VMM	172
De regreso a la programación en Windows	174
Windows y la SFT	175
Recorriendo la cadena de dispositivos	176
Nombre verdadero	180
Windows y el PSP	184
Espiando por las ventanas del DOS desde un programa Windows	188
Una breve introducción a la programación VxD	211
Cronometrado de las llamadas del DOS	214

CAPITULO 4

Otros DOS: del DR DOS y NetWare a MVDM de OS/2 y Windows NT	217
De CPM al DR DOS y al Novell DOS	220
El número de la versión del DR DOS	224
Novell DOS no documentado	225
Observando el DR DOS	229
Desensamblado del DR DOS	230
¿Cuánto se parece el DR DOS al MS-DOS?	231
SysVars, la estructura del directorio actual y el redirector	232
La Tabla de Archivos del Sistema y SHARE	233
Bloques de Control de Memoria	233
Los TSR y el Area de Datos Intercambiables	235
Funcionalidades adicionales de DR DOS y Novell DOS	235
Novell NetWare	237
NETX y la INT 21h	237
NetWare 4.0 y el redirector de red	239
Cómo modifica NETX a la INT 21h	240
NetWare sin documentar	248
OS/2 2.x ¿“Un DOS mejor que el DOS”?	249
MVDM y VDD	251
Entonces, ¿qué versión del DOS pretende ser esta emulación?	252
Carga de un DOS genuino	255
OS/2 2.x y el DOS no documentado	256
Nuevos servicios OS/2 para antiguos programas del DOS	259
Emulación del DOS bajo Windows NT	262
El modelo Cliente/Servidor	264
NTVDM, NTIO y NTDOS	265
Píldoras mágicas y Bops	266
¿Qué es el NTVDM.EXE?	268
DOS 5.50	270
Funcionalidad adicional de NTDOS	272
NT no documentado	273

CAPITULO 5

INTRSPY: un programa para explorar el DOS	277
¿Por qué un depurador controlado por sucesos y guión?	277
Una excursión con cicerone	278
Controladores de dispositivos	283
Observando la XMS	286
Enganches dinámicos	289
INTRSPY: guía del usuario	291
Empleo de INTRSPY.EXE	291
Empleo de CMDSPY.EXE	291
Lenguaje del guión	292
Sintaxis	293
Sintaxis de INCLUDE	293
Sintaxis de STRUCTURE	294
Sintaxis de INTERCEPT	294
Sintaxis de GENERATE	297
Sintaxis de RUN	298
Sintaxis de REPORT, STOP y RESTART	298
Sintaxis de DEBUG	298
Constantes predefinidas	299
Mensajes de error	300
Mensajes de compilación de CMDSPY	300
Operando CMDSPY e INTRSPY	300
Guiones de utilidades INTRSPY	301
UNDOC	301
LSTOFLST	304
Registro de la actividad de la máquina	307
Monitorización de la E/S de disco	308
MEM	313
Escritura de un gestor de interrupciones genérico	314
El problema con las INT de INTEL	316
Cambios en la implementación de INTRSPY 2.0	317
Implementación	318
Trampas en las que cayó el autor	318
El futuro de INTRSPY	320

CAPITULO 6

Desensamblado del DOS	321
¿Qué es el MS-DOS?	322
Desensamblado del IO.SYS y del MSDOS.SYS	324
Vectores de interrupción y encadenamiento	328
Seguimiento de una llamada a la INT 21h del DOS	339
Desensamblado de las funciones Obtener/Establecer PSP	348
Desensamblado de la INT 21h AH=33h	349
Examen del fragmento de memoria baja para DOS=HIGH	350
Examen de la función distribución de la INT 21h	352

Examen de la Tabla de distribución de la INT 21h	360
Obtener SysVars y los registros de los llamadores	363
Una mirada muy breve a la E/S de archivo	365
Rastreo de la llamada a la INT 2Fh del DOS	366
¿Cómo efectúa DEBUG el rastreo a través de una INT?	366
INTCHAIN	366
Examen de la cadena de la INT 2Fh	371
Los manipuladores de la INT 2Fh del MSDOS.SYS y del IO.SYS	374
Examen del manipulador de la INT 2Fh AH=12h del MSDOS.SYS	375
Ubicación de la tabla de distribución de la INT 2Fh AH=12h	376
Auténtico desensamblado del DOS	380
Utilización del NICEDBG	383
Examen de algunas funciones del DOS	393
Examen de la función Lseek del DOS	396
Otras partes del DOS	403
¿Nos van a meter en la cárcel por esto?	405
¡Utilicemos el código fuente, Luke!	409
Kit de adaptación para OEM del DOS de Microsoft (OAK)	413

CAPITULO 7

Gestión de los recursos del MS-DOS: memoria, procesos, dispositivos	417
Gestión de la memoria	418
Bloques de control de memoria	418
El HMA y los UMB	421
Empleo de los UMB	422
El Area de Memoria Alta	424
Forma de encontrar el principio de la cadena de los MCB	426
Forma de investigar en la cadena de los MCB	427
Comprobación de la consistencia de los MCB	431
Un programa UDMEM más detallado	433
Precauciones en la asignación	443
Estrategias de asignación de la RAM	444
Estrategia Primer ajuste	444
Estrategia Mejor ajuste	445
Estrategia Ultimo ajuste	445
Gestión de los procesos	446
Archivos de programas y procesos	446
El formato de los archivos COM	447
El formato de los archivos EXE	447
El PSP: forma de identificar un proceso	448
Historia, objetivo y empleo	448
Identificador de proceso único (normalmente)	449
Areas sin documentar del PSP	450
Dirección de terminación del DOS	451
Otros campos del PSP	452
Generación de procesos hijos	453
Localización del proceso padre	454

Localización de antepasados	454
Empleo de esta capacidad	454
Gestión de dispositivos	455
Por qué existen controladores de dispositivos	455
Detalles dependientes del hardware	456
Funciones requeridas lógicamente	456
Congruencia de archivos y dispositivos	457
Rastreando la cadena de controladores	458
Organización de la cadena de controladores de dispositivos	459
Cómo se inician los controladores	459
Localizar el principio de la cadena	460
Rastreando de parte a parte	461
Carga de controladores de dispositivos desde la línea de órdenes del DOS	463
Cómo trabaja DEVLOD	465
DEVLOD.C	469
MOVUP.ASM	478
TESTNAME.ASM	479
CO.ASM	481
El archivo Make	481
¿Qué tal funciona DEVLOD?	482

CAPITULO 8

El sistema de archivos del DOS y el redirector de red	485
Una rápida visión general del sistema	487
El sistema de archivos del DOS	492
Superficies, Pistas y Sectores	493
Registros de partición y de inicialización	494
El registro de inicialización y el bloque de parámetros del BIOS (BPB)	497
Los números de sector lógico y el concepto de cluster	499
La tabla de asignación de archivos (FAT)	500
Estructura del directorio en el DOS	510
El bloque de parámetros de unidad (DPB)	526
Memorias intermedias y cachés de disco	529
La estructura del directorio actual (CDS)	537
Contenido de la CDS	541
Recorrido de la matriz CDS	544
Detección de los discos RAM	546
Unidades DoubleSpace	546
Unidades del Stacker	557
Unidades de Novell NetWare	560
Creación y supresión de las letras de las unidades	561
Tablas de archivo del sistema (SFT) y Tabla de archivo de trabajo (JFT)	565
¿Cuántos FILES=?	571
Nombre de archivo procedente del gestor	574
¿Qué archivos están ahora abiertos?	577
Liberación de los gestores de archivo huérfanos	586
Más gestores de archivo	590

Los FCB del sistema	594
Los enganches SHARE	597
El redirector de red del MS-DOS	602
Empleo de la interfaz del redirector de red	605
Enganches frontales y controladores de dispositivos frente a redirectores dorsales	605
Qué proporciona el DOS	607
Qué debe aportar un redirector	613
Rastreo de una función Open, revisita	613
El Phantom	619
Implementación del Phantom	621
Inicialización de la CDS	621
El manipulador del redirector de la INT 2Fh	623
¿Cómo podemos saber si la llamada es para nosotros?	625
Manipulación de una sentencia Read	627
El sistema de archivos XMS del Phantom	630
Manipulación de una sentencia Open	633
Manipulación de la orden Chdir	637
Manipulación de la orden Mkdir	637
Diferencias entre las distintas versiones del DOS	641
Especificación del redirector de red	641
Empleo de las funciones internas del DOS	652
El futuro del sistema de archivos del DOS	658

CAPITULO 9

Software residente en memoria: aparición instantánea y multitarea	661
TSR: parece un error, pero es una característica	663
¿Dónde entra el DOS no documentado?	665
TSR MS-DOS	669
El TSR genérico	670
Programación de TSR con Microsoft y Borland C/C++	672
Mantener un programa residente en Microsoft C	677
No siendo residente	679
Agitar la pila	680
Funciones del DOS para los TSR	682
Indicadores del MS-DOS	682
Obtener/Establecer PSP	684
Información de error extendida	687
Información de interrupción extendida	688
Interrupción 28h	690
Interior de un TSR genérico	691
Argumentos del TSR desde la línea de órdenes	713
Escritura de TSR con el área de datos intercambiables del DOS	714
Gestores de tareas y TSR	723
Eliminación de un TSR	734
Ejemplos de programas TSR	738
TSRFILE	738

TSRMEM	740
TSR2E	742
TSR multitarea	744
Conmutación de tareas	746
Instalación de MULTI	746
Interrupción temporizada	747
Interrupción inactiva	747
Interrupción de teclado	747
Imprimir	748
MULTI.C	748
CAPITULO 10	
Intérpretes de órdenes	757
Interior del COMMAND.COM	758
Requisitos de un intérprete de órdenes	762
Obtención de la información tecleada por el operador	762
El carácter de petición de órdenes del DOS	762
Pulsaciones del teclado	762
Archivos de procesamiento por lotes	763
Mejoras de archivos de procesamiento por lotes y compiladores	763
Interpretación de las peticiones del operador	766
Análisis sintáctico para inclusión en el PSP	766
SWITCHAR	767
Redireccionamiento de la línea de órdenes y tuberías	768
Distinción entre órdenes internas y externas	771
Búsqueda y ejecución de las órdenes internas	773
Distribución de los procesos apropiados	774
Localización y carga de órdenes externas	774
Tratamiento de los archivos BAT	774
Tratamiento de los archivos COM y EXE	775
La idea del código de salida	776
Órdenes instalables	777
TSHELL, un sencillo intérprete de órdenes	782
Forma de funcionar de COMMAND.COM	785
Por qué los shells son sus propios padres	786
Cómo y por qué el COMMAND.COM se carga a sí mismo	787
Los puntos de división	788
Porciones residente, de inicialización y transitoria	788
Dónde se cargan estas porciones	789
¿Por qué deja de funcionar, a veces, la F3?	790
DOSKEY	793
Utilización del entorno	794
Cómo utiliza el entorno el COMMAND.COM	794
Localización del entorno	795
Otras formas de localizar el entorno	797
Encontrar el entorno "activo"	803
Búsqueda del entorno	804

La INT 2Eh, la puerta trasera	807
La función	808
Su empleo	809
Alternativas a COMMAND.COM	813
4DOS.COM	813
Un cambio total, más aún	813
No utiliza características sin documentar	814
Programa ejemplo: un editor del entorno	815
Conclusión	825
APENDICE	
El DOS no documentado: funciones y estructuras de datos	827
Agradecimientos	827
Ejemplo de entrada	827
Glosario	1023
Bibliografía comentada	1027
Vocabulario técnico bilingüe	1043
Indice analítico	1053