PowerPC disassembler V. 2

Un désasembleur pour code PowerPC 601 (et supérieur) et fonctionnant sur ordinateur Macintosh 680x0.

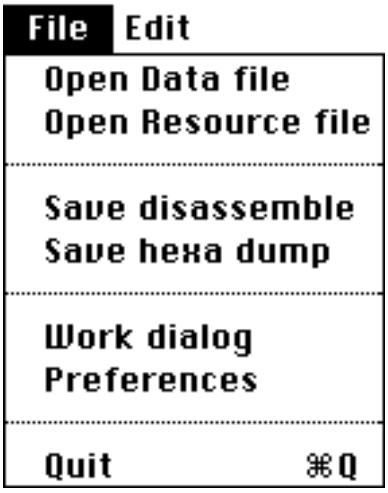
PowerPCdisas est une application qui désassemble du code pour le microprocesseur PowerPC, c-à-d qu'elle convertit une suite de nombres formant un programme (le code) en un texte d'instructions mnémotechniques telles que définies par Motorola (le fabricant du microprocesseur PowerPC), texte qui peut ensuite être lu pour comprendre le déroulement du programme.

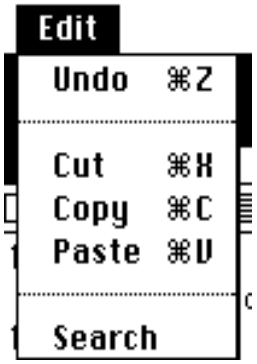
Le dossier PPCdis

Ce dossier est constitué de trois fichiers: PowerPCdisas.French, la documentation en français, PowerPCdisas.English, la documentation anglaise et PowerPCdisas, l'application désasembleur. **Ce logiciel est gratuit et peut être distribué librement à la condition de donner l'ensemble des trois fichiers.**

A l'ouverture

L'application peut désassembler un fichier de données, une ressource à l'intérieur d'un fichier ou une seule instruction à la fois. A l'ouverture de PowerPCdisas, vous verrez les menus habituels **File** et **Edit**. Le menu **File** contient 7 éléments:



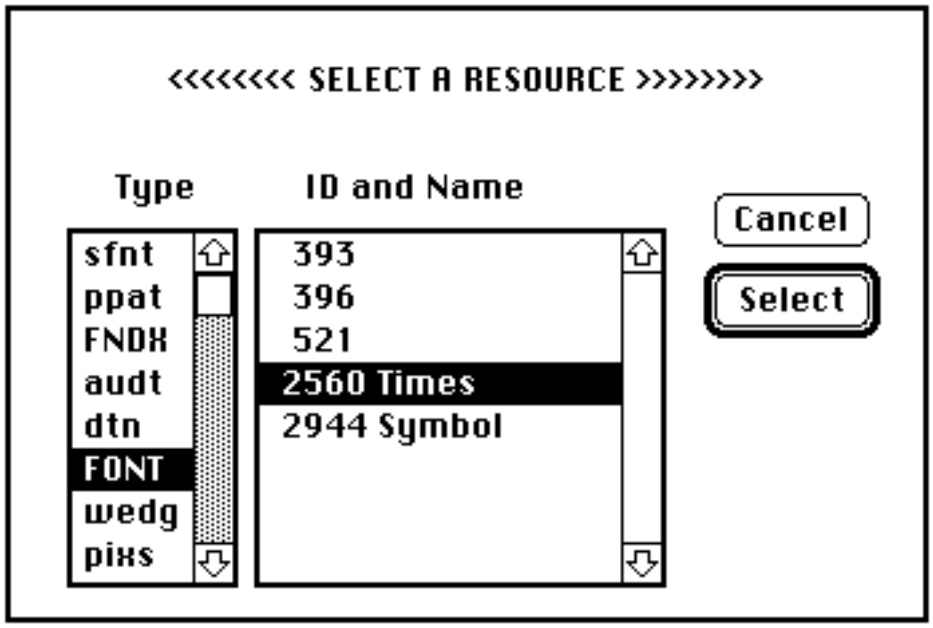


Open Data file

Présente la boîte de dialogue standard pour sélectionner le fichier de données à désassembler.

Open ressource file

Présente un boîte de dialogue standard pour sélectionner le fichier à désassembler. Une seconde boîte de dialogue permet de choisir la ressource désirée.



En sélectionnant un type particulier dans la fenêtre de gauche, la fenêtre de droite affichera le numéro et le nom de toutes les ressources de ce type. Pour désassembler une ressource, vous devez sélectionner un type et un numéro de ressource.

Save disassemble

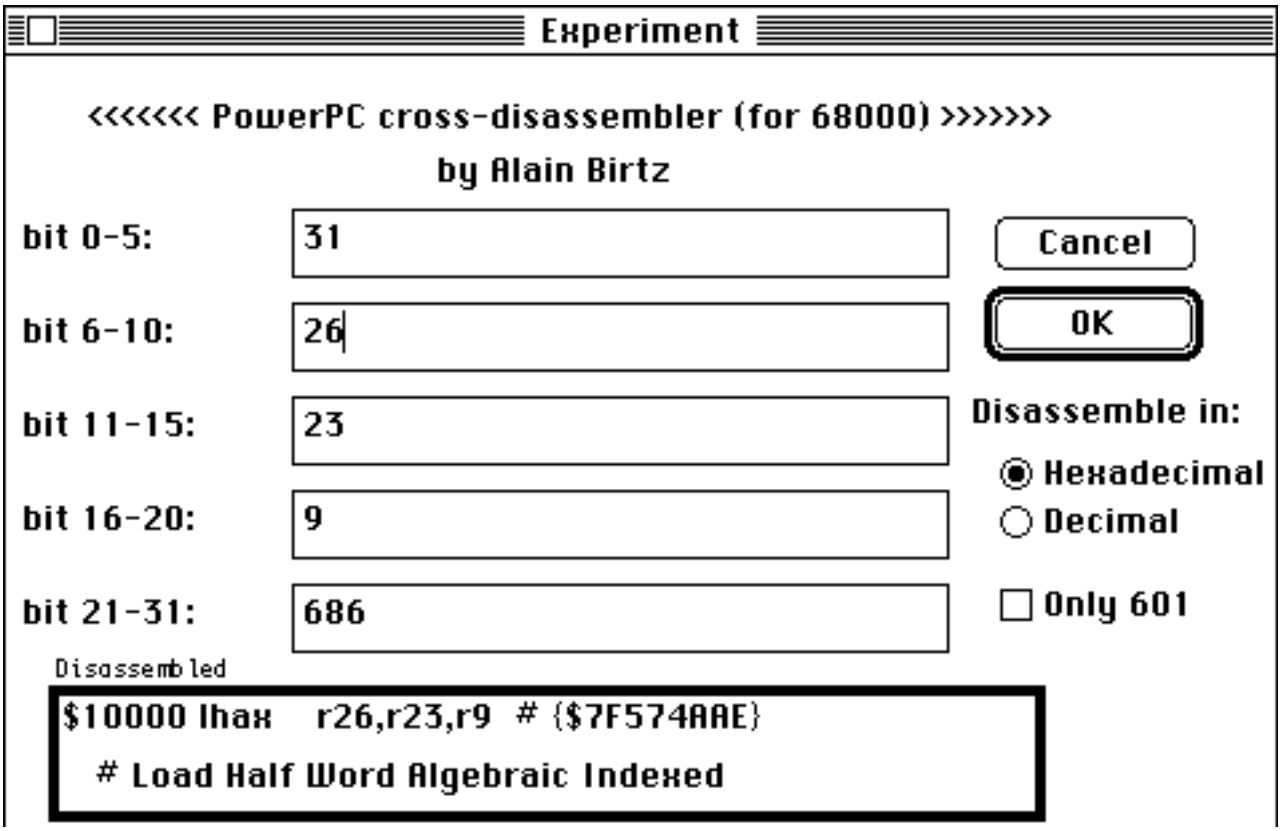
Présente la boîte de dialogue standard pour sauvegarder le texte du dernier fichier desassemblé.

Save hexa dump

Présente la boîte de dialogue standard pour sauvegarder le texte du dernier fichier représenté sous forme hexadécimale et ascII.

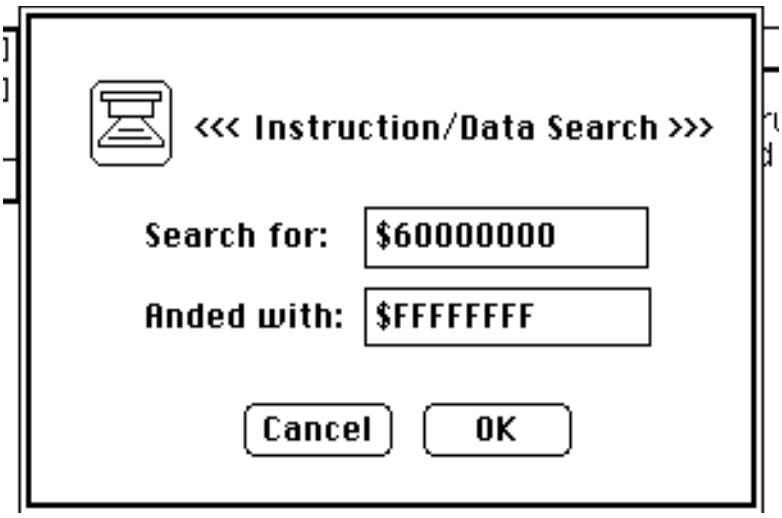
Work dialog

Présente la boîte de dialogue de travail pour désassembler une instruction à la fois. Les cinq premiers champs d'édition représentent la répartition binaire la plus courante d'une instruction pour le microprocesseur PowerPC. Vous pouvez entrer les valeurs en nombres décimaux ou hexadécimaux. Pour ces derniers, vous devez ajouter le préfixe **$**. Le rectangle du bas montre le résultat lorsque la clé **Return** ou **Enter** est pressée ou lorsque le bouton **OK** est utilisé. Les nombres affichés dans ce rectangle seront en décimal ou hexadécimal selon l'état de deux boutons-radio **Hexadecimal** et **Decimal**. La case **Only 601**, si cochée, force le désassemblage du code PowerPC 601 seulement. Autrement le code est désassemblé même pour les instructions qui n'appartiennent pas au 601, mais qui sont définies dans le manuel de Motorola (pour 604 ou 620 ?).

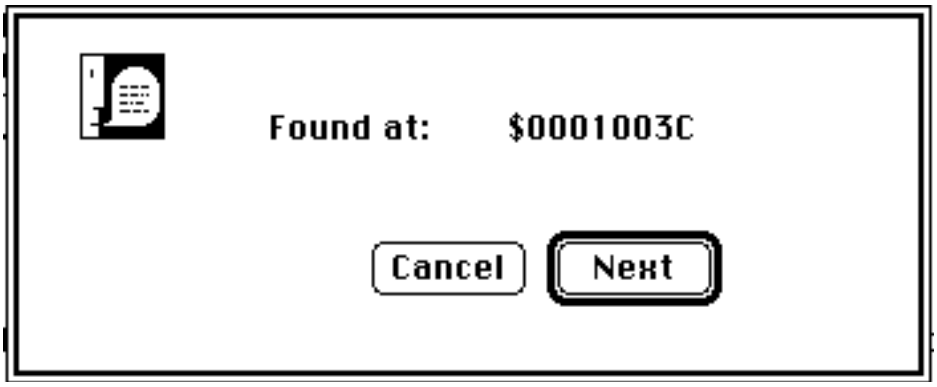


Le menu Edit

Utilisez ce menu pour les opérations de copier-coller habituelles. Vous ne pouvez sélectionner et copier qu'une seule ligne à la fois dans les fenêtres **Hexa Dump** et **Disassemble**. Les équivalents clavier commande-c, commande-v sont reconnus. L'item Search permet de rechercher un mot de 4 octets dans la ressource ou le fichier de données ouvert. La boîte de dialogue ci-dessous sert à entrer le mot à rechercher et le masque de recherche.



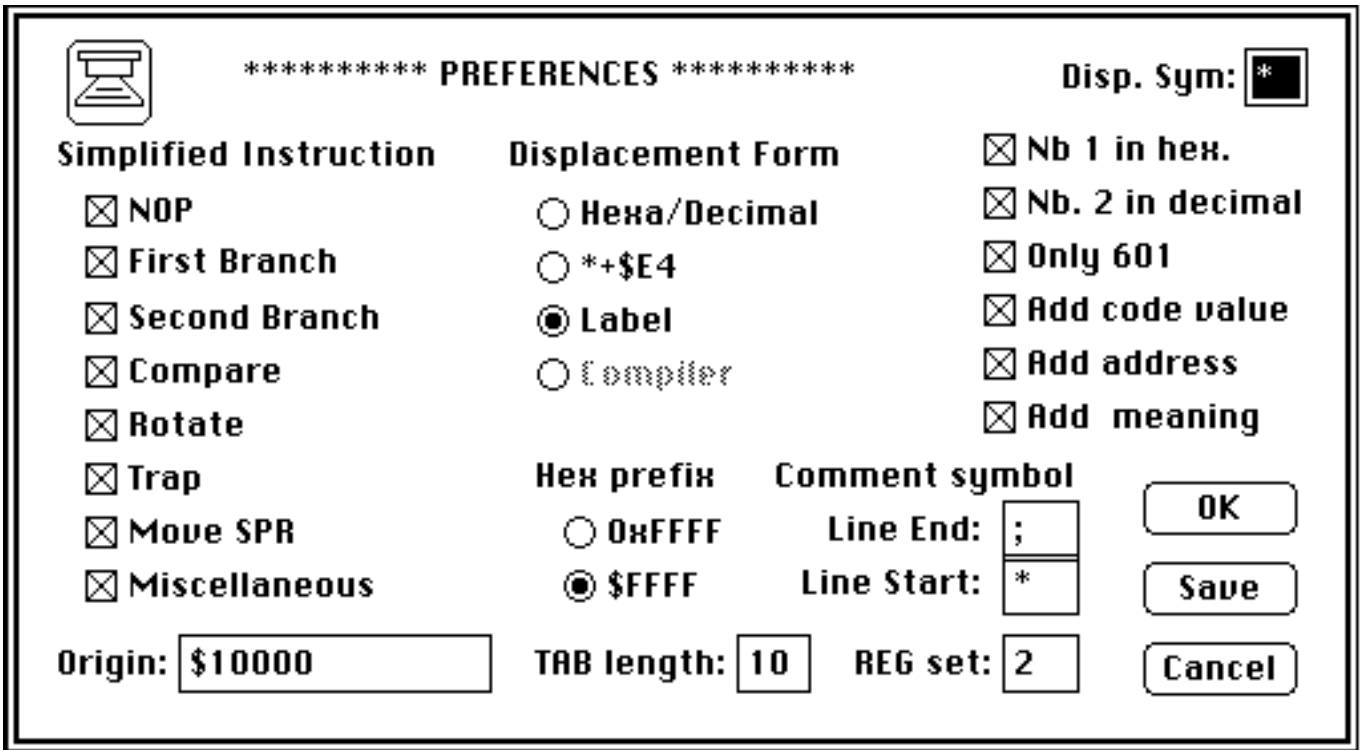
Chaque mot de 4 octets est masqué (seuls les bits 1 du masque sont considérés pour la recherche) et comparé avec le mot recherché. Si la comparaison est positive, la boîte de dialogue suivante apparaît:



Avec le bouton **Next** la recherche se poursuit, tandis que le bouton **Cancel** annule la recherche et retourne au menu.

Preferences

Présente la boîte de dialogue des préférences.



Simplified Instruction cette case détermine l'usage des formes simplifiées des instructions PowerPC 601 désassemblées.

NOP: remplace **ori 0,0,0**. Cette instruction ne fait rien

First Branch: pour tous les branchements **bc**, **bca**, **bclr** and **bcctr**

Second Branch: formes alternatives pour les instructions "branchement si vrai" ou "branchement si faux"

Compare: pour les instructions **cmp**, **cmpl**, **cmpi**, **cmpli**

Rotate: pour les instructions **rlwnm**, **rlwinm**, **rlwimi**

Trap: pour les instructions **tw** et **twi**

Move SPR: pour les instructions **mtspr** et **mfspr** instructions

Miscellaneous: pour **addi**, **addis** avec premier argument égal à r0 et **or**, **nor** avec les deux derniers arguments égaux (**mr**, **not**)

Note: La clé **s** est utilisée pour employer ou non ces formes simplifiées

Displacement Form ces boutons-radio déterminent la forme des opérandes destination dans les instructions de branchement, et les adresses des instructions en début de ligne

Hexa/Decimal: opérandes et adresses sont montrés sous forme de nombres (hexadécimaux, ou décimaux selon la case **NB 1 in hex.**)

***+$E4**: les opérandes sont montrés comme déplacement relatif au PC (déplacement hexadécimaux, ou décimaux selon la case **NB 1 in hex** et symbole PC comme défini dans le champ d'édition **Disp. Symb.**)

Label: opérandes et adresses sont montrés sous forme d'étiquettes LR_23 (pour les étiquettes provenant d'instructions de branchement relatif au compteur de programme, c-à-d ceux qui mettent à 1 le bit LK), LA_23 (pour les étiquettes provenant d'instructions de branchement absolu,c-à-d ceux qui mettent à 0 le bit LK) et LB_23 (pour les étiquettes provenant d'instructions des deux formes)

Compiler: pas encore implanté dans cette version

Note: La clé ***** key peut être utilisée pour passer d'une forme à l'autre

Hex Prefix ces boutons-radio déterminent le préfixe utilisé pour les nombres hexadécimaux: **$** ou **0x**

Comment Symbol ces champs d'édition déterminent les caractères utilisés pour les commentaires

Line Start: pour 68K, une ligne complète de commentaires débute par *, le Power PC utilise **#**

Line End: pour 68K, un commentaire en fin the ligne débute par un point-virgule, le PowerPC utilise **#**

Origin est le champ d'édition qui contient l'adresse de la première instruction à désassembler

Tab Lengh ce champ d'édition contient la longueur des tabulations utilisées entre les différents champs des lignes désassemblées

Register Set champ d'édition qui porte le numéro de l'ensemble de registre utilisé:

ensemble 0: r0, r1, r2,..., fr0, fr1,...

ensemble 1: GPR0, GPR1, GPR2,..., F0, F1,...

ensemble2: R0, SP, RTOC,..., FP0, FP1,... (standard Apple)

Note: Utiliser la clé **r** pour passer d'un ensemble de registre à un autre

Nb 1 in hex. cette case, si cochée, montre adresse, déplacement et valeurs immédiates en hexadécimal. Autrement ces nombres sont montrés en décimal **Note**: la clé **n** permet de passer d'une forme à l'autre

Nb 2 in decimal cette case, si cochée, montre les petites valeurs telles que les mask et les champs de bits dans les instructions de rotation et décalage, en décimal. Autrement ces nombres sont montrés en hexadécimal **Note**: la clé **n** permet de passer d'une forme à l'autre

Only 601 cette case, si cochée, restreint le désassemblage aux instructions PowerPC 601 seulement. Autrement, les instructions 64 bits sont aussi désassemblées

Add code value cette case, si cochée, ajoute le code hexadécimal, entre accolades, dans l'espace des commentaires, à la fin de la ligne

Add adresse cette case, si cochée, ajoute l'adresse de l'instruction (ou l'étiquette) en début de ligne

Add meaning cette case, si cochée, ajoute une seconde ligne de commentaires contenant la signification du mot clé de l'instruction

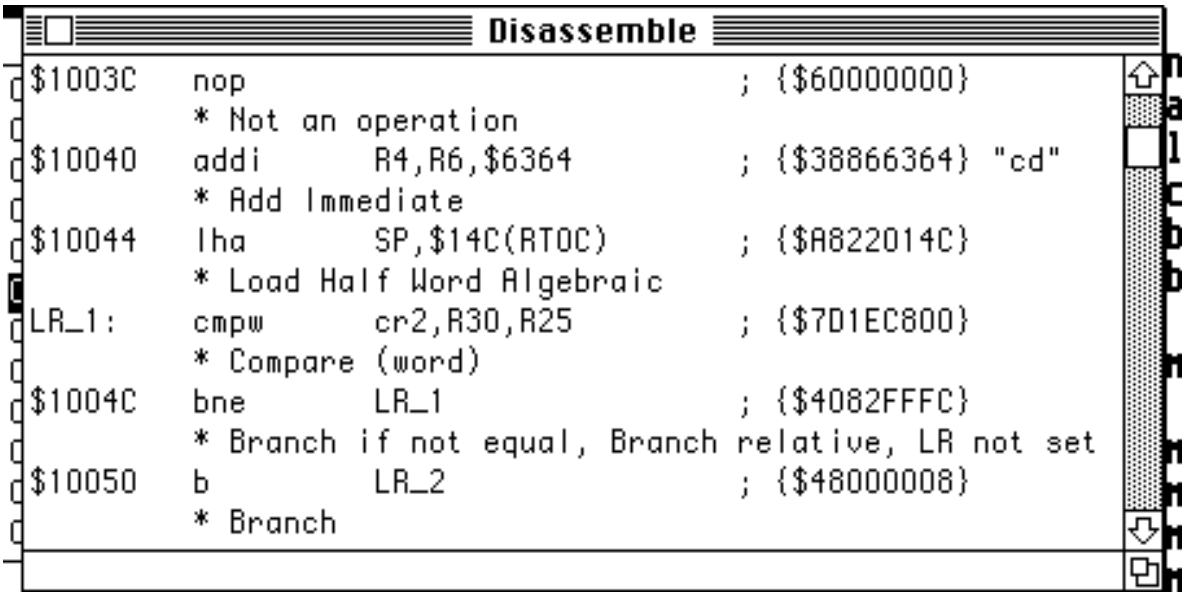
Disp. Symb ce champ d'édition contient le symbole représentant le PC dans les instructions de branchement. Pour le 68K ce symbole est *, dans le PowerPC c'est le symbole $

Save bouton qui ferme la boîte de dialogue, change et sauvegarde la configuration

OK bouton qui ferme la boîte de dialogue, change la configuration, mais ne sauvegarde pas la configuration

Cancel bouton qui ferme la boîte de dialogue sans modifier la configuration

La fenêtre de code désassemblé



Une instruction est désassemblée en deux lignes. La première donne la représentation mnémotechnique de l'instruction et les registres ou valeurs numériques associés. La seconde ligne donne la signification de la représentation mnémotechnique.

Raccourcis clavier

Command C copie la ligne sélectionnée dans le presse-papier

Command W ferme fenêtre et boîte de dialogue

Up arrow défilement d'une ligne vers le bas

Down arrow défilement d'une ligne vers le haut

Shift Up arrow or **Page Down** défilement d'une page vers le bas

Shift Down arrow or **Page UP** défilement d'une page vers le haut

Home va à la première ligne désassemblée

END va à la dernière ligne désassemblée

S ou **s** pour activer ou désactiver les formes simplifiées des instructions

R ou **r** pour passer d'un ensemble de noms registre au suivant

N ou **n** pour passer des nombres en décimal aux nombres en hexadécimal et vice-versa

f clé alignement: ajoute 2 à l'adresse du premier octet du segment à désassembler

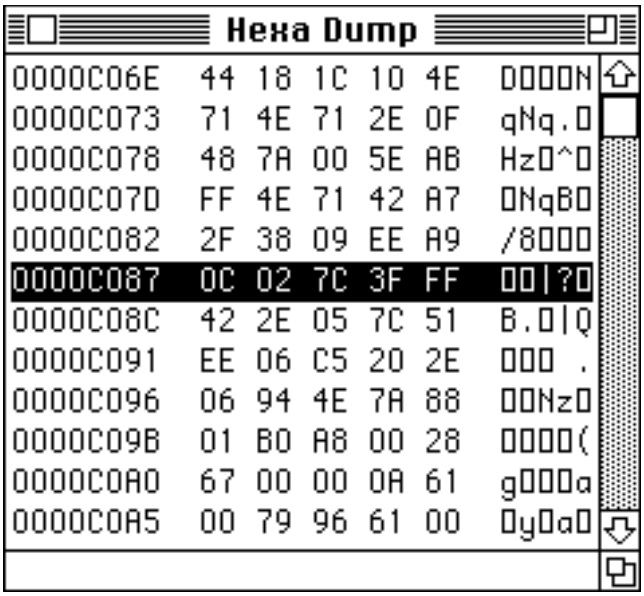
b clé alignement: soustrait 2 à l'adresse du premier octet du segment à désassembler

F clé alignement: ajoute 1 à l'adresse du premier octet du segment à désassembler

B clé alignement: soustrait 1 à l'adresse du premier octet du segment à désassembler

ATTENTION F et B ne doivent pas être employer pour les ordinateurs à base de 68000 puisque ce microprocesseur ne supporte pas le désalignement-mémoire et engendre alors une erreur bus (OK pour 68020, 68030 et 68040).

La fenêtre de représentation hexadécimale



Elle correspond au code de la fenêtre précédente, mais le code est représenté sous forme hexadécimale et ascII.

Rapport d'évaluation

PowerPC disassembler a été testé sur Mac Si et Quadra. Si vous rencontrez certaines difficultés de fonctionnement, s.v.p., laissez un message décrivant les difficultés rencontrées (et le type de matériel utilisé) sur le réseau CompuServe:

[72467,2770]

ou écrivez-moi à:

Alain Birtz
650 Grand St-Charles,
St-Paul d'Abbotsford
P.Q., Canada, J0E-1A0