

# PowerPC disassembler

**Un déssassembleur 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 désassembleur. 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:

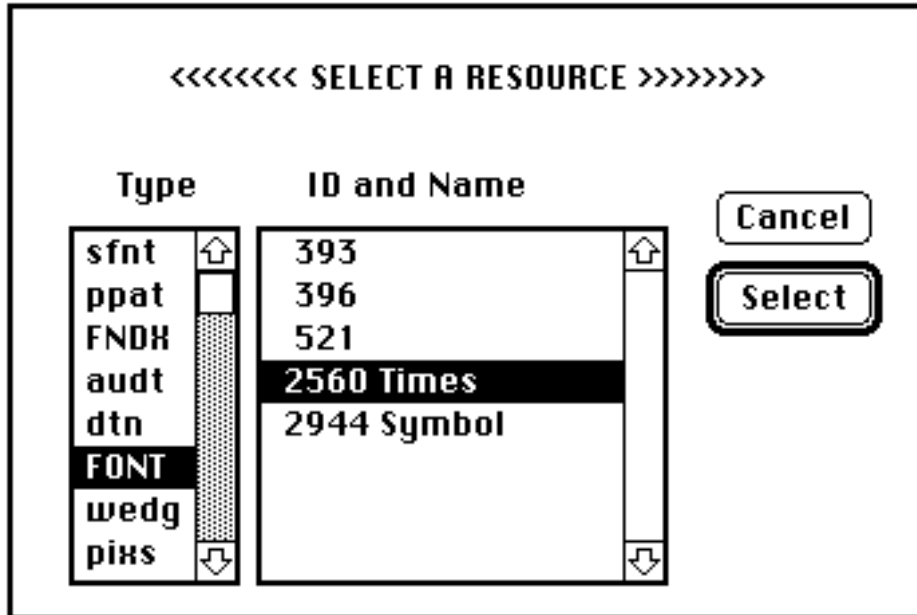
<b>File</b>	<b>Edit</b>
<b>Open Data file</b>	
<b>Open Resource file</b>	
<hr/>	
<b>Save disassemble</b>	
<b>Save hexa dump</b>	
<hr/>	
<b>Work dialog</b>	
<b>Preferences</b>	
<hr/>	
<b>Quit</b>	<b>⌘ Q</b>

## Open Data file

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

### Open resource 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 désassemblé.

### Save hexa dump

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

## 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** 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 ?).

The screenshot shows a window titled "Experiment" with a subtitle "PowerPC cross-disassembler (for 68000) by Alain Birtz". It contains five input fields for bit ranges: "bit 0-5:" (31), "bit 6-10:" (26), "bit 11-15:" (23), "bit 16-20:" (9), and "bit 21-31:" (686). To the right are "Cancel" and "OK" buttons. Below the inputs is a "Disassemble in:" section with radio buttons for "Hexadecimal" (selected) and "Decimal", and a checkbox for "Only 601". At the bottom, a box labeled "Disassembled" shows the instruction: "\$10000 lhax r26,r23,r9 # {\$7F574AAE}" followed by a comment "# Load Half Word Algebraic Indexed".

Field	Value
bit 0-5:	31
bit 6-10:	26
bit 11-15:	23
bit 16-20:	9
bit 21-31:	686

Disassemble in:  
☒ Hexadecimal  
☐ Decimal  
☐ Only 601

Disassembled

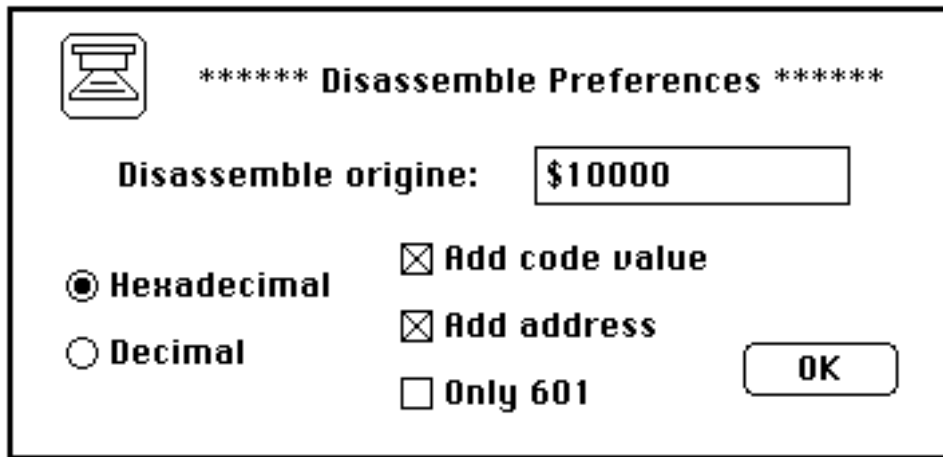
```
$10000 lhax r26,r23,r9 # {$7F574AAE}
# Load Half Word Algebraic Indexed
```

## 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-x, commande-v sont reconnus.

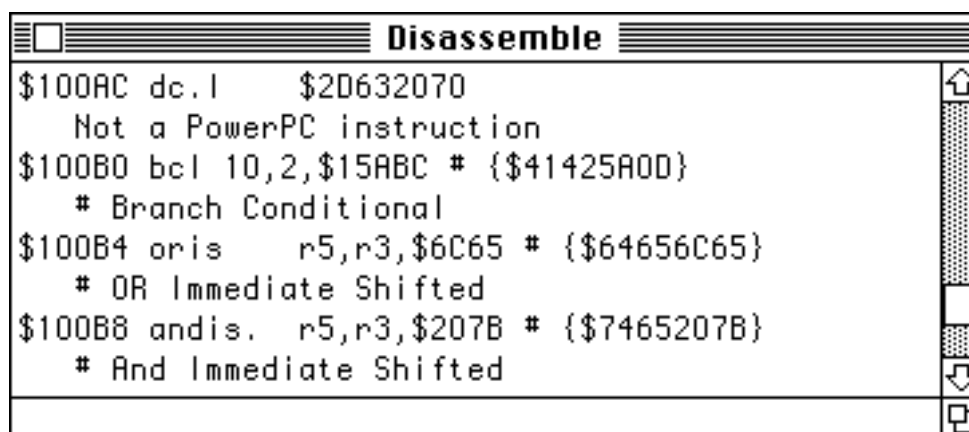
## Preferences

Présente la boîte de dialogue des préférences.



Les deux boutons-radio **Hexadecimal** et **Decimal**, et la case **Only 601**, ont la même signification que ci-dessus. La case **Add code value** ajoute entre accolades la valeur de l'instruction tandis que la case **Add address** ajoute l'adresse de l'instruction en début de ligne. Dans le champ d'édition **Disassemble origine** on fixe l'adresse de la première instruction du code à désassembler.

## 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.

## La fenêtre de représentation hexadécimale

Hexa Dump						
00010000	61	73	6D	20	2D	asm -
00010005	77	62	20	7B	31	wb {1
0001000A	7D	2E	61	0D	69	} .aDi
0001000F	66	20	22	60	65	f " `e
00010014	78	69	73	74	73	xists
00010019	20	2D	66	20	50	-f P
0001001E	6F	77	65	72	50	owerP
00010023	43	64	69	73	61	Cdisa
00010028	73	60	22	0D	20	s " D
0001002D	64	65	6C	65	74	delet
00010032	65	20	50	6F	77	e Pow
00010037	65	72	50	43	64	erPCd

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

## Limitation

Ce désassembleur a été construit à partir du manuel de Motorola seulement. Aucun ordinateur utilisant le PowerPC n'étant actuellement disponible, et aucun assembleur PowerPC n'étant sur le marché, je ne peux pas vérifier l'intégrité du désassembleur.

## Fonctionnement

Compte tenu des remarques précédentes, vous n'avez probablement pas à votre disposition du code natif PowerPC. Pour avoir une idée du fonctionnement du désassembleur, ouvrez un ressource CODE, no. 1, d'une application quelconque. Bien que le code PowerPC n'ait rien en commun avec le code 680x0, vous pourrez voir plusieurs instructions PowerPC désassemblées. Le codage du PowerPC et du 680x0 sont suffisamment dense pour permettre de voir la plupart des instructions PowerPC.

### Développement future

Dès que je pourrais obtenir un (cross) assembleur, je serais en mesure de faire des tests approfondis sur le désassembleur. Je serais aussi en mesure d'ajouter des étiquettes locales pour les instructions de branchement et pourrais utiliser des noms facultatifs pour les formes les plus courantes de branchement.

### Rapport d'évaluation

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

[72467,2770]

ou écrire moi à:

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