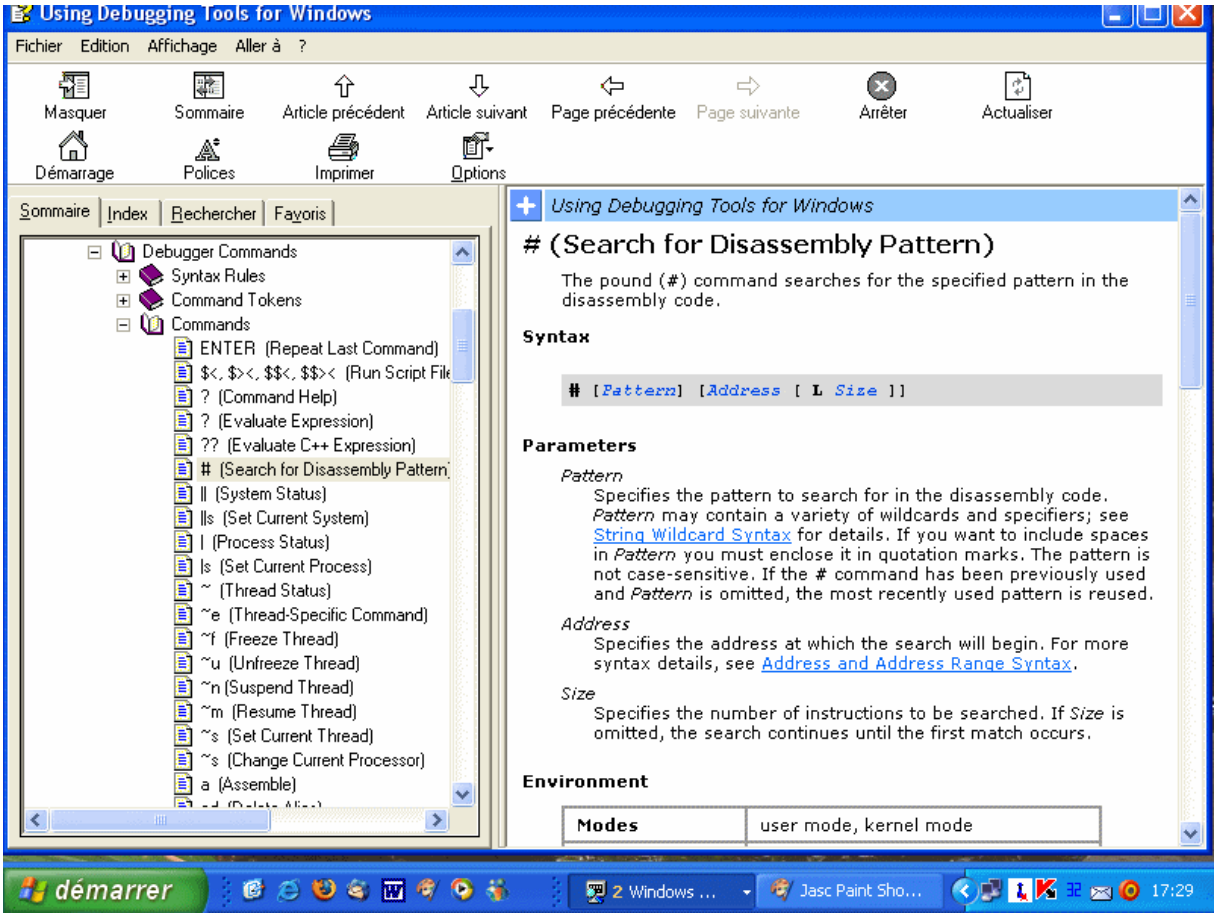
Il existe plusieurs versions de débogueur sur Microsoft. L'outil dépend de son O.S. Ca n'est pas le même pour W 32 W 64 ou Vista.
Une fois choisi son outil il faut lui adjoindre une base appelée Symbols. C'est ce qui va traduire le langage binaire en lignes de commandes style assembleur, VB, C++ etc etc.....Ca dépend aussi de son O.S. Il y a des packs de Symbols différents pour Server 2003, XP 64, XP32, W2000, Vista 32, Vista 64…...
Dans les packs pour XP il faut encore choisir si on utilise SP1 ou SP2 et ça n'est pas le même non plus pour x86 ou Itanium.
Un pack de Symbols est lourd. Le mien installé fait 1 Go. J'ai choisi le pack correspondant à mon systeme exact bien sur.
L'ingénieur Microsoft avec qui je discute parfois du sujet s'est bâti une base de 10 Go. Et il dit qu'il n'a pas tout.

A quoi ça ressemble



On indique dans le débogueur le chemin du dossier Symbols et l'outil ira chercher ses conversions dedans. Convertir le binaire en lignes de commandes n'est pas suffisant. Il faut ensuite faire apparaître les infos en utilisant des commandes en mode texte. Ca ne se fait donc pas tout seul.

Mais que se passe t-il lorsque le fichier à déboguer contient des parties binaires qui ne sont pas dans le pack de Symbols sur le HD ? Tout le monde n'a pas la même configuration évidemment. Il faut aussi configurer le débogueur de manière à ce qu'il aille chercher ce qui lui manque sur le Serveur de Symbols de Microsoft. Dont l'adresse est indiquée sur le site de .....Microsoft. Logique ?

A chaque ouverture de dmp, la recherche se fait d'abord dans le gros fichier sur son HD puis automatiquement va continuer sur le serveur Microsoft.
Microsoft stocke donc l'ensemble de tous les codes binaires ainsi que toutes les conversions en lignes de programmes pour tout ce qui est contenu dans tous les Windows officiels ainsi qu'un grand nombre de fichiers d'éditeurs non Microsoft. Microsoft appelle ça les versions released. Lorsque la conversion n'est pas possible pour des fichiers il va s'afficher le nom du fichier ainsi que la mention qu'il n'a pas pu trouver de Symbols correspondants. « Failed » derrière le nom du fichier. Ne pas trouver une correspondance fichier ne veut absolument pas dire que celui ci est bogué.

Lorsque l'on trouve une liste importante de « FAILED » dans la recherche des conversions binaires, on peut soupçonner qu'il s'agit de PC de Marques qui, comme chacun aurait intérêt à le savoir, ont l'habitude de tripatouiller les Windows. Et Microsoft ne peut pas tracer pleinement les XP modifiés par les intégrateurs justement dans le but d'empêcher les acheteurs de se débrouiller tout seul. Microsoft n'assure aucun appui direct pour les XP OEM. Que le client se débrouille avec le vendeur et son assistance.

Reste ensuite a connaître la programmation du débogueur pour qu'il se logge la ou il faut en cascade, les commandes internes qui vont lancer les types de recherches concernés et bien entendu l'interprétation des résultats. Tout est en anglais.
Mais avec quelques notions de base en programmation et une petite habitude on s'en sort finalement très bien surtout si l'on est un peu anglophone.

Une fois la cause trouvée, un driver .sys ou un .exe il suffit de consulter les bases sur le web afin de connaître le soft qui utilise ce fichier bogué.
D'ailleurs soi-même sur son PC une fois connu le fichier en cause, il suffit d'afficher ses propriétés et l'on trouve immédiatement à qui il appartient.

Mais lorsqu'il s'agit de fichiers système protégés, c'est beaucoup plus difficile car ce qui a bloque le PC est très rarement la cause directe du plantage mais un élément de la chaîne de processus. Je pense par exemple a ntoskrnl.exe (qui est la dernière étape de la séquence de boot) et qui n'est presque jamais bogué lui-même car il serait remplace automatiquement au reboot. C'est fou ce que ce fichier est concerné dans les analyses.
Dans ce cas précis ça indique une anomalie de la séquence oui mais où ? Difficile.
Pour terminer, il est très facile (lorsque l'on sait déboguer) de trouver les causes des ennuis générés par des softs ou drivers rajoutés. Par contre, il est beaucoup plus difficile de tracer les raisons précises qui génèrent des plantages de certains fichiers système.