Guide d'Aide

-

Sysdata, Minidump, BSOD

http://sysdata.free.fr

SOMMAIRE

I. Les Symptômes

Il existe deux types de symptômes selon la configuration de votre ordinateur.

1. BSOD : Blue Screen Of Death *(écran bleu de la mort)*

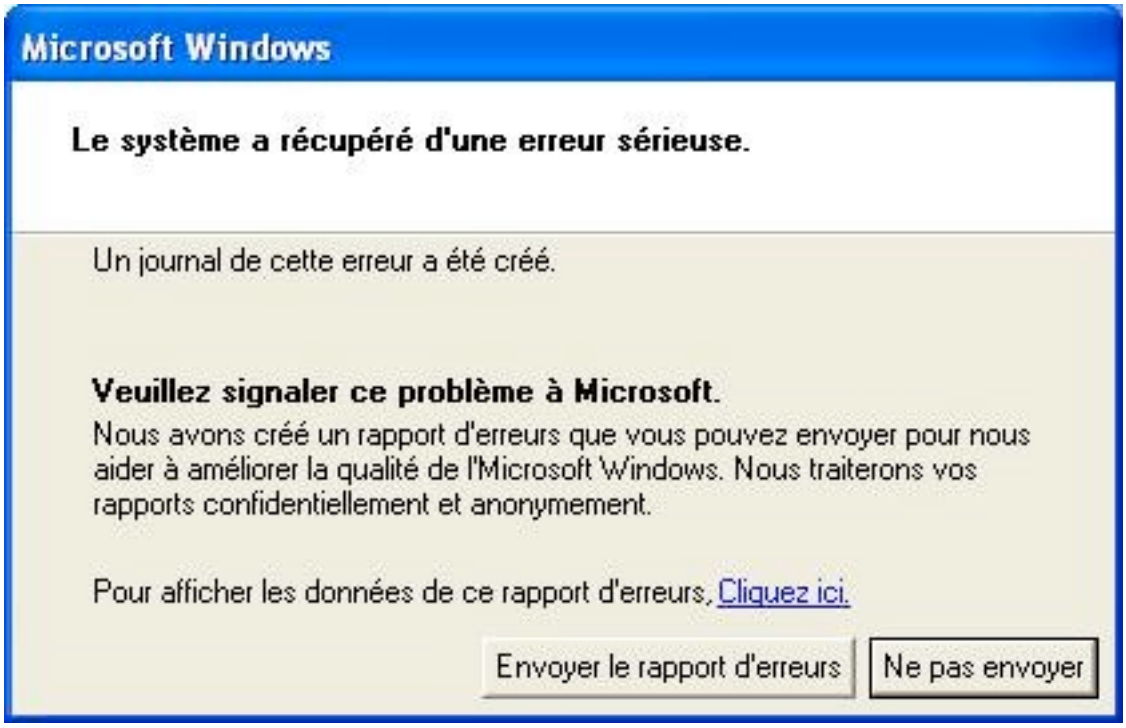
Ce premier symptôme se traduit par un écran qui est entièrement bleu, avec des écritures blanche. Le message suivant peut apparaître.

*** STOP: 0x0000000A(0x00000011,0x0000002,0x00000001,0x80443205)
IRQL_NOT_LESS_OR_EQUAL

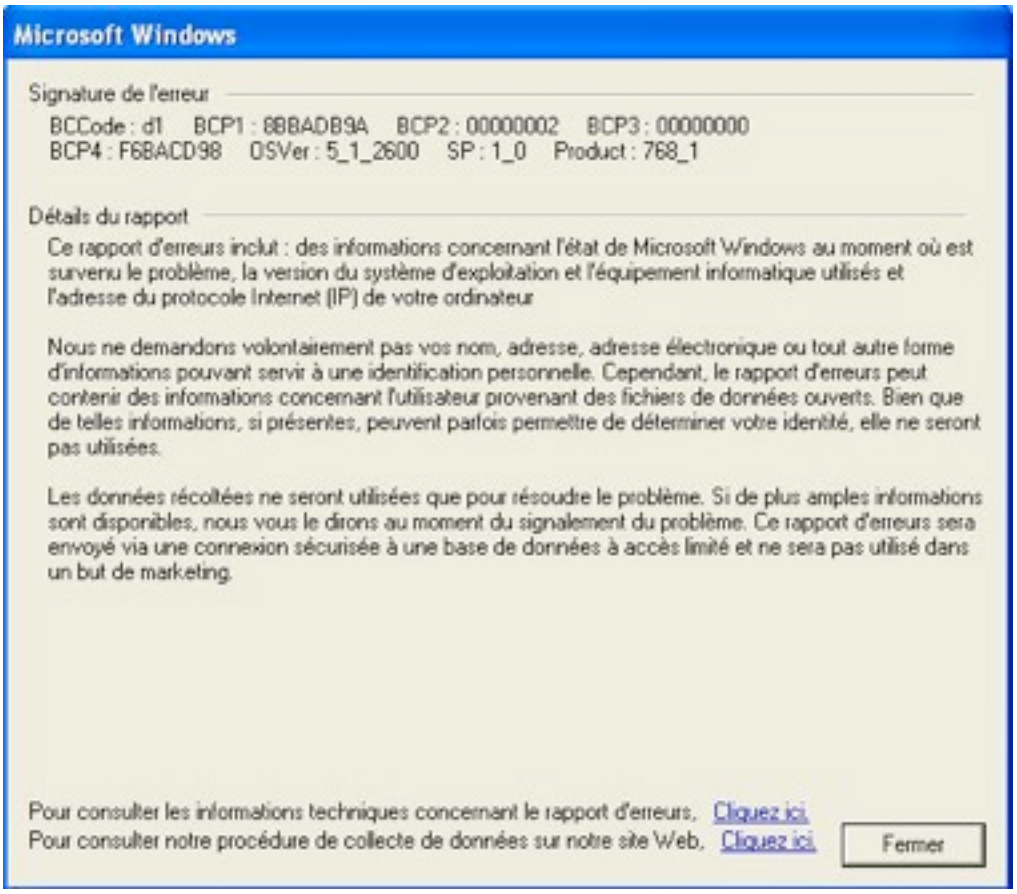
2. Redémarrage Automatique de l'Ordinateur

Ce second symptôme se traduit par un redémarrage non commandé de votre ordinateur. Lors de chaque redémarrage, généralement votre ordinateur crée un rapport d'erreurs que je vulgarise par "Rapport Minidump", si ce n'est pas le cas veuillez configurer sa création automatique.
On peut s'imaginer ce "rapport minidump" comme la boite noire d'un avion, en effet ce fichier contient un ensemble d'information sur votre ordinateur, qui une fois analysé nous indiquera la cause du problème.
Au moment où votre ordinateur a fini de lancer Windows, et que vous arrivez sur le bureau, ce dernier vous tient informer d'une erreur et peut vous afficher le message suivant :

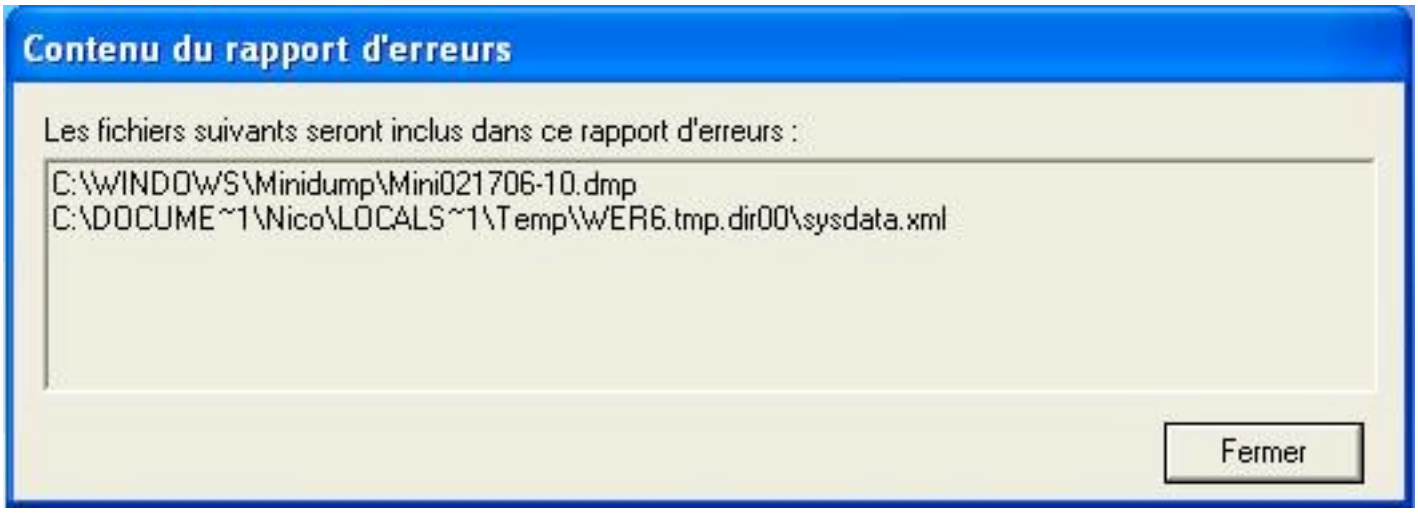
Afin



d'afficher les données du rapport d'erreurs j'appuis sur "Cliquez ici".



Dans cette fenêtre on obtient déjà des informations sur la signature de l'erreur, mais ceci reste difficilement exploitable, on cherche donc à afficher les informations techniques concernant le rapport d'erreurs, j'appuis donc sur le premier "Cliquez ici".



Cette dernière fenêtre commence à révéler des informations qui seront peut être par la suite exploitable:

-l'emplacement du rapport minidump: **C:\WINDOWS\Minidump**

-le nom du rapport minidump : **Mini021706-10.dmp** (ce nom est un exemple)

II. L'explication

Un processus en mode noyau ou un pilote ont tenté d'accéder à un emplacement mémoire sans autorisation. La cause peut être un matériel ou un logiciel défectueux ou incompatible. Dans le message de l'écran bleu il est possible de voir quel est périphérique est responsable, ce qui est un élément non négligeable pour résoudre le problème. Dans ce cas il est conseillé de retirer ou remplacer le périphérique. Il peut aussi s'agir d'un problème de pilote incompatible, d'un service système, d'un antivirus ou d'un programme de sauvegarde.

III. Recherche de la Cause et Résolution du Problème

1. La Méthode Pro

Cette méthode peut paraître longue est complexe au novice, mais elle marche tout le temps, c'est pour cela que je vous la recommande.
L'objectif consiste à exploiter les informations du rapport minidump afin de les analyser, pour trouver l'élément qui ne fonctionne pas.

A. La recherche du rapport minidump

Vous les trouverez généralement à l'emplacement suivant: *C:\WINDOWS\Minidump*

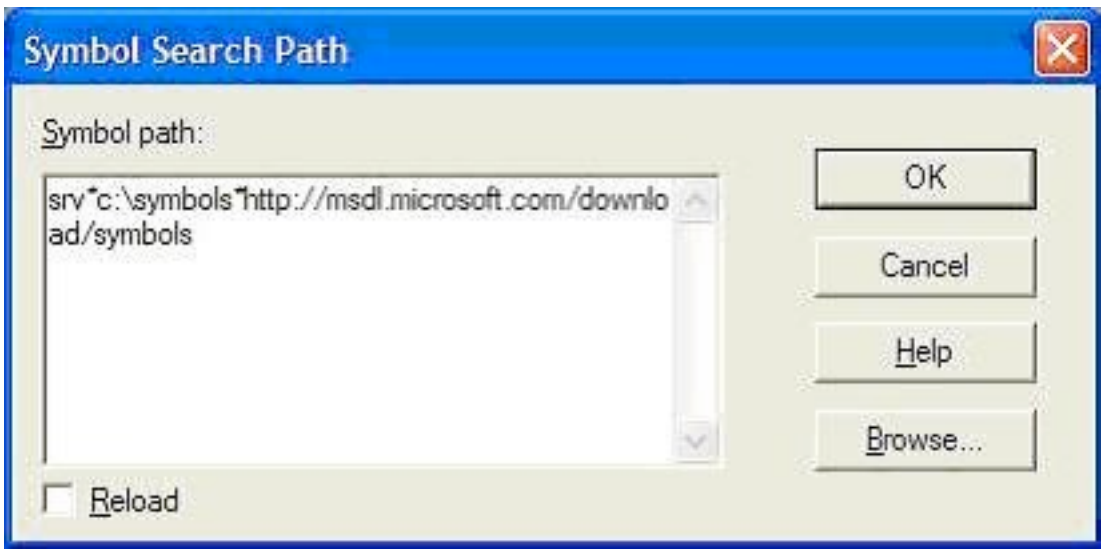
B. Le logiciel d'analyse : Windbg

a. Le Téléchargement

Cette outil est Windbg qui est téléchargeable gratuitement sur :
http://www.microsoft.com/ddk/debugging ou ICI .

b. L'Installation

L'installation du logiciel en soi est assez classique, je me passerai d'explication.
Une fois installé, il est nécessaire de paramétrer le chemin d'accès aux symbols (symboles en français dans le texte) qui permettent notamment de voir quelles sont les fonctions qui ont été appelée dans la pile, de voir les structures,etc ... avec leur petit nom d'origine. La plupart des fonctions et structures du noyau commencent par nt!.
Les symboles sont disponibles en ligne, soit en téléchargement en package, soit sur les CD des produits, soit en téléchargement à la volée. C'est cette dernière option que je vous conseille. Pour cela, allez dans le menu **File** puis **Symbol File Path**… puis tapez :
srv*c:\symbols*http://msdl.microsoft.com/download/symbols



Cela vous permettra de charger automatiquement les symbols dont vous avez besoin et les stocker localement dans le répertoire c:\symbols. Attention, les chargements peuvent être long, les fichiers symbols sont en général assez gros, au minimum de la taille du fichier binaire. L'avantage de cette solution est que vous n'avez pas à vous soucier de choisir les bons symbols, c'est Windbg qui s'en charge pour vous.

C. L'analyse du rapport minidump

Voici le lien d'un tutorial concernant le fonctionnement du programme :

http://www.netix.free.fr/tutos/windbg/windbg.htm

Lancer l'analyse de votre rapport minidump par Windbg. Cette analyse peut être plus ou moins longue, cela dépend de votre rapport. Un fois l'analyse terminé, le logiciel nous expose les conclusions de son analyse, comme dans l'exemple suivant :

```
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

Use !analyze -v to get detailed debugging information.
BugCheck D1, {0, 2, 0, f8b842a4}
*** ERROR: Module load completed but symbols could not be loaded for CRASHDD.SYS
Probably caused by : CRASHDD.SYS ( CRASHDD+2a4 )
Followup: MachineOwner
```

Nous nous intéressons à l'avant dernière ligne de ce rapport qui nous indique la cause probable. Dans cette exemple il s'agit de **CRASHDD.SYS** .

D. La compréhension du problème

Une fois le fichier causant problème identifié, on cherche à trouver le driver dont il fait parti. Pour cela, je vous recommande de faire comme ça :

1. Rechercher le fichier sur le disque
2. Regarder les propriétés de ce fichier, en faisant un "clic droit propriété" sur le fichier puis aller dans l'onglet "version". Les informations que vous y trouverez vous permettront de trouver le fabriquant, des infos pour vous aider à identifier à quoi il sert. Dans le cas où cette description serait vide, il vous reste encore la possibilité de regarder dans quel répertoire est ce fichier et quelle sont ceux qui l'entour. S'il est vraiment tout seul dans un répertoire banalisé ou perdu au milieu du répertoire windows \system32, le dernier espoir est la recherche de toutes les chaînes de caractères du fichier. En général, on y trouve des informations sur les

clés de registre, des messages d'erreur, etc.. Dans le cas d'un fichier appartenant à un driver, utilisez le gestionnaire de périphérique pour retrouver exactement le driver en cause. Accessoirement en dernier recours il vous reste encore Google avec lequel vous pouvez continuer à chercher toute information se rapporte à ce fichier.

3. Une fois le fichier et son environnement identifié, il ne vous reste plus qu'à agir : en général cela passe par l'installation d'un nouveau driver ou le passage d'un bon patch.
   Dans tous les cas, quand le problème est bien identifié vous savez d'ou viens le problème. A partir de là c'est à vous de prendre la décision de changer ou de réparer la source du problème.

E. Une alternative de l'analyse

Pour les plus feignant d'entre vous, il existe la possibilité de laisser Microsoft faire une partie du boulot pour vous, en allant sur le site http://oca.microsoft.com/fr/windiag.asp et en soumettant vos minidump sur le site. Le truc sympa c'est qu'ils font analysés et parfois vous avez une réponse pertinente vous indiquant un driver à mettre à jour. Si vous utilisez Windows XP ou supérieur , à la suite d'un crash, une boîte de dialogue s'ouvre et vous demande si vous souhaitez envoyer un rapport à Microsoft. Faites-le, ils l'utilisent pour savoir d'où viennent les problèmes et les corriger ou les faire corriger par les constructeurs de hardware développant leurs drivers.
Bonne analyse…

2. Divers Petites Méthodes

Je vais traité ici de plusieurs méthodes alternatives à la précédente qui touche une quantité réduite de problème mais qui peut facilement et rapidement résoudre les problèmes de plusieurs d'entre vous.

A. Les causes générale

a. Lorsque toutes les conditions suivantes sont réunies :

• La RAM effectue un vidage hexadécimal vers le disque.
• Le fichier minidump est plein.
• Le fichier d'échange continue d'indiquer que le fichier crash nécessite une réécriture.

Le message d'erreur suivant apparaît :

» x:\DOCUME~1\…\LOCALS~1\Temp\WERb0c2.dir00\Mini120304-02.dmp »
» x:\DOCUME~1\…\LOCALS~1\Temp\WERb0c2.dir00\sysdata.xml »

b. Peut apparaître après :

• Une mise à jour du chipset de votre carte mère
• La modification de votre configuration mémoire RAM (ajout/suppression de barrettes).
• L'overclocking ou la défaillance de votre processeur.
• Une mauvaise fixation du ventilateur du processeur de la carte graphique.
• Une defaillance du ventilateur du processeur (poussière, tension trop faible,…)
• Une attaque virale.

B. Les différentes solution

a. Suppression des Minidump

- Chercher un dossier contenant sysdata, normalement sur C:\windows\minidump.
- Copier ce dossier sous un autre nom (par précaution)
- Supprimer le dossier.

- Supprimez le ou les sous-dossiers nommés « WER1.tmp.dir00″
- Redémarrer
- Windows va recréer automatiquement ce dossier
- Tester
- Supprimer le dossier de « précaution » si tout fonctionne parfaitement.

b. Mise à jour

-Installer les dernières mise à jour de windows.

c. La mémoire RAM

-Tester votre mémoire RAM avec un logiciel comme « Windows Memory Diagnostic »
http://oca.microsoft.com/en/windiag.asp
- Augmenter votre mémoire RAM
- Vérifier la température du processeur.
- Dépoussiérer tous les ventilateurs.

d. Générer la mémoire virtuelle

-Aller dans « propriétés » puis cliquer sur « avancé »
-Choisir « Paramètres de performances » puis « avancé » des « Options de performances »
-Cliquer sur « Modifier » dans la zone « Memoire virtuelle »
-Cocher la case « Taille gérée par le système »
-Redémarrer.

e. Modification de l'image mémoire

-Demarrer en mode sans echec.
-Aller dans « propriétés » puis cliquer sur « avancé »
-Aller dans » Ecriture des informations de déboggage »
-Changez la commande » Image mémoire partielle (64 Ko) » par » Image mémoire complète « .
-Redémarrer.
-Mettre à jour le chipset de la carte mère
-Mettre à jour les drivers de la carte graphique.
-Redémarrer.