

# BSOD (Blue Screen of dead) ECRAN BLEU DE LA MORT

Il arrive fréquemment d'avoir un coup un écran bleu bloquant le pc et au contenu incompréhensible

Ce type de problème peut avoir différentes origines : pilotes mal écrit ou obsolètes, programmes comportant un ou plusieurs bug, incompatibilité entre 2 programmes, panne matériel etc.

Sur certains de ces cas Windows génère alors un fichier de débogage (bugcheck) qu'il place dans un répertoire \minidump du répertoire système (exemple c:\windows\minidump) et a un nom en rapport avec la date du BSOD exemple Mini060307-01.dmp il est alors possible de lire ce fichier pour avoir une information plus précise de la cause du problème

Explication ici :

<http://support.microsoft.com/kb/315263/fr>

Outils téléchargeables ici :

<http://www.microsoft.com/whdc/devtools/debugging/installx86.msp>

Le plus simple c'est :

- Installer les outils
- Aller en invite de commandes dans le répertoire c:\program files\debugging tools for Windows (Sous Vista lancez la ligne de commande en mode administrateur)
- Lancer en ligne de commande par un copié collé :

```
windbg -y srv*c:\symbols*http://msdl.microsoft.com/download/symbols -i  
c:\windows\i386 -z c:\windows\minidump\minidump.dmp
```

(En remplaçant minidump.dmp par le nom du fichier à analyser (Mini060307-01.dmp par exemple) ou en le renommant préalablement en minidump.dmp)

Exemple dans un cas où le BSOD avec une erreur 0x10000001d n'était pas parlant j'ai eu ça en réponse :

```
Unable to load image alcaudsl.sys, Win32 error 0n2
```

```
*** WARNING: Unable to verify timestamp for alcaudsl.sys
```

```
*** ERROR: Module load completed but symbols could not be loaded for alcaudsl.sys
```

```
*** WARNING: Unable to verify timestamp for alcan5wn.sys
```

```
*** ERROR: Module load completed but symbols could not be loaded for alcan5wn.sys
```

```
Probably caused by : alcaudsl.sys ( alcaudsl+2f14 )
```

## **BSOD (Blue Screen of dead) ECRAN BLEU DE LA MORT**

Une petite recherche sur le web indique que alcaudsl.sys est un pilote Alcatel Donc indique que le bugchek est probablement lié aux pilotes d'un modem Alcatel speedtouch ADSL branché sur la machine

Dans d'autre cas, la première réponse peut ne pas être parlante ou sans surprise.

Faire alors une analyse détaillée :

sur cette ligne :

**Use !analyze -v to get detailed debugging information.**

cliquez sur le lien **analyze -v** ça permet d'avoir plus d'informations parfois parlantes.

J'ai eu par exemple le cas d'un BSOD systématique à l'extinction d'un PC depuis l'installation d'un antivirus et la suppression de l'antivirus supprimais aussi le problème donc on se dit : ça viens de l'antivirus et le bugchek indique effectivement qu'il peut être en cause. Hors cet antivirus fonctionnant sur d'autres machines du réseau il n'est alors donc pas seul en cause. En fouillant un peut plus le bugchek on peut alors se rendre compte qu'il y a un message plus parlant dans un lien en bas du 1er rapport et là surprise on trouve parfois un autre protagoniste. Dans mon cas d'antivirus j'ai trouvé ainsi un second soft lié à un lecteur de carte à puce qui n'existait plus sur cette machine une fois celui-ci désinstallé et j'ai laissé l'antivirus sans avoir de BSOD.

En fait à l'extinction l'antivirus tentait de vérifier la présence de virus sur un lecteur fantôme et ça plantais le système. Comme quoi le 1er fautif évident n'est pas forcément le bon.

Attention que l'analyse d'un BSOD n'est pas toujours à la portée de tous, pas toujours interprétable et en anglais