Pourquoi ça plante.

Tous les fichiers qui sont utilisés sur votre machine sont stockés matériellement sur votre disque dur. Mais lorsqu'ils sont en action, ils sont copiés et travaillent dans la ram.
Un fichier peut donc se boguer matériellement sur votre HD (rare) ou bien virtuellement dans la ram. Le virtuel de la ram a un support physique évidemment qui est la ram elle-même.

Un tour par la ram. Cause directe ou indirecte d'une bonne partie des BSOD. C'est le plantage indirect qui est difficile a solutionner.

Très souvent un BSOD survient à cause d'une erreur physique de la ram TOUJOURS IRREPARABLE. A chaque fois qu'une action quelconque va devoir se servir d'une adresse défectueuse de la ram la machine va planter mais de manière plus ou moins grave selon qu'il s'agisse de fichiers système ou bien de fichiers d'applications. Check Memtest86 impératif.
Comme XP a l'installation teste la ram jusqu'au bout même s'il n'en a besoin que de beaucoup moins, s'il rechigne à s'installer, testez la ram.

Les nonames sont des rebuts de fabrication classés B ou C selon la "qualité" de la cochonnerie, qui trouvent des gogos pour les acheter donc pourquoi se gêner ! Elles peuvent passer Memtest et planter. Il suffit qu'elles ne maintiennent pas rigoureusement leurs fréquences. Par exemple au lieu de tourner a 166 la ram peut osciller et passer a 160 ou 163. Memtest ne peut pas le voir car il se sait tracer les fréquences ni contrôler 2 rams en parallèle en relevant les différences. Beaucoup de cartes mère n'aiment pas ça du tout.
Un moyen de verifier : Baisser la fréquence du bus dans le Bios. Par exemple au lieu de 200 mettez 166. Votre machine va être ralentie bien sur mais si ça ne plante plus du tout il s'agit de mauvaise (s) ram en fréquence non stable.

Un impératif. JAMAIS de nonames. Poubelle direct.

2 rams peuvent passer Memtest = ne pas avoir d'erreur et mises ensemble planter. Et deux ram peuvent passer Memtest individuellement et parfois planter en dual. Memtest ne teste pas non plus la synchro des rams multiples.
Nous allons donc aborder les erreurs logiques = qui se remettent toutes seules et que Memtest ne trouvera jamais. Ce sont des plantages vicieux.

Des rams qui fonctionnent très bien en single channel et vont planter en dual. Ce sont souvent des rams qui ne sont pas de la même marque, du même type et des mêmes réglages de latency. Et parfois avec des rams identiques ça peut planter en dual.
Cela provient d'une synchronisation des 2 rams gérée beaucoup trop serrée par certaines cartes mère. Il existe dans les derniers modèles de Bios de qualité une possibilité de modifier la synchro des dual channel, de manière à autoriser des variations plus grandes sans planter. C'est un coche "enabled" ou "disabled".
Ne pas confondre cette synchro avec la synchro ram + bus pour l'overclocking ni avec les 4 réglages de latency. Rien à voir.

D'autres plantages non listés proviennent des cartes mère de très mauvaise qualité comme on trouve dans les machines d'hyper. Les différences de potentiel qui différencient le 0 et le 1 sont maintenant extrêmement faibles alors qu'à l'origine de l'informatique elles étaient de 10 volts. Ces CM bas de gamme sont sensibles aux photons dont l'énergie peut dépasser leur différence puisqu'elles ne possèdent pas de "répétiteurs" permettant de contrôler et maintenir ces tensions. C'est d'autant plus sensible que vous êtes haut. En avion c'est pire.

Et encore plus pendant les éruptions solaires. Des bits peuvent s'inverser. Et aussi au ras du sol.
Ce genre d'incidents a augmenté de 500% en quelques années. Pollution magnétique + qualité de plus en plus déplorable des composants, particulièrement en grande distribution.
Les journaux d'évènements font la différence entre les processus Système et les processus Applications.
Seuls les processus Système génèrent des écrans bleus. Les processus Application sont la plupart du temps "recouvrables" sans rien faire. Ils sont signalés dans DrWatson en mode texte. Dans ce cas "Windows récupère d'une erreur". Un BSOD ne se récupère pas sans devoir rebooter.

Un fichier peut facilement se boguer dans la ram même si celle ci est OK physiquement. Quelque chose peut l'attaquer. Virus, soft mal programmé, conflit de drivers, plages de mémoire qui se chevauchent, permutations de bits causés par certains rayonnements etc. Et c'est le cas infiniment plus souvent qu'une corruption physique sur le HD.

Il ne servirait donc a rien dans beaucoup de cas de plantage kernel = fichiers système protégés, de remplacer tel ou tel élément sur le HD (system32) dont le nom est donné par l'écran bleu ou bien par déboguage.

Il est très difficile d'abîmer un fichier système du noyau protégé de XP à son emplacement dans system32. Par contre, lorsqu'un fichier protégé travaille dans la ram il peut être corrompu comme les autres vu qu'il n'est plus protégé lorsqu'il est virtuel.

Les fichiers protégés de XP possèdent les extensions suivantes:
cpl dll ocx sys drv ime scr ainsi que certains drivers génériques.
Mais ça ne veut pas dire que toutes les dll et autres fichiers de XP sont protégés, seulement ceux du noyau.
C'est protégé par le WPF (Windows Protection File) qui double ces fichiers a d'autres endroits. Dans C:\Windows\drivercache\.....et dllcache.

Si vous voulez vérifier si une dll ou driver .sys ou .exe font partie du noyau protégé de XP c'est facile. Vous « affichez tous les dossiers et le système » dans les Options d'affichage et dans Recherche vous tapez le nom. Si ça se trouve à la fois dans system32 ou system32\drivers et dans un cache c'est que ça fait partie du noyau.

Imaginons que sous la console de récupération DOS (car sinon XP ne va pas se laisser faire) vous supprimiez une dll hyper importante de XP: kernel32.dll. Eh bien au reboot WPF va aller recherche sa copie et la remettre dans system32.

A noter que l'on peut dans le registre désactiver WPF et dans ce cas vous pourrez supprimer (sous console) n'importe quel fichier protége et le boot ne le remettra pas. Très dangereux et réservé aux experts.

Donc lorsque vous avez affaire a un fichier PROTEGE générateur de BSOD il a très peu de risques d'abord qu'il soit attaqué matériellement sur le HD (sinon par un virus, une dégradation physique ou un bogue du système de fichiers) mais même si c'était le cas il serait remis à neuf au reboot.
Et sans devoir rebooter en utilisant la commande sfc /scannow qui va comparer tous les fichiers protégés avec leur originaux.

Par contre un fichier non protége même faisant partie de Windows, et il y en a beaucoup, peut dans certains cas être corrompu aussi sur le HD. Rien ne va venir le réparer et pas non plus la commande de scan. Il faudra le remplacer manuellement en l'extrayant du CD ou du web.

Il est impossible de remplacer un fichier, même non protégé, s'il est en utilisation. Dans un tel cas il faudra travailler en sans échec ou sous Console CMD ou sous Console de Récupération.

Trouver la cause incitatrice d'un plantage est possible avec un débogueur mais trouver la raison exacte de l'attaque c'est beaucoup plus ardu. Sauf si le fichier fait partie d'un logiciel rajouté et alors la c'est facile.
Par exemple tous les drivers NVidia commencent par nv... et ceux d'Ati par ati...Chaque utilitaire a ses drivers propriétaire et dll spécifiques. Les fichiers composants de XP sont listés dans des bases. Avec le coupable donné par le déboguage on trouve le soft ou exécutable ou Service qui génère l'erreur.

Citons le cas des fameux BSOD ntoskrnl et win32k. S'ils sont cités dans beaucoup de cas ça ne veut pas dire qu'ils sont directement responsables d'un plantage noyau mais qu'ils sont impliques dans une séquence plus complexe.
Si votre médecin détecte que vous avez la grippe = il vous a débogué, il ne pourra pas vous dire que vous avez attrapé le virus le 24 à 17h 54 au coin de la rue du Prieuré en croisant Mr Thomson qui a éternué !

Pour trouver l'origine d'un BSOD sans devoir déboguer ou attendre la réponse on peut déjà contrôler ce qui suit:

1) La ram
2) Rappelez vous ce que vous avez rajouté comme matériel ou driver.

Petites statistiques.

Premières causes de plantages BSOD = avec écran bleu.

* La ram. Directement ou indirectement.
* Firewalls autres que celui du sp2= Kerio, ZoneAlarm etc sans oublier le pire de tous, celui de NVidia inclus dans le driver chipset NForce4. Les firewalls non Microsoft causent beaucoup d'ennuis.
* Les drivers USB. Là non plus ce n’est pas triste.

Ces 3 causes génèrent environ 70 à 80% des plantages. (Statistiques sur le déboguage d’environ 800 BSOD)