Pour compléter le « travail en urgence », j'ai créé une clé USB de type boîte à outils. Elle a la particularité de fonctionner sur 2 approches différentes. La première est de s'exécuter en amont du démarrage de l'ordinateur. Elle incorpore une partition « bootable » notamment aux fins de passer les éventuels mots de passe de session Windows. La deuxième approche s'exécute en aval, une fois la session Windows démarrée « autorun ». Elle contient exclusivement des applications dites «portables » sans besoin d'installation au préalable.

Avant toute chose il faut vérifier que l'ordinateur démarre bien, sur le lecteur CD-Rom ou l'USB. En d'autres termes vérifié la séquence de démarrage qui se trouve dans le Bios (First Boot Device). Pour y accéder, il vous suffit simplement au démarrage du PC d'appuyer sur la touche « Suppr ». Une fois dans le Bios, on cherche l'option « Advanced » puis « First Boot Device » et la modifier de façon qu'il affiche CD-Rom/DVD-Rom ou USB. Certaines machines (exemple DELL), ne nécessitent par forcément une modification dans le Bios, un menu raccourcis peut être affiché en appuyant sur la touche F2 au démarrage du PC.

La partition « bootable » a été créée à partir d'une source DOS (fichiers BAT). Un langage facilement abordable ainsi que la création de menu pour l'automatiser au maximum :

1) Permet de réinitialiser le mot de passe contenu dans le Bios. Plus concrètement il permet de supprimer le mot de passe du BIOS si ce dernier a été activé. Pour ce faire sur le menu SESAME, veuillez sélectionner à l'aide des touches directionnelles ou du pavé numérique, le numéro adéquat (1) l'application CMOSPWD. Une fois lancé, l'application vous présente un menu avec trois choix possible :

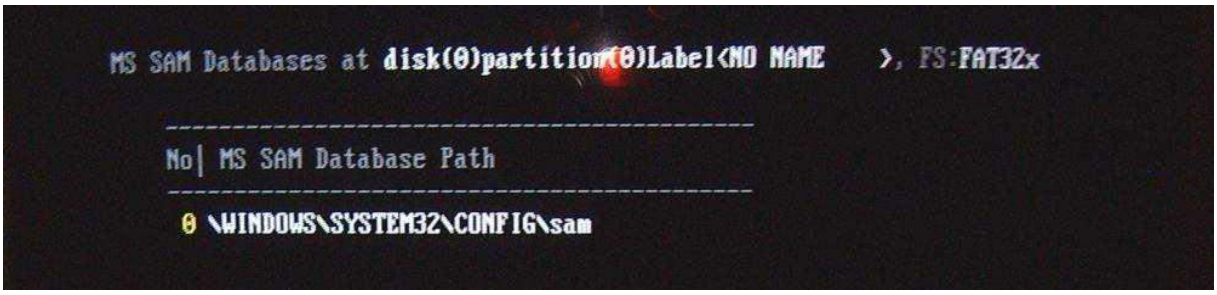
   - (1) Kill cmos
   - (2) Kill cmos (Try to Keep date and time)
   - (0) Abort

   À la ligne « Choice : [ ] », écrivez le numéro correspond a votre choix. Pour notre Exemple on écrira « (1) ».

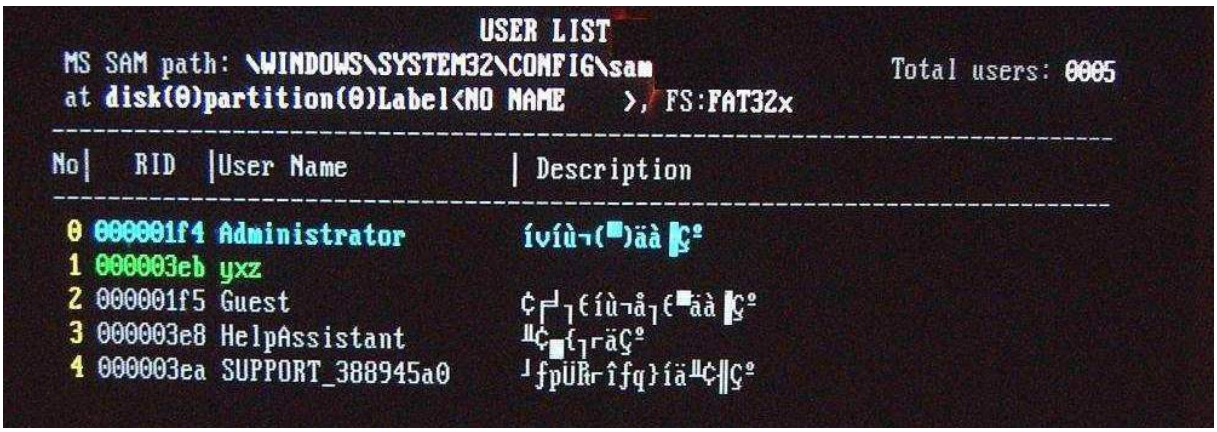
2) Ce logiciel supprime les informations contenues dans le fichier MS SAM de l'ordinateur. En d'autres mots, il permet de supprimer le mot de passe d'une session Administrateur ou utilisateur. Dans le menu SESAME, veuillez sélectionner la touche n°2 ou flèches directionnelles. Un menu OPTION s'affiche :

- (1) Choose logical drive
- (2) Search for MS SAM database(s) on all hard disks and logical drives
- (3) Exit

À la ligne "**Choice : [ ]**", écrivez le numéro correspond à votre choix. Pour notre exemple, on écrira « (1) » (cette option simplifie la recherche du fichier Sam automatiquement). Suivant la configuration de la machine (mémoire), le délai d'attente de recherche du fichier SAM, peut prendre plus ou moins de temps (WAIT).



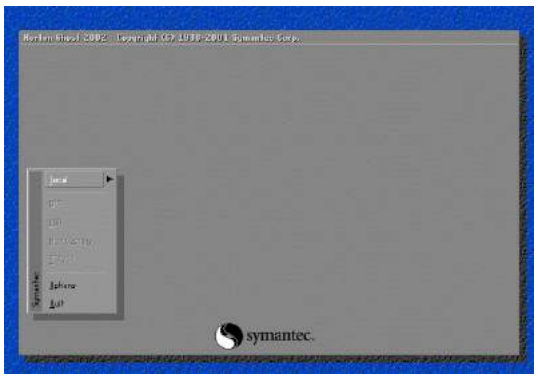
Une fois le fichier SAM trouvé, appuyez sur « Entrer ».

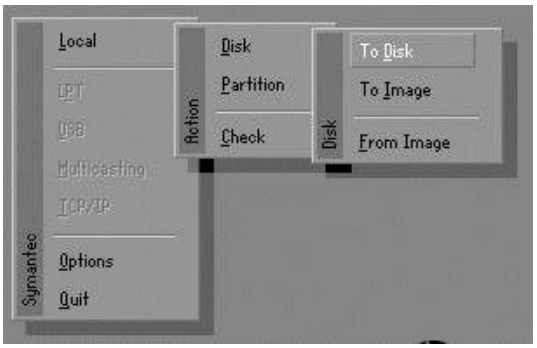


Une liste d'utilisateurs s'affiche (Administrateur, User, invité,…). Au moyen des touches numériques, sélectionner l'utilisateur dont vous voulez effacer le mot de passe dans l'espace « Your CHOICE : ». Puis valider par « Entrer ».

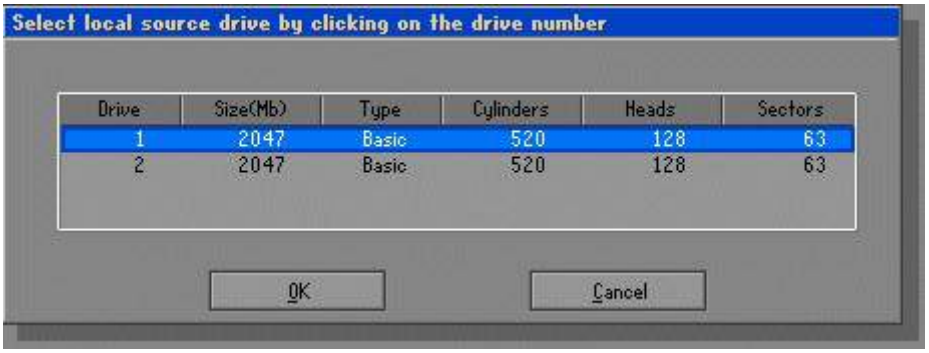
Il vous demande de le confirmer en appuyant sur la touche « Y » ou Esc pour quitter cette sélection (laissez les options par défaut). « Press Y to save changes and exit or Esc to exit without saving ". Appuyez sur Esc plusieurs fois pour sortir de l'application.

3) Ce logiciel clone les disques durs. Il permet de faire une copie exacte d'un disque source vers une image ou disque cible. Dans le menu SESAME, veuillez sélectionner la touche n°3 ou flèches directionnelles. Une fois le logiciel (Norton Ghost 2002 ou 2003) lancer, un message « accord de licence s'affiche ». Cliquer à l'aide de la souris sur « OK » ou appuyer sur « Entrer ».





Une fois ces deux fenêtres d'information passée, vous arrivez sur la fenêtre du MENU. Afin de faire une copie physique de disque dur, aller dans : « Local\Disque\Vers Disque » comme suit l'imprime écran :



Une fois la sélection de « disque\vers disque » fait, il vous faut choisir le disque dur ou lecteur source (il s'agit du disque dur ou lecteur dont on veut faire la copie). Cliqué sur « OK » ou sur « Entrer ». Une fois le disque source choisi, il vous faut choisir à présent le disque de destination (il s'agit du disque sur lequel on copie le disque source). Cliqué sur « OK », ou sur « Entrer ».

4) Ce logiciel est un outil d'investigation. Il fait une copie conforme (Bit à Bit) d'un disque source vers un disque cible. Attention la version dos est uniquement utilisée pour créer une copie, mais ne permet de travailler sur cette copie. Pour cela, il faut utiliser la version ENCASE Win.

Avant toute chose, il faut différencier le disque dur source du disque dur cible. Le disque source est le disque sur lequel sont stockées les informations Le disque cible est le disque sur lequel on va copier les informations. Lors du branchement des disques durs, bien faire attention :

Le disque source à mettre en IDE 1 (connectique bleue dans certains cas)
Le disque cible à mettre en IDE 2 (deuxième emplacement libre)

(Si les disques sont correctement branchés, par défaut l'IDE 1 sera DISK « 0 », et l'IDE 2 sera DISK« 1 »). Une fois les disques branchés correctement sur les IDE(s) respectif, lancez l'application. Dans le menu SESAME, veuillez sélectionner la touche n°4 ou flèches directionnelles.

VÉRIFIER TOUJOURS QUE LE DISK SOURCE SOIT BIEN PROTÉGER EN ÉCRITURE : DISK SOURCE EN POSITION « 0 » SOIT EN « LOCK » !

Pour faire une acquisition de disque suivre les étapes suivantes :

Enlevé la protection d'écriture du disque cible « 1 » : Appuyez sur le bouton LOCK ou sur la touche « L » et sélectionnez le disque cible « 1 » pour le débloquer.

Lancer l'acquisition : Appuyez sur le bouton Acquisition ou sur la touche « A » et sélectionner le disque « 0 ».

La destination : Emplacement d'écriture des données sur le disque cible. Exemple :

« c:\261sc7se ». Sachant que **261** = n° du dossier ; **sc** = scellé ; **7** = n° du scellé ; **se** = réf. du disque (à savoir « se » comme SEGATE), il y a un maximum de 8 caractères et ne pas oublier « c:\ », « C » étant la lettre correspondant au disque dur.

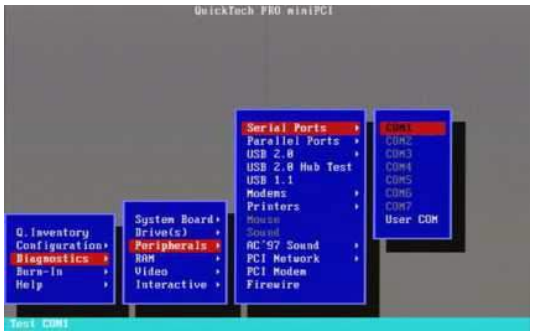
Case Number : comme précédemment, exemple : « 261sc7se ».
Examinateur : indiquer les initiales de la personne qui lance l'acquisition. Exemple Mikaël BONTEMPS = MBO.
Evidence Number : comme pour la destination, exemple : « 261sc7se ».
Description : récapitulatif des renseignements. Appuyez sur « Entrer ».
Date : indique la date d'acquisition en cours. Appuyez sur « Entrer ».
Notes : Emplacement réservé aux notes diverses. Ne rien inscrire !
Compression : demande de compresser les fichiers (réduire la taille de fichier acquis). Appuyez sur YES.
Generate MD Hash : il s'agit essentiellement d'une empreinte numérique d'un dossier ou d'un disque entier (assurance que la copie est bien celle de l'originale). Appuyez sur NO !
Password : emplacement réservé au mot de passe qui serait demandé lors de la lecture des fichiers acquis via le logiciel ENCASE WIN. Ne rien mettre dans ce cadre.
Total sectors : Indique la globalité du disque à acquérir. Appuyez sur « Entrer ».
Max File Size : Indique la taille des fichiers acquis lors du découpage (à savoir que pour un disque de 40Go si la taille sélectionnée est de 1 000Mo alors ENCASE fera 40 fichiers de 1000Mo, utile pour le stockage). Dans cet encadré mettre la taille sur 1 000Mo. Appuyez sur « Entrer ». Maintenant ENCASE est en cour d'exécution, veuillez patienter ! (la durée est proportionnel à la taille du disque dur source et variable par rapport aux connectiques IDE, SATA, AUTRE…).

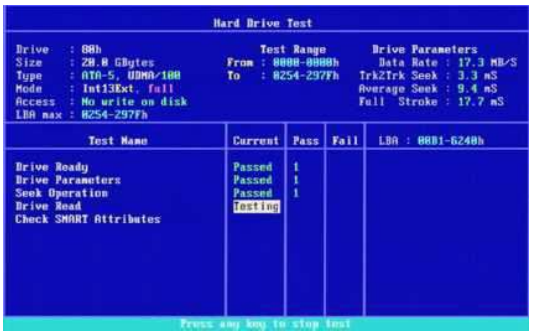
5) Cet outil permet d'évaluer les performances physiques de l'ordinateur. En outre il est capable de détecter la moindre erreur sur un disque dur ou une barrette mémoire…

Appuyez sur une touche !!!
Aux fins de faire des tests approfondis sur les caractéristiques physiques de l'ordinateur, vous avez plusieurs outils à votre disposition :

- Diagnostic
- Burn-in

Elles semblent être les deux fonctions les plus utilisées. Il est impératif de créer un nouveau projet et d'y inclure les tests que vous voulez effectuer. Une fois votre sélection faite, allez sur l'onglet « **Burn-In** » puis « **run** » puis appuyez sur « Entrer ».

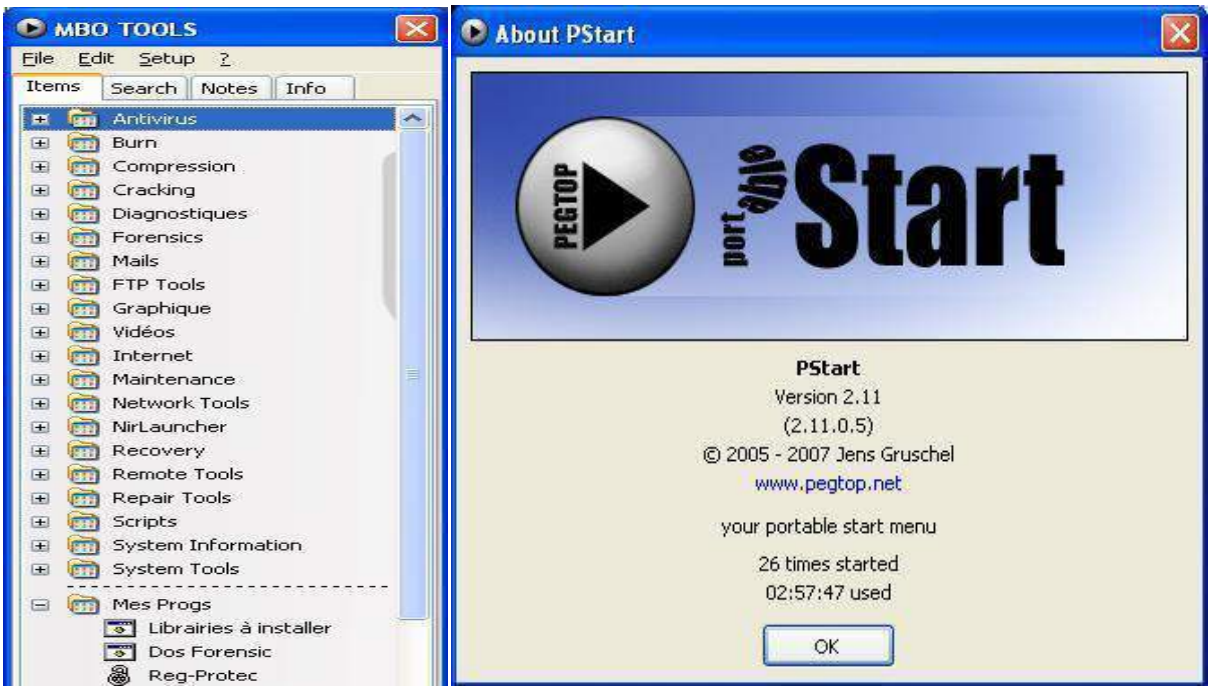




La partition « Autorun » permet, sous un système Microsoft Windows d'afficher un certain nombre d'outils d'investigation, bureautique, autre….

Après avoir démarré une session utilisateur (démarrage de Windows), vous insérez le CD-Rom dans le lecteur où vous connectez la clé USB sur un des ports libres de l'ordinateur, et une application se lance automatiquement. Il s'agit d'un menu « PStart » de Jens Gruschel, regroupant l'ensemble des logiciels présents à la racine du CD-Rom ou clé USB.

Au vu du nombre important de logiciels présents sur cette boîte à outils, je ne détaillerai pas son contenu. Mais en pratique il s'agit uniquement d'application ne nécessitant aucune installation sur une machine. S'exécute automatique depuis le menu de la boîte à outils.



Astuce : dans l'onglet « Notes », j'y ai écrit tout un tas d'infos utiles sur les raccourcis Windows, les clés de registres intéressantes, la localisation de fichiers pertinents….