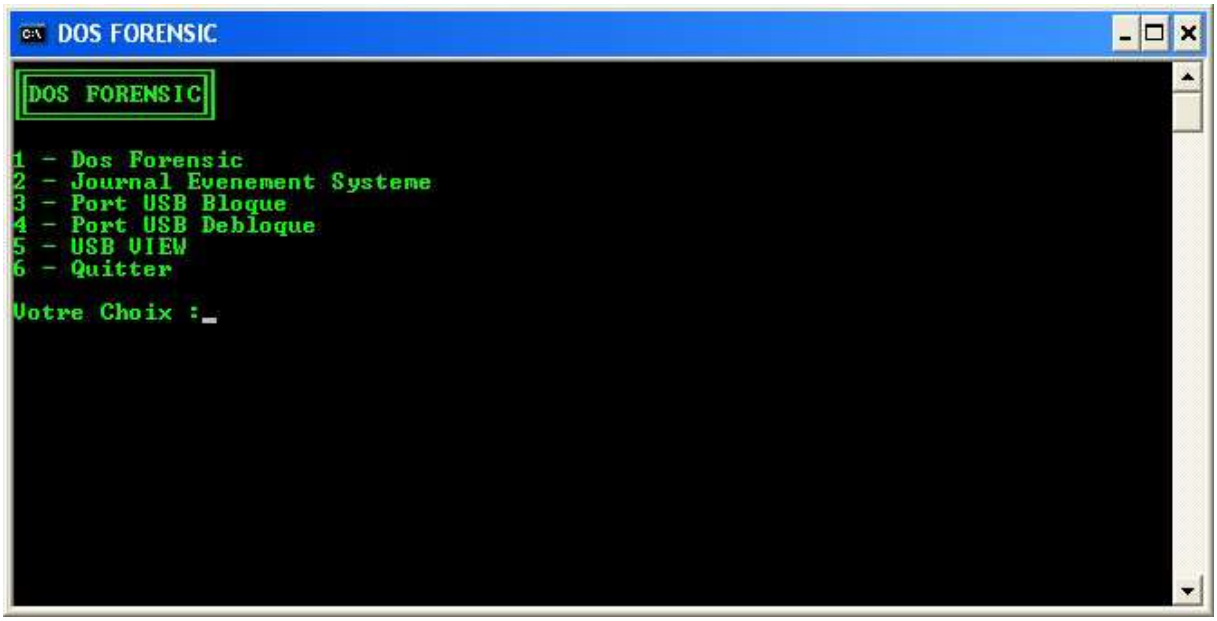
Pour le rendre « Portable », j'ai placé dans un dossier « DOS FORENSIC » 2 sous-répertoires « Logiciel » et « Reg » ainsi que l'exécutable « Dos Forensic.bat ». Dans le répertoire « Logiciel » se trouve un exécutable pour consulter l'historique de connexions USB sur un poste informatique. Dans

Le répertoire « Reg », 2 fichiers registre avec les clés pour modifier l'écriture ou non des périphériques USB (voir paragraphe 3.7).

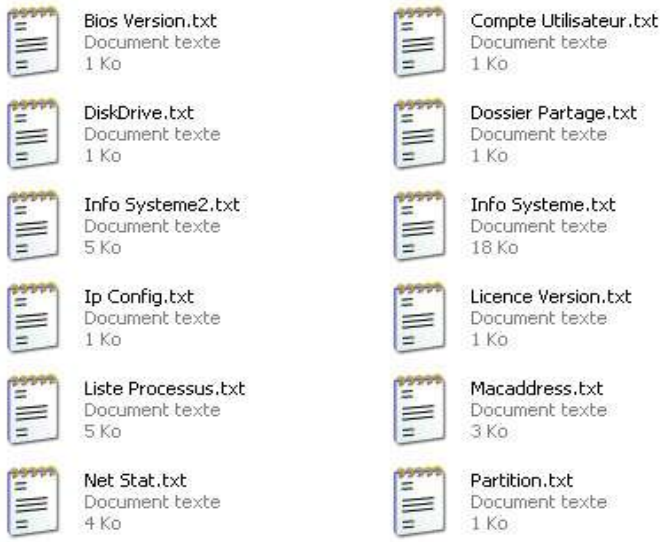
Double-clic sur « Dos Forensic.bat » pour afficher le terminal DOS avec le menu suivant :



Nota : depuis les versions Vista à maintenant, penser à faire clique droit sur « Dos Forensic.bat » et l'exécuter en mode Administrateur.

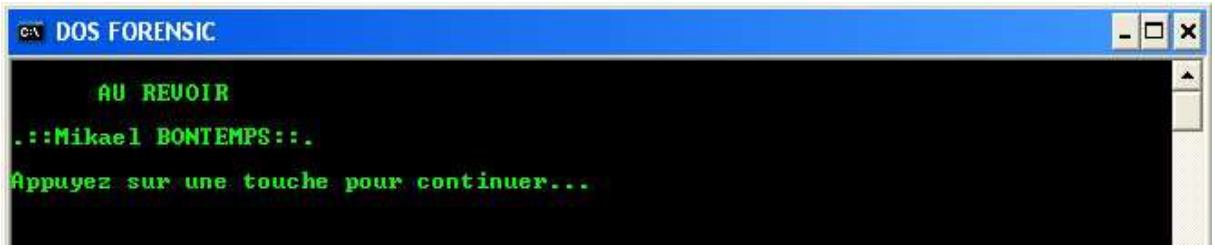
Descriptif des choix :

1- Dos Forensics : permet de lancer automatiquement une suite de commandes DOS qui va exporter des informations sur l'identité de l'ordinateur et autres informations pouvant servir à la présentation du scellé. (système d'exploitation, date d'installation, dossier de partage, réseau, …). Le processus créé automatique un répertoire nommé de la date du jour (AAAAJJMM) avec les différents Logs récupérés :



Nota : lorsque le processus est en cours, le curseur clignote dans le terminal DOS. Bien attendre que le curseur revienne à la ligne « votre choix : ».

2- Journal Événement Système : Il ouvre l'application Journal de Windows qui enregistre tous les logs « evt » et « evtx » de la machine (système, application, sécurité, …).
3- Port USB Bloque : fait appel à un fichier « reg » présent dans le répertoire racine REG. Il exécute une commande dans la base de registre permettant de bloquer tous les ports USB en écriture.
4- Port USB Débloque : Commande inverse du 3.
5- USB VIEW : Lance le programme usbview présent dans le répertoire racine LOGICIEL. Il affiche toutes les connexions USB et leurs propriétés qui ont été connectées sur la machine en cours.
6- Quitter : ferme le terminal DOS sans exécuter aucune autre action :



4.2.3 Commande Linux

Sous Linux, on peut consulter les fichiers « /etc/issue » et « /etc/issue.net » pour connaitre la version du système, ainsi que les commandes suivantes dans un terminal :

To get Serial # from command in Ubuntu
#sudo dmidecode -s system-serial-number

To get Serial # and Product # from command in Linux(Redhat/CentOS/Fedora/SuSe)
#sudo dmidecode -t 1 | egrep -i "serial|product"