# Documentation A2IMP-linux

## (A2IMP : Aide a l'Acquisition d'Informations sur une Machine Piratée)

Version 2011-12 pour la boîte à outils *A2IMP-linux* v2

Auteurs : Denis Pugnère <d.pugnere@ipnl.in2p3.fr>
Contributions : Cédric Hillembrand <Cedric.Hillembrand@cesr.fr>
Christophe Dubois <Christophe.Dubois@certa.ssi.gouv.fr>
Marie-Claude Quidoz <Marie-Claude.Quidoz@urec.cnrs.fr>
Relectures : Nicole Dausque <nicole.dausque@urec.cnrs.fr>

**Résumé :**

Cette documentation a été réalisée pour décrire comment utiliser la boîte à outils a2imp-linux (**Aide à l'Acquisition d'Information sur une Machine Piratée** – version Linux). Cette documentation contient les références, conseils et commandes utiles pour réaliser l'étape d'acquisition de traces sur une machine piratée, dans le but de pouvoir analyser ultérieurement ces traces. L'analyse de traces ne sera pas abordée dans ce document.

**Information :**
Ce document propose une méthode. Compte-tenu des spécificités de chaque site, qui doivent être privilégiées, il se peut que cette méthode ne puisse pas être suivie à la lettre.

**Notes de révisions :**

2006-09-15 : Denis
- ajout paragraphe sur la vérification des images,
- ajout paragraphe qui indique de ne pas modifier l'heure du système

2006-12-19 : Denis
- ajout paragraphe sur la création d'images compressées,
- ajout d'un nota-bene sur les informations sensibles,
- ajout paragraphe sur les options « conv=noerror,sync »,
- ajout création fifo sur disquette ou clé USB

2006-12-20 : Nicole
- Corrections sur l'ensemble du document

2007-09-18 : Denis
- Mise à jour de la documentation en rapport à la nouvelle boite à outils

2007-09-21 : Denis
- Ajout de références sur la compatibilité binaire de distributions supplémentaires

2009-12-18 : Denis
- § 3 : Ajout de précisions sur le choix des adresses IP
- § 3.6 : Ajout précisions sur le mode de démarrage (sur LiveCD) et sur la sauvegarde des partitions.

2011-12 : Denis
- § 3.3 : la boite a outils A2IMP-linux est aussi utilisable depuis une clé USB

# Table des matières

# 1 Avant de commencer

- **Gérer les priorités** :
  - identifier les services impactés,
  - informer sa hiérarchie,
  - informer les utilisateurs
- Se munir de documentation (celle ci est un bon début !)
- Geler la situation : Débrancher la machine du réseau, l'isoler ou éventuellement filtrer le trafic via les équipements réseaux (*routeur*, *firewall*, *switch*...) :
- Avoir votre boîte à outils *A2IMP-linux* gravée sur CD
- Disposer d'un *switch* ou *hub* rapide pour connecter uniquement cette machine à la machine de sauvegarde (100Mb/s est le minimum en fonction de l'espace à sauvegarder, compter 2 minutes par Go)
- Posséder des cordons *RJ45* droits et/ou croisés
- Avoir à disposition un espace de stockage suffisant :
  - soit un PC (portable ou autre) branché (via switch, hub, cordon croisé) disposant de la commande *nc* présente sur le CD *A2IMP-linux* et pouvant recevoir les données,
  - soit un disque externe (USB, FireWire, SATA...) à brancher sur la machine compromise (attention aux risques relatifs à l'intégrité des données que l'on va enregistrer sur ce disque puisqu'il sera accessible directement en écriture par tout le système compromis),
  - il existe des boîtiers spécifiques dédiés à la copie qui sont plus rapides (et plus chers)

NB :
- Ne pas hésiter à s'appuyer sur les compétences locales (RSSI de l'établissement), régionales (CRSSI, CSSI, collègues) et nationales (CERT-Renater, CERTA, experts)
- **Ce document ne s'applique ni aux informations dites « sensibles » stockées sur les espaces disques ni aux systèmes hébergés dans une unité de recherche qui n'est pas de type ERO (Établissement à Régime Ordinaire) , se renseigner auprès de sa hiérarchie fonctionnelle (chaîne de responsabilité SSI)**.

Conseil :
Il est vivement conseiller de tester et de valider régulièrement les procédures employées pour être à même de les appliquer efficacement et sereinement en situation de crise.

# 2 Principes de base

- ✔ Ne pas faire de modifications sur le système en cours d'acquisition d'informations
- ✔ Ne pas faire confiance aux outils installés sur le système en cours d'acquisition d'informations
- ✔ Garder une trace horodatée des actions réalisées
- ✔ Récupérer les informations et les enregistrer :
  - informations volatiles :
    - l'image de la mémoire *RAM*,
    - processus en cours d'exécution,
    - fichiers ouverts,
    - la liste des communications ouvertes,
    - l'état du système (variables d'environnement, modules, liste des utilisateurs...)
  - informations non volatiles :
    - les informations sur le système de fichiers (partitions...)
    - les partitions utilisées
- ✔ Penser également à recenser et récupérer les traces laissées sur le système d'information en bordure de cette machine (*logs* et filtres des *routeurs*, métrologie réseau, contrôles d'accès...)
- ✔ Sauvegarder les informations sur un support externe, d'une manière fiable
- ✔ S'assurer que les informations sauvegardées sont intègres
- ✔ S'assurer qu'aucune modification n'a été faite ou ne peut se faire sur les informations sauvegardées.

# 3 Méthode d'acquisition des données

Cette méthode détaille les commandes à taper pour réaliser la phase d'acquisition de données en tenant compte des principes de base précédemment décrits. Nous posons l'hypothèse que nous avons une machine dite propre « de sauvegarde » connectée en réseau à la machine compromise via un câble croisé ou par l'intermédiaire d'un *switch* réseau, cette machine de sauvegarde recevra les données pour les stocker sur le disque local, elle contiendra les commandes « *nc* » et « *md5sum* » fournies.

Nous supposons que la machine compromise n'a pas encore été redémarrée car si c'était le cas, la sauvegarde de la mémoire RAM n'aurait plus aucun intérêt.

Voici le déroulement de la méthode :
- Vérification de la date et de l'heure sur le système compromis
- Création de la main courante
- Montage de la boîte à outils (CDROM ou clé USB, montage NFS...)
- Sauvegarde des informations volatiles à l'aide des commandes de la boîte à outils
  - Ouverture d'un socket sur la machine de sauvegarde
  - Enregistrement continu des informations saisies par la commande « *script* »
  - Sauvegarde de la mémoire RAM
  - Obtention des informations sur l'état du système
- Arrêt-redémarrage de la machine à partir d'un média bootable (CD, DVD, clé USB)
- Sauvegarde de l'espace de stockage
  - Sauvegarde de l'espace de stockage SWAP
  - Sauvegarde de l'espace de stockage des partitions système
- Vérification de la signature des images
- Arrêt de la session

⇒ Nous allons supposer que la machine compromise s'appelle « compro » et qu'elle a comme adresse IP 10.0.0.1. Le prompt de la machine compromise sera :

```
[root@compro] #
```

⇒ Nous allons également supposer que la machine où l'on va sauvegarder les informations s'appelle « sauvegarde » et qu'elle a comme adresse IP 10.0.0.2. Le prompt de cette machine sera :

```
[user@sauvegarde] #
```

Les adresses IP 10.0.0.1 et 10.0.0.2 choisies sont totalement arbitraires. Vous êtes libres de choisir les adresses IP qui vous conviennent le mieux. Cependant, pour que les machines compromises et de sauvegarde puissent communiquer ensemble, il faut quand même qu'elles appartiennent au même réseau IP, cela impose que la conjonction de l'adresse IP et du masque du sous réseau (par exemple 255.255.255.0) des deux machines leur permettent de communiquer sans avoir besoin de passer par un routeur (qui peut être filtrant). Cela permet aussi à ces deux machines de communiquer mêmes si elles sont connectées ensemble par l'intermédiaire un cordon croisé.

## 3.1 Vérification de la date et de l'heure sur le système compromis

La première action est de vérifier date et heure du système compromis et de noter la différence par rapport à une source de temps sûre.

Cette opération peut se réaliser de plusieurs manières :

- on peut utiliser la commande *date* (présente sur le CD *A2IMP-linux*), le résultat de la commande est à comparer avec une source sûre : serveur *NTP* de confiance ou alors l'horloge parlante (numéro de téléphone : 3699)
- pour vérifier éventuellement que le système est synchronisé avec une source réseau précise (par exemple ntp) : commandes *ntpstat* ou *ntpdc*

Il ne faut pas modifier l'heure du système, si une modification est faite, il faut noter cette modification dans la main courante pour pouvoir en tenir compte par la suite.

## 3.2 Création de la main courante

Cette main courante peut être traditionnelle (stylo + papier) ou électronique (édition d'un fichier et le stocker sur un système et sur un stockage sûr). Le principe est de noter chaque action réalisée ainsi que la date et l'heure à laquelle elle a été lancée. Le résultat de cette commande pourra être stocké à part.

⇒ À partir de maintenant, on va donc noter sur la main courante chaque action et l'horodatée.

## 3.3 Montage de la boîte à outils (CDROM, clé USB)

Sur la machine compromise, nous allons monter le CDROM *A2IMP-linux* sur le point de montage */mnt/cdrom.* Si la boite à outils A2IMP-linux est sur une clé USB, le principe est identique (on utilise l'outil système *mount* pour cela, on ne peut pas faire autrement), exemple :

```
[root@compro] # mkdir /mnt/cdrom
[root@compro] # mount /dev/cdrom /mnt/cdrom
[root@compro] # cd /mnt/cdrom
```

Le CDROM *A2IMP-linux* contient les commandes systèmes compilés en statique pour plusieurs systèmes. À ce jour, les binaires système ont été compilés pour les distributions suivantes :

- Redhat Linux 6.2, 7.0, 7.1, 7.2, 9
- Redhat Enterprise Linux 3, 4, 5

Les binaires sont également compatibles avec les distributions suivantes (liste non exhaustive) :

- Debian 2.2, 3.0, 3.1, 4.0
- Ubuntu 6.06, 6.10, 7.04
- Suze 7.2 et autres
- Mandrake et autres

Le fichier lisezmoi.*txt* présent sur le CDROM détaille le contenu des répertoires et les distributions supportées par la boite à outils. Par exemple les commandes compilées pour une distribution Linux « *Redhat Linux 9* » se trouve dans le répertoire /mnt/cdrom/rh-9/

À partir de maintenant, toutes les commandes que l'on tapera sur la machine compromise seront celles réputées sûres car exécutées depuis le CDROM, en spécifiant le chemin d'accès aux commandes. Si on suppose que le système compromis est une distribution Linux « *Redhat Linux 9* », si on veut exécuter la commande « date » on tapera :

```
[root@compro] # /mnt/cdrom/rh-9/date
```

## *3.4 Sauvegarde des informations volatiles*

### 3.4.1 Ouverture d'un socket sur la machine de sauvegarde

Sur la machine de sauvegarde : ouverture d'un port en écoute (ici 10000) pour sauvegarder les informations sur les commandes tapées sur la machine compromise à l'aide de la commande *nc* (*netcat*):

```
[user@sauvegarde] # nc -l -p 10000 > session.txt
```

⇒ S'assurer qu'aucun filtre de paquets (*iptables, ipchains, pf, ipfilter*...) ne bloque le flux qui sera envoyé sur ce port, car si c'est le cas, aucune information ne sera enregistrée sur la machine de sauvegarde.

### 3.4.2 Enregistrement continu des informations saisies par la commande « script »

Sur la machine compromise, on ne doit pas modifier les informations sur le disque et donc avoir un minimum d'impact sur les informations volatiles. De plus on doit garder une trace des actions réaliser pour pouvoir par la suite expliquer les éventuelles modifications systèmes.

Pour réaliser cette action, nous créons une *fifo.* Puis nous utiliserons la commande « *script »* qui enverra tout ce qui a été tapé en local dans la *fifo*, *et nous utiliserons la* commande *nc* pour l'envoi sur la machine de sauvegarde.

Création de la *fifo* (ici, le fichier *fifo* est /tmp/session-a2imp, on peut aussi créer cette fifo sur une disquette ou sur une clé USB préalablement montées) :

```
[root@compro] # /mnt/cdrom/rh-9/mkfifo /tmp/session-a2imp
```

On prépare l'envoi à distance (à l'adresse IP 10.0.0.2, port tcp 10000) via la commande *nc*) de tout ce qui sera envoyé dans la fifo :

```
[root@compro] # /mnt/cdrom/rh-9/cat /tmp/session-a2imp | /mnt/cdrom/rh-9/nc 10.0.0.2 10000
```

Depuis un autre *terminal*, lancer la commande « script » qui enregistre tout ce qui est lancé et tous les résultats dans la *fifo* précédemment créée :

```
[root@compro] # /mnt/cdrom/rh-9/script -f /tmp/session-a2imp
```

> ⇒ Maintenant, grâce à la commande « *script* », tout ce qui est tapé et affiché **dans ce terminal** sera envoyé à distance (sur le port 10000) sur la machine de sauvegarde.

### 3.4.3 Sauvegarde de la mémoire RAM

> ⇒ Dans certains cas la sauvegarde de la *RAM* n'est pas possible. Par exemple, si la protection *SELinux* est activée, celle ci empêche de lire le contenu de la *RAM* avec la commande dd. L'option *SELinux* est activée par défaut sur les systèmes *Redhat Entreprise Linux v4* (voir le fichier */etc/selinux/config* et le code de retour de la commande *selinuxenabled*).

On va sauvegarder le contenu de la *RAM* en exécutant un « *nc* » qui écoute sur un port (ici *9000*) sur la machine de sauvegarde (ne pas réutiliser le port *10000* toujours en cours d'utilisation pour l'enregistrement des commandes tapées dans le terminal). Le *dump* envoyé depuis la machine compromise sera reçu sur la machine de sauvegarde et sera enregistré dans le fichier *compro-RAM.dd.*

*Création de la socket de réception sur la machine* de sauvegarde et enregistrement des informations reçues dans le fichier *compro-RAM.dd* :

```
[user@sauvegarde] # nc -l -p 9000 > compro-RAM.dd
```

> ⇒ S'assurer (comme précédemment) qu'aucun filtre de paquets (*iptables, ipchains, pf, ipfilter*...) ne bloque le flux qui sera envoyé sur ce port, car si c'est le cas, aucune information ne sera enregistrée sur la machine de sauvegarde.

Maintenant, on sauvegarde le contenu de la *RAM* à l'aide de la commande *dd* : La mémoire RAM est accessible par les fichiers */dev/mem* ou */proc/kcore*

Horodatage :

```
[root@compro] # /mnt/cdrom/rh-9/date
```

Puis la sauvegarde :

```
[root@compro] # /mnt/cdrom/rh-9/dd if=/dev/mem | /mnt/cdrom/rh-9/nc 10.0.0.2  9000
```

Puis, une fois le transfert terminé :

```
[root@compro] # CTRL + C
```

Création de la somme de contrôle (hash) sur la machine de sauvegarde :

```
[user@sauvegarde] # md5sum compro-RAM.dd >  compro-RAM.dd.md5
```

### 3.4.4 Sauvegarde de l'espace de stockage SWAP

Il est important de sauvegarder l'espace SWAP, car il révèle potentiellement des informations sur des processus précédemment lancés. Il est possible que l'espace de stockage SWAP soit chiffré.

On peut réaliser l'opération à chaud (avec le système encore en fonctionnement), ou à froid (le système ayant été rebooté sur un live CD ou live USB). Voici les quelques avantages et inconvénients de chaque méthode :

| | **Sauvegarde du SWAP à chaud** | **Sauvegarde du SWAP à froid** |
|---|---|---|
| **Avantages** | - Possibilité de garder le maximum de traces,<br>- accès aux informations même si le SWAP est chiffré | Certaines informations ont été altérées ou effacées au cours de l'opération d'arrêt du système |
| **Inconvénients** | La procédure et les commandes tapées pour réaliser la copie vont altérer le SWAP | L'accès aux données ne sera pas possible si le SWAP est chiffré |

Linux peut utiliser le *SWAP* sur une partition dédiée ou utiliser un « *fichier swap* ». Le script « *a2imp-auto.sh* » exécute la commande « `cat /proc/swaps` » qui permet de connaître les espaces de swap utilisés par le système.

Pour sauvegarder le contenu de chaque zone *SWAP*, on exécute d'abord un « *nc* » qui écoute sur le port *9000* sur la machine de sauvegarde, le *dump* qui sera reçu sera enregistré dans le fichier *compro-SWAP-sda2.dd* :

```
[user@sauvegarde] # nc -l -p 9000 > compro-SWAP-sda2.dd
```

Horodatage :

```
[root@compro] # /mnt/cdrom/rh-9/date
```

Maintenant, on sauvegarde le contenu du *SWAP* de la partition /dev/sda2 :

```
[root@compro] # /mnt/cdrom/rh-9/dd if=/dev/sda2 | /mnt/cdrom/rh-9/nc 10.0.0.2 9000
[root@compro] # CTRL + C
```

Création de la somme de contrôle (hash) sur la machine de sauvegarde :

```
[user@sauvegarde] # md5sum compro-SWAP-sda2.dd > compro-SWAP-sda2.dd.md5
```

Il peut arriver que certaines zones du disque soient endommagées (donc illisibles) et empêchent la copie par *dd* : dans ce cas, on peut ajouter les options « *conv=noerror,sync* » qui permettent de remplacer dans l'image les zones illisibles par une suite de zéros. Exemple :

```
[root@compro] # /mnt/cdrom/rh-9/dd if=/dev/sda2 conv=noerror,sync | /mnt/cdrom/rh-9/nc
                                                                    10.0.0.2 9000
```

> ⇒ Si vous utilisez les options «  conv=noerror,sync » sur un disque qui a des secteurs défectueux, il faudra bien penser à créer une signature de l'image, par contre il sera impossible de vérifier l'intégrité de l'image prise par rapport à l'original (disque physique ou partition).

Il existe aussi un utilitaire (*dcfldd*), ayant la capacité de calculer la somme de contrôle en même temps que la copie de la zone du disque, exemple de calcul de hash md5 (attention, dans cet exemple, le fichier md5.log est stocké localement) :

```
[root@compro] # /mnt/cdrom/rh-9/dcfldd if=/dev/sda2 conv=noerror,sync hash=md5
                                                    hashlog=md5.log | /mnt/cdrom/rh-9/nc 10.0.0.2 9000
```

Maintenant, nous disposons du maximum d'informations volatiles issues de la RAM et du swap, nous avons maintenant la possibilité de récupérer d'autres informations volatiles utiles comme la liste des processus en cours d'exécution, liste des connexions ouvertes...

### 3.4.5 Obtention des informations sur l'état du système

Maintenant que l'on a sauvegardé le contenu de la RAM, on peut exécuter le script « *a2imp-auto.sh* » existant sur le CDROM. Il lance des commandes qui permettent d'obtenir des informations sur l'état du système : connexions réseaux, liste des processus, partitions, environnement, modules. On peut l'exécuter avec la commande :

```
[root@compro] # cd /mnt/cdrom/rh-9
[root@compro] # ./a2imp-auto.sh
```

Ces informations (qui seront sauvegardées dans la main courante) nous seront utiles pour rechercher des traces de compromission par la suite.

## *3.5 Arrêt de la machine*

Pour minimiser les risques d'incohérences, il est préférable de réaliser l'opération de sauvegarde de l'espace de stockage (partitions systèmes) depuis les systèmes de fichiers démontés. Il faut tout d'abord stopper la machine proprement en utilisant la procédure habituelle (par exemple, la commande *shutdown*).

Il faut noter que cette opération présente quelques risques : l'opération d'arrêt d'une machine *Unix* est une opération qui exécute séquentiellement plusieurs dizaines de scripts et exécutables, qui modifie plusieurs fichiers (notamment les fichiers de *logs* systèmes et applicatifs). Cette opération laisse donc une grande quantité de traces dans les fichiers systèmes.

La procédure d'arrêt de la machine va couper la session d'enregistrement des commandes tapées (cf paragraphe 3.4.2), il faudra donc ouvrir une nouvelle session pour enregistrer la suite des opérations.

## 3.6 Sauvegarde de l'espace de stockage

Pour la sauvegarde, il y a plusieurs manières de réaliser cette opération :

- Démarrer sur un LiveCD (CD bootable, clé USB bootable ou autre...), puis accéder à la fois aux partitions à sauvegarder (**sans les monter, même en read-only**) mais aussi à un espace de stockage ou l'on pourra stocker les partitions à sauvegarder.
- On peut aussi extraire physiquement le disque dur et utiliser un boîtier spécialisé pour réaliser la sauvegarde des partitions ou du disque dans son intégralité.

Le principe utilisé pour la sauvegarde des partitions est la sauvegarde bloc-à-bloc des partitions. Pour cette opération :

- aucun système de fichier ne sera monté,
- la copie intégrale bloc-à-bloc de la partition sera réalisée (sa taille sera donc indépendante du taux d'occupation de la partition,
- donc aucune modification n'aura lieu sur la partition,
- cela nous permettra de contrôler l'intégrité de l'image de la partition ainsi crée par rapport à la partition originale.

Si on utilise un LiveCD ou autre (clé USB...), il faudra qu'il reconnaisse les périphériques, les contrôleurs et disques du système, **mais il ne devra faire aucune modification sur les partitions systèmes, de données ni de SWAP**. Ainsi il ne devra pas monter automatiquement les systèmes de fichiers ni utiliser le SWAP.

> ⇒ Il faut vraiment se méfier des LiveCD qui ont tendance à monter tout ce qui est possible pour faciliter la vie de l'utilisateur. Dans notre cas, nous utiliserons par exemple de l'option *noswap* au *boot Linux* d'une knoppix).

D'autre part, afin d'accéder à tous les supports de stockage présents sur la machine compromise, il faut que le CD :

- contienne le support des pilotes des cartes Ethernet et contrôleurs disques (*SATA, SCSI*...)
- supporte de partitionnement utilisés par le système (*LVM, LVM2, EVMS*), mais également les systèmes de fichiers (*ext2, ext3, ext4, xfs, reiserfs*...)
- contienne également les commandes nécessaires pour la sauvegarde (*dd, nc, date*...)

Le partitionnement des disques durs peut être obtenu par des commandes comme « *fdisk -l* » ou *df*. Les informations sur les systèmes de fichiers montés, sur les disques et partitions ont été relevées par le script *a2imp-auto.sh* précédemment lancé. Voir le fichier *session.txt* présent sur le système de sauvegarde.

Exemple : pour connaître la liste des partitions :

```
[root@compro] # /mnt/cdrom/rh-9/date
[root@compro] # /mnt/cdrom/rh-9/fdisk -l

Disk /dev/sda: 18.3 GB, 18373349376 bytes
```

```
255 heads, 63 sectors/track, 2233 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot    Start       End    Blocks   Id  System
/dev/sda1   *         1      1275  10241406   83  Linux
/dev/sda2          1276      1657   3068415   82  Linux swap
/dev/sda3          1658      2233   4626720   83  Linux

Disk /dev/sdb: 18.3 GB, 18373349376 bytes
255 heads, 63 sectors/track, 2233 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot    Start       End    Blocks   Id  System
/dev/sdb1   *         1       637   5116671   83  Linux
/dev/sdb2           638      1019   3068415   83  Linux
```

On voit ici qu'il y a des partitions Linux de type systèmes de fichiers et SWAP.

### 3.6.1 Sauvegarde de l'espace de stockage des partitions système

La procédure de sauvegarde des partitions système est différente de celle pour la sauvegarde de la partition SWAP.

Les partitions que l'on va sauvegarder sont principalement les partitions systèmes, c'est-à-dire celles où un intrus aurait pu déposer ses outils utilisés pour la compromission. Dans la plupart des cas, cela ne sert à rien de sauvegarder les partitions utilisateurs (généralement /home), mais c'est à apprécier au cas par cas.

La sauvegarde des disques ou partitions systèmes est à répéter pour chaque partition et/ou disque à sauvegarder. Dans la liste des partitions données par la commande *fdisk*, nous avons */dev/sda1*, */dev/sda3*, */dev/sdb1* et */dev/sdb2*

Exemple pour sauvegarder la partition */dev/sda1* :

```
[user@sauvegarde] # nc -l -p 9000 > compro-dd-sda1
```

Horodatage :

```
[root@compro] # /mnt/cdrom/rh-9/date
[root@compro] # /mnt/cdrom/rh-9/dd if=/dev/sda1 | /mnt/cdrom/rh-9/nc 10.0.0.2 9000
[root@compro] # CTRL + C
```

ou
Pour sauvegarder l'ensemble du disque (ici /dev/sda) en « morceaux » de 2Go :

```
[user@sauvegarde] # nc -l -p 9000 | split -d -b 2000m - compro-dd-sda.split
```

Horodatage :

```
[root@compro] # /mnt/cdrom/rh-9/date
```

```
[root@compro] # /mnt/cdrom/rh-9/dd if=/dev/sda | /mnt/cdrom/rh-9/nc-10.0.0.2 9000
[root@compro] # CTRL + C
```

Création de la somme de contrôle (*hash*) sur la machine de sauvegarde (ici sur la sauvegarde de la partition */dev/sda1*) :

```
[user@sauvegarde] # md5sum compro-dd-sda1 >  compro-dd-sda1.md5
```

Il est aussi possible de compresser les images des partitions ou du *SWAP* pendant ou après le transfert sur la machine de sauvegarde, exemple :

```
[user@sauvegarde] # nc -l -p 9000 > compro-dd-sda1.gz
```

```
[root@compro] # /mnt/cdrom/rh-9/date
[root@compro] # /mnt/cdrom/rh-9/dd if=/dev/sda1 | /mnt/cdrom/rh-9/gzip -c | /mnt/cdrom/rh-9/nc——
                                                                                10.0.0.2 9000
[root@compro] # /mnt/cdrom/rh-9/date
[root@compro] # /mnt/cdrom/rh-9/md5sum /dev/sda1
```

```
[user@sauvegarde] # md5sum compro-dd-sda1.gz >  compro-dd-sda1.gz.md5
```

⇒ Si vous compressez les images des partitions ou des disques, penser à créer à la fois une signature de l'original mais aussi une signature de l'image compressée.

## *3.7 Vérification des images*

Nous avons créé des images du *SWAP*, des disques ou des partitions, nous avons également pris le soin de créer des signatures de ces images, grâce à cela, nous pouvons maintenant contrôler l'intégrité de l'image par rapport à sa somme de contrôle.

Exemple :

```
[user@sauvegarde] # md5sum -c compro-SWAP.dd.md5
compro-SWAP.dd: OK
```

Dans ce cas, la signature est bonne car la somme de contrôle de l'image correspond à la somme de contrôle calculée précédemment.

Autre exemple :

```
[user@sauvegarde] # md5sum -c compro-SWAP.dd.md5
compro-SWAP.dd: : FAILED
md5sum: WARNING: 1 of 1 computed checksum did NOT match
```

Dans ce cas précis, la signature de l'image ne correspond pas à la signature, on en déduit que l'image a été modifiée, elle est donc à considérer comme non valide.

# 4 Arrêt de la session

Depuis le *terminal* où a été lancée la commande « *script* » qui enregistre tout ce qui est lancé, il faut taper « exit » ou la combinaison de touches Control-D pour arrêter l'enregistrement de la session

```
[root@compro] # exit
```

# 5 Références

Note CERTA-2002-INF-002-002 : Les bons réflexes en cas d'intrusion sur un système d'information http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002

RFC 3227 : Guidelines for Evidence Collection and Archiving
http://www.ietf.org/rfc/rfc3227.txt

## Annexe : contenu du script a2imp-auto.sh de la boîte à outils a2imp-linux

```
#!./bash
./echo "a2imp-auto.sh version 2007-09-19"
./echo "script d'automatisation de collecte d'information sur un systeme a l'aide"
./echo "de la boite a outils A2IMP-linux"
./echo "(c) CNRS / D.Pugnere"
./echo "################################################################################"
./echo -e "### => date : Verification  et affichage de l'heure locale du systeme"
./date
./echo -e "\n### => uname -a : version du kernel en cours d execution"
./uname -a
./echo -e "\n### => cat /proc/sys/kernel/hostname : hostname"
./cat /proc/sys/kernel/hostname
./echo -e "\n### => cat /proc/cpuinfo : cpuinfo"
./cat /proc/cpuinfo
./echo -e "\n### => cat /proc/sys/kernel/osrelease : version du kernel"
./cat /proc/sys/kernel/osrelease
./echo -e "\n### => cat /proc/cmdline : parametres passés au kernel"
./cat /proc/cmdline
./echo -e "\n### => cat /proc/modules : liste des modules du kernel"
./cat /proc/modules
./echo -e "\n### => sysctl -a : liste de toutes les variables du kernel"
./sysctl -a
./echo -e "\n### => df : liste des montages actifs vus par la commande df"
./df
./echo -e "\n### => cat  /proc/partitions : liste des partitions des disques detectés par le
kernel"
./cat /proc/partitions
./echo -e "\n### => cat  /proc/mounts : liste des montages vus par le kernel"
./cat /proc/mounts
./echo -e "\n### => cat  /proc/swaps : liste des espaces swap utilisés par le système"
./cat /proc/swaps
./echo -e "\n### => fdisk -l /dev/(h|s)d[a-z] : liste des partitions des disques par fdisk"
for disk in `./tail -n+3 /proc/partitions | ./grep -E " (h|s)d[a-z]\b" | ./tr -s ' ' ' ' | ./cut
-d" " -f 5`;
 do
   ./fdisk -l /dev/$disk;
 done
./echo -e "\n### => uptime"
./uptime
./echo -e "\n### => who : liste des personnes connectées"
./who
./echo -e "\n### => w : liste des personnes et leur activité"
./w
./echo -e "\n### => lsmod : liste des modules du kernel"
./lsmod
./echo -e "\n### => printenv : liste des variables d'environnement"
./printenv
./echo -e "\n### => ifpromisc : verification du mode PROMISC sur les interfaces ethernet"
./ifpromisc
./echo -e "\n### => ifconfig -a : liste des interfaces reseau"
./ifconfig -a
./echo -e "\n### => arp -an : Table ARP"
./arp -an
./echo -e "\n### => netstat -s : statistiques des protocoles reseaux"
./netstat -s
./echo -e "\n### => netstat -nr : table de routage"
./netstat -nr
./echo -e "\n### => route -Cn : table de routage"
./route -Cn
./echo -e "\n### => netstat -anp : liste des connexions reseaux"
./netstat -anp
./echo -e "\n### => lsof -n -i4 : liste des connexions reseau IPv4"
./lsof -n -i4
./echo -e "\n### => lsof -n -i6 : liste des connexions reseau IPv6"
./lsof -n -i6
./echo -e "\n### => ps -eaxf : liste des processus"
./ps eaxf
./echo -e "\n### => pstree : arborescence des processus"
./pstree
./echo -e "\n### => lsof -n -P -l : liste de tous les processus, des librairies et des fichiers
ouverts"
./lsof -n -P -l
./echo -e "\n### => chkproc : verification des processus cachés dans ps"
./chkproc
./echo -e "\n### => listps : "
./listps
```

```
./echo "#############################################################################"
./echo "Processus en cours d'execution"
./echo "#############################################################################"
./ls /proc | ./sort -n | ./grep -v "[a-z,A-Z]" | while read PID
  do
        ./echo "Process ID $PID:"
        ./echo "/proc/$PID/cmdline:"
        ./cat /proc/$PID/cmdline
        ./echo
        ./echo "/proc/$PID/environ:"
        ./cat /proc/$PID/environ
        ./echo
        ./echo "/proc/$PID/maps:"
        ./cat /proc/$PID/maps
        ./echo
        ./echo "/proc/$PID/stat:"
        ./cat /proc/$PID/stat
        ./echo
        ./echo "/proc/$PID/statm:"
        ./cat /proc/$PID/statm
        ./echo
        ./echo "/proc/$PID/status:"
        ./cat /proc/$PID/status
        ./echo
        ./echo "/proc/$PID/root:"
        ./ls -ld /proc/$PID/root
        ./echo
        ./echo "/proc/$PID/cwd:"
        ./ls -ld /proc/$PID/cwd
        ./echo
        ./echo "/proc/$PID/exe:"
        ./ls -ld /proc/$PID/exe
        ./echo
        ./echo "/proc/$PID/fd/*:"
        ./ls -lrta /proc/$PID/fd/
        ./echo
        ./echo "========================================================="
        ./echo
  done
./echo "#############################################################################"
```