Documentation A2IMP-linux

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

Version 0.5 du 31/03/2014 pour le LiveCD A2IMP v0.9.62

Auteurs : Hervé Ballans <herve.ballans@ias.u-psud.fr>
David Delavennat <david.delavennat@math.polytechnique.fr>

D'après la documentation A2IMP-linux de Denis Pugnère <d.pugnere@ipnl.in2p3.fr>
(voir note des auteurs en bas de cette page)

Résumé :

Cette documentation a été réalisée pour décrire comment utiliser le LiveCD A2IMP sur système Linux (**Aide à l'Acquisition d'Information sur une Machine Piratée**).
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 :

v0.3/0.4/0.5 : précisions apportées dans certains chapitres et mises à jour d'éléments relatifs à la nouvelle version du LiveCD

v0.2 : documentation fournie lors de la formation aux CSSI du 29/11/2012

Note des auteurs :

Cette documentation est fortement inspirée de la documentation d'origine fournie lors de la formation initiale A2IMP en 2006 (rédigée par Denis Pugnère avec des contributions de Cédric Hillebrand, Christophe Dubois et Marie-Claude Quidoz et relue par Nicole Dausque)
La dernière version du document d'origine est disponible sur le site de la DSI /ARESU : https://aresu.dsi.cnrs.fr/IMG/pdf/documentation-a2imp-linux-201112.pdf

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 !)

- Disposer du **matériel** adéquat, le « kit A2IMP » qui contient notamment :
  - Un bloc-notes (ou un ordinateur portable avec un éditeur!)
  - Le LiveCD A2IMP (à jour!)
  - un disque externe de capacité suffisante et formaté en ext3

Note concernant le disque externe : dans la mesure où il est branché sur une machine compromise et que celui ci est accessible directement en écriture, il peut exister des risques relatifs à l'intégrité des données que l'on va enregistrer dessus.

- Geler la situation au plus vite : Débrancher la machine du réseau, l'isoler ou éventuellement filtrer le trafic via les équipements réseaux (*routeur*, *firewall*, *switch*...).

Note concernant l'arrêt des services réseaux sur la machine compromise : si vous disposez du « kit A2IMP » au moment de la découverte de la compromission (et uniquement dans ce cas), dans la mesure où l'acquisition des informations volatiles est très rapide, vous pouvez effectuer cette première étape avant de couper le réseau. Cela devrait permettre de récupérer le maximum d'informations.

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 outils à utiliser pour réaliser la phase d'acquisition de données en tenant compte des principes de base précédemment décrits.
Dans notre méthode, la sauvegarde des données s'effectue sur un support externe branché sur un port USB de la machine compromise.

Nous supposons que la machine compromise n'a pas encore été redémarrée car si c'était le cas, la sauvegarde des informations volatiles 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
- Insertion du LiveCD A2IMP
- Montage du support de sauvegarde
- Sauvegarde des informations volatiles à l'aide des commandes de la boîte à outils a2impLinux
  - Récupération du nom du point de montage du media de sauvegarde
  - Sauvegarde des informations volatiles en cours sur le système
  - Sauvegarde de l'espace de stockage swap à chaud
  - Sauvegarde de la mémoire RAM (si possible)
- Arrêt-redémarrage de la machine à partir du même LiveCD A2IMP
- Sauvegarde de l'espace de stockage
  - Démarrage du programme de copie disque
  - Sauvegarde de l'espace de stockage des partitions système
  - Sauvegarde de l'espace de stockage swap (si cela n'a pas été fait à chaud)
- Arrêt définitif du système compromis

Conventions utilisées dans cette documentation :
- la machine compromise s'appelle « compro »
- cette machine comporte 1 disque dur interne monté physiquement sur /dev/sda
- le support de sauvegarde externe est monté physiquement sur /dev/sdb
- le support de sauvegarde externe sera vu sur le point de montage /media/copie

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 LiveCD *A2IMP*), le résultat de la commande est à comparer avec une source sûre : serveur *NTP* de confiance ou alors l'horloge parlante (numéro de téléphone : 3669)
- 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'horodater.

A noter que les outils du LiveCD vont faciliter cette tache en horodatant systématiquement les fichiers de sortie (le nom du fichier contient une date)

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

Sur la machine compromise toujours en fonctionnement, nous allons en premier lieu insérer le LiveCD A2IMP. Lors de l'insertion, il y a 2 possibilités :

- soit le LiveCD est automatiquement monté par le système
- soit il faudra le faire manuellement

Note : en général, la plupart des Linux monte les media externes au niveau de /media/

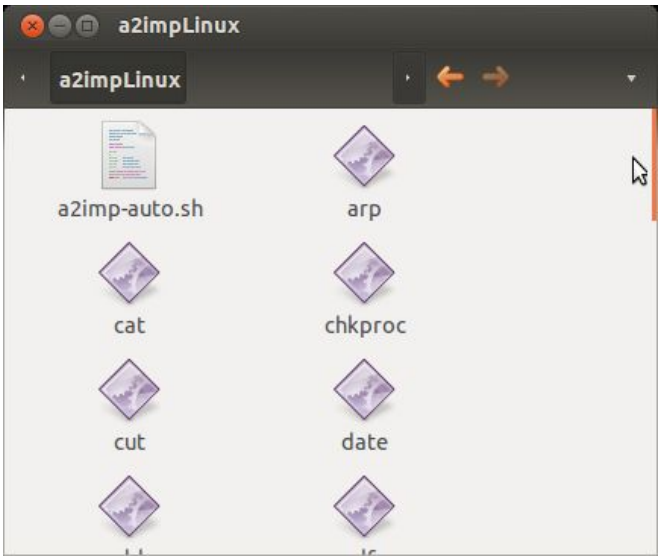
Dans notre exemple, le LiveCD sera vu sur le montage logique :
/media/A2IMP_SL6_LiveCD

Si le media n'est pas monté automatiquement, il faut procéder comme suit :
Ouvrir un terminal et utiliser le compte root (« *su -* » ou *sudo* selon la version de Linux) :

```
[root@compro] # mkdir /media/A2IMP_SL6_LiveCD
[root@compro] # mount /dev/cdrom /media/A2IMP_SL6_LiveCD
```

L'acquisition des données volatiles va s'effectuer grâce au script **a2imp-auto.sh** placé dans le répertoire a2impLinux (ce dernier étant situé à la racine du LiveCD).

Ce script shell fait appel à des commandes systèmes compilées en statique pour Linux.
Les commandes utilisées sont celles contenues dans le LiveCD d'origine (compilées par Denis Pugnère en 2006).
Le script a été testé avec succès sur des systèmes Linux récents dont Ubuntu 12.04 et Scientific Linux 6.1.



Pour connaître en détail les commandes utilisées par le script, voir l'**annexe A**

3.4 Sauvegarde des informations volatiles

3.4.1 Montage du support de sauvegarde

Brancher le disque externe ext3 sur l'un des ports USB de la machine compromise.

Si celui ci n'est pas monté automatiquement, le faire manuellement :

```
[root@compro] # mkdir /media/copie
[root@compro] # mount -t ext3 /dev/sdb1 /media/copie
```

3.4.2 Sauvegarde des informations sur l'état du système

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 réalisées pour pouvoir par la suite expliquer les éventuelles modifications systèmes.

Nous effectuons cette étape en premier car c'est la plus rapide. Le script va récupérer un nombre conséquents d'informations en quelques secondes. Il se charge également de récupérer le contenu des répertoires `/tmp` et `/dev/shm`.

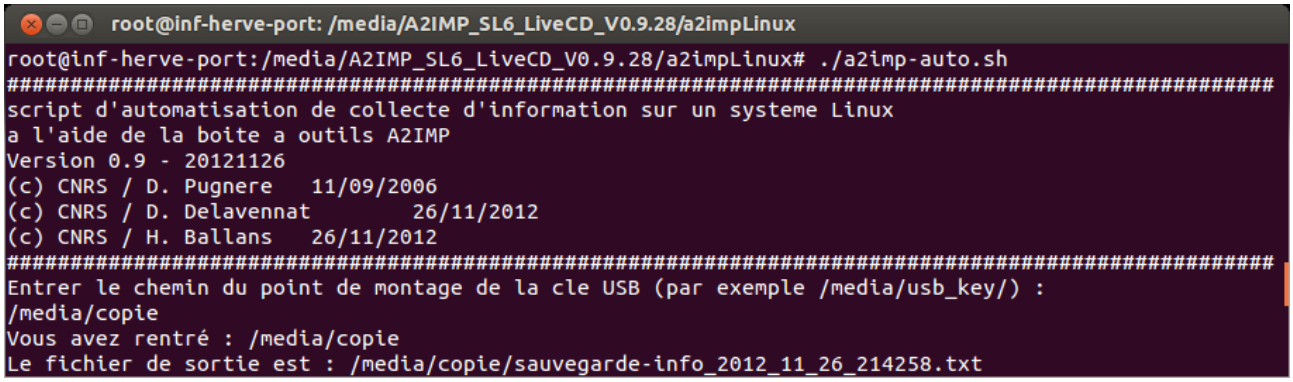
Le script « *a2imp-auto.sh* » lance des commandes qui permettent d'obtenir des informations sur l'état du système : connexions réseaux, liste des processus, partitions, environnement, modules. On peut l'exécuter avec la commande :

```
[root@compro] # cd /media/A2IMP_SL6_LiveCD
[root@compro] # cd a2impLinux
[root@compro] # ./a2imp-auto.sh
```

Avant d'exécuter sa série de commandes, le script demande le chemin du point de

montage du support de sauvegarde. Dans notre exemple, selon la convention choisie, il faudra donc rentrer le chemin /media/copie pour pouvoir enregistrer les informations sur le disque externe.

Le nom du fichier de sauvegarde sera automatiquement créé à cet endroit et sera de la forme : **sauvegarde-info_YYYY_MM_DD_hhmmss.txt**



Ces informations nous seront utiles pour rechercher des traces de compromission par la suite.

Note concernant le fichier sauvegarde-info_YYYY_MM_DD_hhmmss.txt :
Le fichier généré par le script *a2imp-auto.sh* peut contenir plus de 50000 lignes d'informations, soit plus de 1000 pages de document. Il est évident que ce fichier n'est pas destiné a être imprimé ! Les services compétents qui l'analyseront rechercheront des traces de compromission en effectuant des recherches de motifs dans ce fichier.

3.4.3 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.

Il y a deux manières de faire : on peut réaliser l'opération à chaud (avec le système encore en fonctionnement), ou à froid (le système ayant été rebooté sur un LiveCD ou LiveUSB). 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, - 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.

On peut également connaître la partition de swap, si elle existe, avec la commande « *fdisk -l* ». Sachant que le type de cette partition est 82 :

```
[root@compro] # fdisk -l /dev/sda | grep 82
```

On utilise l'utilitaire dcfldd (à défaut, dd) qui permet de copier une image exacte de la partition swap et de calculer à la volée l'empreinte de l'image générée.
Si, par exemple, la swap est montée en /dev/sda2 :

```
[root@compro] # cd /media/A2IMP_SL6_LiveCD/a2impLinux
[root@compro] # dcfldd if=/dev/sda2 conv=noerror,sync hash=sha1
                                hashlog=/media/copie/swap.dd.sha1 of=/media/copie/swap.dd
```

3.4.4 Sauvegarde de la mémoire RAM

Cette étape est aujourd'hui de loin la plus complexe.

> ⇒ Dans certains cas la sauvegarde de la *RAM* n'est plus possible directement. 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 de la famille *Redhat Entreprise Linux* (voir le fichier */etc/selinux/config* et le code de retour de la commande *selinuxenabled*).

Lorsque la mémoire RAM est accessible par les fichiers */dev/mem* ou */proc/kcore,* on sauvegarde son contenu à l'aide de la commande dcfldd (comme pour la swap).
Par exemple :

```
[root@compro] # dcfldd if=/dev/mem conv=noerror,sync hash=sha1
                                hashlog=/media/copie/ram.dd.sha1 of=/media/copie/ram.dd
```

Lorsque la sauvegarde de /proc/kcore ou /dev/mem n'est pas possible, il faut utiliser des librairies qui existent sou forme de module du noyau chargeable (LKM).
Nous étudions actuellement le module LKM LiME (Linux Memory Extractor) qui permet de faire cela, mais faute de tests suffisants, nous ne sommes pas en mesure d'intégrer cette technique dans notre méthode. Les résultats, si ils sont fructueux, seront disponibles dans une future version de ce document.
Pour en savoir plus sur la sauvegarde de la mémoire sur Linux, voir l'**annexe B**.

3.5 Arrêt de la machine

Nous disposons désormais du maximum d'informations volatiles en provenance de la machine compromise. Si cela n'a pas encore été effectué, il est temps désormais de débrancher la machine du réseau.
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.

3.6 Sauvegarde de l'espace de stockage

Pour la sauvegarde de l'espace de stockage, il est nécessaire de redémarrer la machine à partir du LiveCD A2IMP.
Cette opération est donc identique quelque soit le système compromis (Linux ou Windows). La différence réside surtout dans le nombre de partitions à sauvegarder (en général, un Windows comporte moins de partitions).

Note : on ne traite pas ici de la technique qui consiste à extraire physiquement le disque dur et à utiliser un boîtier spécialisé pour réaliser la sauvegarde des partitions ou du disque dans son intégralité.

Pour réaliser l'opération de sauvegarde de manière optimale, le LiveCD prend soin :
- **de démarrer avec l'option noswap** pour ne pas modifier la partition de swap
- **de ne pas monter les partitions des disques internes** de la machine

Le LiveCD A2IMP utilise un kernel récent (3.9.4) qui permet de démarrer sur de nombreux matériel et contient un nombre important de pilotes pour pouvoir reconnaître :
la plupart des supports de stockage mais également des pilotes réseaux et de contrôleurs disques (RAID...)
La plupart des types de partitionnement utilisés par un système (LVM, LVM2, EVMS), ainsi que les systèmes de fichiers (ext3, ext4, xfs, reiserfs, vfat, ntfs,...)

Si votre carte graphique est très récente, dans grub, choisir la ligne :
Boot (Modern Graphic Card)

En outre, un utilitaire de copie a été développé spécifiquement pour le LiveCD A2IMP et offre un confort pour réaliser cette opération en toute assurance. Cet utilitaire propose notamment :
- une interface graphique pour le choix des partitions disponibles
- une barre de progression graphique qui montre l'avancement de la copie
- la création d'un rapport à la fin de la copie avec les empreintes md5 et sha1 des images sauvegardées

L'utilitaire se base sur l'outil dcfldd qui effectue une sauvegarde bloc-à-bloc des partitions. L'avantage de cette méthode est de sauvegarder tous les secteurs de la partition, y compris les secteurs « vides », ce qui permettra par la suite d'effectuer une restauration des données effacées (si nécessaire).

Principes de base pour l'opération de sauvegarde :
- aucun système de fichier ne sera monté,
- la copie intégrale bloc-à-bloc de la partition sera réalisée (la taille de l'image sera donc indépendante du taux d'occupation de la partition et sera strictement égale à

la taille 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 créée par rapport à la partition originale (ce qui est fait automatiquement par dcfldd)

⇒ A noter que si vous utilisez d'autres LiveCD, se méfier car ils ont tendance à monter tout ce qui est possible pour faciliter la vie de l'utilisateur.

Note sur le partitionnement des disques durs : celui-ci peut être obtenu sous Linux par des commandes comme « *fdisk -l », df ou « cat /proc/partitions »*.
L'utilitaire de copie disque propose la liste des partitions du système sous forme de liste dans un tableau (les partitions propres au LiveCD sont exclues de cette liste).
Aussi, les informations sur les systèmes de fichiers montés, sur les disques et partitions ont été relevées par le script *a2imp-auto.sh* précédemment lancé.

3.6.1 Sauvegarde de l'espace de stockage des partitions système

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.

La sauvegarde des disques ou partitions systèmes est à répéter pour chaque partition et/ou disque à sauvegarder.

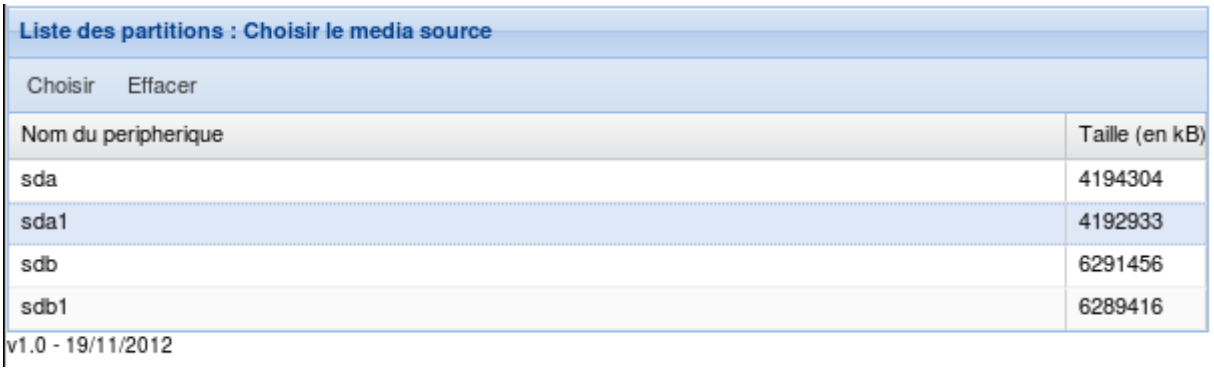
A noter que l'utilitaire de copie disque proposé horodate chaque copie et calcule automatiquement l'empreinte de chaque copie (md5 et sha1)

Une fois que l'on a démarré sur le LiveCD, on branche notre disque externe sur le port USB de la machine compromise. Celui ci sera monté automatiquement. Il s'agira de le démonter manuellement, dans la mesure ou notre utilitaire de copie disque va se charger de monter automatiquement ce périphérique de sauvegarde sur le point de montage /media/copie

Voici un exemple d'utilisation pour sauvegarder la partition /dev/sda1 sur la partition du périphérique externe vu en /dev/sdb1 :

1 - Cliquer sur l'icône « A2IMP Copie disque » qui se trouve sur le bureau

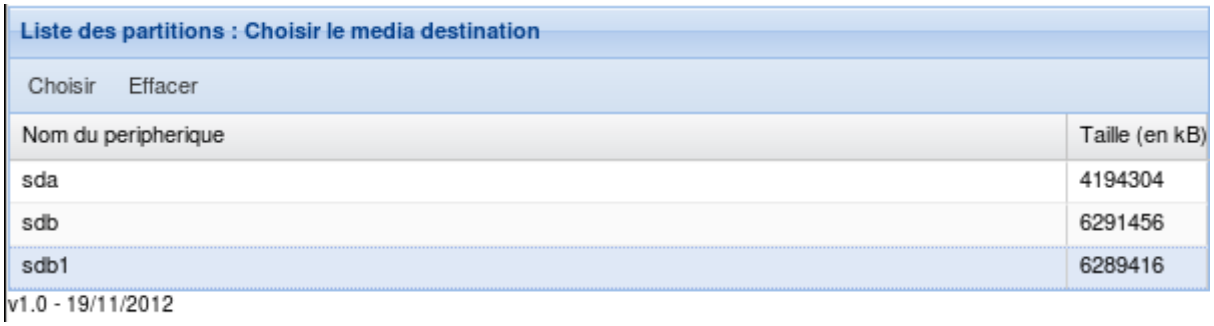
2 - Sélectionner la partition à copier : sda1 et cliquer sur « Choisir »



3 - Par défaut, le choix « Image sur disque local » est sélectionné. Cliquer sur « Choisir »

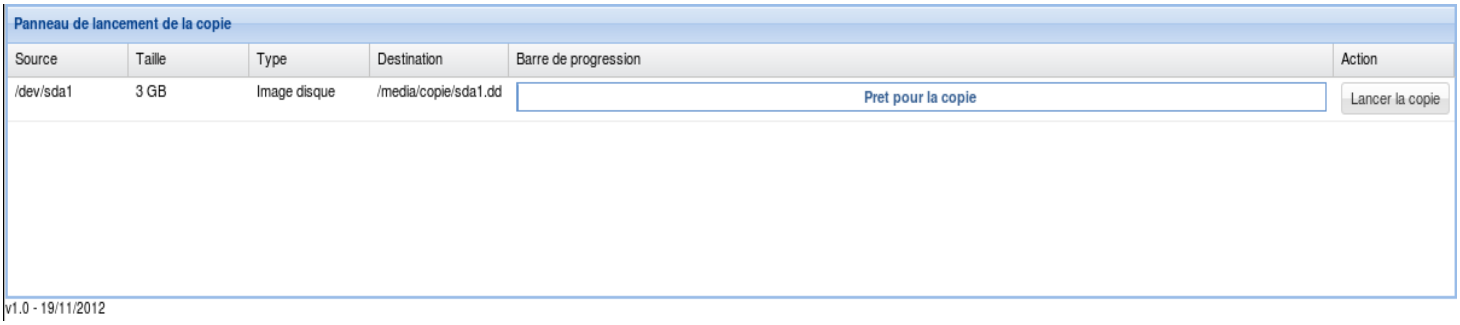
4 - Sélectionner la partition de destination.

Ce choix doit concerner une partition et non un disque (on récupère un fichier image).
En outre, la partition de destination doit avoir une taille supérieure à la source :)

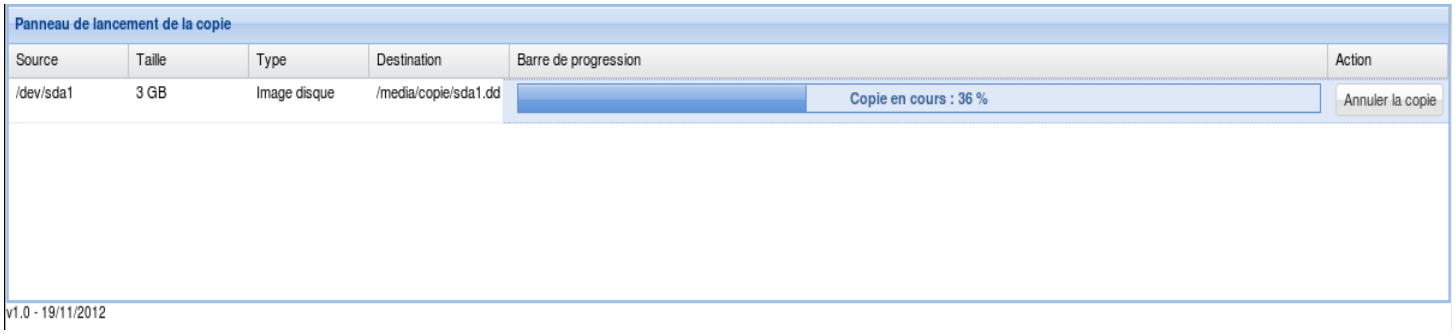


La partition sélectionnée sera automatiquement montée sur le point de montage /media/copie

5 - Lancer la copie en cliquant sur le bouton Action « Lancer la copie »



La progression de la copie s'affiche en temps réel :



A la fin de la copie, un fichier est automatiquement créé sur le même media que l'image de la partition.

Ce fichier report contient :

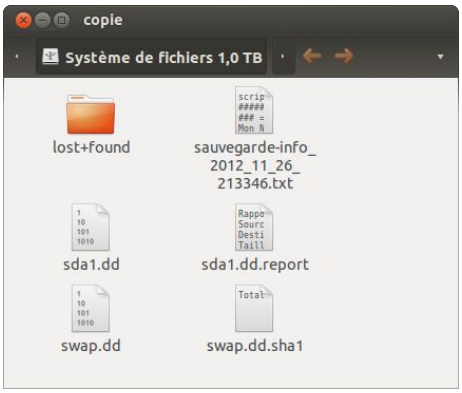
- un horodatage de la copie
- les empreintes md5 et sha1 des images
- la ligne de commande utilisée pour la copie :

```
dcfldd if=/dev/sda1 conv=noerror status=off hash=md5,sha1
md5log=/tmpdir/md5log_dcfldd sha1log=/tmpdir/sha1log_dcfldd | pv -n -s -s sizek
2 > /tmpdir/output_dcfldd | cat > /media/copie/sda1.dd
```

Cette opération doit être répétée pour toutes les partitions présentes sur le disque compromis.
Pour la partition de swap, si elle a déjà été sauvegardée à l'étape précédente, ce n'est pas la peine de la sauvegarder de nouveau ici.

4 Contenu final du media de sauvegarde

Le media de sauvegarde (/media/copie/) doit au final contenir au moins 5 fichiers :



1. Le fichier de sauvegarde des données volatiles (sauvegarde-info...)
2. La copie du disque ou d'une partition
3. Le rapport de la copie disque qui contient entre autre l'empreinte sha1 de l'image disque
4. Le fichier de sauvegarde de la swap
5. L'empreinte sha1 du fichier de sauvegarde de la swap

Note pour **4** et **5** : Le nom du fichier de sauvegarde de la swap dépendra de l'étape à laquelle vous avez effectuée cette opération. Si c'est à chaud, le nom sera celui que vous aurez donné en sortie de la commande dcfldd (dans notre cas swap.dd). Si c'est à froid avec l'utilitaire de copie disque, le nom sera celui de la partition de swap (par exemple sda2.dd).

En plus de ces fichiers, on peut aussi trouver :

- Le fichier de sauvegarde de la RAM (ram.dd) et son fichier d'empreinte associé (ram.dd.sha1)
- Autant de fichiers qu'il y a de partitions sur le(s) disque(s) compromis accompagné(s) de leur fichier de rapport de copie avec l'empreinte sha1 (sd*Xn*.dd et sd*Xn*.dd.report)
- Le fichier de main courante si celui ci a été rédigé de façon numérique

5 Références

Note CERTA-2002-INF-002-004 : Les bons réflexes en cas d'intrusion sur un système d'information http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002
Mise à jour en juillet 2012

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

Incidents de sécurité sur le site de la DSI pôle ARESU :
https://aresu.dsi.cnrs.fr/spip.php?rubrique97

Annexe A : Contenu du script a2imp-auto.sh du LiveCD A2IMP

```
#!/bin/bash
#a2imp-auto.sh version 20121126
echo "#############################################################################################################"
echo "script d'automatisation de collecte d'information sur un systeme Linux"
echo "a l'aide de la boite a outils A2IMP"
echo "Version 0.9 - 20121126"
echo "(c) CNRS / D. Pugnere       11/09/2006"
echo "(c) CNRS / D. Delavennat    26/11/2012"
echo "(c) CNRS / H. Ballans       26/11/2012"
echo "#############################################################################################################"
DAY=`./date +%Y_%m_%d`
TIME=`./date +%k%M%S`
echo "Entrer le chemin du point de montage de la cle USB (par exemple /media/usb_key/) :"
read path
FILENAME=$path\/sauvegarde-info\_$DAY\_$TIME.txt
echo "Vous avez rentré : $path"
echo "Le fichier de sortie est : $FILENAME"
echo "script d'automatisation de collecte d'information sur un systeme Linux a l'aide de la boite a outils A2IMP"
> $FILENAME
echo "#############################################################################################################" >>
$FILENAME
echo -e "### => date : Verification de l heure" >> $FILENAME
./date >> $FILENAME
echo -e "\n### => uname -a : version du noyau en cours d execution" >> $FILENAME
./uname -a >> $FILENAME
echo -e "\n### => cat /proc/sys/kernel/hostname : hostname" >> $FILENAME
./cat /proc/sys/kernel/hostname >> $FILENAME
echo -e "\n### => cat /proc/sys/kernel/osrelease : version du kernel" >> $FILENAME
./cat /proc/sys/kernel/osrelease >> $FILENAME
echo -e "\n### => uptime" >> $FILENAME
./uptime >> $FILENAME
echo -e "\n### => who : liste des personnes connectées" >> $FILENAME
./who  >> $FILENAME
#echo -e "\n### => w : liste des personnes et leur activité"
#./w
#echo -e "\n### => last : liste des dernières connexions sur ce système"
#./last
#echo -e "\n### => lsmod : liste des modules du noyau"
#./lsmod
echo -e "\n### => cat /proc/modules : liste des modules du noyau" >> $FILENAME
./cat /proc/modules  >> $FILENAME
echo -e "\n### => Logs du kernel depuis le boot" >> $FILENAME
./dmesg >> $FILENAME
echo -e "\n### => ifconfig -a : liste des interfaces reseau" >> $FILENAME
./ifconfig -a  >> $FILENAME
echo -e "\n### => arp -a : Table ARP" >> $FILENAME
./arp -a >> $FILENAME
echo -e "\n### => netstat -s : statistiques des protocoles reseaux" >> $FILENAME
./netstat -s >> $FILENAME
echo -e "\n### => netstat -nr : table de routage" >> $FILENAME
./netstat -nr >> $FILENAME
echo -e "\n### => route -Cn : table de routage" >> $FILENAME
./route -Cn >> $FILENAME
echo -e "\n### => netstat -anp : liste des connexions reseaux" >> $FILENAME
./netstat -anp >> $FILENAME
echo -e "\n### => lsof -n -i4 : liste des connexions reseau IPv4" >> $FILENAME
./lsof -n -i4 >> $FILENAME
echo -e "\n### => lsof -n -i4 : liste des connexions reseau IPv6" >> $FILENAME
./lsof -n -i6 >> $FILENAME
echo -e "\n### => ps -eaxf : liste des processus" >> $FILENAME
./ps -eaxf >> $FILENAME
#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" >>
$FILENAME
./lsof -n -P -l >> $FILENAME
echo -e "\n### => sysctl -a : liste de toutes les variables du kernel" >> $FILENAME
./sysctl -a >> $FILENAME
echo -e "\n### => printenv : liste des variables d'environnement" >> $FILENAME
./printenv >> $FILENAME
echo -e "\n### => df : liste des montages actifs" >> $FILENAME
./df >> $FILENAME
echo -e "\n### => cat  /proc/self/mounts : liste des montages" >> $FILENAME
./cat /proc/self/mounts >> $FILENAME
echo -e "\n### => cat  /proc/partitions : liste des partitions des disques detectés par le kernel" >> $FILENAME
./cat /proc/partitions >> $FILENAME
echo -e "\n### => fdisk -l /dev/(h|s)d[a-z] : liste des partitions des disques par fdisk" >> $FILENAME
for disk in `./tail -n +3 /proc/partitions | ./grep -E " (h|s)d[a-z]\b" | ./tr -s ' ' ' ' | ./cut -d" " -f 5`;
do ./fdisk -l /dev/$disk >> $FILENAME; done
echo -e "\n### => ifpromisc : verification du mode PROMISC sur les interfaces ethernet" >> $FILENAME
./ifpromisc >> $FILENAME
echo -e "\n### => chkproc : verification des processus cachés dans ps" >> $FILENAME
./chkproc >> $FILENAME
echo -e "\n### => listps : " >> $FILENAME
./listps >> $FILENAME
echo -e "\n### => cat /proc/swaps : information de sawp renvoye par le kernel" >> $FILENAME
./cat /proc/swaps >> $FILENAME
./echo "#########################################################################" >> $FILENAME
./echo "Processus en cours d'execution" >> $FILENAME
./echo "#########################################################################" >> $FILENAME
./ls /proc | ./sort -n | ./grep -v "[a-z,A-Z]" | while read PID
  do
        ./echo "Process ID $PID:" >> $FILENAME
        ./echo "/proc/$PID/cmdline:" >> $FILENAME
        ./cat /proc/$PID/cmdline >> $FILENAME
```

```
        ./echo >> $FILENAME
        ./echo "/proc/$PID/environ:" >> $FILENAME
        ./cat /proc/$PID/environ >> $FILENAME
        ./echo >> $FILENAME
        ./echo "/proc/$PID/maps:" >> $FILENAME
        ./cat /proc/$PID/maps >> $FILENAME
        ./echo >> $FILENAME
        ./echo "/proc/$PID/stat:" >> $FILENAME
        ./cat /proc/$PID/stat >> $FILENAME
        ./echo >> $FILENAME
        ./echo "/proc/$PID/statm:" >> $FILENAME
        ./cat /proc/$PID/statm >> $FILENAME
        ./echo >> $FILENAME
        ./echo "/proc/$PID/status:" >> $FILENAME
        ./cat /proc/$PID/status >> $FILENAME
        ./echo >> $FILENAME
        ./echo "/proc/$PID/root:" >> $FILENAME
        ./ls -ld /proc/$PID/root >> $FILENAME
        ./echo >> $FILENAME
        ./echo "/proc/$PID/cwd:" >> $FILENAME
        ./ls -ld /proc/$PID/cwd >> $FILENAME
        ./echo >> $FILENAME
        ./echo "/proc/$PID/exe:" >> $FILENAME
        ./ls -ld /proc/$PID/exe >> $FILENAME
        ./echo >> $FILENAME
        ./echo "/proc/$PID/fd/*:" >> $FILENAME
        ./ls -lrta /proc/$PID/fd/ >> $FILENAME
        ./echo >> $FILENAME
        ./echo "========================================================" >> $FILENAME
        ./echo >> $FILENAME
  done >> $FILENAME
./echo "#########################################################################" >> $FILENAME
echo -e "\n### => Copie du repertoire /tmp" >> $FILENAME
./tar -cPzvf $path/tmp.tgz /tmp/* >> $FILENAME
echo -e "\n### => Copie du repertoire /dev/shm" >> $FILENAME
./tar -cPzvf $path/dev_shm.tgz /dev/shm/* >> $FILENAME
```

Annexe B : Sauvegarde de la mémoire physique sur Linux

http://www.forensicswiki.org/wiki/Tools:Memory_Imaging#Linux