Documentation A2IMP-Windows

(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 Windows (**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!)
  - Une clé USB de capacité suffisante et formatée en NTFS
  - Un disque externe de capacité suffisante et formaté en ext3

Pourquoi 2 supports différents ? L'idéal serait en effet 1 seul gros disque externe formaté en NTFS. Mais nous rencontrons actuellement un problème avec ces disques lorsque l'on travaille sur le LiveCD, ce qui empêche d'effectuer les images des partitions. On pense à un problème de pilote ntfs et cela devrait être résolu dans une future version du LiveCD...

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
- Sauvegarde des informations volatiles à l'aide des commandes de la boîte à outils a2impWin
  - Insertion de la clé USB
  - Sauvegarde des informations volatiles en cours sur le système
  - Sauvegarde de la mémoire
- Arrêt-redémarrage de la machine à partir du même LiveCD A2IMP
- Sauvegarde de l'espace de stockage
  - Insertion du disque dur externe
  - Démarrage du programme de copie disque
  - Sauvegarde de l'espace de stockage des partitions système
- Arrêt définitif du système compromis

Conventions utilisées dans cette documentation :
- Le LiveCD est monté sur le lecteur Z:\
- La clé USB est montée sur le lecteur G:\
- 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 (serveur *NTP* de confiance ou horloge parlante au 3669).

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.

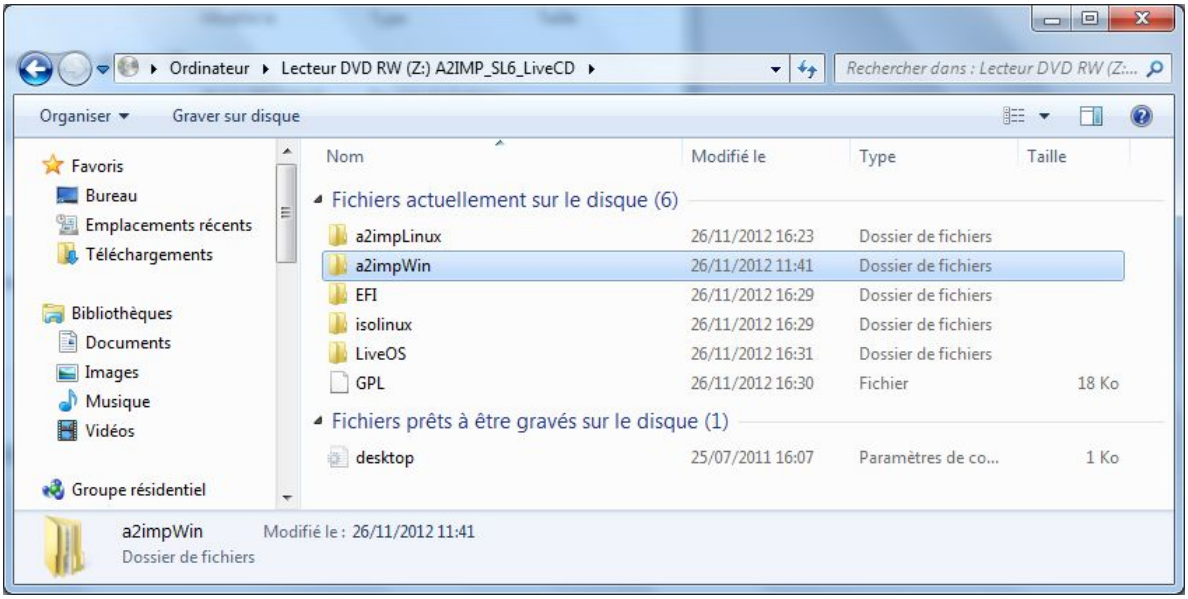
⇒ À partir de maintenant, on va donc noter sur la main courante chaque action et l'horodater.

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)

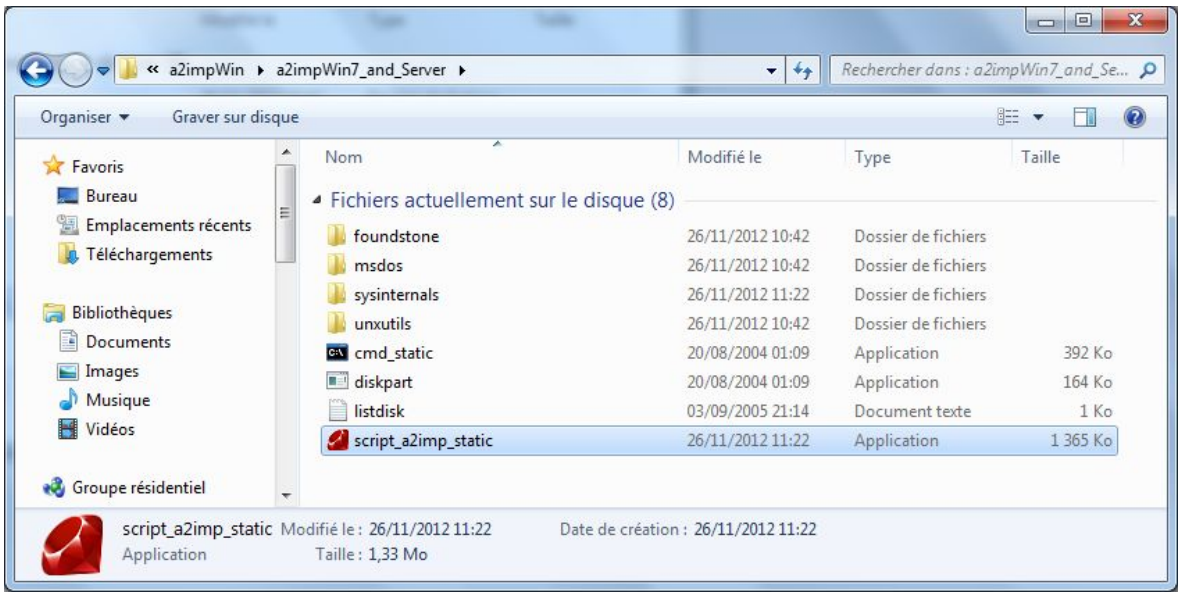
3.3 Montage de la boîte à outils (CDROM, clé USB)

Sur la machine compromise toujours en fonctionnement, nous allons en premier lieu insérer le LiveCD A2IMP.

L'acquisition des données volatiles va s'effectuer grâce à l'exécutable **script_a2imp_static.exe** placé dans le répertoire a2impWin (ce dernier étant situé à la racine du LiveCD).



Cet exécutable (programmé en ruby) fait appel à des commandes systèmes et utilitaires qui fonctionnent de manière statique sous Windows.
Parmi ces commandes, on peut trouver des commandes msdos classiques mais aussi des utilitaires tiers (comme les très bons utilitaires sysinternals). Voir l'**annexe B** pour plus de détails concernant les utilitaires qui composent la boite à outils a2impWin.
L'exécutable a été testé avec succès sur Windows XP, Vista, 7, 8 et 2003 Serveur (versions 32 et 64 bits)



Pour connaître en détail les commandes lancées par l'exécutable, voir l'**annexe A**

3.4 Sauvegarde des informations volatiles

3.4.1 Montage du support de sauvegarde

Brancher la clé USB NTFS sur l'un des ports USB de la machine compromise.
Cette clé doit avoir une capacité supérieure à celle de la mémoire vive de la machine compromise.

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.

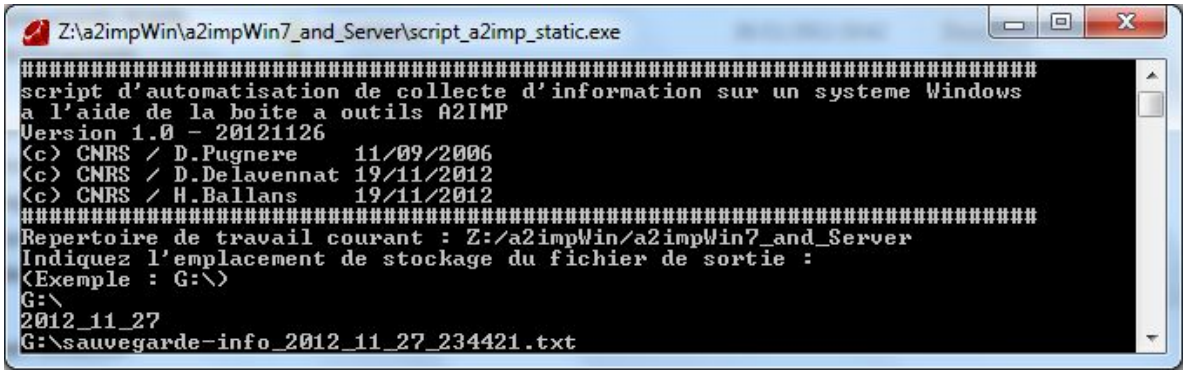
Nous effectuons cette étape en premier car c'est la plus rapide. Le script va récupérer un nombre conséquents d'informations en quelques secondes.

L'exécutable « *script_a2imp_static.exe* » lance des commandes qui permettent d'obtenir des informations sur l'état du système : connexions réseaux, liste des processus, partitions, environnement, modules.

Pour récupérer le maximum d'informations, il faut exécuter ce programme avec les droits administrateur . Si le compte sur lequel on est connecté n'est pas administrateur, il suffit de cliquer bouton droit sur le .exe et de sélectionner « **Exécuter en tant qu'administrateur** ».

Avant d'exécuter sa série de commandes, le script demande le chemin du support de sauvegarde. Dans notre exemple, selon la convention choisie, il faudra donc rentrer le chemin G:\ pour pouvoir enregistrer les informations sur la clé USB.

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 : l'anti-virus installé sur le système peut considérer le programme comme une menace potentielle. Outrepasser l'alerte éventuelle de cet anti-virus en acceptant de continuer l'exécution du programme.

Note concernant le fichier sauvegarde-info_YYYY_MM_DD_hhmmss.txt :
Le fichier généré par le script *script_a2imp_static.exe* peut contenir plus de 13000 lignes d'informations, soit plus de 250 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.

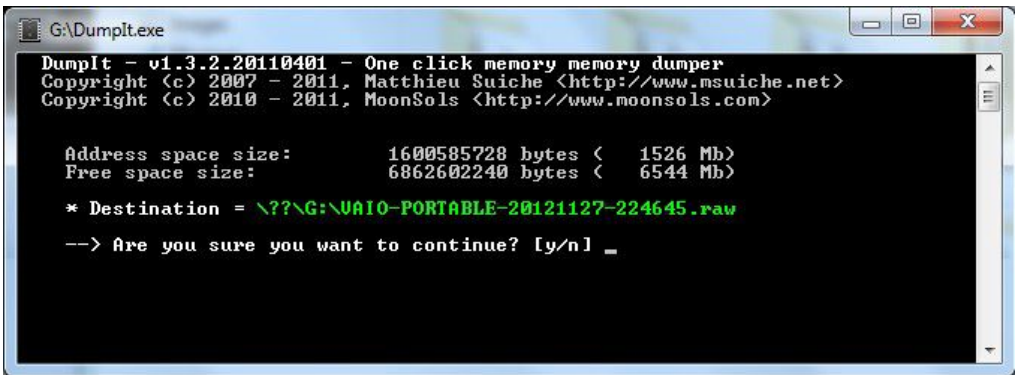
3.4.3 Sauvegarde de la mémoire

Cette opération était relativement complexe en 2006.

Elle est aujourd'hui grandement simplifiée grâce à l'utilitaire DumpIt (MoonSols).
Cet utilitaire étant à usage personnel, nous n'avons pas pu l'insérer dans notre LiveCD.

Il faut donc récupérer celui-ci et le placer sur la clé USB.
L'utilitaire est téléchargeable à l'adresse suivante :
http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7

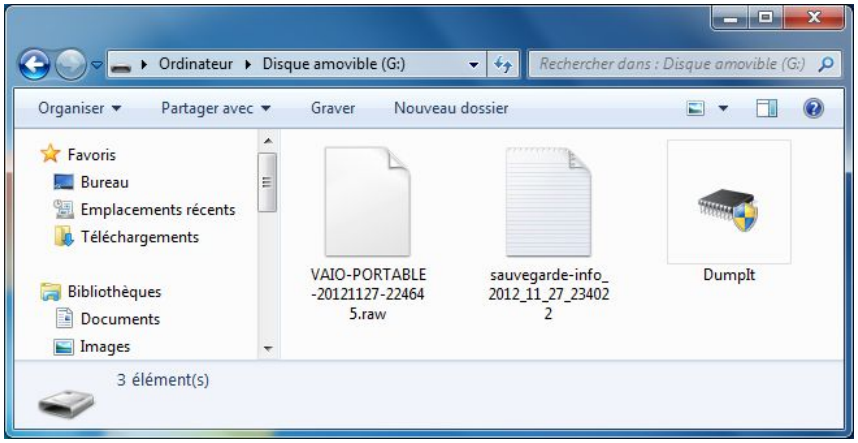
L'image générée est stockée à l'endroit d'où est lancé le programme. C'est pourquoi il faut le placer sur la clé USB.
Cette image aura pour nom : *NOM_NETBIOS*-YYYYMMDD-hhmmss.raw



Note : Le LiveCD contient également l'utilitaire *winpmem* qui est une alternative GPL à DumpIt. Cet utilitaire, écrit en python, est situé dans *a2impWin/memory/winpmem-1.3.1.*

3.5 Arrêt de la machine

Nous disposons désormais du maximum d'informations volatiles en provenance de la machine compromise. Hormis l'utilitaire DumpIt, votre clé USB doit donc à ce stade contenir 2 fichiers : le fichier de sauvegarde des informations volatiles et une image de la mémoire RAM.



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, *Démarrer → Arrêter !*).

Il faut noter que cette opération peut présenter quelques risques dans le cas où un script se lancerait avant extinction. De même, l'arrêt de la machine peut entraîner l'installation de mises à jour Windows, ce qui modifiera l'état de la machine et laissera des traces dans les journaux d'événements. On comprend ici l'importance de l'horodatage dans la collecte des informations...

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 programme script_*a2imp_static.exe* 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. Très généralement sur un Windows, la partition système (C:\) est situé sur la première partition du premier disque dur (soit /dev/sda1).

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

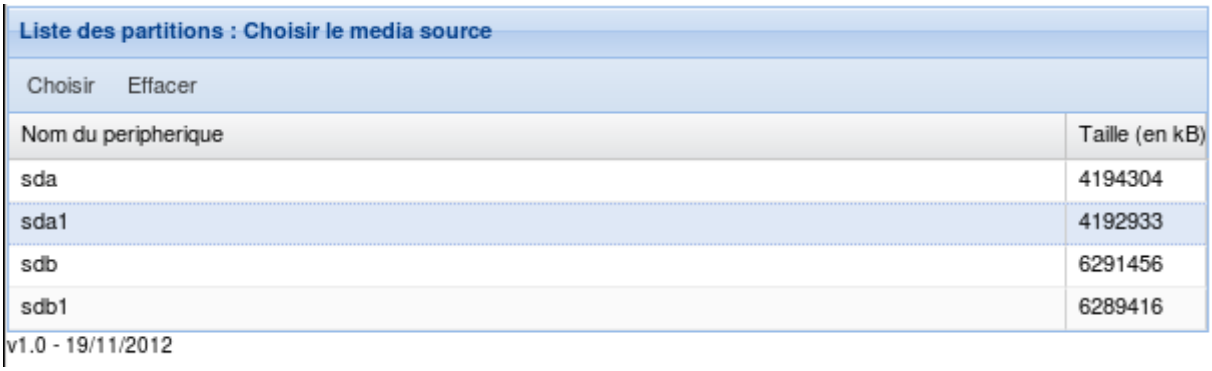
A noter que l'utilitaire de copie disque proposé horodate chaque copie et calcule automatiquement l'empreinte de chaque copie (md5 et sha1)

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

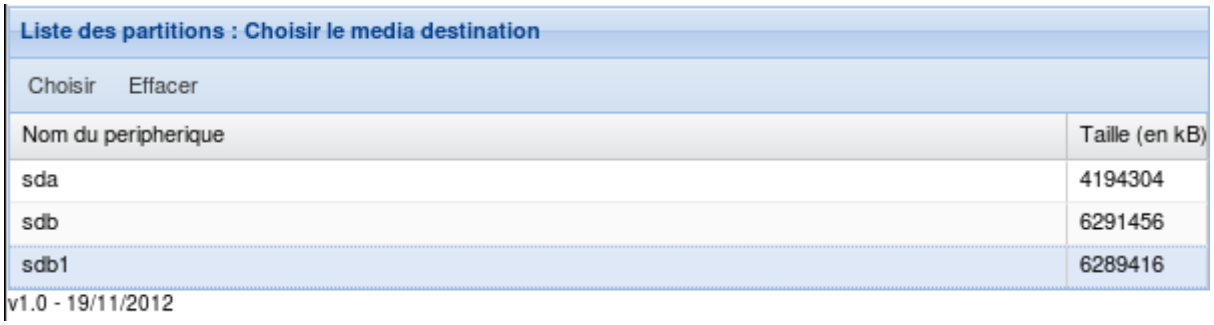
2 - Sélectionner la partition à copier : sda1 et cliquer sur « Choisir »



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

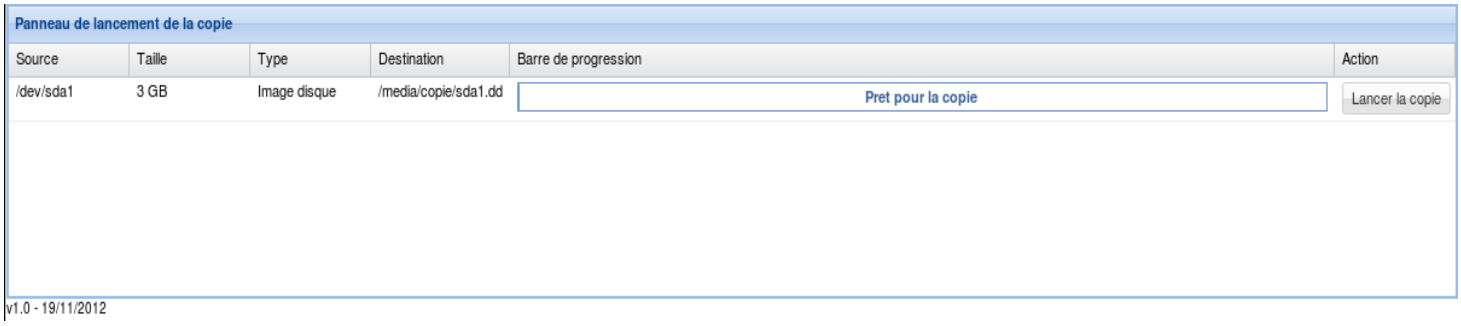
4 - Sélectionner la partition de destination.

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 :)

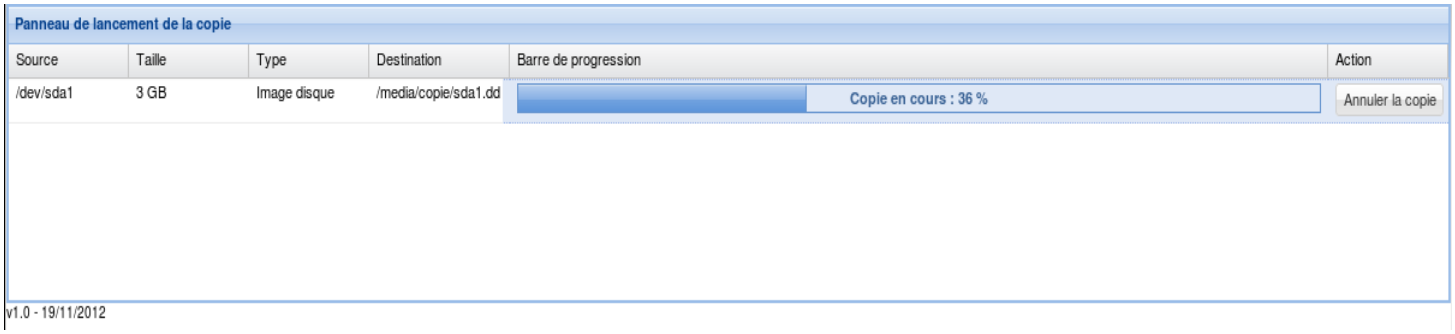


La partition sélectionnée sera automatiquement montée sur le point de montage /media/copie

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
```

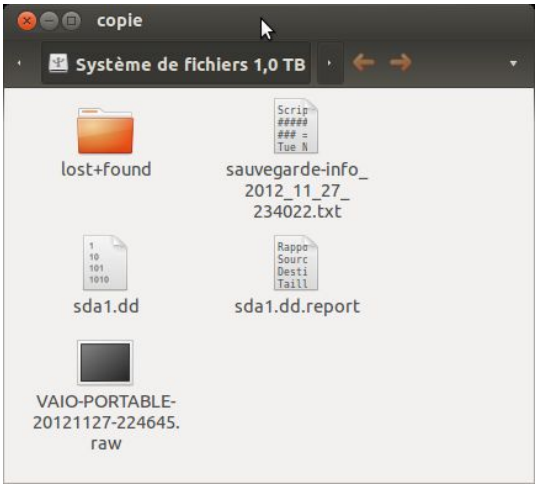
Cette opération doit être répétée pour toutes les partitions présentes sur le disque compromis.

Remarque : Windows dispose d'une mémoire virtuelle, appelée fichier d'échange, qui s'apparente au fichier de swap sous Linux. La taille par défaut du fichier d'échange de la mémoire virtuelle est égale à la capacité de la mémoire vive et peut monter jusqu'à 1,5 fois cette valeur. Ce fichier pagefile.sys est en général situé à la racine du disque dur (pour vérifier, commande > *dir pagefile.sys /a H*).
Aussi, ce fichier sera disponible dans l'image de la partition système.

4 Contenu final du media de sauvegarde

L'idéal est de centraliser tous vos fichiers d'acquisition sur un seul média. Il s'agit donc de copier les 2 fichiers de la clé USB vers le disque externe ext3 qui contient les images des partitions.

Ainsi, le media de sauvegarde (/media/copie/) doit au final contenir au moins 4 fichiers :



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

En plus de ces fichiers, on peut aussi trouver :

- 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 : Programme script_a2imp_static.rb du LiveCD A2IMP

```
#!/usr/bin/env ruby
#Pour creer l'executable, utiliser ocra depuis une invite de commande
#Ex : > ocra script_a2imp_static.rb
puts %Q{########################################################################
script d'automatisation de collecte d'information sur un systeme Windows
a l'aide de la boite a outils A2IMP
Version 1.0 - 20121126
(c) CNRS / D.Pugnere    11/09/2006
(c) CNRS / D.Delavennat 26/11/2012
(c) CNRS / H.Ballans    26/11/2012
########################################################################}

def process_command(file,cmd,output)
        file.puts %Q{################################################################################}
        file.puts %Q{### => #{cmd} : #{output}}
        file.puts %x{#{cmd}}
        file.puts
end

$wd = Dir.pwd
puts "Repertoire de travail courant : " +$wd

cmds_windows = [
  [ 'unxutils/date.exe', "Affichage date et heure locale du systeme"],
  [ 'cmd_static.exe /c ver', "Systeme et version du kernel en cours d execution"],
  [ 'msdos/HOSTNAME.exe', "Nom de la machine"],
  [ 'sysinternals/PsInfo.exe', "Informations sur le systeme"],
  [ 'cmd_static.exe /c net use', "Connexion reseau en cours"],
  [ 'sysinternals/PsLoggedon.exe', "Liste des personnes connectes"],
  [ 'sysinternals/logonsessions.exe', "Liste les ouvertures de session actives"],
  [ 'foundstone/NTLast.exe', "Liste des dernieres connexions sur le systeme"],
  [ 'msdos/ipconfig.exe /all', "Liste des interfaces reseau"],
  [ 'msdos/ARP.exe -a', "Table ARP"],
  [ 'msdos/NETSTAT.exe -s', "Statistiques des protocoles reseaux"],
  [ 'msdos/NETSTAT.exe -nr', "Table de routage"],
  [ 'msdos/NETSTAT.exe -ano', "Liste des connexions reseaux"],
  [ 'msdos/NETSTAT.exe -ban', "Liste des connexions reseaux avec les DLL utilises"],
  [ 'foundstone/Fport.exe', "Liste des connexions reseaux"],
  [ 'sysinternals/PsService.exe security', "Liste des services avec leur permission"],
  [ 'sysinternals/PsList.exe', "Liste des processus"],
  [ 'sysinternals/PsList.exe -t', "Arborescence des processus"],
  [ 'sysinternals/Listdlls.exe', "Liste des DLLs charges (par processus)"],
  [ 'sysinternals/psfile.exe', "Verifie les fichiers ouverts a distance"],
  [ 'cmd_static.exe /c set', "Liste des variables d environnement"],
  [ 'cmd_static.exe /c net share', "Liste des partages offerts"],
  [ 'cmd_static.exe /c net use', "Liste des disques montes"],
  [ 'sysinternals/diskext.exe', "Affiche les mappages de disques de volumes"],
  [ 'diskpart.exe /s listdisk.txt', "Liste des volumes, des disques et des partitions"]
]

puts "Indiquez l'emplacement de stockage du fichier de sortie : "
puts "(Exemple : G:\\)"
$path = gets.chomp
$date = Time.now.strftime("%Y_%m_%d")
puts $date
$time = Time.now.strftime("%H%M%S")
$file = $path+"sauvegarde-info_"+$date+"_"+$time+".txt"
puts $file

system('reg add HKCU\Software\Sysinternals\DiskExt /v EulaAccepted /t REG_DWORD /d 1 /f')
system('reg add HKCU\Software\Sysinternals\Listdlls /v EulaAccepted /t REG_DWORD /d 1 /f')
system('reg add HKCU\Software\Sysinternals\LogonSessions /v EulaAccepted /t REG_DWORD /d 1 /f')
system('reg add HKCU\Software\Sysinternals\psfile /v EulaAccepted /t REG_DWORD /d 1 /f')
system('reg add HKCU\Software\Sysinternals\PsInfo /v EulaAccepted /t REG_DWORD /d 1 /f')
system('reg add HKCU\Software\Sysinternals\PsList /v EulaAccepted /t REG_DWORD /d 1 /f')
system('reg add HKCU\Software\Sysinternals\PsLoggedon /v EulaAccepted /t REG_DWORD /d 1 /f')
system('reg add HKCU\Software\Sysinternals\PsService /v EulaAccepted /t REG_DWORD /d 1 /f')

File.open($file,'w') do |title|
        title.puts "Script d'automatisation de collecte d'information sur un systeme Windows a l'aide de la boite
a outils A2IMP"
end

File.open($file,'a') do |file|
        cmds_windows.each{|cmd|
        process_command file,cmd[0],cmd[1]
        }
end
```

Annexe B : Contenu de la boîte à outils a2impWin

Elle a été construite à partir d'utilitaires provenant de sources sûres (!).
Tous les binaires s'utilisent en ligne de commande dans une fenêtre « cmd »

Binaires Windows (récupérés depuis un système sûr) :

1. cmd.exe (renommé en cmd_static.exe)
2. dispart.exe
3. hostname.exe
4. ipconfig.exe
5. net.exe
6. netstat.exe
7. reg.exe

Note : pour fonctionner en mode statique sur des systèmes > Windows XP, les binaires ipconfig, arp et netstat doivent être accompagnés de leur fichier de description .mui (placés dans le dossier fr-FR)

Outils sysinternals

1. PsInfo.exe
2. PsLoggedon.Exe
3. logonsessions.exe
4. PsService.exe
5. PsList.exe
6. Listdlls.exe
7. psfile.exe
8. diskext.exe

unxutils

1. date.exe
2. md5sum.exe

foundstone

1. NTLast.exe
2. Fport.exe