Dans le cadre de

SECURIDAY 2010

Et sous le thème de

Computer Forensics Investigation

VOUS PRÉSENTE L'ATELIER :

Réplication des données

Chef Atelier : **Afef EL GARES** (RT5)

- **Meher BOUANENI**(Esprit)
- **Safa HAMDOUN** (RT5)
- **Sawssen BEN TICHA** (RT5)

1. Présentation de l'atelier et de l'outil

Si vous gérer ou administrer des systèmes d'information et des réseaux, vous devez comprendre recherche de preuves informatiques ou « Computer forensics ». Cette dernière est le processus d'utilisation des connaissances scientifiques pour la collecte, l'analyse et la présentation des preuves devant les tribunaux.

Dans la première phase de ce processus, la collecte, on trouve la réplication des données. La copie crée sera ce qu'on appelle « bit stream copy ». Cette copie est beaucoup plus complète que celle d'une norme de sauvegarde d'image miroir d'un disque dur. La copie bit stream implique la copie de chaque bit de données sur un disque dur de preuve, qui comprend entre autres l'espace non réservé par le système de fichier duquel des fichiers et des e-mails supprimés sont souvent récupérés.

Cette copie est très importante car :

- ✓ Permet à l'examinateur d'analyser l'ensemble des activités qui ont eu lieu sur le disque dur, et pas seulement les fichiers qui existent actuellement. L'examinateur peut rechercher et localiser les fichiers supprimés et des communications (e-mails).
- ✓ Fichiers Internet temporaires sont un autre avantage qui ne vient que d'une copie conforme. Une fois examinées et analysées, ces fichiers fournissent souvent des informations sur des sites Internet spécifiques que le suspect a visités.

- ✓ Conversations de « Chat rooms », qui ne sont pas enregistrées dans un fichier, et peuvent être reconstruit à partir de fragments trouvés dans l'espace disque temporaire.

Sur le marché il ya une compile de logiciels qui peuvent répondre à nos besoins :

- ➢ Payants :
  - Environnement windows
    - PcCloner
    - R Drive Image
    - Save-N-Sync

- Free :
  - Environnement windows
    - liveview
    - Helix
    - Drive Image XML
  - Environnement Linux:
    - Advanced Forensic Format Library (afflib)
    - dcfl-dd
    - dd
    - dd_rescue

Pour Réaliser cet atelier on a choisi d'utiliser 2 logiciels :

- dd ou dc3dd avec la GUI : AIR, sur Linux
  - ✓ Auto-détection des disques IDE et SCSI, CD-ROM et lecteurs de bandes
  - ✓ Choix d'utiliser dd ou dc3dd
  - ✓ Vérification de l'image entre la source et copie via MD5 ou SHA1/256/384/512
  - ✓ Compression d'image / décompression via GZip/BZip2
  - ✓ Image sur un réseau TCP / IP via netcat / cryptcat
  - ✓ Prend en charge les lecteurs de bandes SCSI
  - ✓ Essuyage (zéro) ou des partitions disques
  - ✓ Images se divisant en plusieurs segments
  - ✓ Journalisation détaillée avec la date / heure et complète des lignes de commande utilisés
- Drive Image XML, sur Windows.
  - ✓ La sauvegarde (backup)
  - ✓ La restauration (restore)
  - ✓ La réplication du disque
  - ✓ La réplication du disque à chaux
  - ✓ Parcourir un fichier image (et en extraire des fichiers si besoin).
  - ✓ Programmer des sauvegardes automatiques

2. Environnement logiciel

Dd / dc3dd avec la GUI : AIR (Automated Image and Restore)

On l'a installé sur UBUNTU 9.10 et comme pré requis il faut avoir :

- ✓ Uudecode : retrouver un fichier binaire à partir d'un fichier Uuencodé (convertir des données binaires codées sur 8 bits en un format de codage sur 7 bits)
- ✓ Perl/Tk version supérieure à (804.028): environnement graphique

Et eventuellement :

- ✓ dc3dd : enhanced dd crée par la « Defense Cyber Crime Center »
- ✓ nc : (netcat) permet la réplication à travers le réseau
- ✓ cryptcat : nc avec encryption

Drive Image XML

Il utilise le service VSS (Volume Shadow Services) de Microsoft, permettant de créer des copies sûres à chaud, c'est-à-dire même pour les disques en cours d'utilisation.

Il fonctionne uniquement sous Windows XP Home, XP Professionel et Windows Server 2003. Le programme sauvegarde et restaure des disques utilisant les systèmes de fichier FAT12, FAT16, FAT32 et NTFS.

3. Installation et configuration

Dd / dc3dd avec la GUI : AIR (Automated Image and Restore)

Téléchargeable à partir :
http://sourceforge.net/projects/air-imager/
Vous devez faire cette opération en étant root puisque l'installeur va presque tout mettre dans /usr/local/bin.

2.) décompressez le fichier install-air-x.x.x.tar.gz:

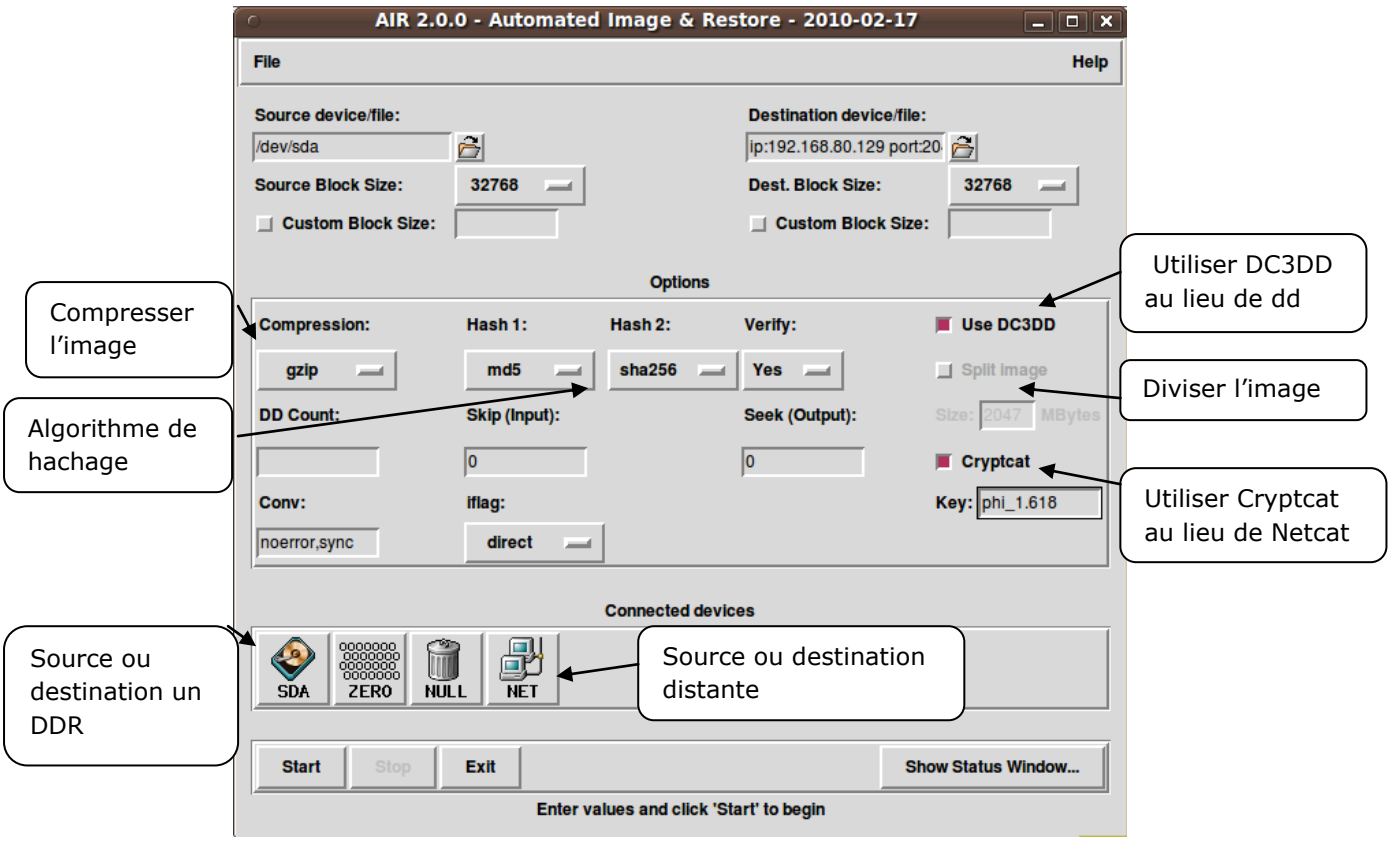
```
$ tar zxvf install-air-x.x.x.tar.gz
```

3.) L'installeur est un fichier SHAR (archive shell) qui doit être exécutable pour fonctionner. Ensuite vous exécutez tout simplement le script:

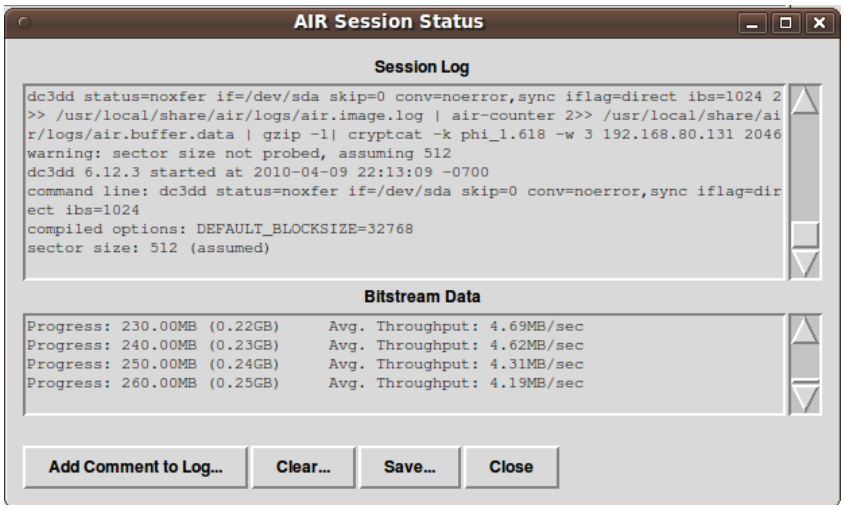
```
$ chmod +x install-air-x.x.x
$ sudo ./install-air-x.x.x  (ou bien ./install-air si vous êtes root)
```

4.) Vous pouvez lancer votre application :

$ sudo air



Cliquez sur Show status windows pour voir l'avancement de la copie



A la fin de la copie vous aurez une comparaison entre les hashs et la date de fin de l'opération :

```
VERIFY SUCCESSFUL: Hashes match
Orig = 2c33cda950a7c1b04daf7f3a92326695
Copy = 2c33cda950a7c1b04daf7f3a92326695
```

```
Progress: 0.04MB (0.00GB)       Avg. Throughput: 0.04MB/sec
Finished: 0.04MB (0.00GB)       Avg. Throughput: 0.04MB/sec
Command completed: Fri Feb 23 18:09:45 EST 2007
```

Drive Image XML

Téléchargeable à partir :
http://www.runtime.org/driveimage-xml.htm

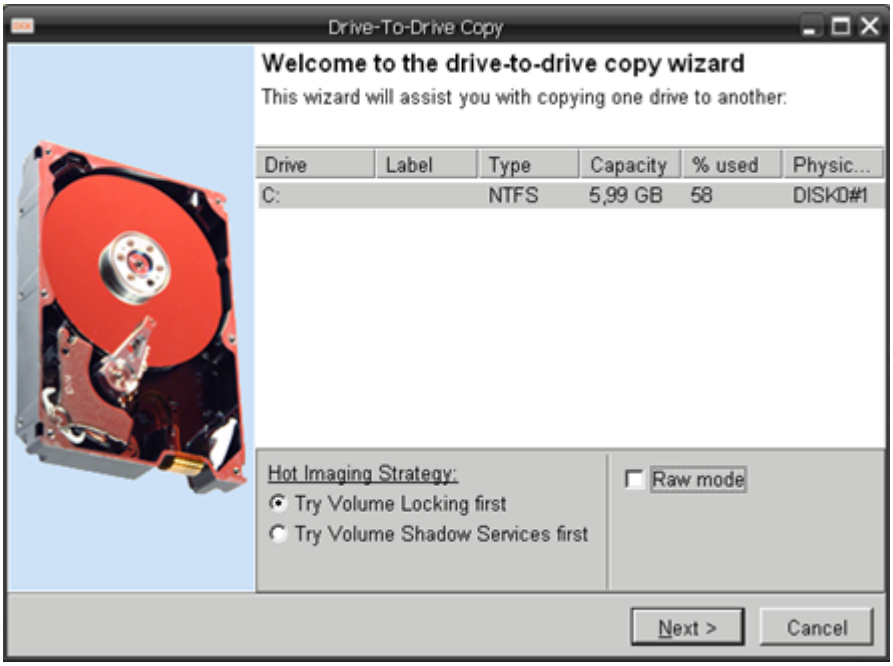
Après avoir téléchargé l'exécutable il suffit de cliquer dessus pour commencer l'installation, ensuite vous serez guidés par l'interface :

Voici l'interface principale du logiciel:

1. Cliquez sur Drive to Drive pour lancer l'opération de réplication de donnée.

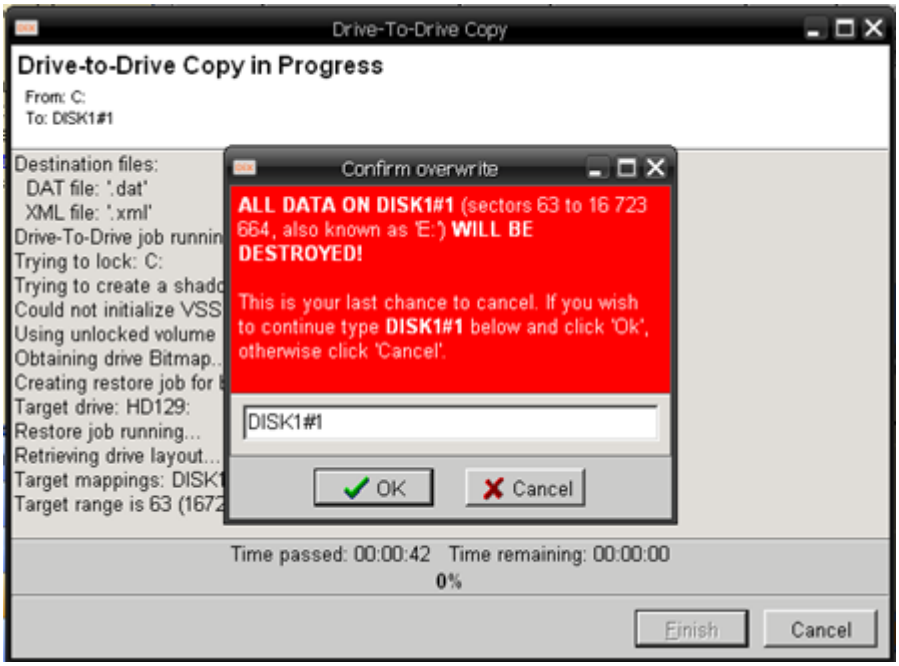
2. Le logiciel va rapidement passer en revue votre PC pour détecter ses disques. Il affichera ensuite la liste des disques et des informations les concernant. Sélectionner le disque image puis cliquez sur Next.

3. Vous êtes alors dans l'assistant de réplication. S'il s'agit bien du disque à dupliquer (backup) cliquez le bouton Next.



4. Pour que la réplication puisse commencer, il convient d'indiquer à l'assistant où on veut dupliquer l'image, indiquer le chemin complet dans la ligne Directory.

5. Le logiciel ouvre l'assistant et va vous demander où se trouve le fichier image, donnez-le lui



6. Une fois fait, une dernière confirmation vous sera demandée.

Remarques:

- Il faut que l'espace disque libre à cet emplacement soit plus grand que la taille du disque d'origine.

- *Raw mode*: Si vous sélectionnez raw mode, ce logiciel créera une image secteur par secteur de votre disque, c'est à dire de TOUS les secteurs de votre disque y compris ceux qui ne contiennent pas de données. L'image aura donc exactement la même taille que votre disque logique ou partition.

4. Un petit scénario de test

La réplication des données entre dans la phase de collecte du processus de « Computer forensics ».Pour tester l'outil, il suffit de :

- Ajouter, effacer des fichiers
- Naviguer sur Internet
- Tchatcher
- Modifier quelques fichiers à distance et essayer d'effacer ses traces en utilisant par exemple un anti forensics.

Ensuite de faire une image et travailler sur cette image pour analyser les donner er extraire les preuves

5. Conclusion

La réplication des données est une phase très importante dans l'opération d'investigation car elle permet de ne rien toucher au disque de preuve et faire toutes les opérations nécessaires à inculper le suspect ou le trouver sur le disque image. Il existe sur le marché plusieurs outils répondants à ce besoin