Dans le cadre de

SECURIDAY 2010

Et sous le thème de

Computer Forensics Investigation

VOUS PRÉSENTE L'ATELIER :

Collecte des données à partir d'un pc

Chef Atelier : **Walid Badreddine (RT5)**

- **Mahmoud Chaar (RT4)**
- **Hajer Aini (RT4)**
- **Oussama Achouri (RT3)**

1. Présentation de l'atelier :

L'atelier « Collecte des données à partir d'un pc », est la première étape dans la procédure du « Forensics ». Cette collecte de données s'effectuera sur une image des disques de la machine victime et aura pour objectif de rassembler un maximum d'informations pouvant servir dans l'enquête.

L'atelier comportera cinq sections principales :

* le montage des images des disques de la machine victime sur un environnement virtuel.

* la collecte des fichiers logs sous Linux.

* la collecte des fichiers logs sous Windows.

* La collecte des informations des registres.

* La recherche et la collecte d'informations dans les répertoires et autres fichiers (images, texte, vidéos, …)

1.1 – Montage des images des disques :

Cette section est consacrée au montage des images des disques de la machine victime sur un environnement virtuel en utilisant « virtual box » sous Linux ou « VMware » sous Windows.

Cette étape est une étape de préparation à la collecte d'informations, elle permet de recréer un environnement similaire à celui de la machine victime et évite ainsi de travailler directement sur la vraie machine qui constitue une preuve dans l'enquête judiciaire en cours.

Le montage de l'image se fait de la même manière que lorsqu'on charge un système d'exploitation sur machine virtuelle.

1.2 – collecte des fichiers logs sous Linux :

Les journaux systèmes se trouvent dans le répertoire « /var/log ». tous les évènements survenus dans le système y sont inscrits (processus de démarrage, lancement des services et des applications, les plantages , etc…).

Un fichier log est un fichier texte dont les évènements sont enregistrés ligne par ligne. Chaque ligne ou évènement comporte les informations suivantes :

- La date à laquelle l'évènement a été déclenché.
- Le processus déclencheur de l'évènement.
- Le processus ayant demandé l'ajout du message correspondant au log.
- Le niveau de gravité du message.

En général on s'attarde sur « auth.log » pour repérer les authentifications qui ont échoué (authentication failure) ou les utilisateurs illégaux essayant de se connecter (invalide users).

Le fichier « /etc/syslog.conf » permet de configurer le démon de journalisation « syslog » en déterminant de quelle manière seront traitées les différents logs systèmes.

Ce fichier est séparé en deux parties :

- 1ère partie : le processus demandeur et son niveau de priorité <dispositif>.<niveau>

  «dispositif» est appelé « facility » qui désigne le type de message parmi les suivants :

Auth/authpriv	=> trace sécurité/identification
cron	=> trace d'un cron
daemon.*	=> trace d'un daemon
kern.*	=> trace du noyau
lpr.*	=> trace du système d'impression
mail	=> trace du système de messagerie
news	=> trace d'un service de news/réseau
syslog	=> trace du service syslog lui-même
user	=> trace des processus utilisateurs
local0 à 7	=> trace issue des klogd

  « niveau » donne la « priority » du message parmi les suivants : debug, info, notice, warning, error, critique, alert, emergency.

- 2ème partie : le fichier log correspondant qui reçoit le message et l'ajoute à sa liste de messages <fichier log>.

Vérification des utilisateurs logged sur la machine :

La commande « last » permet d'afficher l'historique des utilisateurs qui se sont connectés sur la machine.

« last » recherche dans le fichier « /var/log/wtmp » et affiche une liste de tous les utilisateurs connectés (et déconnectés) depuis que le fichier a été créé. Les noms des utilisateurs peuvent être donnés en argument dans ce cas la commande affichera les entrées correspondantes à ces arguments.

Le fichier est réinitialisé à chaque fois que le système redémarre. Ainsi, le reboot de « last » affiche un journal de tous les redémarrage depuis la création du fichier.

« lastb » affiche le journal « /var/log/btmp » qui contient toutes les tentatives de connexions échouées.

Le fichier log « /etc/passwd » :

Ce fichier contient tous les nouveaux comptes crées, les comptes sans mots de passe, les changements d'UID, et toutes les informations relatives aux comptes et aux utilisateurs.

Pou le visualiser : « cat /etc/passwd ».

1.3 – Collecte des fichiers logs sous Windows :

Le service journal des évènements consigne les évènements d'applications, de sécurité, et des évènements système dans l'observateur d'évènements.

Windows enregistre les évènements dans l'un des trois journaux suivants :

Journal des applications :

Contient les évènements enregistrés par les programmes. Les évènements écrits dans ce journal sont déterminés par les développeurs du programme. Ce fichier se trouve dans : %SystemRoot%\System32\Config\AppEvent.evt

Journal de sécurité :

Le journal de sécurité enregistre des événements tels que les tentatives d'ouverture de session valides et non valides et tous les événements liés à l'utilisation des ressources, comme la création, l'ouverture ou la suppression de fichiers. Par exemple, lorsque l'audit d'ouverture de session est activé, un événement est enregistré dans le journal de sécurité chaque fois qu'un utilisateur essaie d'ouvrir une session sur l'ordinateur. Vous devez avoir ouvert une session en tant qu'administrateur ou en tant que membre du groupe Administrateurs pour pouvoir activer, utiliser et indiquer les événements qui sont enregistrés dans le journal de sécurité. Ce fichier se trouve dans: %SystemRoot%\System32\Config\SecEvent.evt

Journal système :

Le journal système contient les événements consignés par les composants système de Windows XP. Par exemple, si un pilote ne parvient pas à se charger au cours du démarrage, un événement est enregistré dans le journal système. Windows XP prédéfinit les événements qui sont consignés par les composants système. Ce fichier se trouve dans : %SystemRoot%\System32\Config\SysEvent.evt

Procedure pour afficher les détails des évènements :

Pour afficher des détails sur un événement, procédez comme suit :

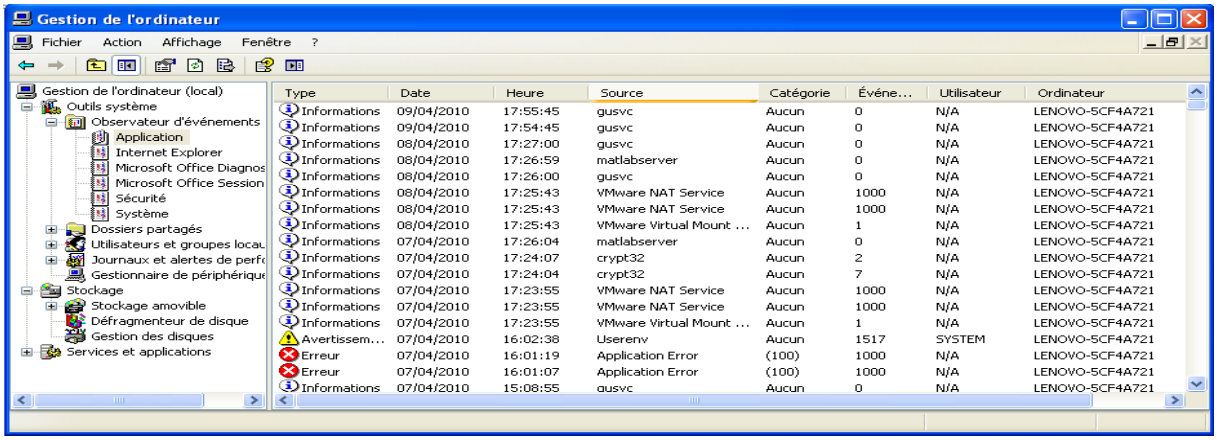
1. Cliquez sur Démarrer, puis sur Panneau de configuration. Cliquez sur **Performances et maintenance**, sur **Outils d'administration**, puis double-cliquez sur **Gestion de l'ordinateur**. Dans l'arborescence de la console, développez Observateur d'événements, puis cliquez sur le journal contenant l'événement que vous voulez afficher.

   Si le fichier journal d'évènements (.evt) provient d'une autre machine, cliquez sur **Action** dans la barre de tâches puis sur Ouvrir un fichier Journal.

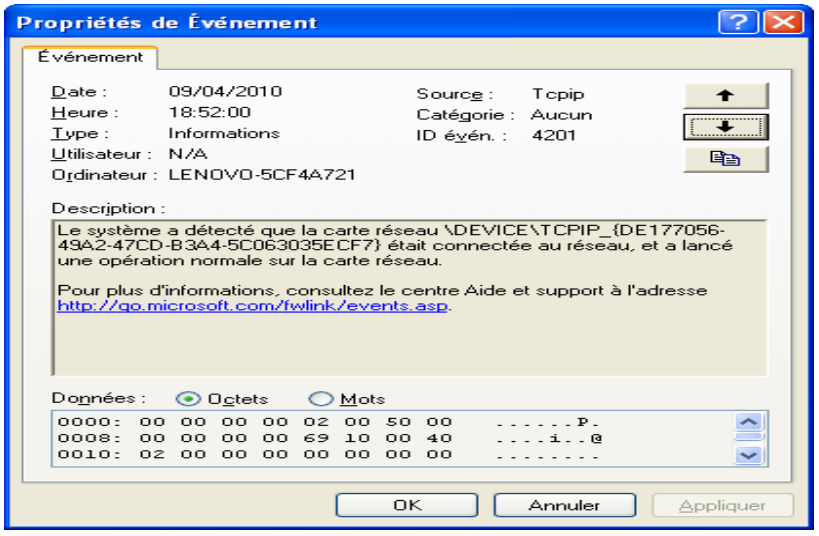
Il est important de notifier que lors de l'importation d'un journal, il faut aussi importer les dll correspondantes (emplacement : %SystemRoot%\System32).

2. Dans le volet de détails, double-cliquez sur l'événement à afficher.

   La boîte de dialogue Propriétés de l'événement contenant des informations d'en-tête et une description de l'événement s'affiche.



Dans l'arborescence de la console, sous le dossier Observateur d'évènements, on choisit un journal pour afficher les évènements qu'il contient. Ensuite, il faut double-cliquer sur l'évènement qui nous intéresse pour en voir les détails.



Cet évènement du journal système faire référence à la connexion à un réseau.

Procédure pour interpréter un évènement :

Chaque entrée de journal est classée par type, et contient des informations d'en-tête ainsi qu'une description de l'événement.

En-tête de l'événement

- *Date* : Date à laquelle l'événement s'est produit.

- *Heure* : Heure à laquelle l'événement s'est produit.
- *Utilisateur* : Nom de l'utilisateur qui avait ouvert la session lorsque l'événement s'est produit.
- *Ordinateur* : Nom de l'ordinateur sur lequel l'événement s'est produit.
- *ID événement* : Numéro d'événement permettant d'identifier le type d'événement. L'ID événement peut être utilisé par les techniciens spécialistes du produit pour comprendre ce qui s'est produit sur le système.
- *Source* : Source de l'événement. Il peut s'agir du nom d'un programme, d'un composant système ou d'un composant individuel d'un programme plus important.
- *Type* : Type de l'événement. Il peut s'agir de l'un des cinq types suivants : Erreur, Avertissement, Information, Audit des succès ou Audit des échecs.
- *Catégorie* : Classification de l'événement en fonction de sa source. Celle-ci est essentiellement utilisée dans le journal de sécurité.

Types d'événement

La description de chaque événement consigné dépend du type de cet événement. Chaque événement d'un journal peut être classé comme appartenant à l'un des types suivants :

Information :

Événement décrivant la réussite d'une tâche, comme une application, un pilote ou un service. Par exemple, un événement de type Information est consigné lorsque le chargement d'un pilote réseau aboutit.

Avertissement :

Événement qui n'est pas nécessairement important mais qui peut, cependant, indiquer la possibilité d'un problème futur. Par exemple, un message de type Avertissement est consigné lorsque l'espace disque commence à être saturé.

Erreur :

Événement qui décrit un problème important, comme l'échec d'une tâche essentielle. Les événements de type Erreur peuvent entraîner une perte de données ou de fonctionnalité. Par exemple, un événement de type Erreur est consigné si un service ne parvient pas à se charger au démarrage.

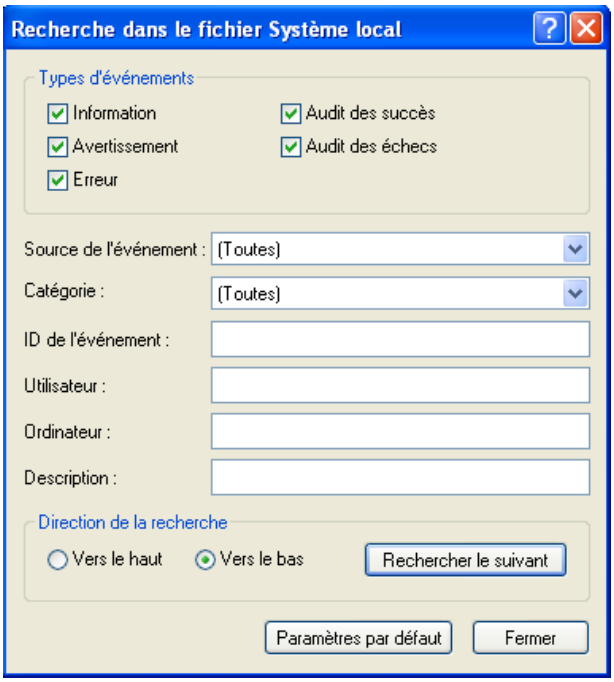
Audit des succès (journal de sécurité) :

Événement qui décrit la réussite d'un événement de sécurité audité. Par exemple, un événement de type Audit des succès est consigné lorsque l'utilisateur ouvre une session sur l'ordinateur.

Audit des échecs (journal de sécurité) :

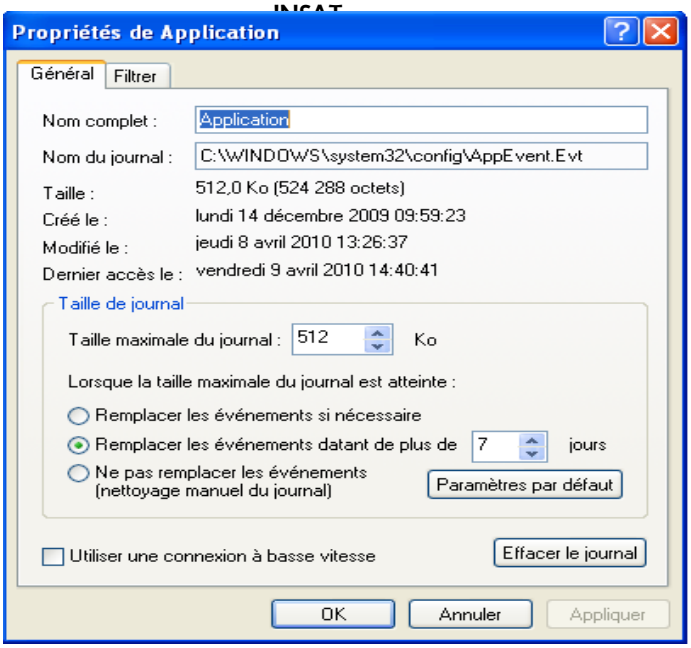
Événement qui décrit l'échec d'un événement de sécurité audité. Par exemple, un événement de type Audit des échecs est consigné lorsqu'un utilisateur ne parvient pas à accéder à un lecteur réseau.

Il est possible de **Rechercher** et de **Filtrer** les évènements des différents journaux suivants des critères spécifiques.



La fonctionnalité « recherche » permet de retrouver des évènements plus rapidement suivant des critères d'affinement. Cependant, la fonctionnalité « filtrer » est paramétrée pour sélectionner les évènements qui seront sauvegardés dans le journal.

Par défaut, la taille maximum initiale d'un journal est de 512 Ko, et lorsque cette taille est atteinte, les nouveaux événements remplacent au fur et à mesure les événements les plus anciens.



On peut redéfinir la taille d'un journal et ses options de remplacements ou effacer son contenu. Enfin on peut exporter le contenu d'un journal en fichier « .txt », « .evt », « .csv ».

1.4 – Collecte des informations des registres :

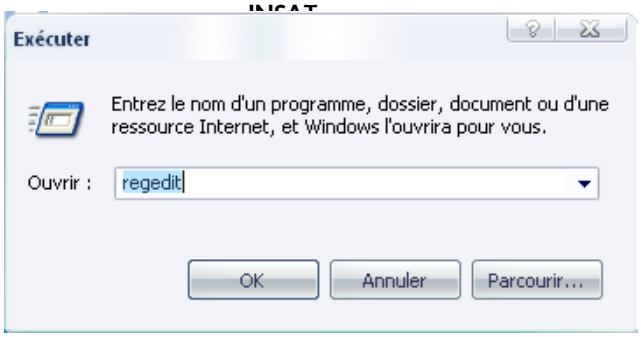
La base de registre Windows est appelée aussi registre ou BDR. Windows utilise constamment ces informations dès le démarrage du système et lors de son fonctionnement. Le registre est sollicité à chaque modification d'une propriété par une boite de dialogue Windows. Les informations contenues dans les registres sont variées parmi elles : les variables d'environnement, les profils de chaque utilisateur de la machine, les informations relatives au matériel du système, les informations relatives aux programmes installés et les informations sur les mots de passe, etc…

Les registres sous Windows se trouvent dans plusieurs répertoires :

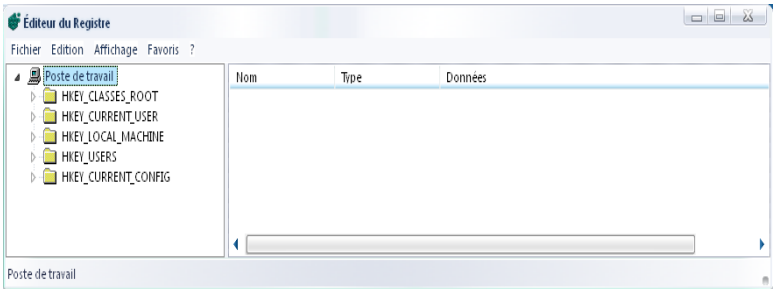
- C:\Documents and Settings\%USERPROFILE%\ *(\%USERPROFILE%\ -> correspond au nom des sessions)*
- C:\Documents and Settings\%USERPROFILE%\Local Settings\Application Data\Microsoft\Windows\
- C:\Windows\System32\Config\
- C:\Windows\System32\Config\systemprofile\
- C:\Windows\System32\GroupPolicy\

Les principaux noms de ces fichiers : ntuser.dat, UsrClass.dat, default, SAM, SECURITY, software, system …

⇨ Pour manipuler les registres sous Windows on utilise l'éditeur de registre avec la commande exécutable « regedit ».



La fénêtre qui s'ouvre alors est divisée en 2 partie, celle de gauche contient une arborescence de dossiers et à droite se trouve le contenu à affciher des registres.



Cinq branches principales regroupent les différents registres de Windows :

- **HKEY_CLASSES_ROOT** : cette branche contient tous les mappages d'association des fichiers pour supporter la focntion de glisser-déposer, l'information OLE, les raccourcis Windows et l'aspect cœur de l'interface utilisateur Windows.
- **HKEY_CURRENT_USER** : cette branche est liée à l'utilisateur actuellement en session sur la machine et contient les informations comme les noms d'ouverture de sessions, la configuration du bureau et les options du menu Démarrer.
- **HKEY_LOCAL_MACHINE** : cette branche contient les informations relatives à la machine, au type de matériels, de logiciels, et autres préférences.
- **HKEY_USERS** : cette branche contient les préférences individuelles de chaque utilisateur représenté par son SID.
- **HKEY_CURRENT_CONFIG** : liée à la branche HKEY_LOCAL_MACHINE correspondante à la configuration matérielle courante.

Chaque clé ou sous-clé du Registre peut contenir des données appelées "valeurs". Certaines rubriques contiennent des informations spécifiques à chaque utilisateur, d'autres concernent tous les utilisateurs de l'ordinateur. Une rubrique comprend trois parties : le nom de la valeur, le type de données de la valeur et la valeur elle-même.

Il existe trois types de valeurs: ***Chaîne***, ***Binaire***, et ***DWORD***. Leur utilisation dépend du contexte.

Chaque valeur de base de registre est établie sous la forme de l'un des cinq types de données principales suivantes :

REG_BINARY - Ce type contient la valeur sous forme d'une ligne de donnée binaire. La plupart des informations concernant les composants matériels sont stockées sous forme d'une donnée binaire, et peuvent être affichées à l'aide d'un éditeur de format hexadécimal.

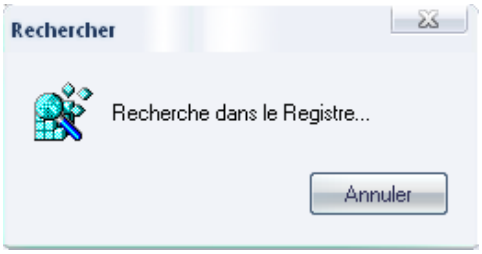
REG_DWORD - Ce type représente les données par un nombre de quatre octets et est couramment utilisé pour les valeurs booléennes, comme "0" pour désactivé et "1" pour activé ou inversement (c'est en fonction du nom de la valeur). De plus, beaucoup de paramètres de pilotes de périphériques et de services sont de ce type et peuvent être affichés avec *REGEDT32* au format binaire, hexadécimal et décimal, ou avec *REGEDIT* au format hexadécimal et décimal.

REG_EXPAND_SZ - Ce type est une chaîne de données extensible dont la chaîne contient une variable qui sera remplacée quand elle est appelée par une application. Par exemple, pour la valeur suivante, la chaîne "%SystemRoot%" sera remplacée par l'emplacement actuel du répertoire qui contient les fichiers système de Windows.

REG_MULTI_SZ - Ce type est une chaîne multiple, il est utilisé pour représenter les valeurs qui contiennent des valeurs de liste ou multiples, chaque entrée étant séparée par un caractère NULL.

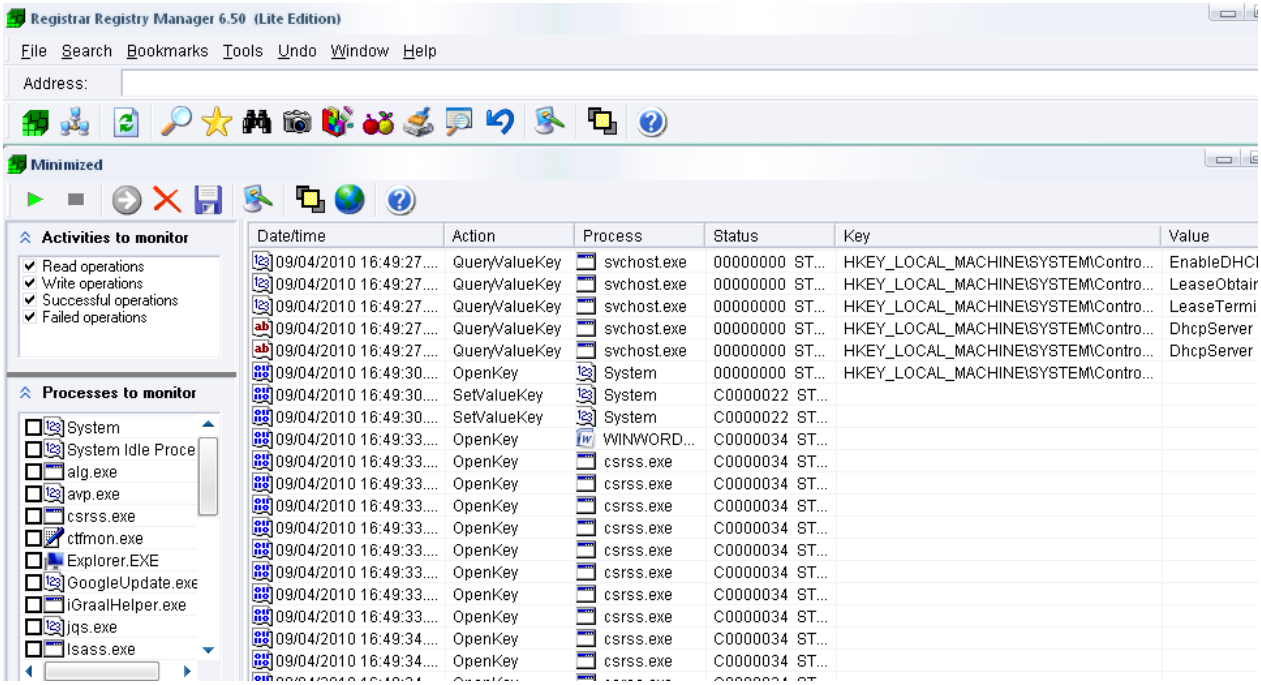
REG_SZ - Ce type est une chaîne standard, utilisé pour représenter des valeurs de texte contrôlables.

La fonction *Rechercher* sert beaucoup, principalement pour supprimer des valeurs ou clés de logiciels que l'on a désinstallés mais dont certaines clés subsistent.



- **Registrar Registry Manager :**

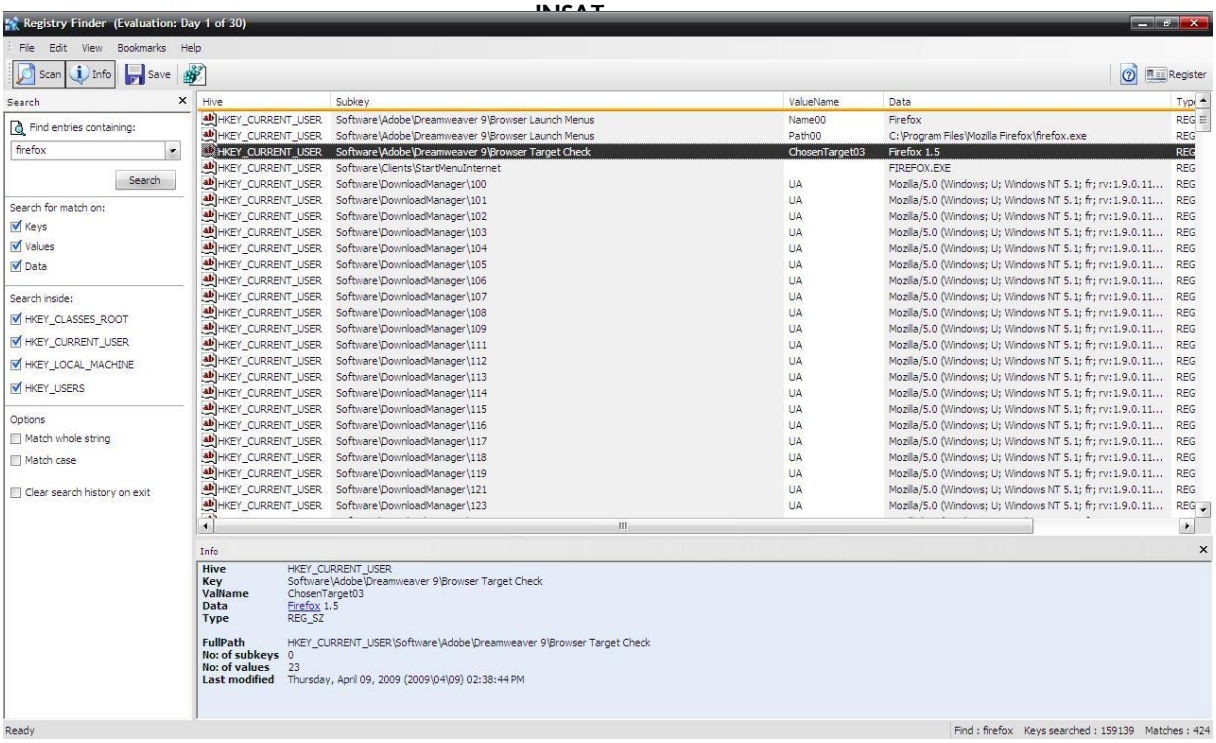
Ce logiciel permet de visualiser les activités du système : opérations de lecture, d'écriture, les opérations réussies et les opérations non réussies.



⇨ http://www.resplendence.com/registrar (evaluation version)

- **Registry Finder :**

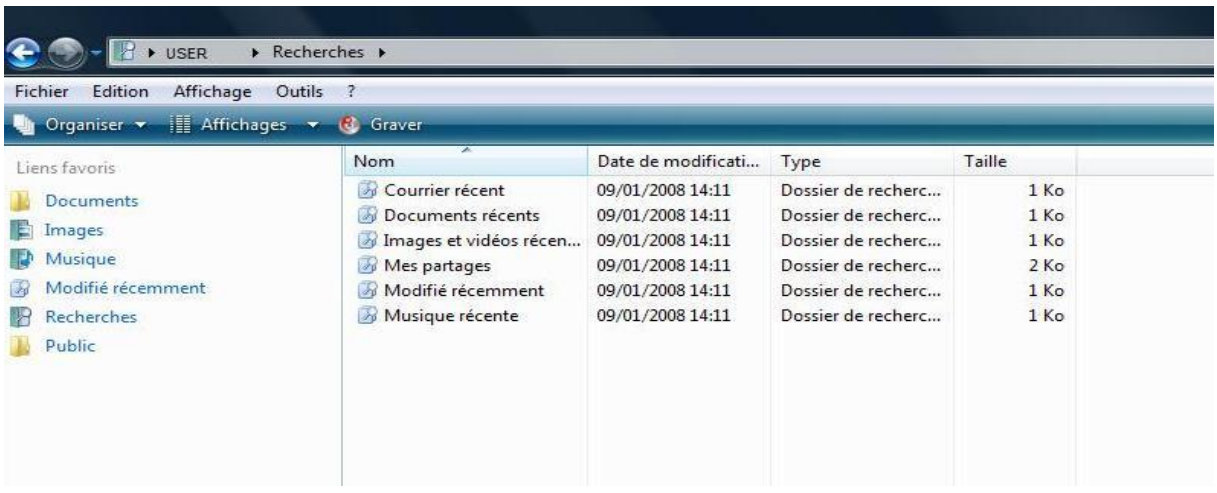
Permet la recherche et la localisation des variables par leur nom, et d'afficher leurs valeurs.



⇨ http://www.acelogix.com/regfinder.html (evaluation version)

1.5 – recherche et collecte de fichiers de divers types :

Cette section est relative à la recherche des fichiers de différents types dans les répertoires de la machine victime. Parmi les fichiers à rechercher : les images, vidéos, textes, logiciels, audio. La recherche sous Windows se fera avec l'utilitaire de recherche classique intégré dans le système :



Sous Linux par contre la recherche se fait par ligne de commande, il faut néanmoins avoir quelques critères de recherche en tête tel que la taille du fichier, son nom, son type, son extension, sa taille.

Plusieurs commandes existent notamment si le fichier est une commande à localiser :

whereis fichier

which fichier

type fichier

Autre commande, après avoir fait un "**updatedb**" en tant que "root" : **locate** fichier.

et puis la commande principale "**find**" (*voir man find pour plus de détails*) :

find / -name "fichier".

2. Environnement logiciel

* Ubuntu 9.10

* Windows Vista

* Virtual Box (Linux)

* VMware (Windows)

* Regedit

*Registrar Registry Manager (http://www.acelogix.com/regfinder.html evaluation version)

*Registry Finder (http://www.acelogix.com/regfinder.html evaluation version)

3. Installation et configuration

* Les outils utilisés sont tous sur Windows, leur installation se fait comme tout autre programme ou logiciel Windows.

* Virtual Box sous Linux est un package à installer depuis le gestionnaire de package Ubuntu.

4. Scénario :

Toute attaque sur une machine laissera surement des traces que ce soit dans les fichiers logs ou dans les registres.

La première étape à faire c'est d'accéder aux logs d'authentification pour avoir une idée sur l'utilisateur qui s'est connecté juste avant l'attaque. Une fois qu'on a eu le nom de cet utilisateur ou son ID, on pourra alors allez chercher du côté des logs les applications qu'il a lancé, ou les modifications qu'il a fait aux paramètres système.

Ce n'est pas tout, le nom de l'utilisateur nous permettra d'explorer la base des registres à la recherche de toute trace laissée par cet utilisateur lors de sa connexion.

Dans le cas où on n'a pas eu un nom particulier, on peut lancer notre collecte de données en nous basant sur les dates ainsi on pourra facilement afficher tous les utilisateurs, applications et modifications récentes grâce aux fonctions de recherche avancées dans Windows ou Linux. Ceci nous permettra de remonter à l'utilisateur à l'origine de l'attaque.

5. Conclusion :

Cet atelier est consacré à la collecte de données à partir d'un pc, il est relatif au « dead forensics » catégorie d'investigation qui traite les données gardées par la machine même après redémarrage du système. Nous avons traité au cours de cet atelier :

* la localisation et la collecte de données à partir des logs Linux

* la localisation et la collecte des logs sous Windows

* la localisation et la collecte d'informations des registres sous Windows

* la recherche de fichiers de types divers sous Windows et Linux.

Toutes les manipulations au cours de cet atelier ont été faites sur une image des disques de la machine victime qu'on a chargée dans une machine virtuelle à fin de recréer l'environnement de la machine victime et préserver les données originales.

⇨ L'étape suivante maintenant est l'analyse des données collectées.