

# Aide à l'utilisation de RtCA

<http://code.google.com/p/omnia-projets/>

V0.1 **DRAFT** – 19/11/2014

# Table des matières

1.Présentation.....	4
1.1.Introduction.....	4
1.2.Attention.....	4
1.3.Objectifs.....	4
1.4.Fonctionnalités.....	5
1.4.1.Outils intégrés.....	5
1.4.2.Collecte de données.....	6
1.5.Fichiers de l'application.....	7
1.5.1.Liste des fichiers.....	7
1.5.2.Fichiers de configuration.....	8
« RtCA.ini ».....	8
« tools.cfg ».....	8
1.6.Interfaces de l'application.....	10
1.6.1.Fenêtre principale.....	10
1.6.2.Fenêtre de configuration du proxy.....	12
1.6.3.Fenêtre de création de session.....	13
2.Extraction des données.....	14
2.1.Depuis une machine locale.....	14
2.1.1.Utilisation du GUI de RtCA.....	14
Extraction : Files and directories.....	15
Extraction : LNK Files.....	18
Extraction : Audit logs.....	19
Extraction : Disks.....	20
Extraction : Clipboard.....	21
Extraction : Local variables.....	21
Extraction : Scheduled tasks.....	22
Extraction : Process.....	23
Extraction : Prefetch.....	25
Extraction : Pipes.....	26
Extraction : Network.....	26
Extraction : Routing table.....	27
Extraction : DNS resolv.....	28
Extraction : ARP cache.....	29
Extraction : Shares.....	29
Extraction : Registry – Settings.....	30
Extraction : Registry – Service & Driver.....	31
Extraction : Registry – USB.....	32
Extraction : Registry – Software.....	33
Extraction : Registry – Update & Packages.....	34
Extraction : Registry – Start.....	35
Extraction : Registry – Users & groups.....	36
Extraction : Registry – UserAssist.....	37
Extraction : Registry – MRU & MUICache & history.....	38
Extraction : Registry – Shell bags.....	40
Extraction : Registry – Accounts & passwords.....	43
Extraction : Registry – All path & open command.....	44
Extraction : Security guide.....	45
Extraction : Registry – Deleted key.....	47

Extraction : Antivirus.....	47
Extraction : Firewall.....	48
Extraction : Firefox – History (local time).....	49
Extraction : Chrome – History (local time).....	49
Extraction : IE – History.....	50
Extraction : Android – History (local time).....	50
Extraction : LDAP AD datas.....	50
2.1.2.Utilisation de RtCA en ligne de commande.....	51
2.2.Depuis une machine à distance.....	54
2.2.1.Connexion à distance avec PsExec.....	54
2.3.Depuis des fichiers déjà extraits.....	54
3.Exploitation des données.....	55
3.1.Analyse rapide.....	55
3.2.Corrélation d'extractions.....	55
3.3.Cas pratique de recherche.....	55
3.3.1.Par séquence de démarrage de programme malveillant.....	55
3.3.2.Par l'analyse en live depuis la machine.....	55
3.3.3.Par attaque de type force brute sur un compte.....	55
3.3.4.Actions de malveillance d'un utilisateur.....	55
3.3.5.Identification de la source d'infection.....	55
4.Liste des outils intégrés.....	56
4.1.Copie de fichiers.....	56
4.2.DD.....	57
4.3.Process list.....	57
4.4.Registry explorer.....	59
4.5.Network live capture.....	61
4.6.Decode date.....	64
4.7.Hexa reader.....	64
4.8.SQLITE Editor.....	65
4.9.Global analyser.....	66
5.Et demain.....	67

# 1. Présentation

RtCA : Outil d'aide à l'extraction et l'exploitation d'évidences pour les investigations numériques. La dernière version de l'application et sa documentation peuvent être téléchargées ici : [https://drive.google.com/folderview?id=0Bw4s9\\_iTp9ESQUNzb29udldRSkk&usp=sharing](https://drive.google.com/folderview?id=0Bw4s9_iTp9ESQUNzb29udldRSkk&usp=sharing)

## 1.1. Introduction

RtCA (Read to Catch All) : est une boîte à outils permettant l'extraction et l'analyse d'évidences lors d'incidents de sécurité.

Codé en langage C Win32/Win64 avec Code::Blocks (<http://www.codeblocks.org/>) et compilé avec MinGW (<http://www.mingw.org/>).

Licence : GPLv3

Auteur : Nicolas Hanteville

Librairies utilisées :

- SQLite : <http://www.sqlite.org/>
- LiteZip : <http://www.codeproject.com/Articles/13370/LiteZip-and-LiteUnzip>
- Crypto libs : d3des, des, rc4, sha2, md5

Sources de RtCA : <https://code.google.com/p/omnia-projetcs/source/checkout>

## 1.2. Attention

Attention, RtCA est une boîte à outils open source sous licence GPLv3.

Son objectif n'est qu'à titre d'investigation, administration, tests d'intrusion et apprentissage seulement.

Vous l'utilisez à vos propres risques, aucun résultats n'est garantis par cet outil.

Cet outil ne contient aucun programme malveillant et n'effectue pas de sauvegarde des données extraites sur Internet.

De plus, cette documentation ainsi que l'outil sont soumis à la même licence. Il peuvent être modifiés et reproduits mais doivent être distribués sous la même licence.

Enfin en cas de questions, remarques particulières ou bugs, vous pouvez laisser des messages ou nous contacter au travers de la page <https://code.google.com/p/omnia-projetcs/>

## 1.3. Objectifs

L'objectif de RtCA est de permettre avec un seul exécutable l'extraction autonome des données aussi bien sur un système en cours de fonctionnement qu'éteint ou à distance, à partir d'une image voir directement par des fichiers de configuration.

Afin de faciliter au maximum l'extraction et l'exploitation il rassemble un grand nombre d'outils.

Il est compatible avec les versions 32/64bits Wine  $\geq 1.7$  (Unix, Linux et Mac), Microsoft Windows XP, 2003, Vista, 8, 8.1, 2008 et 2012.

L'extraction de données à partir de fichiers déjà extraits des systèmes Windows NT 4.x et 2000 est aussi supportée.

Le programme est portable, des versions 32bits et 64bits de l'exécutable sont disponibles.

## 1.4. Fonctionnalités

### 1.4.1. Outils intégrés

- **Copie de fichiers**
  - Sauvegarde des évidences dans un conteneur ZIP
  - Copie du fichier d'Active Directory NTDIS.DIT
  - Copie de fichiers protégés par le système (base de registre, fichiers de démarrage, etc.)
- **Capture d'écran**
  - Sauvegarde vers des fichiers BMP
- **Image de disque**
  - D'une partition, d'un disque, de la MBR
- **Explorateur de processus**
  - Liste des processus et informations associées
  - Liste des ports ouverts pour chaque processus et informations associées
  - Mise en évidence des processus cachés
  - Signature des binaires
  - Empreintes SHA256 des binaires
  - Fonctionnalités avancées :
    - Injection/suppression direct de DLL dans un processus exécuté
    - Extraction d'un processus en mémoire
    - Tuer un processus
    - Extraction des résultats en CSV/XML/HTML
    - Possibilité de vérifier les empreintes SHA256 sur VirusTotal
- **Explorateur de fichiers de registre brute**
  - Lecture des clés et valeurs de registre
  - ClassID, GUID des clés de registre
  - Récupération des clés et valeurs de registre effacées
  - Extraction des résultats en CSV/XML/HTML
- **Capture des flux réseau**
  - En RAW socket (sans driver, nécessite des privilèges d'administration)
  - Prise en compte en natif d'un grand nombre de protocole
  - Extraction des données par session possible
  - Filtre par type de flux, port et destination
  - Extraction des résultats en CSV/XML/HTML
- **Décodeur de date**
  - Décode simultanément les différents formats de date les plus utilisés
- **Explorateur hexadécimal**
  - Lecture de fichier en hexadécimal et en chaîne de caractère
  - Informations sur le fichier
  - Recherche de données
- **Éditeur SQLite**
  - Ouverture, affichage et modification du contenu des bases SQLite
  - Extraction des résultats en CSV/XML/HTML

- **Analyseur global**
  - Timeline d'une ou plusieurs session
  - Filtre possible par artefact, type, date
  - Mise en évidence des éléments critiques
  - Statistique sur les journaux
  - Extraction des résultats en CSV/XML/HTML

## 1.4.2. Collecte de données

**Plusieurs systèmes de collecte des données sont possibles :**

- En direct sur le système
- A partir de fichiers déjà extraits
- Par recherche automatique des fichiers sur une partition ou un répertoire
- Par sauvegarde des éléments dans un fichier ZIP

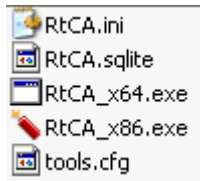
**Ce qui est collecté :**

- La liste des fichiers, répertoires
- Les journaux d'audit
- La liste des disques
- Le presse papier
- Les variables globales
- Les tâches planifiées
- La liste des processus
- Le prefetch
- Les pipes
- La configuration réseau
- La table de routage
- Le cache DNS
- Le cache ARP
- La liste des partages réseaux
- La base de registre :
  - La configuration système
  - La liste des services et drivers
  - Les supports amovibles
  - Les logiciels et patches de sécurité
  - Les programmes exécutés au démarrage
  - La liste des utilisateurs et groupes
  - Les clés UserAssist, MRU, MRUCache, historiques, Shell bags
  - Les mots de passes identifiés sur le système
  - Les paramètres d'exécution standards
  - L'application des guides de sécurisation
  - (seulement à partir des fichiers brute) Les clés de registre supprimées
- La configuration Antivirus
- Les règles de filtrage système
- L'historique de navigation pour Firefox, Chrome et IE
- Les historiques Android
- La configuration de l'Active Directory sous forme LDAP

## 1.5. Fichiers de l'application

### 1.5.1. Liste des fichiers

L'application se compose des fichiers suivants :



**RtCA.ini** : fichier de configuration permettant au programme de sauvegarder les préférences de l'utilisateur.

**RtCA.sqlite** : fichier de base de données au format SQLite v3, il contient la majorité des éléments de configuration et de langage. Lors de la génération d'extraction de configuration, les données sont sauvegardées dans ce fichier. En cas d'absence, il est créé au démarrage.

**RtCA\_x64.exe** : représente le binaire de l'application à exécuté pour les systèmes 64bits.

**RtCA\_x86.exe** : version 32bits de l'application fonctionne aussi en mode compatibilité sur les systèmes 64bits.

Le programme principal seul est suffisant, lors de la première exécution il génère automatiquement le fichier .ini et .sqlite.

**tools.cfg** : fichier de configuration facultatif permettant d'ajouter des menus dans l'application afin d'exploiter directement les données dans des programmes externes.

## 1.5.2. Fichiers de configuration

### « RtCA.ini »

Fichier de configuration par défaut, il permet de configurer un éventuel proxy pour la mise à jour de la BDD et la récupération des informations de fichiers sur le site Web VirusTotal.

#### Format du fichier :

```
[CONF]
DEFAULT_LANG_ID=1

[PROXY]
PROXY_URL=http://proxy:8080
PROXY_LOGIN=test
PROXY_PASSWORD=p# H
```

Le paramètre **DEFAULT\_LANG\_ID** correspond à l'identifiant de la langue de l'interface configuré. Initialement, seulement deux langues sont disponibles : Anglais (1) et Français (2).

Les paramètres dans la section **PROXY** sont utilisés pour la configuration du proxy. Le mot de passe s'il est sauvegardé, est enregistré de manière réversible avec un algorithme maison qui reste malgré tout assez simple. Il n'est donc pas conseillé de sauvegarder le mot de passe du proxy, mais de le renseigner à chaque démarrage de RtCA.

#### Note :

Il est conseillé de ne pas modifier ce fichier de configuration directement, mais d'utiliser l'interface graphique de RtCA.

### « tools.cfg »

Ce fichier de configuration est utilisé pour personnaliser les menus, comme par exemple dans la section **Fichiers**, pour ouvrir directement un fichier ou l'éditer avec un programme particulier.

#### Format du fichier :

```
#####
# Import tool configuration for RtCA #
#####
# Format : Operation;Title;Command;Parameter
#
##Operation : 00 : Open file
#              01 : Edit file
#              02 : Open file with extern program
#
##Title : Description in popup menu in RtCA
##Command : Use in 02 Operation, program to execute
##Parameter : Use in 02 Operation, parameter before file name

00;Open file;;
02;Open with NotePad++;notepad++.exe;
```

La configuration peut être modifiée directement en éditant le fichier.



La création d'une nouvelle entrée se fait suivant le format :

**Opération:Titre:programme:paramètre**

Il y a 3 types d'opérations:

00 : ouvrir un fichier

01 : éditer un fichier

02 : utiliser un programme externe

Le titre est utilisé dans le menu contextuel pour identifier l'action.

La commande est le programme à exécuter.

Si des paramètres sont nécessaires avant de préciser le chemin du fichier à ouvrir, il faut les spécifier ici.

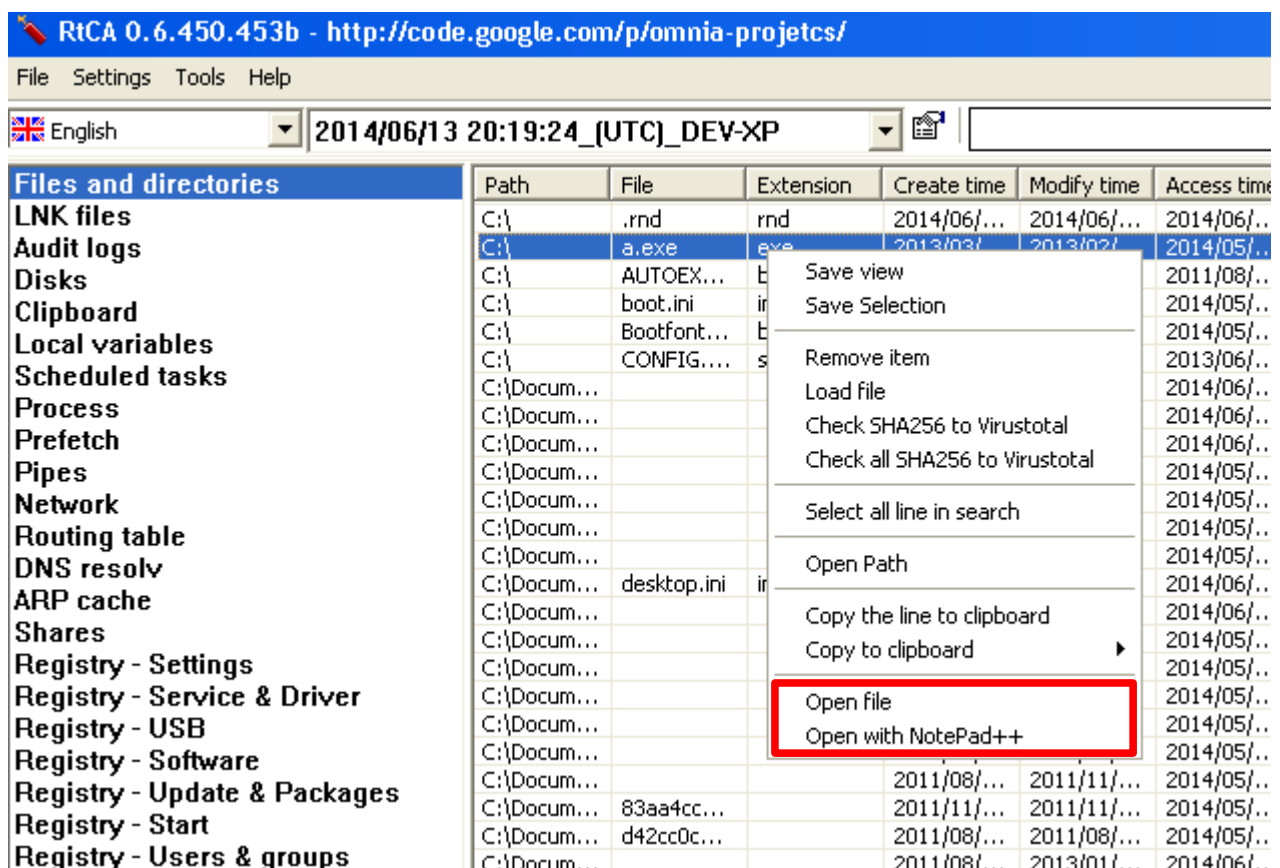
### Exemples :

```
00;Open file;;  
02;Open with NotePad++;notepad++.exe;
```

La ligne commençant par **00** permet d'ouvrir le fichier/répertoire en fonction de l'application par défaut sur le système.

La ligne commençant par **02** permet d'ouvrir le fichier avec l'application notepad++.

Ce menu s'affiche comme suit :

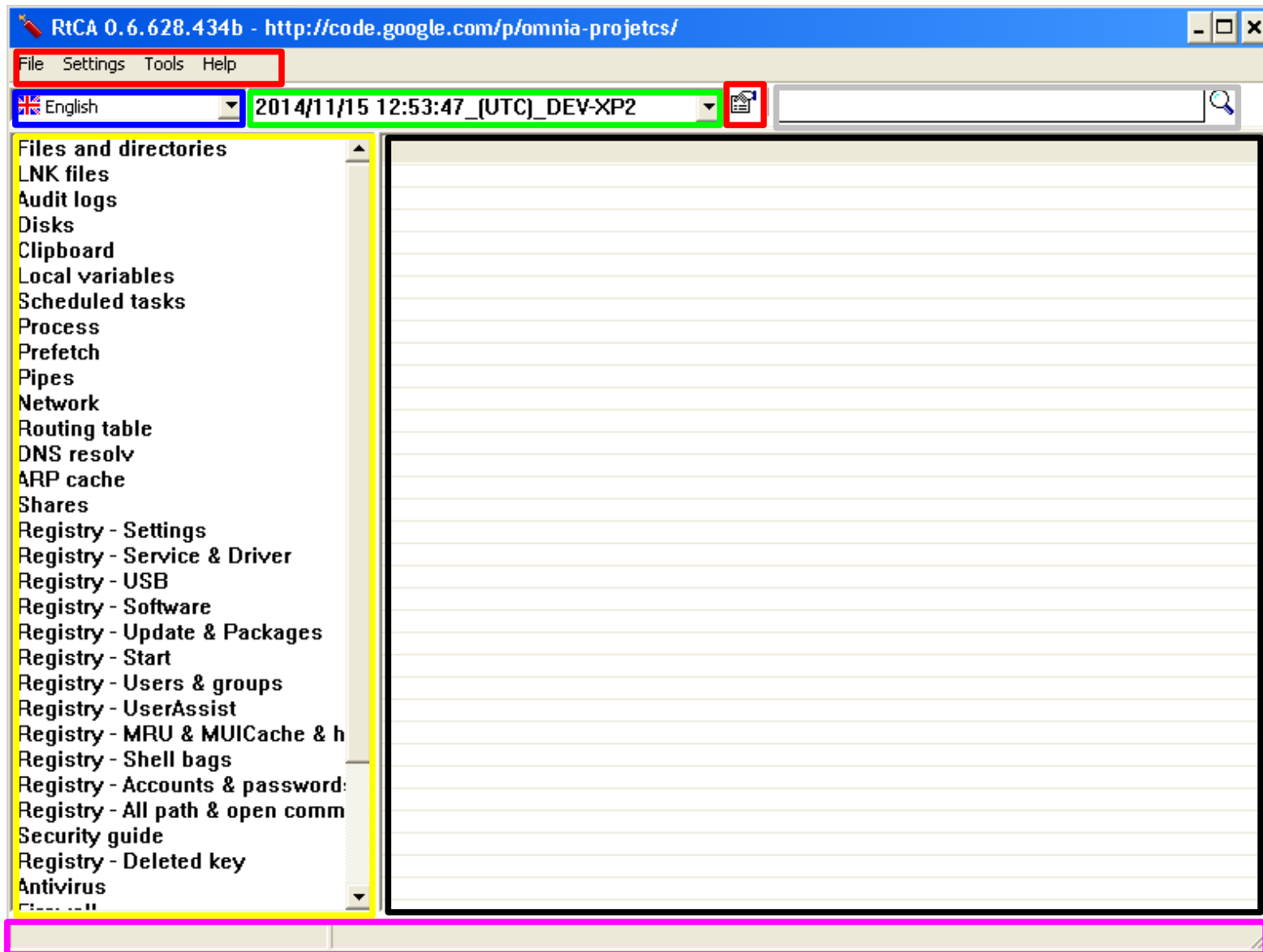


## 1.6. Interfaces de l'application

L'application comporte de multiples interfaces. Elles sont toutes présentées ici.

### 1.6.1. Fenêtre principale

Cette fenêtre est ouverte par défaut lors de l'exécution standard du programme (sans paramètre) :



- Menus, le menu secondaire (icône) permet de lancer une extraction.
- Sélection de la langue (par défaut Anglais/Français).
- Sélection de la session, permettant d'afficher les résultats de l'analyse.
- Module de recherche permettant des recherches dans les résultats de la section active.
- Liste des différentes sections d'extraction.
- Zone des résultats. En sélectionnant la liste des section, les résultats s'affichent ici.
- Zone de notification de l'état de chargement, messages d'information et d'erreur,

**Le menu de cette fenêtre se présente comme tel :**

- **File**
  - **New session** (Création d'une nouvelle session d'extraction)
  - **Refresh session list** (Pour mettre à jour la liste des session. Utile en cas d'utilisation du fichier de base de donnée simultanément par plusieurs binaires).
  - **Save all results** (Sauvegarde de tous les onglets pour la session courante au format définis avec pout nom de fichier RtCA[nom de session]\_section)
    - **CSV** : format CSV standard avec ; comme séparateur et les données entre ".  
Format compatible avec Microsoft Office et Libre Office
    - **HTML** : résultats sous forme de tableau
    - **XML** : format compatible avec Microsoft Office
  - **Delete current session**
  - **Delete all sessions**
  - **Load an other database** (Pour lire un fichier SQLite d'une autre session ou version de RtCA)
  - **Merge to database** (Pour fusionner une autre base SQLite avec la base actuelle)
  - **Save database** (Pour effectuer une sauvegarde de la base)
  - **Quit** (Pour fermer l'application)
- **Settings**
  - **Stay on top** (Permet de laisse la fenêtre de RtCA au premier plan)
  - **Search match case** (Pour activer lors des recherches, la recherche en vérifiant les minuscules et majuscules. Par défaut désactivé.)
  - **Desactivate the grid** (Pour enlever la grille au niveau de l'affichage des résultats)
  - **Screenshot** (Permet d'activer ou désactiver l'utilitaire d'imprime écran automatique en fichier BMP)
  - **Proxy** (Interface de configuration du proxy pour les mises à jour de la base et vérification VirusTotal)
  - **SQLite FULL SPEED** (Permet de désactivé les journaux de cache d'écriture pour le SQLite, rend l'extraction 100 fois plus rapide en moyenne. Activé par défaut!)
- **Tools**
  - **Copy all registry files** (Permet la copie de tous les fichiers brute de registre des ruches)
  - **Copy all audit files** (Permet la copie de tous les fichiers d'audit répertoriés sur le système, \*.evtx, \*.evt, \*.log...)
  - **Copy NTDIS.DIT(AD) file** (Copie du fichier ou est stocké toutes les informations de configuration d'un contrôleur de domaine. Ne fonctionne que sur un contrôleur de domaine)
  - **Copy specific file** (Système de copie permettant de passer outre les protections du système afin de copier un fichier)
  - **Save all local datas to ZIP file** (Extraction de l'ensemble des fichiers de données importants connus afin d'effectuer une investigation à l'exception des mémoires et des

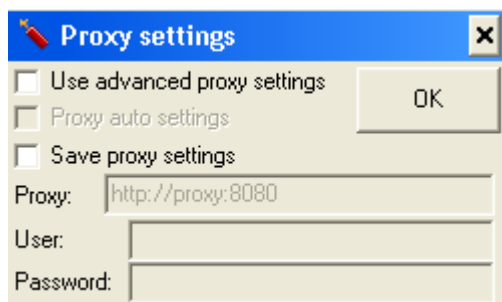
disques)

- **DD** (Permet l'image de disque, partition et de la MBR vers un fichier .RAW)
- **List of process** (Affiche l'outil de gestion des processus en live)
- **Registry explorer** (Affiche l'outil de traitement des fichiers brute de registre)
- **Network live capture** (Affiche l'outil de capture de flux réseau)
- **Decode date** (Affiche l'utilitaire de décodage de date)
- **Hexa reader** (Affiche l'utilitaire de lecture hexadécimal de fichier)
- **SQLITE ED** (Affiche l'éditeur SQLite)
- **Global analyser** (Affiche l'interface d'analyse globale des sessions)
- **Help**
  - **Update database** (Mettre à jour la base de donnée)\*
  - **Open RtCA home** (Aller sur la page Web de RtCA)
  - **About** (Afficher les informations de licence pour RtCA)

### 1.6.2. Fenêtre de configuration du proxy

Cette fenêtre permet la configuration du proxy pour aller sur Internet. Cette connexion n'est utilisée que pour deux choses :

- La mise à jour des tables de la base de donnée relative aux fichiers et entrée DNS malveillants
- Suite à la demande de l'utilisateur, la vérification sur VirusTotal des empreintes des fichiers. (Aucun fichier n'est envoyé, seule la vérification de la présence des empreintes dans la base de VirusTotal est effectuée).




Cette fenêtre permet d'activer la connexion à Internet depuis un proxy.

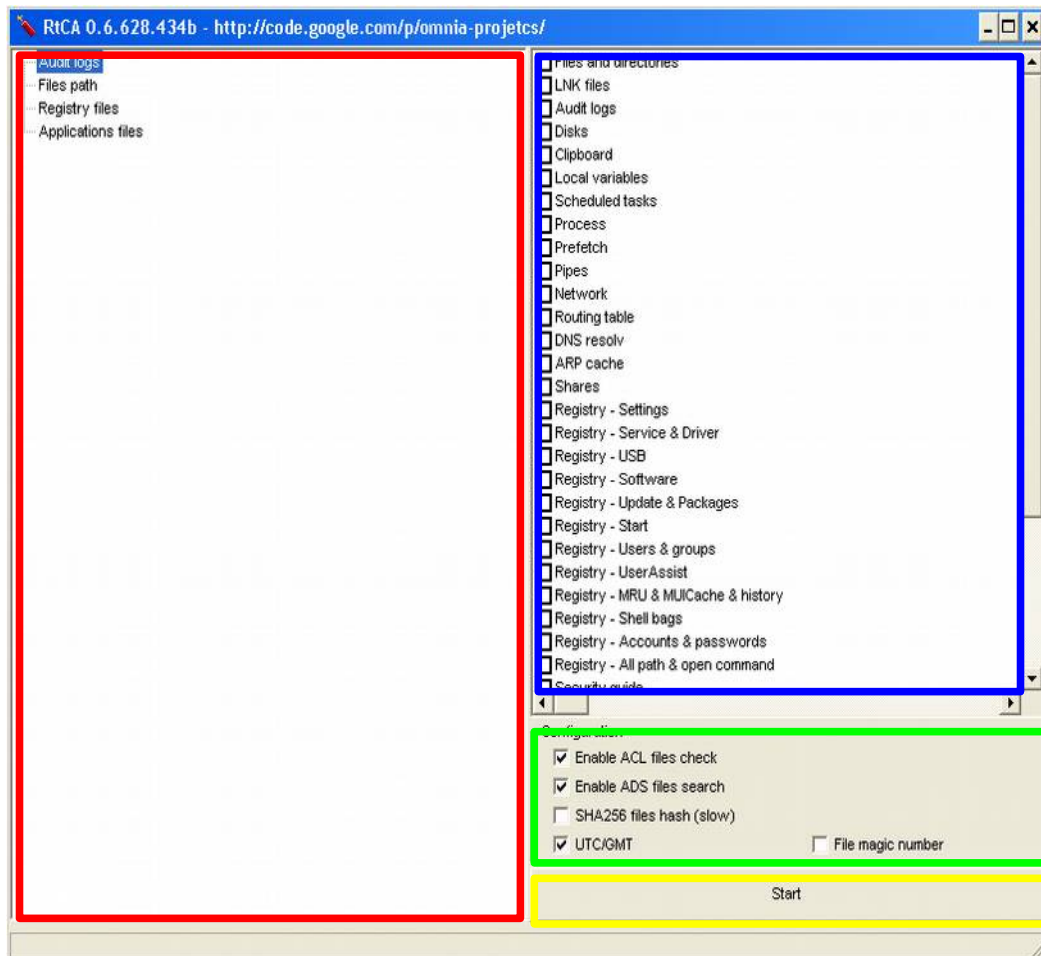
En cochant la case **Use advanced proxy settings**, vous pouvez spécifier :

- **Proxy auto settings** (permet d'utiliser le proxy et la chaîne d'authentification gérée par le système de manière transparente)
- L'utilisation d'un utilisateur et d'un mot de passe.
- **Save proxy settings** (Permet la sauvegarde des paramètres de configuration proxy. Cette option permet aussi la sauvegarde dans un algorithme maison réversible du mot de passe. Son utilisation n'est pas recommandée. En cas d'utilisation, les paramètres sont sauvegardés dans le fichier tools.cfg)

### 1.6.3. Fenêtre de création de session

Pour accéder à cette fenêtre, il faut aller dans le menu de la fenêtre principale et faire :

**File->New Session** ou cliquer sur le bouton 



Liste des fichiers à traiter si on choisi (optionnel).

Sélection de la liste des tests à effectuer (un clic droit permet de tout sélectionner/désélectionner)

Options des tests à activer ou non.

Démarrer l'extraction. Si aucun fichier n'est ajouté dans l'interface de gauche, l'extraction est faite localement.

**Dans l'interface de gauche pour la liste des fichiers à traiter, un menu existe :**

- **Add file/Add path** (permet l'ajout d'un fichier ou d'un chemin)
- **Item UP/DOWN** (permet de déplacer un fichier ou chemin ajouté dans une autre section)
- **Remove selected item/Clean all** (supprimer un élément ou vider la liste)
- **Open path** (Ouvrir le répertoire du fichier ou du chemin)
- **Auto search/Auto search (on path)** (Ajout automatique des éléments depuis le système actuel ou d'un chemin définis)
- **Import list / Export list** (permet d'importer ou sauvegarde la liste des fichiers et chemins)

## 2. Extraction des données

L'extraction de données est sauvegardées en base de données sous forme de session lié au nom de la machine ainsi qu'à la date et l'heure d'extraction des données.

Pour effectuer une extraction sur une machine, il est seulement nécessaire au démarrage du fichier RtCA\_x86.exe ou RtCA\_x64.exe. Ces fichiers correspondent au type de système d'exploitation à savoir 32bits (x86 compatible avec quasiment tous les systèmes d'exploitation Windows à partir de Windows XP à l'exception des serveurs en 64bits ne comportant pas le mode de compatibilité) ou 64bits (x64). Afin d'éviter des bugs potentiels liés au mode compatibilité et aux différents effets de virtualisation sous les systèmes 64bits, il est fortement recommandé d'utiliser la version 64bits sur ceux-ci.

Une fois l'extraction effectuée, il est important de bien penser à garder le fichier de base de données SQLite : RtCA.sqlite qui contient le résultat des tests.

Ce fichier peut atteindre une taille importante en fonction du type et du nombre de session extraites. Le fichier obtenu est compatible avec l'ensemble des version de RtCA x86 et x64 confondues.

### 2.1. Depuis une machine locale

Afin d'obtenir une maximum d'information il est primordial d'exécuter RtCA avec un maximum de privilèges (Administrateur). En cas de limitation, RtCA est capable d'obtenir la majorité des informations avec de moindres privilèges.

#### 2.1.1. Utilisation du GUI de RtCA

Afin d'effectuer une extraction des données de la machine locale, il est nécessaire de créer une nouvelle session. Pour ce faire, il faut aller dans le menu de la fenêtre principale et faire :

**File->New Session** ou cliquer sur le bouton 

Les différentes parties de l'interface sont explicitées dans le chapitre [#1.6.3.Fenêtre de création de session](#)

Dans la partie droite de l'interface, il est nécessaire de sélectionner les tests à effectuer.

Attention ! L'extraction des tests **Registry - Accounts & passwords** et des historiques des navigateurs risques d'extraire des comptes et mots de passes en clair ou de manière chiffrés.

Une fois les tests sélectionnés et exécutés en appuyant sur **Start**, les tests terminés sont automatiquement désélectionnés par l'application. Une fois tous les tests terminés, retour à la fenêtre principale ou la session a été ajoutée dans la liste des sessions. Pour consulter les résultats, il suffit maintenant de sélectionner la session et de naviguer dans les sections des tests désirés.

**Note :** Les tests peuvent être arrêté à tout moment en appuyant sur le bouton **Stop**. Les résultats déjà extraites étant exploitables.

Une fois les tests terminés, le nom de la session est créé de la manière suivante :

- Date et heure de démarrage des tests
- (UTC) Si l'option UTC/GMT a été sélectionné cet élément est ajouté
- Nom de la machine ou File si des fichiers ont été exploités directement

**Exemple :**

---

**2014/11/18 09:08:45\_[UTC]\_DEV-XP2**

## Extraction : Files and directories

Ce test a pour objectif d'énumérer avec un maximum d'information la liste des fichiers et répertoires présents sur le système. Il fait partie des tests les plus gourmand en accès disque et les plus long. En effet, la rapidité de ce test dépend entièrement des performances du disque ainsi que de la mise en cache (indexation) des fichiers.

**Plusieurs options sont disponibles et impactent ce test et sa rapidité :**

- Sur la fenêtre principal, dans le menu **Settings->SQLite FULL SPEED**, si cette option n'est pas cochée, le temps d'extraction est multiplié par dix.
- Sur le fenêtre de création de session, dans la partie **Configuration** :
  - **Enable ACL files check** : active l'extraction des droits d'accès sur les fichiers et dossiers (impact peu les performances).
  - **Enable ADS files search** : active l'extraction des Alternatives Data Stream qui permettent de cacher des fichiers dans d'autres fichiers sur les partitions NTFS (impact moyennement les performances).
  - **SHA256 files hash (slow)** : active la création des empreintes SHA256 pour tous les fichiers de taille supérieur à 50mo. (Impact beaucoup les performances).
  - **UTC/GMT** : les dates extraites ne sont pas générées à la date actuelle du système mais par rapport à l'UTC (GMT/UTC+0). Il est donc nécessaire de faire une conversion des dates pour l'analyse. (N'impacte pas les performance).
  - **File magic number** : extraction des 16 premiers octets de chaque fichier et vérification du type associé par défaut (impact moyennement les performances).

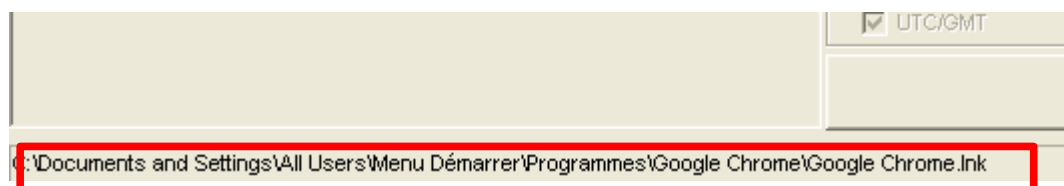
**L'extraction des informations peut être faite de plusieurs manières :**

- L'extraction par défaut, on laisse RtCA vérifier l'ensemble des disques sur physique de l'ordinateur.
- On indique dans la partie de gauche de l'interface un chemin. Permettant l'analyse par exemple d'un partage réseau ou d'un support de stockage externe (clé USB, CD/DVD, disque, etc.).
- On utilise la recherche automatique pour analyser l'ensemble des lecteurs identifiés (disques, partages, clés USB, CD/DVD, etc.).

**Attention !** En cas de sélection d'un répertoire spécifique, les tests sélectionnés à gauche porteront exclusivement sur les éléments/fichiers fournis à droite de l'interface. Ainsi aucune extraction d'artefacts locaux autre que les éléments ajoutés ne seront traités.

Enfin, L'ajout d'un élément dans la partie de gauche active automatiquement les tests compatibles.

**Note :** Le suivi de l'extraction pour ce test est fournis en bas de la fenêtre, le fichier en cours de traitement y étant indiqué.



### Les données extraites à partir de ce test sont :

- **Path** (Répertoire du fichier ou répertoire analysé)
- **File** (Fichier analysé)
- **Extension** (Extension du fichier)
- **Create time** (Date de création au format local ou UTC)
- **Modify time** (Date de dernière modification au format local ou UTC)
- **Access time** (Date de dernière accès au format local ou UTC) **Attention, l'utilisation en live de RtCA modifie cette date lors de son accès au fichier.**
- **Size** (Taille du fichier)
- **Owner** (Nom et domaine du propriétaire)
- **RID** (RID du propriétaire)
- **SID** (SID du propriétaire)
- **ACL** (Access List du fichier/répertoire analysé)
- **Hidden** (Indique si le fichier est un fichier caché)
- **System** (Indique si le fichier système)
- **Archive** (Indique si le fichier est compressé par le système)
- **Encrypted** (Indique si le fichier est chiffré par le système)
- **Temporary** (Indique si ce fichier est un fichier temporaire)
- **ADS** (Si l'option est cochée, affiche les fichiers cachés dans le fichier, pour les partitions en NTFS)
- **SHA256** (Si l'option est cochée et que la taille du fichier est <50mo, indique l'empreinte SHA256 du fichier)
- **VirusTotal** (Désactivé par défaut, pour obtenir cette information, il est nécessaire de lancer la fonctionnalité après extraction avec un accès Internet)
- **Description** (Si l'option est cochée, description du type de fichier en fonction du Magic Number)

### Limitations des résultats :

- Si le système est analysé en live :
  - La date d'accès des fichiers est modifiée lors de l'accès par RtCA
  - Les fichiers masqués par un *hook* global sur le système ne sont pas visibles
- Si le système est analysé après :
  - Les nom des propriétaires, groupes et domaines peuvent ne pas être résolus (seul les RID et SID sont visibles)



## Exemple d'extraction obtenu pour un fichier avec toutes les options activées :

```
Files and directories
-----

[Path]
C:\

[File]
a.exe

[Extension]
exe

[Create time]
2013/03/30 13:38:39

[Modify time]
2013/02/10 15:40:04

[Access time]
2014/11/18 08:05:55

[Size]
1363456o (1Mo)

[Owner]
DEV-XP2\nico

[RID]
01003

[SID]
S-1-5-21-1606980848-507921405-1957994488-1003

[ACL]
rwx (ALLOWED) BUILTIN\Administrateurs S-1-5-32-544
rwx (ALLOWED) AUTORITE NT\SYSTEM S-1-5-18
rwx (ALLOWED) DEV-XP2\nico S-1-5-21-1606980848-507921405-1957994488-1003
rwx (ALLOWED) BUILTIN\Utilisateurs S-1-5-32-545

[Archive]
A

[SHA256]
6564ecc0afab6d3f169fcf9abeaa97a8805f0ee7474b493354d9129c97c875e0

[VirusTotal]
Unknow Ratio : (Last analysis : NULL) Url :
https://www.virustotal.com/file/6564ecc0afab6d3f169fcf9abeaa97a8805f0ee7474b493354d9129c97c875e0/a
nalysis/

[Description]
Executable (COM, DLL, DRV, EXE, PIF, QTS, QTX, SYS)
```

## Extraction : LNK Files

Ce test dépend de l'activation du test **Files and directories**. S'il n'est pas activé aucun résultat ne pourra être obtenu.

L'objectif de ce test est d'extraire les informations contenues dans les fichiers de raccourcis LNK. Le temps d'extraction de ces informations est insignifiant au regard des autres tests.

### Plusieurs options impactant ce test sont disponibles lors du lancement des tests :

- Sur la fenêtre principal, dans le menu **Settings->SQLite FULL SPEED**, si cette option n'est pas cochée, le temps d'extraction est multiplié par dix.
- Sur le fenêtre de création de session, dans la partie **Configuration** :
  - **UTC/GMT** : les dates extraites ne sont pas générées à la date actuelle du système mais par rapport à l'UTC (GMT/UTC+0). Il est donc nécessaire de faire une conversion des dates pour l'analyse. (N'impacte pas les performance).

**Note** : L'extraction des données fonctionne sur un grand nombre de format de fichiers LNK mais certains fichiers mal formés peuvent ne rien donner.

### Les données extraites à partir de ce test sont :

- **File** (Fichier analysé)
- **Create time** (Date de création au format local ou UTC du raccourcis, sans aucun lien avec la date de création du fichier disponible dans la partie **Files dans directories**.)
- **Last access time** (Date de dernier utilisation du raccourcis au format local ou UTC du raccourcis, sans aucun lien avec la date de création du fichier disponible dans la partie **Files dans directories**.)\*
- **Modify time** (Date de la dernière modification du raccourcis au format local ou UTC du raccourcis, sans aucun lien avec la date de création du fichier disponible dans la partie **Files dans directories**.)
- **Local path** (utilisé pour spécifier le chemin local dans le cas par exemple de fichier présent sur un lecteur réseau)
- **Link** (Fichier exécuté lors du double clic sur le raccourcis)

### Exemple d'extraction obtenu pour un raccourcis vers un fichier sur un partage réseau :

```
LNK files
-----

[File]
C:\Documents and Settings\All Users\Menu Démarrer\MinGW Installation Manager.lnk

[Create time]
2013/12/07 09:41:05

[Last access time]
2013/10/04 20:20:58

[Modify time]
2013/10/04 20:20:58

[Local path]
\\VBOXSVR\partage_vm

[Link]
Z:\MinGW2\libexec\mingw-get\guimain.exe
```

## **Extraction : Audit logs**

Ce test permet l'extraction des entrées des journaux d'audit.

### **Les formats de journaux d'audit supportés sont :**

- Tous les journaux d'audit (capture live) sur les systèmes Windows
- Les fichiers EVT (prise en charge total) pour les systèmes Windows < Vista
- Les fichiers EVTX (prise en charge partielle) pour les systèmes Windows à partir de Vista
- Les journaux d'audit au format txt/log de type Linux et Windows

Les données extraites ne sont pas aussi complète que sur un système Windows, et les textes extraites sont de la langue du système local depuis lequel ils ont été extraites.

### **Les données extraites à partir de ce test sont :**

- **Event** (Source de l'événement fichier ou nom)
- **Record number** (numéro d'enregistrement unique : indexe)
- **Send date** (Date et heure d'émission de l'enregistrement au format local ou UTC)
- **Write date** (Date et heure d'écriture de l'enregistrement au format local ou UTC)
- **Source** (Émetteur de l'enregistrement)
- **Event ID** (Identifiant du type d'ID)
- **Description** (Champs d'aide dépendant de la langue de l'interface de RtCA)
- **State** (État d'importance de l'enregistrement)
- **User** (Utilisateur et domaine associé ayant émis l'enregistrement)
- **RID** (RID de l'émetteur)
- **SID** (SID de l'émetteur)
- **Datas** (Données complémentaires de précision sur l'enregistrement)
- **Critical** (Données devant être analysés en priorité et pouvant être la source de problèmes sur le systèmes ou d'attaques)

### **Limitations des résultats :**

- Si le système est analysé en live :
  - Les descriptions d'enregistrement sont dans la langue local du système
- Si le système est analysé après :
  - Les nom des propriétaires, groupes et domaines peuvent ne pas être résolus (seul les RID et SID sont visibles)
  - Impossibilité de résoudre les informations de services (elles dépendent du registre et des DLL du système analysé)
  - Certains éléments des enregistrement peuvent être omis

## Exemple d'extraction à partir d'un système Windows XP SP3 :

```
Audit logs
-----

[Event]
Application

[Record number]
00000432

[Send date]
2014/09/15 11:19:55

[Write date]
2014/09/15 11:19:55

[Source]
LoadPerf

[Event ID]
00001000

[Description]
Performance counters for the service installed successfully

[State]
INFORMATION

[Datas]
Les compteurs de performances pour le service WmiApRpl (WmiApRpl) ont été chargés.
Les données d'enregistrement contiennent les nouvelles valeurs d'index
assignées à ce service.
```

### **Extraction : Disks**

Ce test permet d'obtenir des information sur la liste des partitions/lecteurs reconnus par Windows.

#### **Les données extraites à partir de ce test sont :**

- **Drive** (Lettre du lecteur)
- **Type** (Type de lecteur : CD, partage réseau, partition, etc.)
- **File system** (Système de fichier)
- **Name** (Nom du lecteur)
- **Free space** (Espace disponible de stockage sur ce lecteur)
- **Global space** (Taille total du lecteur)

#### **Exemple d'extraction :**

D..	Type	File system	Name	Free space	Global space
C:\	DRIVE_FIXED	NTFS		0.75 Go	3.99 Go
D:\	DRIVE_CDROM				
Z:\	DRIVE_REMOTE	VBoxShared...	VBOX_partage_vm	225.01 Go	407.93 Go

## Extraction : Clipboard

Ce test permet d'obtenir le presse papier de chaque utilisateur connecté. Cet élément ne peut être capturé par RtCA que lors d'extraction en live sur le système.

### Les données extraites à partir de ce test sont :

- **Format** (Type de format du presse papier)
- **Code** (Identifiant du type de format)
- **Description** (Source du type de données)
- **Datas**
- **User** (Propriétaire des données)

### Exemple d'extraction :

Format	Code	Description	Datas	U...
UNKNOWN	49161	DataObject	EA056200 ..b.□□	nico
UNKNOWN	49298	Rich Text Format	{\rtf1\ansi\ansicpg1252\deff0\deflang1036-{\fonttbl{\f0\fnill\fcharset0 ...	nico
UNKNOWN	49399	Rich Text Format Without Objects	7B5C727466315C616E73695C616E7369 {\rtf1\ansi\ansi□□63706731...	nico
UNKNOWN	49397	RTF As Text	7B5C727466315C616E73695C616E7369 {\rtf1\ansi\ansi□□63706731...	nico
UNKNOWN	49171	Ole Private Data	00000000F80000000100000005000000 .....□□0000000000...	nico

## Extraction : Local variables

Les variables locales sont utilisées pour les programmes et le système pour l'exécution d'application ou le chargement de ressources. En cas de corruption, un programme malveillant peut modifier ces variables afin de s'injecter dans les processus.

Les variables sont stockées en mémoire lors de la session courante de l'utilisateur ou dans la base de registre en hors ligne.

### Les données extraites à partir de ce test sont :

- **User/File** (Utilisateur propriétaire de la session ou fichier source de registre)
- **Source** (Clé de registre en cas de chargement par fichier)
- **Var** (Variable et sa valeur)

### Exemple d'extraction à partir d'un système Windows XP SP3 :

Local variables
-----
[User/File]
nico
[Var]
ALLUSERSPROFILE=C:\Documents and Settings\All Users

## Extraction : Scheduled tasks

Les programmes malveillants ayant pour objectif de se répandre et d'être pérennes, ils cherchent des moyens afin de pouvoir être démarrés à chaque lancement de machine ou de session utilisateur.

Les tâches planifiées sont donc une source d'injection potentiel à vérifier. Ces fichiers peuvent être analysés hors ligne. Ce test permet l'extraction des informations comprises dans les fichiers de tâches planifiés stockés sur le système dans : C:\WINDOWS\Tasks\\*.job

Les données extraites à partir de ce test sont :

- **ID** (Fichier source de tâche planifiée)
- **Type** (État et périodicité de démarrage de la tâche)
- **Command** (Commande exécutée à chaque lancement de la tâche)
- **Next run** (Prochain démarrage, si cet élément est configuré, il est > 1999/01/01 00:00:00)
- **Job date creation** (Au format local ou UTC, cette donnée peut être différente des attributs du fichier job.)
- **Last job update** (Au format local ou UTC, cette donnée peut être différente des attributs du fichier job.)
- **Last job access** (Au format local ou UTC, cette donnée peut être différente des attributs du fichier job.)
- **Add from** (Créateur de la tâche)
- **Strings** (Informations sur la machine, la tâche, etc.)

Exemple d'extraction à partir d'un système Windows XP SP3 :

```
Scheduled tasks
-----

[Id]
C:\WINDOWS\Tasks\GoogleUpdateTaskMachineUA.job

[Type]
ENABLE,TASK_FLAG_START_ONLY_IF_IDLE

[Command]
C:\Program Files\Google\Update\GoogleUpdate.exe

[Next run]
2014/06/29 14:02:14

[Job date creation]
2014/05/23 20:52:52

[Last job update]
2014/11/18 10:02:00

[Last job access]
2014/11/18 10:02:00

[Add from]
nico

[Strings (computer name, path, description)]
/ua /installsource scheduler, Permet de maintenir votre logiciel Google à jour. Si cette tâche est désactivée ou interrompue, votre logiciel Google ne sera plus mis à jour. Toute faille de sécurité susceptible d'apparaître ne pourrait alors pas être réparée et certaines fonctionnalités
```

## **Extraction : Process**

La liste des processus courant peut être extrait ici. RtCA utilise plusieurs type de routines afin de déterminer si un programme est protégé par un hook sur les tables de processus et ainsi afficher les processus cachés. Un processus caché étant par défaut potentiellement malveillant.

L'extraction de ce test n'est possible avec RtCA qu'en live.

Ce test fait partis des tests diminuant les performances lors de l'extraction, en raison des processus de détection de programmes cachés.

### **Les données extraites à partir de ce test sont :**

- **Process** (Le nom du processus :fichier binaire)
- **PID** (Identifiant unique d'exécution du processus)
- **Path** (Chemin complet du processus)
- **Command** (La ligne d'exécution complète du processus)
- **Owner** (Nom de l'utilisateur ayant exécuté le programme)
- **RID** (RID de l'utilisateur exécutant le programme)
- **SID** (SID complet du propriétaire ayant exécuter le programme)
- **Start Date** (Au format local ou UTC, date et heure à laquelle le programme a été lancé)
- **Protocol** (Protocole réseau des ports ouverts sur ce processus : UDP ou TCP)
- **IP src** (IP source de la carte réseau ayant ouvert le port)
- **Port src** (Port source ouvert en local sur la machine)
- **IP dst** (IP de destination connectée au port source du processus si TCP)
- **Port dst** (Port de destination connecté au port source du processus si TCP)
- **State** (État des ports ouverts)
- **Hidden** (Utilisation du scanne des tables des processus afin d'identifier les processus masqués par des drivers ou routines. Quand le processus est détecté, un X est présent dans cette colonne)
- **Parent process** (Chemin du processus ayant exécuter le processus actuel)
- **Parent PID** (PPID : identifiant unique d'exécution du processus ayant exécuter le processus actuel)
- **sha256** (L'empreinte du binaire en SHA256 si le fichier est <50mo. Un module lors de l'exploitation permet de vérifier la présence de cette signature sur le site VirusTotal)
- **Signed** (État de vérification de la signature du binaire, Si la signature est bonne, **WINTRUST\_ACTION\_GENERIC\_VERIFY\_V2 OK** est affiché)

Pour une analyse en live, l'outil **Process list** permet une interaction avec les processus : [#4.3.Process list|outline](#)

## Exemple d'extraction à partir d'un système Windows XP SP3 :

```
Process
-----

[Process]
svchost.exe

[Pid]
01092

[Path]
C:\WINDOWS\system32\svchost.exe

[Command]
C:\WINDOWS\system32\svchost.exe -k netsvcs

[Owner]
BUILTIN\Administrateurs

[SID]
S-1-5-32-544

[Start date]
2014/11/13 14:42:51

[Protocol]
UDP

[IP src]
10.0.2.15:dev-xp2

[Port src]
123

[IP dst]
*.*:dev-xp2

[State]
LISTENING

[Parent process]
C:\WINDOWS\system32\services.exe

[Parent PID]
00656

[sha256]
6234155d6c02c67689744d21380b17db5fe395bc8622c71b046e40ca1767785a

[Signed]
File not signed!
```



## Extraction : Prefetch

Les fichiers de prefetch sont utilisés sur les environnement Microsoft Windows afin d'optimiser les programmes exécutés. Ils sont situés dans C:\WINDOWS\Prefetch\\*.pf

Pour chaque programme exécuté, un fichier prefetch est créé. Pour chaque exécution de ce même programme, le fichier prefetch est mis à jour. En cas d'un même exécutable à plusieurs emplacements, un fichier prefetch est créé pour chaque emplacement.

Ces fichiers peuvent être analysés hors ligne.

### Les données extraites à partir de ce test sont :

- **File** (Fichier prefetch)
- **Path** (Chemin du fichier exécuté)
- **Create time** (Au format local ou UTC, cette donnée peut être différente des attributs du fichier pf.)
- **Modify time** (Au format local ou UTC, cette donnée peut être différente des attributs du fichier pf.)
- **Access time** (Au format local ou UTC, cette donnée peut être différente des attributs du fichier pf.)
- **Execution counter** (Nombre d'exécution du fichier)
- **Last run** (Au format local ou UTC, cette donnée peut être différente des attributs du fichier pf.)
- **Depend** (Liste des DLL chargées par le programme à son exécution)

### Exemple d'extraction à partir d'un système Windows XP SP3 :

```
Prefetch
-----

[File]
C:\WINDOWS\Prefetch\FIREFOX.EXE-28641590.pf

[Path]
\device\harddiskvolume1\program files\mozilla firefox\firefox.exe

[Create time]
2011/08/08 17:57:31

[Modify time]
2014/06/13 17:43:21

[Access time]
2014/11/17 12:27:17

[Execution counter]
00000312

[Last run]
2014/06/13 17:43:21

[Depend]
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\NTDLL.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\KERNEL32.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\UNICODE.NLS
...
```

## **Extraction : Pipes**

Les tunnels de communication I/O (pipes) servent de moyen communication entre plusieurs processus et peuvent permettre d'identifier des programmes malveillant les utilisant.

L'extraction de ces information ne peut être fait avec RtCA qu'en live.

**Les données extraites à partir de ce test sont :**

- **Pipe** (Nom du pipe)
- **Owner** (Créateur du pipe)
- **RID** (RID du créateur du pipe)
- **SID** (SID du créateur du pipe)

**Exemple d'extraction à partir d'un système Windows XP SP3 :**

```
Pipes
-----

[Pipe]
\\.\pipe\winlogonrpc

[Owner]
BUILTIN\Administrateurs

[SID]
S-1-5-32-544
```

## **Extraction : Network**

Configuration réseau extraite à partir de la base de registre. Ces éléments peuvent être obtenus à partir de la ruche SYSTEM du registre hors ligne et en live.

**Les données extraites à partir de ce test sont :**

- **Source** (Clé de registre ou chemin du fichier de registre SYSTEM)
- **Card** (Identifiant système de la carte réseau)
- **Description** (Nom visible pour les utilisateurs de la carte)
- **GUID** (IDentifiant système associé à la carte)
- **IP** (Adresse IP de la carte)
- **Netmask** (Masque réseau de communication IP associé à l'IP)
- **Gateway** (Passerelle réseau)
- **DNS** (Liste des serveurs DNS pour la carte)
- **Domain** (Domain associé à la carte)
- **DHCP** (Si X : les informations IP, Netmask, Gateway et DNS ont été fournies par un serveur DHCP)
- **DHCP server** (Serveur ayant fournis les informations IP précédente pour la carte si activé)

- **WiFi** (Configuration WiFi pour les systèmes < Vista)
- **Last update** (Date de dernière modification des clés de registre associés aux informations de la carte. Cette date dépend de la configuration UTC ou local time choisi)

### Exemple d'extraction à partir d'un système Windows XP SP3 :

```
PNetwork
-----

[Source]
HKEY_LOCAL_MACHINE\SYSTEM

[Card]
pci\ven_1022&dev_2000

[Description]
Carte AMD PCNET Family Ethernet PCI

[GUID]
{41D54AD0-EDB5-4EA7-8EB6-6CB8D81D6BC6}

[IP]
10.0.2.15

[Netmask]
255.255.255.0

[Gateway]
10.0.2.2

[DNS]
10.16.8.254 212.27.40.240

[DHCP]
X

[DHCP server]
10.0.2.2

[Last update]
2014/11/18 05:57:54
```

### **Extraction : Routing table**

Ce test d'extraction de la table de routage ne peut être exécuté avec RtCA qu'en live, ces éléments n'étant pas sauvegardés..

Il a pour objectif de vérifier si des routes d'interception n'ont pas été mise en place ou tout mauvaise configuration au niveau des routes réseau.

### Les données extraites à partir de ce test sont :

- **Destination**
- **Netmask**
- **Gateway**
- **Metric** (Correspond à la priorité de la route)

### Exemple d'extraction obtenue :

Destination	Netmask	Gateway	Metric
0.0.0.0	0.0.0.0	10.0.2.2	20
10.0.2.0	255.255.255.0	10.0.2.15	20
10.0.2.15	255.255.255.255	127.0.0.1	20
10.255.255.255	255.255.255.255	10.0.2.15	20
127.0.0.0	255.0.0.0	127.0.0.1	1
224.0.0.0	240.0.0.0	10.0.2.15	20
255.255.255.255	255.255.255.255	10.0.2.15	1

### Extraction : DNS resolv

Ce test représente le cache de résolution des DNS en IP utilisés par le système lors de l'extraction et n'ayant pas expiré. Ce cache est en partie statique a travers du fichier host (C:\WINDOWS\system32\drivers\etc\hosts) et dynamique en live. Les informations ne peuvent donc être obtenu qu'en live.

Afin de vérifier si le nom de domaine résolu n'est pas une source malveillante, la table `malware_dns_list` contient l'ensemble des domaines considérés comme dangereux depuis les listes :

- [https://easylist-downloads.adblockplus.org/malwaredomains\\_full.txt](https://easylist-downloads.adblockplus.org/malwaredomains_full.txt)
- <http://malc0de.com/bl/BOOT>
- <http://www.malwaredomainlist.com/hostslist/hosts.txt>

Ces listes contenues en base de données peuvent être mise à jour avec un accès Internet à partir de la fenêtre principale et du menu **Help->Update database** ou manuellement par l'utilisateur en ajoutant des enregistrement dans la table `malware_dns_list` de la base SQLite (Les mise à jour de la base ne supprimant pas les entrées).

### Les données extraites à partir de ce test sont :

- **File** (Spécifie le fichier host utilisé)
- **Ip** (IP obtenue après résolution du nom DNS)
- **Name** (Nom DNS résolu)
- **Malware check** (En cas de domaine considéré comme malveillant, la liste de référence utilisé est spécifiée ici)
- **Last file update/Duration (in second)** (Date de dernière modification du fichier ou temps avant expiration de l'entrée du cache en seconde)

### Exemple d'extraction :

File	Ip	Name	Malware check	Last file update/Dur...
C:\WINDOWS\system...	127.0.0.1	localhost		2002/08/30 12:00:00
	200.151.157.1	www.virustotal.com		1425 (s)
	74.125.34.46	www.virustotal.com		1425 (s)
	127.0.0.1	localhost		447498 (s)

### **Extraction : ARP cache**

Le cache ARP peut permettre de gagner du temps lors de la recherche d'équipement lié à la communication avec la machine de test. En effet, en cas d'échange avec un autre élément réseau, le cache ARP local est mis à jour.

**Les données extraites à partir de ce test sont :**

- **Ip**
- **MAC** (Adresse MAC correspondante à l'IP ou à la passerelle permettant le dialogue avec l'IP)
- **Type** (Type d'entrée dans le cache ARP)

**Exemple d'extraction :**

Ip	MAC	Type
10.0.2.2	52:54:00:12:35:02	MIB_IPNET_TYPE_DYNAMIC

### **Extraction : Shares**

Ce test permet l'énumération des partages réseau ouverts sur la machine locale. Le résultat peut permettre d'identifier dans certains cas la cause d'intrusion. Ces données peuvent être extraites si elles sont statiques depuis la base de registre et en live si elles sont dynamiques.

**Les données extraites à partir de ce test sont :**

- **File** (En cas d'extraction depuis un fichier de registre, permet de spécifier le fichier source)
- **Share** (Nom du partage)
- **Path** (Chemin correspondant au partage)
- **Description** (Description associée au partage)
- **Type**
- **Connexion** (Nombre de connexion au partage sur le nombre maximum d'accès autorisé)

**Exemple d'extraction :**

File	Share	Path	Description	Type	Connexion
	IPC\$		IPC distant	RPC	0/-
	ADMIN\$	C:\WINDOWS	Administration à ...	SPECIAL	0/-
	C\$	C:\	Partage par défaut	SPECIAL	0/-

## **Extraction : Registry – Settings**

Ce test a pour objectif de faciliter les investigations en récupérant les informations utiles pour la description du poste. La liste des informations à obtenir n'est pas limitée et peut facilement être enrichie par l'utilisateur en ajoutant des champs dans la table **extract\_registry\_settings\_request** de la base SQLite.

L'extraction peut être faite en live ou hors ligne.

**Le format autorisé dans cette table est :**

- **id** (valeur automatique d'index)
- **id\_test\_string** (Identifiant, permet d'associer une chaîne de caractère multi-langue au test. La liste des chaînes associées sont présentes dans la table **tests\_string**.)
- **hkey** (Ruche de la base de registre ou lire l'information)
- **key** (Chemin de la clé dans le registre)
- **value** (Valeur de registre à lire)
- **value\_type** (Type de donnée à lire)
  - TYPE\_VALUE\_STRING : 0 (Correspond à une chaîne standard)
  - TYPE\_VALUE\_DWORD : 1 (Correspond à une valeur de type chiffre)
  - TYPE\_VALUE\_MULTI\_STRING : 2 (Correspond à une chaîne comprend plusieurs chaînes espacées par un 0)
  - TYPE\_VALUE\_FILETIME : 4 (Format binaire d'une date)
  - TYPE\_VALUE\_MULTI\_WSTRING : 5 (Correspond à une chaîne en Unicode comprenant plusieurs chaînes espacées par 00)
  - TYPE\_VALUE\_WIN\_SERIAL : 100 (Format binaire d'un numéro de série Microsoft)
  - TYPE\_ENUM\_STRING\_VALUE : 200 (Énumérer toutes les valeurs d'une clé de registre)
- **search\_key** (Chaîne d'information correspondant à la clé et valeur de registre à lire. Utilisé pour l'affichage des résultats.)
- **type\_id** (Identifiant, permet d'associer une chaîne de caractère multi-langue au test pour le type. La liste des chaînes associées sont présentes dans la table **tests\_string**.)
- **description\_id** (Identifiant, permet d'associer une chaîne de caractère multi-langue au test pour la description. La liste des chaînes associées sont présentes dans la table **tests\_string**.)

**Les données extraites à partir de ce test sont :**

- **File** (En cas d'extraction depuis un fichier de registre, permet de spécifier le fichier source)
- **Root key** (Ruche de la clé)
- **Key**
- **Value**
- **Data** (Données de la valeur de registre)
- **Type**
- **Description**
- **Parent key update** (Correspond à la date de dernière modification de la clé parent de la valeur, dépend de la configuration UTC lors de l'exécution du test.)

## Exemple d'extraction :

Root key	Key	Value	Data	Type	Description	Parent key update
HKEY_LOCAL_MACHINE	software\mic...	productname	Microsoft Win...	Settings	Operating System	2014/11/13 14:42:51
HKEY_LOCAL_MACHINE	software\mic...	csdversion	Service Pack 3	Settings	OS Service Pack	2014/11/13 14:42:51
HKEY_LOCAL_MACHINE	software\mic...	digitalproductid	DYBIM-RYFJ...	Serial	MS product serial	2014/11/13 14:42:51
HKEY_LOCAL_MACHINE	software\mic...	systemroot	C:\WINDOWS	Settings	System path	2014/11/13 14:42:51
HKEY_LOCAL_MACHINE	software\mic...	debugger	ntsd -d	Malware entry	Used for redirect ap...	2011/08/08 19:35:13

## Extraction : Registry – Service & Driver

Les services et drivers sont gérés de manière quasi identiques sous les systèmes Microsoft Windows. Ils sont exécutés avec des privilèges systèmes. Il est donc important de vérifier si un programme malveillant ne s'est pas installé de manière récurrente sur le système.

Ces données peuvent être extraites en live ou depuis les fichiers de registre brute. Elles sont présentes dans la base de registre à la ruche SYSTEM à la clé :

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\

### Les données extraites à partir de ce test sont :

- **File** (En cas d'extraction depuis un fichier de registre, permet de spécifier le fichier source)
- **Root key** (Ruche de la clé)
- **Key**
- **Name** (Le nom du service/driver)
- **State** (État de démarrage du service)
- **Path** (Emplacement du fichier \*.sys chargé)
- **Description** (La description visible dans la liste des services sous Windows)
- **Type** (Si un driver et à quoi il sert)
- **Last update** (Correspond à la date de dernière modification de la clé parent de la valeur, dépend de la configuration UTC lors de l'exécution du test.)

## Exemple d'extraction :

```
Registry - Service & Driver
-----

[Root key]
HKEY_LOCAL_MACHINE

[Key]
SYSTEM\CurrentControlSet\Services\AsyncMac

[Name]
Pilote de média asynchrone RAS

[State]
Manual start

[Path]
system32\DRIVERS\asynmac.sys

[Description]
Pilote de média asynchrone RAS

[Type]
Kernel driver

[Last update]
2012/06/01 13:47:44
```

## Extraction : Registry – USB

La liste des supports externes USB déjà connectée sur un système peut permettre d'identifier la source d'une infection voir la dernière fois ou une clé a été utilisée.

Ces données peuvent être extraites en live ou depuis les fichiers de registre brute. Elles sont présentes dans la base de registre à la ruche SYSTEM à la clé :

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\

### Les données extraites à partir de ce test sont :

- **File** (En cas d'extraction depuis un fichier de registre, permet de spécifier le fichier source)
- **Root key** (Ruche de la clé)
- **Key**
- **Name** (Le nom du support externe)
- **Vendor ID** (Identifiant dédié à la société éditrice du support)
- **Product ID** (Numéro de produit)
- **Description** (Type de support)
- **USB Parent** (Identifiant système pour la clé)
- **Driver letter** (Lettre de lecteur si le support externe était connecté au moment du test)
- **Last use** (Correspond à la date de dernière modification de la clé parent de la valeur, dépend de la configuration UTC lors de l'exécution du test.)

### Exemple d'extraction :

```
Registry - USB
-----

[Root key]
HKEY_LOCAL_MACHINE

[Key]
SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Lexar&Prod_USB_Flash_Drive&Rev_1100\E9BQEDHFSSXF2Y9
5ZB6Z&0

[Name]
Lexar USB Flash Drive USB Device

[Vendor ID]
05DC

[Product ID]
A788

[Description]
DiskDrive @disk.inf,%genmanufacturer%;(Lecteurs de disque standard)
(Disk&Ven_Lexar&Prod_USB_Flash_Drive&Rev_1100)

[USB Parent]
VID_05DC&PID_A788

[Last use]
2012/06/01 13:48:25
```



## Extraction : Registry – Software

Afin de vérifier si un programme peut être la source d'infection ou de service indésirable.

Ces données peuvent être extraites en live ou depuis les fichiers de registre brute. Elles sont présentes dans la base de registre à la ruche SOFTWARE aux clés :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node
\Microsoft\Windows\CurrentVersion\Uninstall\
```

**Note :** Sous certains systèmes la liste des logiciels est fusionnée avec la liste des packages et mises à jours. De plus, attention, dans certains cas l'exécution de la version RtCA\_x86 sur un système 64bits peut ne pas permettre l'extraction de la liste des logiciels 64bits. En effet pour les programmes 32bits, une virtualisation de clé de registre est présente.

### Documentations Microsoft:

<http://msdn.microsoft.com/en-us/library/windows/desktop/aa384253%28v=vs.85%29.aspx>

<http://msdn.microsoft.com/en-us/library/aa965884%28VS.85%29.aspx>

<http://msdn.microsoft.com/en-us/library/ms724072%28v=vs.85%29.aspx>

### Les données extraites à partir de ce test sont :

- **File** (En cas d'extraction depuis un fichier de registre, permet de spécifier le fichier source)
- **Root key** (Ruche de la clé)
- **Key**
- **Name** (Le nom du logiciel ou package)
- **Publisher** (Éditeur)
- **Uninstall string** (Commande de désinstallation du programme)
- **Path** (Emplacement de l'application)
- **Date install/update** (Correspond à la date de dernière modification de la clé parent ou de l'installation du programme, dépend de la configuration UTC lors de l'exécution du test.)
- **Install user**
- **URL**
- **Source**
- **Checked** (Actuellement cette fonctionnalité est désactivée)

### Exemple d'extraction :

```
Registry - Software
-----

[Root key]
HKEY_LOCAL_MACHINE

[Key]
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\KB2485663

[Name]
Mise à jour de sécurité pour Windows XP (KB2485663) (1)

[Publisher]
Microsoft Corporation

[Uninstall string]
"C:\WINDOWS\$_NtUninstallKB2485663$\spuninst\spuninst.exe"

[Path]
HKLM\SOFTWARE\Microsoft\Updates\Windows XP\SP4\KB2485663
```

```
[Date install/update]
2011/09/17 12:49:49

[URL]
http://support.microsoft.com
```

## **Extraction : Registry – Update & Packages**

Afin de vérifier si une mise à jour peut être la source d'infection ou de service indésirable.

Ces données peuvent être extraites en live ou depuis les fichiers de registre brute. Elles sont présentes dans la base de registre à la ruche SOFTWARE aux clés :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Updates\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node \Microsoft\Windows\Updates\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Component Based
Servicing\Packages\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node \Microsoft\Windows\Component Based
Servicing\Packages\
```

### **Les données extraites à partir de ce test sont :**

- **File** (En cas d'extraction depuis un fichier de registre, permet de spécifier le fichier source)
- **Root key** (Ruche de la clé)
- **Key**
- **Component** (Service pack ou package dont fait parti le correctif ou package)
- **Name**
- **Uninstall string** (Commande de désinstallation du programme)
- **Install by**
- **Description**
- **Install date/last update** (Correspond à la date de dernière modification de la clé parent ou de l'installation de la mise à jour, dépend de la configuration UTC lors de l'exécution du test.)

### **Exemple d'extraction :**

```
Registry - Update & Packages
-----

[Root key]
HKEY_LOCAL_MACHINE

[Key]
SOFTWARE\Microsoft\Updates\Windows XP\SP4\KB2485663\

[Component]
Windows XP

[Name]
KB2485663

[Installed by]
nico

[Description]
Mise à jour de sécurité pour Windows XP (KB2485663)

[Install date/last update]
2011/09/17 12:49:49
```

## Extraction : Registry – Start

Ce test a pour objectif d'identifier l'ensemble des programmes démarrés au démarrage suivant les fonctionnalités systèmes liées à la base de registre. Sont omis de cette partie les tâches planifiées et la liste des services et drivers qui font parties d'autres tests.

Ces données peuvent être extraites en live ou depuis les fichiers de registre brute. Elles sont présentes dans la base de registre aux ruches SYSTEM, SOFTWARE de HKEY\_LOCAL\_MACHINE et du HKEY\_CURRENT\_USER. Les clés étant assez nombreuses et pouvant être modifiées, la table **extract\_registry\_start\_request** y est dédiée.

**Le format autorisé dans cette table est :**

- **id** (valeur automatique d'index)
- **hk** (Ruche de la base de registre ou lire l'information)
- **key** (Chemin de la clé dans le registre)
- **type** (Type de format de données à lire)
  - 0 : Énumération des clés
  - 1 : Chaîne de caractère
  - 2 : Chiffres
- **value** (Valeur de registre à lire)
  - \* : toujours cette valeur si le type 0 est sélectionné.
- **key\_search** (Chaîne d'information correspondant à la clé et valeur de registre à lire. Utilisé pour l'affichage des résultats.)

**Les données extraites à partir de ce test sont :**

- **File** (En cas d'extraction depuis un fichier de registre, permet de spécifier le fichier source)
- **Root key** (Ruche de la clé)
- **Key**
- **Value**
- **Data** (Données lues)
- **Parent key update** (Correspond à la date de dernière modification de la clé parent , dépend de la configuration UTC lors de l'exécution du test.)

**Exemple d'extraction :**

```
Registry - Start
-----

[Root key]
HKEY_LOCAL_MACHINE

[Key]
SOFTWARE\Microsoft\Windows\CurrentVersion\Run

[Value]
VBoxTray

[Data]
C:\WINDOWS\system32\VBoxTray.exe

[Parent key update]
2014/11/13 15:16:37
```

## Extraction : Registry – Users & groups

Liste des utilisateurs locaux présent sur la machine. Ce test, s'il est associé avec le test [Registry - Account & passwords](#) permet l'extraction des empreintes des mots de passe des comptes directement exploitables avec [John the ripper](#) ou tout autre logiciel de cassage de mot de passe.

Ces données peuvent être extraites en live ou depuis les fichiers de registre brute. Elles sont présentes dans la base de registre à la ruche SAM. La ruche SYSTEM est nécessaire en cas de récupération des empreintes des mots de passe des utilisateurs.

### Les données extraites à partir de ce test sont :

- **Source** (Fichier source ou clé de registre)
- **Name** (Domaine\Utilisateur)
- **RID** (RID de l'utilisateur)
- **SID** (SID complet de l'utilisateur)
- **Group** (Liste des groupes dont fait parti l'utilisateur)
- **Description**
- **Last logon** (Correspond à la date de dernière connexion de l'utilisateur , dépend de la configuration UTC lors de l'exécution du test.)
- **Last password change** (Correspond à la date de dernière modification du mot de passe de l'utilisateur , dépend de la configuration UTC lors de l'exécution du test.)
- **Nb connexion** (Nombre d'authentification de ce compte sur la machine)
- **Type** (Type de compte)
- **State** (Si le compte est activé, désactivé ou verrouillé)

### Exemple d'extraction :

```
Registry - Users & groups
-----

[Source]
HKEY_LOCAL_MACHINE\SAM

[Name]
DEV-XP2\Administrateur

[RID]
00500

[SID]
S-1-5-21-1606280848-507921505-1957994488-500

[Group]
Administrateurs

[Description]
Compte d'utilisateur d'administration Rights : Local Administrator

[Last logon]
Never

[Last password change]
2011/08/08 19:36:28 (Password never expire)

[Nb connexion]
0

[Type]
2 : Administrator

[State]
Enable
```

## Extraction : Registry – UserAssist

L'ensemble des exécutions et ouvertures de fichiers sont tracées par défaut sur les systèmes Microsoft Windows dans la clé d registre UserAssist.

Ces données peuvent être extraites en live ou depuis les fichiers de registre brute. Elles sont présentes dans la base de registre à la ruche HKEY\_CURRENT\_USER (NTUSER.DAT) à la clé :

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\

En cas de multiples utilisateurs connectés sur la machine, cette clé est virtualisée dans :  
HKEY\_USER\<SID de l'utilisateur>\Software\Microsoft\...

Les valeurs stockées à cette clé correspondant au chemin du fichier sont encodées en ROT13 (Rotation de 13 caractères par rapport à l'alphabet de 26 lettres) et les données associées permettent d'obtenir des informations sur l'exécution.

### Les données extraites à partir de ce test sont :

- **File** (En cas d'extraction depuis un fichier de registre, permet de spécifier le fichier source)
- **Root key** (Ruche de la clé)
- **Key**
- **RAW type** (type de données enregistrées)
- **Type** (Description du RAW type)
- **Path** (Chemin du fichier)
- **Use count** (Nombre d'ouverture du fichier)
- **Session number** (Numéro de la session utilisateur associée avec la dernière ouverture du fichier)
- **Focus time** (Temps où le fichier ouvert a été utilisé, cette valeur est présente depuis Windows Vista)
- **Last use** (Correspond à la date de dernière utilisation du fichier, dépend de la configuration UTC lors de l'exécution du test.)
- **User**
- **RID**
- **SID**

### Exemple d'extraction :

```
Registry - UserAssist
-----

[Root key]
HKEY_USERS

[Key]
S-1-5-21-1606280848-507921505-1957994488-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-
006097DEACF9}\Count

[RAW type]
UEME_RUNPATH

[Type]
Executables

[Path]
\\VBOXSVR\partage_vm\Install\7z920.exe

[Use count]
00000001
```

```
[Session number]
00000001

[Last use]
2011/08/08 17:56:42

[User]
BUILTIN\Administrateurs

[SID]
S-1-5-32-544
```

### ***Extraction : Registry – MRU & MUICache & history***

Ce test comporte un grand nombre d'historiques générés par le système lors de l'ouverture d'un fichier par certaines applications. MRU (Most Recent Used, correspond aux derniers fichiers ouverts).

Ces données peuvent être extraites en live ou depuis les fichiers de registre brute. Elles sont présentes dans la base de registre à la ruche HKEY\_CURRENT\_USER (NTUSER.DAT).

En cas de multiples utilisateurs connectés sur la machine, la clé est virtualisée dans : HKEY\_USER<SID de l'utilisateur>\\...

Les clés étant assez nombreuses et pouvant être modifiées, la table **extract\_registry\_mru\_request** y est dédiée.

**Le format autorisé dans cette table est :**

- **id** (valeur automatique d'index)
- **hkey** (Ruche de la base de registre ou lire l'information)
- **key** (Chemin de la clé dans le registre)
- **value** (Valeur à ne pas prendre en compte dans l'énumération. Représente la valeur d'index qui correspond à la liste des identifiants dans l'ordre d'importance des MRU)
- **value\_type** (Type de format de données à lire)
  - TYPE\_VALUE\_STRING : 0 (Une chaîne)
  - TYPE\_VALUE\_WSTRING : 3 (Une chaîne Unicode)
  - TYPE\_ENUM\_SUBNK\_DATE : 101 ()
  - TYPE\_DBL\_ENUM\_VALUE : 102 (Toutes les données)
  - TYPE\_ENUM\_STRING\_VALUE : 200 (Toutes les chaînes)
  - TYPE\_ENUM\_STRING\_RVALUE : 201 (Toutes les chaînes comprise sous une sous clé non connue)
  - TYPE\_ENUM\_STRING\_RRVALUE : 202 (Toutes les chaînes comprise sous deux sous clés non connues)
  - TYPE\_ENUM\_STRING\_R\_VALUE : 203 (Toutes les chaînes comprise sous une sous clé non connue et après une clé connue)
  - TYPE\_ENUM\_STRING\_WVALUE : 210 (Toutes les chaînes Unicode)
  - TYPE\_ENUM\_STRING\_NVALUE : 211 (Toutes les chaînes avec comme début de nom MRU)

- **search\_key** (Chaîne d'information correspondant à la clé et valeur de registre à lire. Utilisé pour l'affichage des résultats.)
- **type\_id** (Identifiant, permet d'associer une chaîne de caractère multi-langue au test pour le type. La liste des chaînes associés sont présentes dans la table **tests\_string**.)
- **description\_id** (Identifiant, permet d'associer une chaîne de caractère multi-langue au test pour la description. La liste des chaînes associés sont présentes dans la table **tests\_string**.)

#### Les données extraites à partir de ce test sont :

- **File** (En cas d'extraction depuis un fichier de registre, permet de spécifier le fichier source)
- **Root key** (Ruche de la clé)
- **Key**
- **Value** (Nom de la valeur lue)
- **Data** (Nom du fichier lue)
- **Description**
- **Parent key update** (Correspond à la date de dernière modification de la clé parent, dépend de la configuration UTC lors de l'exécution du test.)
- **User**
- **RID**
- **SID**

#### Exemple d'extraction :

```
Registry - MRU & MUICache & history
-----

[Root key]
HKEY_USERS

[Key]
S-1-5-21-1606280848-507921505-1957994488-
1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

[Value]
a

[Data]
regedit\1

[Description]
Run history

[Parent key update]
2013/08/17 13:37:52

[User]
DEV-XP2\nico

[RID]
01003

[SID]
S-1-5-21-1606280848-507921505-1957994488-1003
```

## Extraction : Registry – Shell bags

Correspond à la liste des fichiers et répertoires accédés depuis la machine.

Ces données peuvent être extraites en live ou depuis les fichiers de registre brute. Elles sont présentes dans la base de registre à la ruche HKEY\_CURRENT\_USER (NTUSER.DAT).

En cas de multiples utilisateurs connectés sur la machine, la clé est virtualisée dans :  
HKEY\_USER\<SID de l'utilisateur>\...

Pour chaque accès, une arborescence du registre est créé et une valeur de donnée. Cette valeur est un index permettant de régénérer le chemin parcouru.

Ainsi l'index 0, 1, 2 signifiera une concaténation entre les données associées :

<data de 0>\<Data de 1>\<data de 2>

### Les données extraites à partir de ce test sont :

- **File** (En cas d'extraction depuis un fichier de registre, permet de spécifier le fichier source, ou sinon la ruche de la clé)
- **Key**
- **Value** (Nom de la valeur lue servant d'index au regard de la clé)
- **Data** (Nom du répertoire ou fichier de passage)
- **SID** (SID de l'utilisateur concerné)
- **Last key update** (Correspond à la date de dernière modification de la clé associée, dépend de la configuration UTC lors de l'exécution du test.)

### Exemple d'extraction :

```
Registry - Shell bags
-----

[File]
HKEY_USERS

[Key]
S-1-5-21-1606280848-507921505-1957994488-1003\Software\Microsoft\Windows\Shell\BagMRU\0\0\0\0\1

[Value]
0

[Data]
Sources

[SID]
S-1-5-21-1606280848-507921505-1957994488-1003

[Last key update]
2011/08/09 21:39:36
```

### Exemple d'exploitation à partir de plusieurs données :

Ici le fichier qui nous intéresse `test.zip`. L'index nous informe de la position des autres éléments du chemin. L'ID complet de cet item est donc `0\0\0\0\0\2\0\1`

```
[Key]
...\Software\Microsoft\Windows\Shell\BagMRU\0\0\0\0\2\0

[Value]
1

[Data]
test.zip
```



## Pour le reconstituer :

L'ID 0 :

```
[Key]
...\Software\Microsoft\Windows\Shell\BagMRU\0

[Value]
0

[Data]
Tout le réseau
```

L'ID 0\0 :

```
[Key]
...\Software\Microsoft\Windows\Shell\BagMRU\0\0

[Value]
0

[Data]
VirtualBox Shared Folders
```

L'ID 0\0\0 :

```
[Key]
...\Software\Microsoft\Windows\Shell\BagMRU\0\0\0

[Value]
0

[Data]
\\Vboxsvr
```

L'ID 0\0\0\0 :

```
[Key]
...\Software\Microsoft\Windows\Shell\BagMRU\0\0\0\0

[Value]
0

[Data]
\\VBOXSVR\partage_vm
```

L'ID 0\0\0\0\0 :

```
[Key]
...\Software\Microsoft\Windows\Shell\BagMRU\0\0\0\0\0

[Value]
0

[Data]
Install
```

L'ID 0\0\0\0\2 :

```
[Key]
...\Software\Microsoft\Windows\Shell\BagMRU\0\0\0\0\2

[Value]
0

[Data]
a tester_dir
```

L'ID 0\0\0\0\2\0 :

```
[Key]
...\Software\Microsoft\Windows\Shell\BagMRU\0\0\0\0\2\0

[Value]
0

[Data]
A tester !!!
```

**Ce qui donne comme chemin dans le système :**

Tout le réseau->VirtualBox Shared Folders->\\Vboxsvr : \\VBOXSVR\partage\_vm\Install\atester\_dir\A tester !!!\test.zip

## **Extraction : Registry – Accounts & passwords**

Ce test a pour objectif une extraction d'un grand nombre d'empreintes et mots de passe sur le système. Il peut être utilisé dans le cadre de tests d'intrusion ou pour des besoins utilisateur.

L'extraction est tributaire de l'activation des tests Registry User & groups et des Historiques des différents navigateurs et Android. Ces données peuvent être obtenues en live ou depuis les fichiers de registre et d'historiques des navigateur et d'Android.

### **Types d'éléments extraits :**

- VNC (mot de passe en clair et déchiffré)
- Écrans de veille sur les systèmes (En clair ou en utilisant la clé Windows)
- Terminal server (En clair ou en utilisant la clé Windows)
- Compte d'auto connexion (compte, domaine et mot de passe en clair)
- Empreintes des comptes locaux
- Mots de passe d'historique des navigateurs Firefox/Chrome et d'Android (Désactivé pour le moment)

### **Les données extraites à partir de ce test sont :**

- **Source** (Fichier source du registre ou d'historique)
- **Login** (Domaine\utilisateur)
- **Password** (Mot de passe en clair)
- **RAW Password** (Empreinte ou mot de passe avant déchiffrement)
- **Description**

### **Exemple d'extraction :**

```
Registry - Accounts & passwords
-----

[Source]
HKEY_LOCAL_MACHINE\SAM

[Login]
DEV-XP2\test

[RAW password]
DEV-XP2\test:1004:NO PASSWORD*****:NO PASSWORD*****:::

[Description]
Local user account
```

**Note :** Une sauvegarde au format de PWDUMP est possible pour une attaque par dictionnaire.

### **Extraction : Registry – All path & open command**

Les programme malveillants peuvent s'insérer dans un grand nombre de mécanisme d'exécution système. Ce test a pour objectif de lister un maximum de chemin d'exécution contenu dans la base de registre.

Ces données peuvent être extraites en live ou depuis les fichiers de registre brute. Elles sont présentes dans la base de registre à la racine HKEY\_LOCAL\_MACHINE\Software et HKEY\_CURRENT\_USER.

#### **Les données extraites à partir de ce test sont :**

- **File** (En cas d'extraction depuis un fichier de registre, permet de spécifier le fichier source)
- **Root key** (Racine de la clé)
- **Key**
- **Value** (Nom de la valeur lue)
- **Data** (Commande d'exécution)
- **User**
- **RID**
- **SID**
- **Parent key update** (Correspond à la date de dernière modification de la clé parent, dépend de la configuration UTC lors de l'exécution du test.)

#### **Exemple d'extraction :**

```
Registry - All path & open command
-----

[Root key]
HKEY_LOCAL_MACHINE

[Key]
SOFTWARE\Classes\Connection Manager Profile\shell\open\command

[Data]
C:\WINDOWS\system32\CMMGR32.EXE "%1"

[User]
BUILTIN\Administrateurs

[SID]
S-1-5-32-544

[Parent key update]
2011/08/08 17:36:43
```

## **Extraction : Security guide**

Ce test a pour objectif de permettre la vérification de configuration au niveau du registre en live ou depuis les fichiers de registre brute. Il peut être utilisé pour des tests de conformité. Par défaut quelques tests standards sont pré-remplis.

La table dédiée à la configuration des tests est **extract\_guide\_request**.

**Le format autorisé dans cette table est :**

- **id** (valeur automatique d'index)
- **hk** (Ruche de la base de registre ou lire l'information)
- **key** (Chemin de la clé dans le registre)
- **value** (Valeur à extraire et tester)
- **test** (Type de test à faire)
  - GUIDE\_REG\_TEST\_IDENTIQUE : 0 (La valeur lue doit être identique à data)
  - GUIDE\_REG\_TEST\_CONTIENT : 1 (Data doit être contenu dans la valeur lue)
  - GUIDE\_REG\_TEST\_EXIST : 2 (La valeur doit exister)
  - GUIDE\_REG\_TEST\_NEXISTPAS : 3 (La valeur ne doit pas exister)
- **OS** (Type d'OS Windows cible du test)
  - ALL
  - ALL\_ONLY\_32 (Seulement les systèmes 32bits)
  - ALL\_ONLY\_64 (Seulement les systèmes 64bits)
  - 2000
  - XP
  - XP\_64
  - 2003
  - 2003\_64
  - Vista
  - Vista\_64
  - 7
  - 7\_64
  - 2008
  - 2008\_64
  - 8
  - 8\_64
- **title\_id** (Identifiant de chaîne correspondant à la description dans la table tests\_string)
- **description\_id** (Identifiant de chaîne correspondant à l'URL de référence ou un complément d'information dans la table tests\_string)
- **value\_type** (Type de format de données à lire)
  - TYPE\_VALUE\_STRING : 0 (Une chaîne)
  - TYPE\_VALUE\_DWORD : 1 (Chiffres)
  - TYPE\_VALUE\_MULTI\_STRING : 2 (Plusieurs chaînes de caractères séparées par 0)
  - TYPE\_VALUE\_WSTRING : 3 (Une chaîne Unicode)
  - TYPE\_VALUE\_MULTI\_WSTRING : 5 (Plusieurs chaînes Unicode de caractères séparées par 00)
- **search\_key** (Chaîne d'information correspondant à la clé et valeur de registre à lire. Utilisée pour l'affichage des résultats.)

- **data** (Valeur de référence à vérifier avec la valeur lue)

#### Les données extraites à partir de ce test sont :

- **File** (En cas d'extraction depuis un fichier de registre, permet de spécifier le fichier source)
- **Root key** (Ruche de la clé)
- **Key**
- **Value** (Nom de la valeur lue)
- **Data** (Données attendues)
- **Read data** (Données lues)
- **Title** (Description)
- **Description** (Complément d'information)
- **OK** (État de conformité, OK ou NOK)

#### Exemple d'extraction :

```
Security guide
-----

[Root key]
HKEY_LOCAL_MACHINE

[Key]
SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

[Value]
shutdownwithoutlogon

[Data]
0

[Read data]
1

[Title]
Disable the Shut Down Button on the Logon Information Window

[Description]
http://support.microsoft.com/kb/216083

[OK]
NOK
```

### **Extraction : Registry – Deleted key**

Ce test permet l'extraction des clés de registre effacées ou déplacées à partir d'un fichier de registre brute. En cas d'investigation en live, ce test n'est pas activé.

**Les données extraites à partir de ce test sont :**

- **File** (Fichier source)
- **Key**
- **Value**
- **Data**
- **Type** (Format des données)
- **SID** (SID du propriétaire de la clé)
- **Last key update** (Correspond à la date de dernière modification de la clé parent, dépend de la configuration UTC lors de l'exécution du test.)

### **Extraction : Antivirus**

Afin d'identifier les types d'Antivirus installés, leurs état et mise à jour. Ces éléments sont lus dans la base de registre et peuvent donc être lues en live ou à partir des fichiers de registre brutes SOFTWARE.

**Liste des Antivirus supportés (sous couvert des nouvelles versions) :**

- Microsoft Antimalware
- AVG
- G Data AntiVirenKit
- Avira Antivir
- Avast
- Kaspersky
- Bitdefender
- Panda
- Sophos
- Coranti
- rising RAV
- TrendMicro
- Symantec
- Comodo
- VirusScan
- McAfee
- VirusGuard
- ZoneAlarm

**Les données extraites à partir de ce test sont :**

- **Path** (Emplacement de l'Antivirus)
- **Name**
- **Publisher**
- **Engine** (Version du moteur)
- **BDD** (Version de la base)
- **Update URL**
- **Enable** (Si l'analyse temps réel est bien activée)
- **Last update** (Correspond à la date de dernière mise à jour ou de modification de la clé parent, dépend de la configuration UTC lors de l'exécution du test.)

## Extraction : Firewall

Liste les programmes autorisés par le par-feu Windows.

Ces éléments sont lus dans la base de registre et peuvent donc être lues en live ou à partir des fichiers de registre brutes SYSTEM.

Les informations sont contenues dans les clés :

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\

### Les données extraites à partir de ce test sont :

- **File** (En cas d'extraction depuis un fichier de registre, permet de spécifier le fichier source)
- **Root key** (Ruche de la clé)
- **Key**
- **Application** (Chemin de l'application autorisée ou refusée)
- **Rule** (règle appliquée)

### Exemple d'extraction :

```
Firewall
-----

[Root key]
HKEY_LOCAL_MACHINE

[Key]
SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\Authorize
dApplications\List

[Application]
%windir%\system32\sessmgr.exe

[Rule]
%windir%\system32\sessmgr.exe:*:enabled:@xpsp2res.dll,-22019
```



### **Extraction : Firefox – History (local time)**

Les données de Firefox et Chrome étant en SQLite, l'extraction des données est effectuée par des requêtes SQLite directement dans les bases associées.

Ce test peut être effectué en ligne ou depuis les fichiers SQLite des navigateurs.

Les tables dédiées à la configuration des tests sont **extract\_firefox\_request** et **extract\_chrome\_request**.

**Le format autorisé dans ces tables est :**

- **id** (valeur automatique d'index)
- **id\_tests\_string** (identifiant de la chaîne contenu dans la table **tests\_string**)
- **sql** (Requête à exécuter dans la base du navigateur)
- **params** (Informations pour l'extraction. Liste des attributs dans l'ordre de la requête)

**Les données extraites à partir de ce test sont :**

- **File** (Fichier source)
- **Parameter** (Chaîne de description des attributs dans l'ordre contenu dans le champ **params**)
- **Data** (Données lues)
- **Description** (Information sur le type de données lues)
- **Date** (Date de création/modification/ajout au format local time de la machine au moment de l'extraction)

**Exemple d'extraction :**

```
Firefox - History (local time)
-----

[File]
C:\Documents and Settings\nico\Application
Data\Mozilla\Firefox\Profiles\m3kxtm6x.default\places.sqlite

[Parameter]
url, title, frecency, last_visit_date

[Data]
http://omni-a.blogspot.com/2011/10/rtca-v01-outil-daide-aux-analyses.html, Omnia's house: RTCA
v0.1 - Outil d'aide aux analyses Forensic, 20

[Description]
Form history/Cookies

[Date]
2012/04/15 19:01:09
```

### **Extraction : Chrome – History (local time)**

Voir les informations dans le chapitre [#2.1.1.32.Extraction : Firefox – History \(local time\)](#)

### ***Extraction : IE – History***

Le format des données d'historiques obtenues est identiques à l'historique Firefox et Chrome

[#2.1.1.32.Extraction : Firefox – History \(local time\)](#)

Ces données peuvent être obtenues en live et à partir des fichiers index.dat présent dans les répertoires des profils utilisateurs.

### ***Extraction : Android – History (local time)***

Ce test permet à partir des fichiers de configuration SQLite d'Android d'extraire un maximum d'historique. Le format des données d'historiques obtenues est identiques à l'historique Firefox, Chrome et IE [#2.1.1.32.Extraction : Firefox – History \(local time\)](#)

Ces données peuvent être obtenues en live et à partir des fichiers SQLite du système Android (sans extension ou \*.db) présent dans les répertoires des profils utilisateurs.

### ***Extraction : LDAP AD datas***

L'extraction des données LDAP de l'Active Directory ou est connecté la machine prend beaucoup de ressources réseau et accès disque. Les données énumérées dépendent des droits de l'utilisateur courant dans l'AD. Le résultat des données est fournis sous forme LDAP.

**Les données extraites à partir de ce test sont :**

- **Dit**
- **DN**
- **Value**
- **Data**

### 2.1.2. Utilisation de RtCA en ligne de commande

Afin de permettre une extraction à distance, RtCA peut être exécuté en ligne de commande. La majorité des fonctionnalités de base et tests y sont présents.

**Note :** Attention, un grand nombre d'informations d'états ne sont pas disponibles.

#### Aide disponible (Option -h) :

```
C:\>RtCA.exe -h
*****
** RtCA 0.6.632.461b - http://code.google.com/p/omnia-projetcs/
*****

SYNOPSIS
    RtCA.exe [-l|-L|-t]
              [-r][-0][-1][-2]
              [-f "..."]
              [-p "..."]
              [-a|-A|-s ...]
              [-o "..."][-F [CSV|XML|HTML]]

DESCRIPTION
    Tool To help forensic investigations :)

OPTIONS
    -l  List all sessions or select the session number.
        Exemple: -l 125
    -L  List all languages or select it for export.
        Exemple for english export (default): -L 1
    -t  List all tests.

    -0  Enable ACL check in files test.
    -1  Enable ADS check in files test.
    -2  Enable SHA in files test.
    -T  Export in UTC time.
    -S  Disable SQLITE FULL SPEED.

    -a  Start all tests.

    -A  Start all tests in safe mode with no Files and no Logs test.
    -s  Select test to start.
        Exemple: -s 0 1 2 3 4 5 6

    -o  Export all data to path.
        Exemple: -o "c:\\"
    -F  Format to export : CSV (default), XML or HTML

    -e  SHA256deep of directories (recursive).
        Exemple: -e "C:\path\\" >> sha256deep_directory_results.txt
    -d  disk imaging to file.
        Exemple with no size limit: -d \\.\PhysicalDrive0 -- c:\image.raw
        Exemple with partition and size limit in byte: -d \\?\C: -512 c:\image.raw
    -Z  Extract local computer file's to investigate in ZIP file, ex : -Z <file to save.zip>
```

#### Liste de tous les tests disponibles (Option -t) :

```
C:\>RtCA.exe -t
*****
** RtCA 0.6.632.461b - http://code.google.com/p/omnia-projetcs/
*****

List of tests:
    [00] - Files and directories
    [01] - LNK files
    [02] - Audit logs
    [03] - Disks
```

```

[04] - Clipboard
[05] - Local variables
[06] - Scheduled tasks
[07] - Process
[08] - Prefetch
[09] - Pipes
[10] - Network
[11] - Routing table
[12] - DNS resolv
[13] - ARP cache
[14] - Shares
[15] - Registry - Settings
[16] - Registry - Service & Driver
[17] - Registry - USB
[18] - Registry - Software
[19] - Registry - Update & Packages
[20] - Registry - Start
[21] - Registry - Users & groups
[22] - Registry - UserAssist
[23] - Registry - MRU & MUICache & history
[24] - Registry - Shell bags
[25] - Registry - Accounts & passwords
[26] - Registry - All path & open command
[27] - Security guide
[28] - Registry - Deleted key
[29] - Antivirus
[30] - Firewall
[31] - Firefox - History (local time)
[32] - Chrome - History (local time)
[33] - IE - History
[34] - Android - History (local time)
[35] - LDAP AD datas

```

### Sauvegarde de l'ensemble des évidences connues (Option -Z <fichier\_zip>) :

```

C:\>RtCA.exe -Z g:\datas.zip

Vssadmin 1.0 - Outil de ligne de commande d'administration du service
de cliché instantané de volumes
(C) Copyright 2000 Microsoft Corp.

Syntaxe :

vssadmin list shadows [/set={GUID du jeu de cliché instantané}]
    Liste les clichés instantanés dans le système, triés par identificateur
de copies.

vssadmin list writers
    Liste les enregistreurs du système

vssadmin list providers
    Liste les fournisseurs de cliché instantané actuellement installés

L'opération s'est bien déroulée

L'opération s'est bien déroulée

Error:  Accès refusé.

L'opération s'est bien déroulée

L'opération s'est bien déroulée
DD 512 b \\.\PhysicalDrive0 -> C:\mbr.raw

```

**Note :** Des erreurs peuvent survenir en cas d'absence comme ci-dessus des versions vssadmin pour l'accès aux fichiers protégés à partir des copies Shadow.

Cette option permet d'obtenir la liste des évidences dans un fichier ZIP et ainsi faciliter le rapatriement.

#### Arborescence du fichier :

- *<Nom de la machine>*
  - **Disk** (Image de la MBR du premier disque sous forme RAW)
  - **eventlog** (Journaux d'événements EVT/EVTX)
  - **logs** (Fichiers d'audit complémentaires au format txt)
  - **Navigator** (Historique des navigateurs présents sur le système)
    - Chrome
    - Firefox
    - IE
  - **Prefecth** (Tous les fichiers \*.pf accessibles sur le système)
  - **Process** (Liste des processus et fichier binaires exécutés lors de l'extraction)
    - Process\_list.csv (Liste des processus et informations associées)
  - **Registry** (Ruches au format RAW)
  - **Tasks** (Fichiers \*.job des tâches planifiées)
  - **Log.txt** (Sources des fichiers copiés)

#### Extraire toutes les tests en UTC avec toutes les options (Option -a) très long :

```
C:\>RtCA.exe -0 -1 -2 -T -a
```

#### Faire un SHA256deep d'un répertoire vers un fichier txt (Option -e) assez long :

```
C:\>RtCA.exe -e « C:\ » " z:\sha256deep.txt
```

#### DD d'un disque (Option -e) :

```
C:\>RtCA.exe -e « C:\ » " z:\sha256deep.txt
```

**Note :** Certains fichiers de l'image de disque peuvent être corrompus en cas de modification du fichier lors de l'image de disque. Dans certains cas le DD de disque à distance peut être bloqué par des mécanismes de sécurité.

## 2.2. Depuis une machine à distance

### 2.2.1. Connexion à distance avec PsExec

Avant de pouvoir exécuter RtCA à distance, il est nécessaire de récupérer les outils Ps\* de la suite Sysinternals de Microsoft :

<http://technet.microsoft.com/en-us/sysinternals/>

Il faut ensuite avoir un compte administrateur sur la machine distance pouvant se connecter aux partage réseau de celle-ci.

Pour l'exemple nous avons copier au préalable RtCA dans le répertoire C:\extract\RtCA.exe

Il n'est pas nécessaire d'y copier la base de donnée sauf si elle a été mise à jour. En effet lors de l'exécution de RtCA si la base n'existe pas il la crée.

Afin de se prémunir des problème d'authentification avec PsExec (surtout sur les systèmes à partir de Vista) il est préférable d'exécuter PsExec depuis un invité de commande DOS exécuté avec les privilèges de l'administrateur pouvant se connecter sur la machine à distance (nécessite d'être dans un domaine).

Afin de pouvoir profiter un maximum des fonctionnalités de RtCA il est recommande de l'exécuter depuis un invite de commande plutôt que directement depuis PsExec.

#### Cas d'exécution de PsExec avec un compte d'administration du domaine :

```
PsExec.exe -h \\computer -c cmd.exe  
  
cd c:\extract\  
RtCA.exe ...
```

#### Cas d'exécution de PsExec avec un compte spécifique d'administration :

```
PsExec.exe -u Administrator -p MonBoPassword \\computer -c cmd.exe  
  
cd c:\extract\  
RtCA.exe ...
```

Une fois l'extraction effectuée, il est nécessaire de récupérer le fichier zip (en cas d'extraction des fichiers d'évidence. Fortement recommandé!) ou/et le fichier RtCA.sqlite disponible dans le répertoire de RtCA sur la machine à distance.

**Attention à ne pas écraser d'autres archives locales !**

## 2.3. Depuis des fichiers déjà extraits

Afin d'extraire les informations, il suffit dans l'interface de nouvelle session [#1.6.3.Fenêtre de création de session](#) d'ajouter les fichiers déjà collectés dans l'interface de gauche et d'appuyer sur **Start**. La session apparaîtra différemment en commençant par **Files** au lieu du nom de l'ordinateur.

## **3. Exploitation des données**

### **3.1. Analyse rapide**

Décrire ici la démarche : identification de la machine + heure des tests, etc,,, attention aux dates...

### **3.2. Corrélation d'extractions**

### **3.3. Cas pratique de recherche**

Cette section donne quelques exemples d'analyses avec RtCA sur un système infecté ou ayant subi des attaques.

#### **3.3.1. Par séquence de démarrage de programme malveillant**

(Job, registre, path d'exécution, prefetch)

#### **3.3.2. Par l'analyse en live depuis la machine**

(liste des processus, caches DNS, ARP, capture réseau) explication qu'il est mieux d'utiliser un switch externe + scanne de port de la machine.

#### **3.3.3. Par attaque de type force brute sur un compte**

Analyse des journaux d'audit

#### **3.3.4. Actions de malveillance d'un utilisateur**

Analyse des journaux d'audit

#### **3.3.5. Identification de la source d'infection**

Analyse des journaux de navigation des utilisateurs en rapport avec les programmes, urls identifiées, clés USB, partages accédés... MRU

## 4. Liste des outils intégrés

Les outils intégrés sont accessibles depuis la fenêtre principale dans le menu **Tools**.

### 4.1. Copie de fichiers

La routine de copie de fichier fonctionne suivant la schématique suivante :

- Copie standard d'un fichier
  - Si copie refusée, copie par ouverture de fichier partagée
    - Si copie refusée, utilisation des images shadow pour copier la dernière version du fichier.
      - Si copie refusée, copie par ouverture du disque, interprétation du système de fichier et copie des secteurs.

**Par défaut, plusieurs accès rapides existent :**

- **Copy all registry files** : copie des ruches de la base de registre en RAW (format binaire nécessitant un outil ou RtCA pour le lire). Liste des ruches connues :
  - HKEY\_LOCAL\_MACHINE\SOFTWARE, SYSTEM, SAM, HARDWARE=> SAM, SOFTWARE, SYSTEM, HARDWARE
  - HKEY\_CLASSES\_ROOT => CLASSES.DAT
  - HKEY\_USERS => DEFAULT, <user>\_NTUSER.DAT, <user>\_UsrClass.dat
  - HKEY\_CURRENT\_USER => NTUSER.DAT, CLASSES.DAT
- **Copy all audit files** (Permet la copie de tous les fichiers d'audit répertoriés sur le système, \*.evtx, \*.evt, \*.log...)
- **Copy NTDIS.DIT(AD) file** (Copie du fichier où est stocké toutes les informations de configuration d'un contrôleur de domaine. Ne fonctionne que sur un contrôleur de domaine)
- **Copy specific file** (Système de copie permettant de passer outre les protections du système afin de copier un fichier)
- **Save all local datas to ZIP file** (Extraction de l'ensemble des fichiers de données importants connus afin d'effectuer une investigation à l'exception des mémoires et des disques). Liste des éléments extraits :
  - La MBR des disques dans /Disk
  - Les journaux d'audit dans /eventlog et /log
  - Les historiques des navigateurs dans /Navigator/<nom du navigateur>/<SID\_user>\_fichier
  - Les fichiers de prefetch du système
  - La liste des processus et les binaires exécutés
  - Les ruches du registre
  - Les tâches planifiées
  - Un fichier log.txt de l'ensemble des sources des éléments copiés



## 4.2. DD

Permette d'effectuer une image disque au format brute sur une système exécuté.

Plusieurs options sont proposées :

- La copie de partition
- La copie du MBR (système de démarrage du disque)
- La copie de disque

Le temps de copie dépend de la vitesse des supports. Compter pour un débit correct d'un disque vers un autre sans faire travailler la machine hôte, 100go / heure.

Ne pas effectuer la sauvegarde de l'image sur le même disque que le disque lue, à l'exception de l'extraction MBR ou d'une partition vers une autre. Dans ce cas présent la performance moyenne obtenue est de 30go / heure.

Note : Les temps ne sont qu'à titre indicatif. Un disque de 5400tr en SATA 2 est pris pour les références.

**Attention lors de l'exploitation de ce fichier, l'extraction étant effectuée en live, certaines données peuvent être illisibles !**

## 4.3. Process list

La liste des processus peut être affichée à partir de la fenêtre principale et du menu :

**Tools->Process list.**

Comme dans toutes les listes de l'outil, il est possible de trier par colonne, en sélectionnant l'entête de la colonne.

La liste des processus se présente comme ci-dessous :

Process	PID	Path	Command	Owner	RD	SD	Start date	Pr...	P src	Pr...	P dst	Port...	State	Hidden	Parent process	Par...	Verified	VirusTotal
svchost.exe	00984	C:\WIN...	C:\WINDOWS\system32\svchost.exe...	BUILTIN\Administrateurs			2014/11/13 15:42:51	TCP	0.0.0.0 dev-x...	135	0.0.0.0 dev-x...	55320	LISTENING		C:\WINDOWS...	00056	File not signed	62341556c02c67689744d21380b17d
svchost.exe	01304	C:\WIN...	C:\WINDOWS\system32\svchost.exe...	BUILTIN\Administrateurs			2014/11/13 15:43:00	UDP	10.0.0.15 dev...	1900	**dev-vg2		LISTENING		C:\WINDOWS...	00056	File not signed	62341556c02c67689744d21380b17d
svchost.exe	01484	C:\WIN...	C:\WINDOWS\system32\svchost.exe...	BUILTIN\Administrateurs			2014/11/13 15:43:00	UDP	127.0.0.1 dev...	1900	**dev-vg2		LISTENING		C:\WINDOWS...	00056	File not signed	62341556c02c67689744d21380b17d
svchost.exe	01112	C:\WIN...	C:\WINDOWS\system32\svchost.exe...	BUILTIN\Administrateurs			2014/11/13 15:42:51	UDP	0.0.0.0 dev-x...	1055	**dev-vg2		LISTENING		C:\WINDOWS...	00056	File not signed	62341556c02c67689744d21380b17d
svchost.exe	01112	C:\WIN...	C:\WINDOWS\system32\svchost.exe...	BUILTIN\Administrateurs			2014/11/13 15:42:51	UDP	0.0.0.0 dev-x...	1055	**dev-vg2		LISTENING		C:\WINDOWS...	00056	File not signed	62341556c02c67689744d21380b17d
System	00004			BUILTIN\Administrateurs			2014/11/13 15:42:51	TCP	0.0.0.0 dev-x...	445	0.0.0.0 dev-x...	2192	LISTENING				00000	
System	00004			BUILTIN\Administrateurs			2014/11/13 15:42:51	TCP	0.0.0.0 dev-x...	139	0.0.0.0 dev-x...	20709	LISTENING				00000	
System	00004			BUILTIN\Administrateurs			2014/11/13 15:42:51	UDP	0.0.0.0	445	**		LISTENING				00000	
System	00004			BUILTIN\Administrateurs			2014/11/13 15:42:51	UDP	10.0.0.15	137	**		LISTENING				00000	
System	00004			BUILTIN\Administrateurs			2014/11/13 15:42:51	UDP	10.0.0.15	138	**		LISTENING				00000	
smss.exe	00540	C:\WIN...	C:\WINDOWS\system32\smss.exe...	BUILTIN\Administrateurs			2014/11/13 15:42:49										00004	File not signed
csrss.exe	00598	C:\WIN...	C:\WINDOWS\system32\csrss.exe...	BUILTIN\Administrateurs			2014/11/13 15:42:50								SystemRoot...	00540	File not signed	e1f414acabec4600005f85053cc3bd21
winlogon.exe	00612	C:\WIN...	C:\WINDOWS\system32\winlogon.exe...	BUILTIN\Administrateurs			2014/11/13 15:42:50								SystemRoot...	00540	File not signed	de1998f6209673b0484843b1155590ae
services.exe	00656	C:\WIN...	C:\WINDOWS\system32\services.exe...	BUILTIN\Administrateurs			2014/11/13 15:42:50								SystemRoot...	00612	File not signed	ec0f5a07bac72a99a0a032a4a04143f1
lsass.exe	00668	C:\WIN...	C:\WINDOWS\system32\lsass.exe...	BUILTIN\Administrateurs			2014/11/13 15:42:50								SystemRoot...	00612	File not signed	0ca00776a91502a71be5371a4e484d21
VBoxService.exe	00840	C:\WIN...	C:\WINDOWS\system32\VBoxService.exe...	BUILTIN\Administrateurs			2014/11/13 15:42:50								SystemRoot...	00840	File not signed	d2005c0a6980e46126a899b336ac0d5f
svchost.exe	00908	C:\WIN...	C:\WINDOWS\system32\svchost.exe...	BUILTIN\Administrateurs			2014/11/13 15:42:50								C:\WINDOWS...	00056	File not signed	62341556c02c67689744d21380b17d
svchost.exe	01092	C:\WIN...	C:\WINDOWS\system32\svchost.exe...	BUILTIN\Administrateurs			2014/11/13 15:42:51	UDP	10.0.0.15 dev...	123	**dev-vg2		LISTENING		C:\WINDOWS...	00056	File not signed	62341556c02c67689744d21380b17d
svchost.exe	01092	C:\WIN...	C:\WINDOWS\system32\svchost.exe...	BUILTIN\Administrateurs			2014/11/13 15:42:51	UDP	127.0.0.1 dev...	123	**dev-vg2		LISTENING		C:\WINDOWS...	00056	File not signed	62341556c02c67689744d21380b17d
lsass.exe	01448	C:\PROG...	C:\Program Files\Uniview\lsass.exe...	BUILTIN\Administrateurs			2014/11/13 15:43:00	TCP	127.0.0.1 loc...	5152	0.0.0.0 dev-x...	18595	LISTENING		C:\WINDOWS...	00056	File not signed	550cd79d8f754a4245c7a0cc4018152be7
winlogon.exe	01752	C:\WIN...	C:\WINDOWS\system32\winlogon.exe...	BUILTIN\Administrateurs			2014/11/13 15:43:04								C:\WINDOWS...	00056	File not signed	3208ec10d8992185c13304aa532c3e7
svchost.exe	01396	C:\WIN...	C:\WINDOWS\system32\svchost.exe...	BUILTIN\Administrateurs			2014/11/13 15:43:01								C:\WINDOWS...	00056	File not signed	62341556c02c67689744d21380b17d
explorer.exe	00428	C:\WIN...	C:\WINDOWS\explorer.exe...	DEV-XP2nico		01003	2014/11/13 15:44:07								C:\WINDOWS...	00392	File not signed	1a674a4a472159a5d2d0714e2e1a60b
VBoxTray.exe	00512	C:\WIN...	C:\WINDOWS\system32\VBoxTray.exe...	DEV-XP2nico		01003	2014/11/13 15:44:07								C:\WINDOWS...	00428	File not signed	43c208a5c308a780ba61195c0ba4051
ctmon.exe	00560	C:\WIN...	C:\WINDOWS\system32\ctmon.exe...	DEV-XP2nico		01003	2014/11/13 15:44:07								C:\WINDOWS...	00428	File not signed	2aeb8126577568c9801717e5c2a8373e
TSVNCache.exe	00576	C:\PROG...	C:\Program Files\Toshiba\TSVNCache.exe...	DEV-XP2nico		01003	2014/11/13 15:44:07								C:\WINDOWS...	00428	File not signed	82061f0b0a6808b41e6a660045a5a56c
notepad++ .exe	01936	C:\PROG...	C:\Program Files\Notepad++\notepad++.exe...	DEV-XP2nico		01003	2014/11/13 16:52:45								C:\WINDOWS...	00428	File not signed	e020f809105571704aa00070b2c23
cmd.exe	02004	C:\WIN...	C:\WINDOWS\system32\cmd.exe...	DEV-XP2nico		01003	2014/11/13 16:55:40								C:\WINDOWS...	00428	File not signed	8984d3745094023805052372e2491e
codeblocks.exe	00194	C:\PROG...	C:\Program Files\CodeBlocks\codeblocks.exe...	DEV-XP2nico		01003	2014/11/14 20:13:02								C:\WINDOWS...	00428	File not signed	14584d3742c7efc591c5b0a4a05291e
RtCA.exe	01892	C:\WIN...	C:\WINDOWS\system32\RtCA.exe...	DEV-XP2nico		01003	2014/11/13 11:22:48								C:\WINDOWS...	00428	File not signed	db887087001a05c0a0e7d5d7460e703c

Les informations affichées sont :

- **Process** (Le nom du processus :fichier binaire)
- **PID** (Identifiant unique d'exécution du processus)
- **Path** (Chemin complet du processus)

- **Command** (La ligne d'exécution complète du processus)
- **Owner** (Nom de l'utilisateur ayant exécuté le programme)
- **RID** (RID de l'utilisateur exécutant le programme)
- **SID** (SID complet du propriétaire ayant exécuter le programme)
- **Start Date** (date et heure à laquelle le programme a été lancé)
- **Protocol** (Protocole réseau des ports ouverts sur ce processus : UDP ou TCP)
- **IP src** (IP source de la carte réseau ayant ouvert le port)
- **Port src** (Port source ouvert en local sur la machine)
- **IP dst** (IP de destination connectée au port source du processus si TCP)
- **Port dst** (Port de destination connecté au port source du processus si TCP)
- **State** (État des ports ouverts)
- **Hidden** (Utilisation du scanne des tables des processus afin d'identifier les processus masqués par des drivers ou routines. Quand le processus est détecté, un X est présent dans cette colonne)
- **Parent process** (Chemin du processus ayant exécuter le processus actuel)
- **Parent PID** (PPID : identifiant unique d'exécution du processus ayant exécuter le processus actuel)
- **Verified** (État de vérification de la signature du binaire, Si la signature est bonne, **WINTRUST\_ACTION\_GENERIC\_VERIFY\_V2 OK** est affiché)
- **VirusTotal** (Par défaut contient l'empreinte SHA256 si possible du processus, si une demande d'information a été effectuée, il contient les résultats.

**Un menu est disponible afin de permettre des actions :**

- **Refresh** (Pour mettre à jour la liste des processus. Attention la vérification VirusTotal est réinitialisée avec l'empreinte SHA256)
- **Save view** (Permet la sauvegarde en CSV/XML/HTML de la liste)
- **Open Path** (Permet l'accès direct au répertoire du programme sélectionné)
- **Kill process** (Tue le processus sélectionné)
- **Dump process memory** (Permet l'extraction mémoire du binaire en mémoire)
- **VirusTotal check file/check all files** (Permet d'interroger la base VirusTotal sur la malveillance de la signature SHA256 correspondant au binaire)
- **Dll injection** (Permet d'injecter ou de supprimer une DLL d'un processus ? Nécessite la DLL)
- **Copy the line to clipboard/ copy to clipboard** (Permet comme sur toute l'application de copier dans le presse papier la ligne sélectionnée ou une case précise)

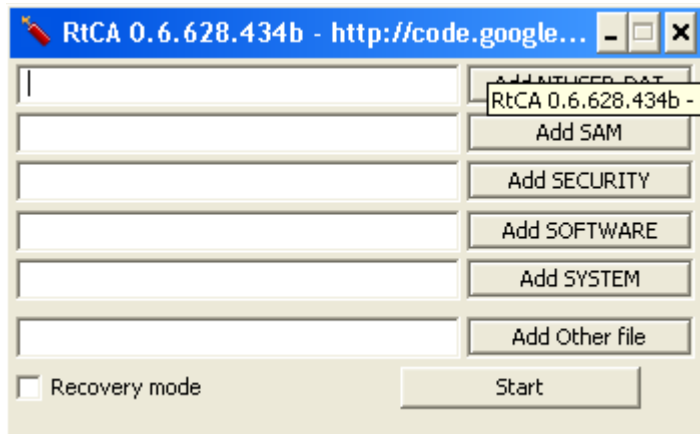
Note : Le double clic sur une ligne permet d'afficher en une fenêtre avec du texte copiable, toutes les informations du processus avec en plus sa liste des DLL chargées.

## 4.4. Registry explorer

L'explorateur de fichiers de registre brute peut être affiché à partir de la fenêtre principale et du menu :

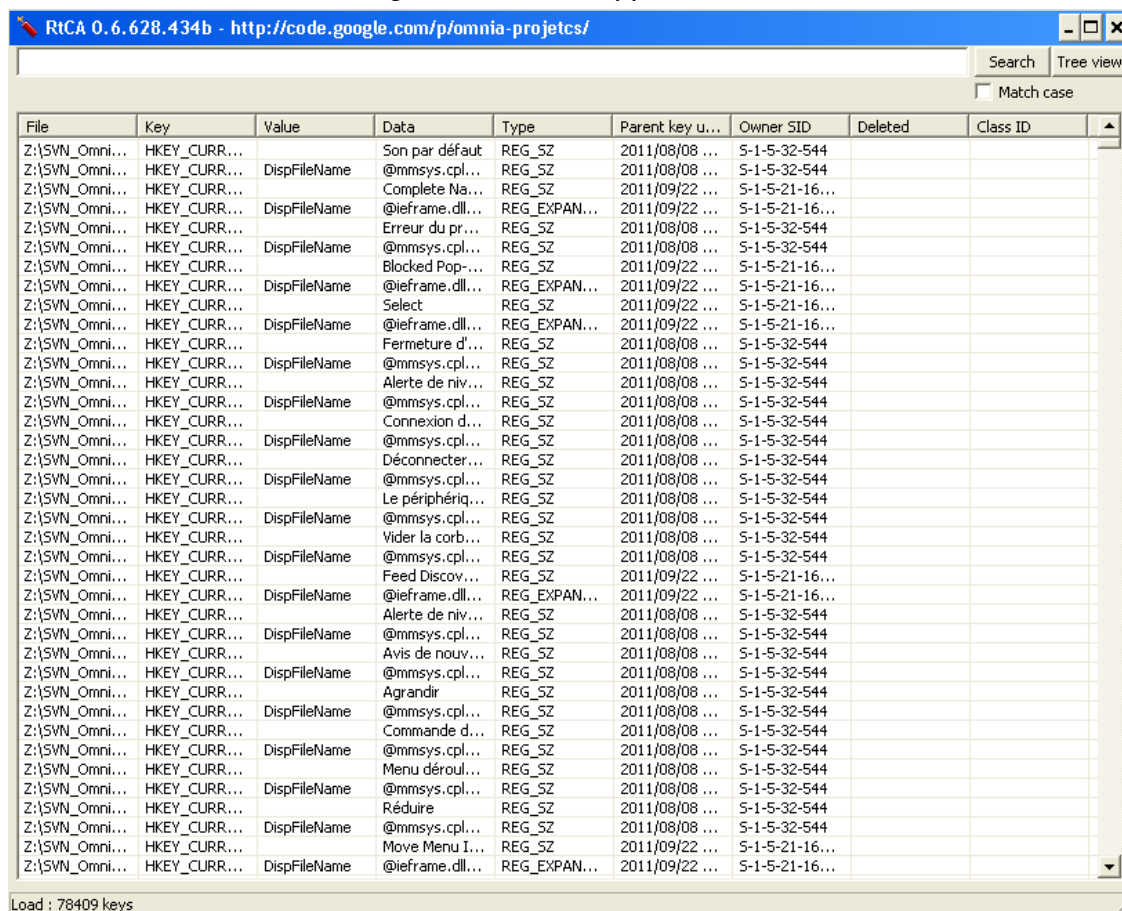
### Tools->Registry explorer

Un fois exécutée, l'interface demande la liste des fichiers de registre à utiliser :



Le **Recovery mode** permet de rechercher les clés de registre effacées. Il est un peu moins rapide que le mode normal.

Une fois les ruches utiles chargées, la fenêtre apparaît :



La zone de notification informe sur le nombre de clés chargée depuis les fichiers.

Les informations sont triées en colonne :

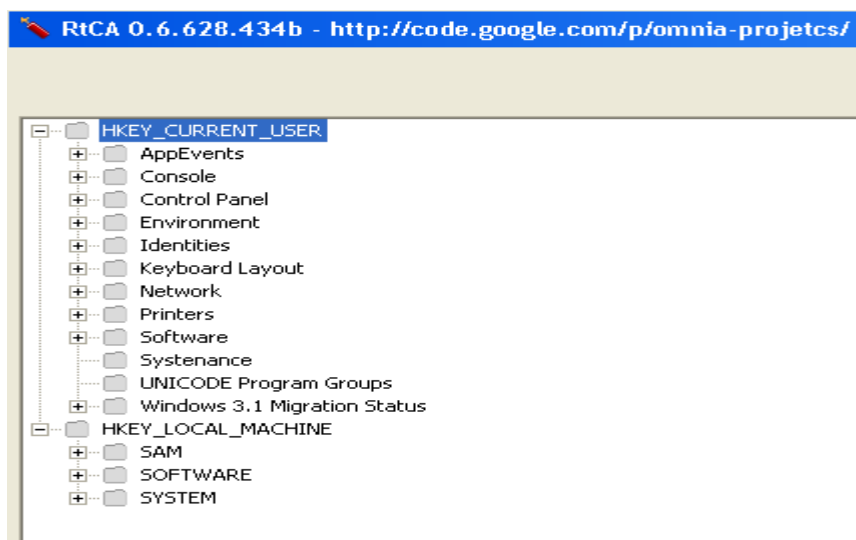
- **File** (Chemin du fichier de registre brute chargé)
- **Key** (Clé de registre correspondante)
- **Value** (Nom de la valeur)
- **Data** (Données contenues dans la valeur)
- **Type** (Format des données)
- **Parent key update** (Date de dernière modification de la clé père de la valeur sur le créneau horaire +0 : UTC)
- **Owner SID** (SID du propriétaire de la clé. Par défaut le propriétaire est celui qui a créé la clé)
- **Deleted** (Indique si cette clé et valeur ont été récupérées)
- **Class ID** (Affiche l'identifiant de la clé s'il existe)

La zone de texte permet d'effectuer des recherches sur l'ensemble des champs présents dans la liste. La case **Match case** permet de prendre en compte les majuscules lors de la recherche.

**Depuis cette interface, un menu est disponible :**

- **Save view/Selection** (Permet de sauvegarder en CSV/XML/HTML les résultats visibles ou sélectionnés)
- **Select all line in search** (Permet lors d'une recherche de sélectionner d'un coup tous les éléments en rapport avec la recherche. Permettant une sauvegarde de la sélection)
- **Open path** (Permet d'ouvrir le répertoire qui contient le fichier de registre brute ouvert)
- **Copy the line to clipboard/ copy to clipboard** (Permet comme sur toute l'application de copier dans le presse papier la ligne sélectionnée ou une case précise)

L'autre vue (Bouton **Tree view** en haut à droite de la fenêtre), permet d'afficher les résultats sous forme d'arborescence :



Depuis cette interface un clic droit sur une clé permet de copier dans le presse papier la clé complète.

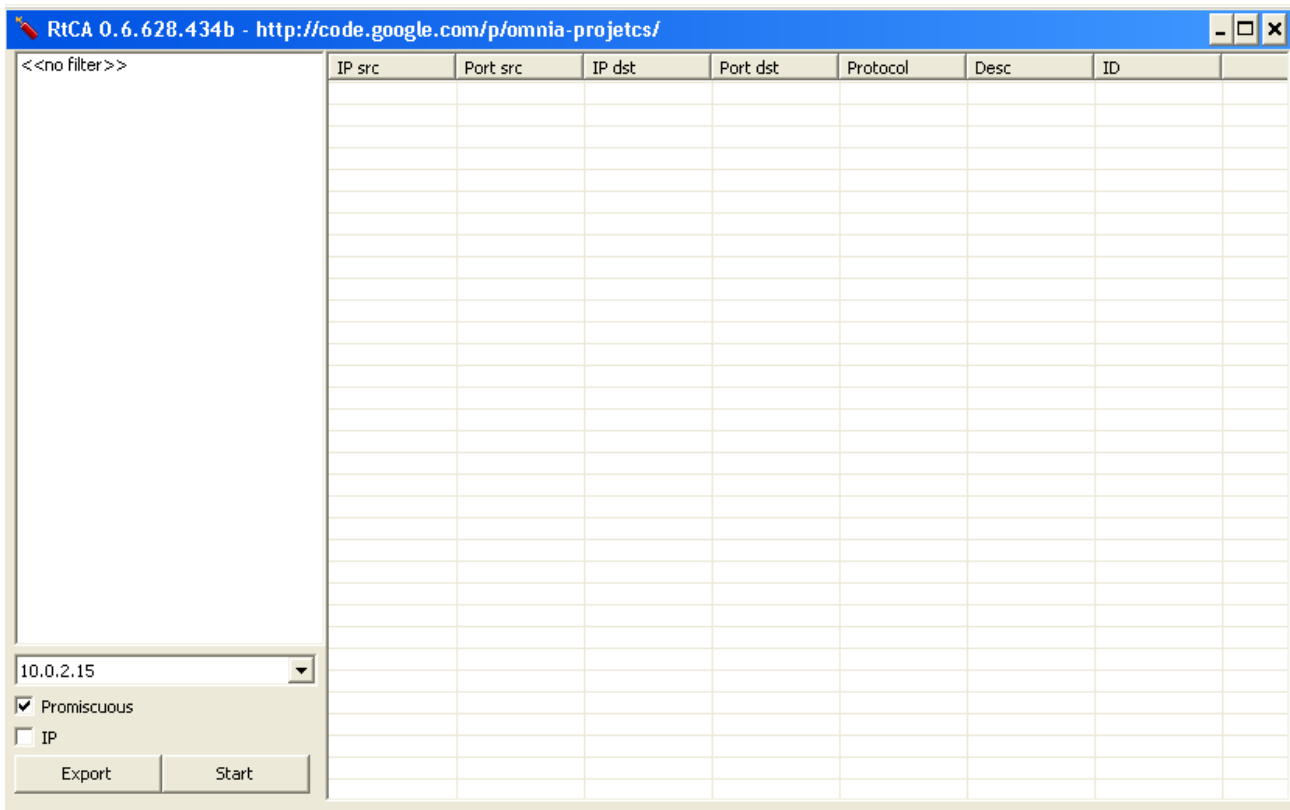
## 4.5. Network live capture

Cet utilitaire a pour objectif de permettre une capture rapide d'éléments sans nécessiter l'installation de programmes sur la machine. Il utilise des privilèges d'administration afin d'obtenir les requêtes RAW passant sur le réseau.

Cette capture n'a que pour but de faciliter une investigation en live sans possibilité de s'interfacer sur le réseau.

Il peut être affiché à partir de la fenêtre principale et du menu :

**Tools->Network live capture (RAW socket)**




Le fonctionnement est assez équivalent à Wireshark en beaucoup plus simple.

Dans un premier temps il est nécessaire de sélectionner la carte réseau présentée ici par une liste d'IP. Puis de sélectionner **Promiscuous** afin d'avoir l'ensemble des paquets sur le réseau (peut poser problème sur des cartes en Wifi/Bluetooth) et d'appuyer sur le bouton **Start**,

Ensuite, les résultats sont colorés en fonction du type de protocole UDP/TCP.

La zone de gauche se remplit au fur et à mesure avec les filtres par défaut qu'il est possible de sélectionner pour un affichage instantané.

Exemple de résultat :


**RtCA 0.6.628.434b - http://code.google.com/p/omnia-projects/**

<<no filter>>

00443/TCP https

00080/TCP http

00053/UDP dns

IP src	Port src	IP dst	Port dst	Protocol	Desc	ID
172.16.8.254	00053/UDP dns	10.0.2.15	01030/UDP	UDP/IPv4		00000052
10.0.2.15	01030/UDP	172.16.8.254	00053/UDP dns	UDP/IPv4		00000053
172.16.8.254	00053/UDP dns	10.0.2.15	01030/UDP	UDP/IPv4		00000054
10.0.2.15	01151/TCP	88.221.83.50	00080/TCP http	TCP/IPv4		00000055
10.0.2.15	01151/TCP	88.221.83.50	00080/TCP http	TCP/IPv4		00000056
88.221.83.50	00080/TCP http	10.0.2.15	01151/TCP	TCP/IPv4		00000057
10.0.2.15	01151/TCP	88.221.83.50	00080/TCP http	TCP/IPv4	GET /qsmi.aspx	00000058
88.221.83.50	00080/TCP http	10.0.2.15	01151/TCP	TCP/IPv4		00000059
88.221.83.50	00080/TCP http	10.0.2.15	01151/TCP	TCP/IPv4	HTTP/1.1 200 C	00000060
88.221.83.50	00080/TCP http	10.0.2.15	01151/TCP	TCP/IPv4	/Text> <instrum	00000061
10.0.2.15	01151/TCP	88.221.83.50	00080/TCP http	TCP/IPv4		00000062
88.221.83.50	00080/TCP http	10.0.2.15	01151/TCP	TCP/IPv4	amp;pq=ramp;js	00000063
10.0.2.15	01151/TCP	88.221.83.50	00080/TCP http	TCP/IPv4		00000064
10.0.2.15	01152/TCP	88.221.83.50	00080/TCP http	TCP/IPv4		00000065
10.0.2.15	01152/TCP	88.221.83.50	00080/TCP http	TCP/IPv4		00000066
88.221.83.50	00080/TCP http	10.0.2.15	01152/TCP	TCP/IPv4		00000067
10.0.2.15	01152/TCP	88.221.83.50	00080/TCP http	TCP/IPv4	GET /qsmi.aspx	00000068
88.221.83.50	00080/TCP http	10.0.2.15	01152/TCP	TCP/IPv4		00000069
88.221.83.50	00080/TCP http	10.0.2.15	01152/TCP	TCP/IPv4	HTTP/1.1 200 C	00000070
88.221.83.50	00080/TCP http	10.0.2.15	01152/TCP	TCP/IPv4	;sc=0-3amp;sp	00000071
10.0.2.15	01152/TCP	88.221.83.50	00080/TCP http	TCP/IPv4		00000072
88.221.83.50	00080/TCP http	10.0.2.15	01152/TCP	TCP/IPv4	239600 </instru	00000073
10.0.2.15	01153/TCP	204.79.197.201	00080/TCP http	TCP/IPv4		00000074
10.0.2.15	01153/TCP	204.79.197.201	00080/TCP http	TCP/IPv4		00000075
204.79.197.201	00080/TCP http	10.0.2.15	01153/TCP	TCP/IPv4		00000076
10.0.2.15	01153/TCP	204.79.197.201	00080/TCP http	TCP/IPv4	GET /search?q=	00000077
204.79.197.201	00080/TCP http	10.0.2.15	01153/TCP	TCP/IPv4		00000078
10.0.2.15	01152/TCP	88.221.83.50	00080/TCP http	TCP/IPv4		00000079
204.79.197.201	00080/TCP http	10.0.2.15	01153/TCP	TCP/IPv4	HTTP/1.1 200 C	00000080
204.79.197.201	00080/TCP http	10.0.2.15	01153/TCP	TCP/IPv4		00000081
10.0.2.15	01153/TCP	204.79.197.201	00080/TCP http	TCP/IPv4		00000082
204.79.197.201	00080/TCP http	10.0.2.15	01153/TCP	TCP/IPv4		00000083
204.79.197.201	00080/TCP http	10.0.2.15	01153/TCP	TCP/IPv4		00000084

10.0.2.15

☒ Promiscuous
 ☐ IP

Export

Stop

Les données sont représentées en colonnes :

- **IP src**
- **Port src** (avec le protocole TCP/UDP et la résolution du service)
- **IP dst**
- **Port dst** (avec le protocole TCP/UDP et la résolution du service)
- **Protocol**
- **Desc** (La zone ASCII passant dans le trames réseau)
- **ID** (Le numéro de trame reçus, pour l'ordre)

Un clic droit sur une trame permet d'obtenir le menu de filtrage et de sauvegarde du résultat :

10.0.2.15	01154/TCP	204.79.197.201	00080/TCP http
204.79.197.201	00080/TCP http	10.0.2.15	01154/TCP
204.79.197.201	00080/TCP http		Filter by source IP
10.0.2.15	01154/TCP		Filter by destination IP
204.79.197.201	00080/TCP http		
204.79.197.201	00080/TCP http		Filter by source port
10.0.2.15	01154/TCP		Filter by destination port
204.79.197.201	00080/TCP http		
204.79.197.201	00080/TCP http		Follow TCP/UDP stream
10.0.2.15	01154/TCP		
204.79.197.201	00080/TCP http		Save view
204.79.197.201	00080/TCP http		Save Selection
10.0.2.15	01154/TCP		

L'option **Follow TCP/UDP stream** permet d'obtenir une vue d'une session :

```
Information
urchin.com,youtu.be,
youtube.com,youtubeducation.com0h00+00000000\0Z0+00+0000000+0http://pki.google.com/GI
00000000000

[88.221.83.50:80->10.0.2.15:1151]TCP000000060
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Vary: Accept-Encoding
X-UA-Compatible: IE=7
P3P: CP="NON UNI COM NAV STA LOC CURa DEVa PSAa PSDa OUR IND"
Content-Length: 1272
Date: Mon, 17 Nov 2014 15:53:19 GMT
Connection: keep-alive
Set-Cookie: _SS=SID=4A9A1E6EDE334278A1B78115300052A6; domain=.bing.com; path=/
Set-Cookie: SRCHUID=V=2&GUID=F834535CE49C4935A9073139FFFD3D91; expires=Wed, 16-Nov-2016

<?xml version="1.0" encoding="utf-8" ?><?pageview_candidate?><SearchSuggestion xmlns="h

[88.221.83.50:80->10.0.2.15:1151]TCP000000061
/Text><instrumentation>qs=AS
```

En cochant la case IP, on obtient la liste des IP identifiées lors des échanges ainsi que les protocoles et OS identifiés:

IP	Name	TTL	OS	Protocol
173.194.40.184		064	Linux	TCP/IPv4
10.0.2.15		128	Windows	TCP/IPv4
173.194.40.183		064	Linux	TCP/IPv4
173.194.45.56				TCP/IPv4

Un double clic sur la ligne permet d'obtenir un résultat complet de la trame (extrait ici) :

```
Information
[10.0.2.15:1153->204.79.197.200:80] 000000077
[IPV4 HEADER]
ip_header_len: 20
ip_version: 4
ip_tos: 0
ip_total_length: 16899
ip_id: 10503
ip_reserved_zero: 0
ip_dont_fragment: 0
ip_more_fragment: 0
ip_frag_offset: 64
ip_ttl: 128
ip_protocol: 6
ip_srcaddr: 10.0.2.15
ip_destaddr: 204.79.197.200

[TCP]
source_port: 33028
dest_port: 20480
```

Enfin, une sauvegarde total ou de la sélection est possible dans les format CSV/XML/HTML pour les informations de base. Pour obtenir la totalité des trames, seul un export en HTML est possible.



## 4.6. Decode date

Le décodeur de date peut être affiché à partir de la fenêtre principale et du menu : **Tools->Decode date**

RtCA 0.6.628.434b - <http://code.google.com/p/o...>

Hex -> Date UTC+00:00

95862000 Dec -> Date

HEX : 5B6BCF0 DEC : 95862000

FileTime/Windows 64 bit (Little Endian) : 1601/01/01 00:00:01

FileTime/Windows 6Create : 4 bit (Big : 1601/01/01 00:00:09

time\_t Unix 32 bit (Little Endian) : 1970/06/07 07:57:15

time\_t Unix 32 bit (Big Endian) : 1973/01/14 12:20:00

Windows NT Time : 2009/04/22 19:26:23

Firefox : 1970/01/01 00:01:35

Unix Milisecond/Android : 1970/01/02 02:37:42

MAC Absolute Time : 2004/01/15 12:20:00

HFS/HFS+ 32 bit (Big Endian) :

HFS/HFS+ 32 bit (Little Endian) :

L'ensemble des dates possibles, du format hexadécimal et décimal sont générés après :

- Sélection du format de date UTC dans la liste à la droite de l'interface
- En remplissant la zone depuis une valeur hexadécimale ou décimale et en appuyant sur le bouton correspondant.

Tous les résultats peuvent être copiés/collés.

## 4.7. Hexa reader

Le lecteur hexadécimal peut être affiché à partir de la fenêtre principale et du menu : **Tools->Hexa reader**

RtCA 0.6.628.434b - <http://code.google.com/p/omnia-projets/>

Stop Close

Type Data

File: Z:\SVN\_Omnia\RtCA\DEV\XP2\Registry\...

Size: 108298240 (10Mo)(0x454000)

SHA256: 061bd70ded6ad9e1d38a071660dea48d59a7

Type: System\Windows Registry (DAT)

Create: 2014/11/17 16:27:55

Last update: 2014/11/17 16:20:07

Last access: 2014/11/17 16:20:07

ACL Owner: ()

ACLs: []

Product Name: ...

File Version: ...

Company Name: ...

File Descripti...

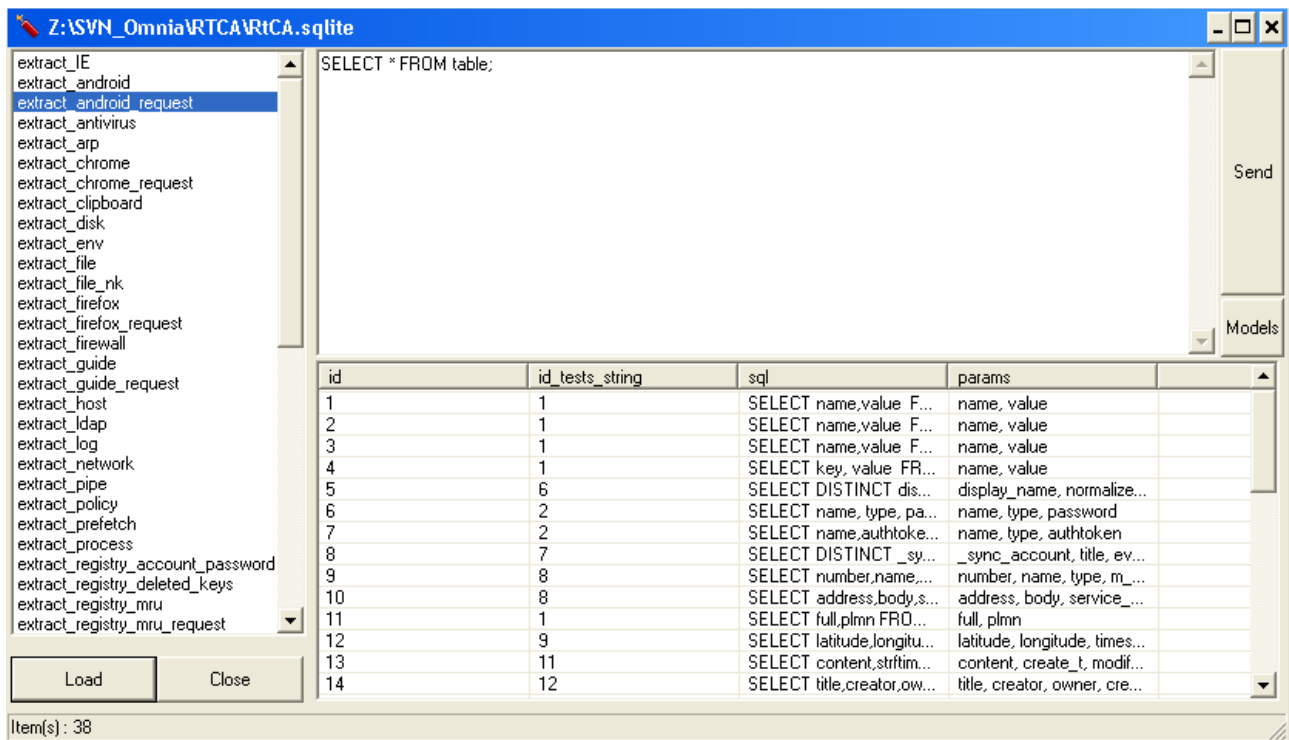
Unicode Hexa Search/Next

Une ligne des résultats peut être copier dans le presse papier en cas de clic droit dessus. Un module de recherche en ASCII/UNICODE/HEXA est disponible en bas à gauche de la page. Il ne différencie pas les minuscules des majuscules.



## 4.8. SQLITE Editor

L'éditeur SQLite être affiché à partir de la fenêtre principale et du menu : **Tools->SQLITE Editor**



### Fonctionnalités :

Le chargement et la fermeture de fichier SQLite est effectuée à partir des boutons **Load** et **Close**.

Une fois un fichier chargé, la liste des tables contenues dans le fichier sont affichées sur la partie de gauche. La sélection d'une table entraîne l'affichage de son contenu dans la partie de droite.

Le double clic sur un enregistrement permet son affichage dans une fenêtre permettant la sélection du texte.

Le tri par colonne est possible en sélectionnant l'entête de la colonne.

La dernière zone située en haut permet l'exécution direct de requêtes sur la base. Le bouton **Send** permettant l'envoi de la requête.

En guise d'aide, le bouton **Models** permet la création de requêtes simples.

Enfin, en cas d'erreur ou de réussite la zone de notification en bas de la fenêtre informe de l'état.

## 4.9. Global analyser

L'analyseur de session global peut être affiché à partir de la fenêtre principale et du menu : **Tools->Global analyser**

La première tâche à faire est de sélectionner dans l'interface en haut à gauche la liste des sessions à prendre en compte pour l'analyse, ainsi que les thèmes (Files, Audits logs, etc.), puis de faire **Load**.

Date	Origine	Source	Info	Description	Owner/User	SID	Session
2014/11/13...	start_date	Process	[pid:00540...	\SystemR...	BUILTIN\...	S-1-5-32-544	2014/11/1...
2014/11/13...	start_date	Process	[pid:00588...	C:\WIND...	BUILTIN\...	S-1-5-32-544	2014/11/1...
2014/11/13...	start_date	Process	[pid:00612...	winlogon.e...	BUILTIN\...	S-1-5-32-544	2014/11/1...
2014/11/13...	start_date	Process	[pid:00656...	C:\WIND...	BUILTIN\...	S-1-5-32-544	2014/11/1...
2014/11/13...	start_date	Process	[pid:00668...	C:\WIND...	BUILTIN\...	S-1-5-32-544	2014/11/1...
2014/11/13...	start_date	Process	[pid:00840...	system32\...	BUILTIN\...	S-1-5-32-544	2014/11/1...
2014/11/13...	start_date	Process	[pid:00908...	C:\WIND...	BUILTIN\...	S-1-5-32-544	2014/11/1...
2014/11/13...	start_date	Process	[pid:00984...	C:\WIND...	BUILTIN\...	S-1-5-32-544	2014/11/1...
2014/11/13...	start_date	Process	[pid:01092...	C:\WIND...	BUILTIN\...	S-1-5-32-544	2014/11/1...
2014/11/13...	start_date	Process	[pid:01092...	C:\WIND...	BUILTIN\...	S-1-5-32-544	2014/11/1...
2014/11/13...	start_date	Process	[pid:01112...	C:\WIND...	AUTORIT...	S-1-5-20	2014/11/1...
2014/11/13...	start_date	Process	[pid:01112...	C:\WIND...	AUTORIT...	S-1-5-20	2014/11/1...
2014/11/13...	start_date	Process	[pid:01384...	C:\WIND...	BUILTIN\...	S-1-5-32-544	2014/11/1...
2014/11/13...	start_date	Process	[pid:01448...	"C:\Progra...	BUILTIN\...	S-1-5-32-544	2014/11/1...
2014/11/13...	start_date	Process	[pid:01484...	C:\WIND...	AUTORIT...	S-1-5-19	2014/11/1...
2014/11/13...	start_date	Process	[pid:01484...	C:\WIND...	AUTORIT...	S-1-5-19	2014/11/1...
2014/11/13...	start_date	Process	[pid:01752...	C:\WIND...	BUILTIN\...	S-1-5-32-544	2014/11/1...
2014/11/13...	start_date	Process	[pid:00428...	C:\WIND...	DEV\XP2\...	S-1-5-21-1...	2014/11/1...
2014/11/13...	start_date	Process	[pid:00512...	"C:\WIND...	DEV\XP2\...	S-1-5-21-1...	2014/11/1...
2014/11/13...	start_date	Process	[pid:00560...	"C:\WIND...	DEV\XP2\...	S-1-5-21-1...	2014/11/1...
2014/11/13...	start_date	Process	[pid:00576...	"C:\Progra...	DEV\XP2\...	S-1-5-21-1...	2014/11/1...
2014/11/13...	start_date	Process	[pid:01936...	"C:\Progra...	DEV\XP2\...	S-1-5-21-1...	2014/11/1...
2014/11/13...	start_date	Process	[pid:02004...	"cmd.exe"...	DEV\XP2\...	S-1-5-21-1...	2014/11/1...
2014/11/14...	start_date	Process	[pid:00184...	"C:\Progra...	DEV\XP2\...	S-1-5-21-1...	2014/11/1...
2014/11/15...	start_date	Process	[pid:01736...	"Z:\SVN_...	DEV\XP2\...	S-1-5-21-1...	2014/11/1...

L'affichage des résultats est concentré dans trois onglets :

- **All** (Toutes les données)
- **Critical** (Tous les éléments pointés comme potentiellement critiques)
- **Log State** (Les statistique sur le nombre d'enregistrement par type d'enregistrement dans les journaux d'audit)

Il est possible de filtrer les résultats par date avec les deux zones d'intervalles en haut à droite en appuyant sur le bouton **Filter**.

Un filtre par chaîne est possible en modifiant le premier champs de recherche. Attention ce champs ne vérifie pas la différence entre les minuscules et majuscules.

Date	Origine	Source	Info	Description
2014/11/13...	start_date	Process	[pid:00588...	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows Sha
2014/11/13...	start_date	Process	[pid:00612...	winlogon.exe
2014/11/13...	start_date	Process	[pid:00656...	C:\WINDOWS\system32\services.exe
2014/11/13...	start_date	Process	[pid:00668...	C:\WINDOWS\system32\lsass.exe
2014/11/13...	start_date	Process	[pid:00908...	C:\WINDOWS\system32\svchost -k DcomLaunch
2014/11/13...	start_date	Process	[pid:00984...	C:\WINDOWS\system32\svchost -k rpcss

## 5. Et demain...

Les objectifs de RtCA n'étant pas complètement remplis, plusieurs points d'améliorations sont en cours de réflexion et développement :

- Capture et analyse de la mémoire
- Extraction des données à distance
- Prise en charge des systèmes Linux et Mac
- Analyse des données depuis une image de disque
- Capacité de récupérer les données effacées depuis une image de disque
- Ajout de nouveaux artefacts sous Windows
- Plus de stabilité, lisibilité, facilité d'analyse et rapidité d'extraction