for(e=n;s<i;c++){attitude();}

Sur environnement Microsoft Windows

Nicolas Hanteville

Il était une fois. . . les investigations forensic !

Pourquoi une investigation ?

- Doutes de malveillance interne
- Corruption de client, serveur, défacement de site. . .
- Identification des processus de malveillance
- Moyens de correction
- . . .

Il était une fois. . . les investigations forensic !

Sources d'investigations numériques :

- L'état instantané du système (mémoire, processus, sockets, fichiers ouverts. . .)
- Le système de fichiers (FAT, NTFS)
- Les journaux d'audit (Evt, Evtx et parfois log)
- La base de registre
- . . .

Système de fichiers

- **Les interactions :** dates d'accès, modification, création...
  Informations modifiables à partir d'un accès en écriture.
  Peu fiables en cas de modification de l'heure système.
  Limitées aux derniers accès, dernières modifications...

- **Les restrictions d'accès :** propriétaire, ACL, Bitlocker...
  Inutiles en cas de démarrage à partir d'un autre système d'exploitation.

- **Les attributs :** caché, protégé système, compressé, chiffré...

- **Les types de fichiers :** répertoires, fichiers, ADS (NTFS Alternative Data Stream)...

Système de fichiers : Modifier les dates en C

```
HANDLE hFile = CreateFile("fichier", GENERIC_READ|GENERIC_WRITE,
                          NULL, OPEN_EXISTING, FILE_ATTRIBUTE_NORMAL, NULL);
if (hFile != INVALID_HANDLE_VALUE)
{
  //Nouvelle date : 13 Mars 2012 08:30:00.00
  SYSTEMTIME sysTime;
  sysTime.wDay                    = 13;
  sysTime.wMonth                  = 03;
  sysTime.wYear                   = 2012;

  sysTime.wHour                   = 8;
  sysTime.wMinute                 = 30;
  sysTime.wSecond                 = 0;
  sysTime.wMilliseconds           = 0;

  //Conversion de la date pour le fichier
  FILETIME fileWriteTime, locTime;
  SystemTimeToFileTime(&sysTime, &locTime);
  LocalFileTimeToFileTime(&locTime, &fileWriteTime);

  //Appliquer au fichier
  SetFileTime(hFile,
              NULL,           /*CreationTime*/
              NULL,           /*LastAccessTime*/
              &fileWriteTime  /*LastWriteTime*/);
}
CloseHandle(hFile);
```

Système de fichiers : Outils - Windows

- McAfee/Foundstone Forensic Toolkit : en ligne de commande, il gère en plus les ACL (ACE+SID) et exporte en texte brut.

  `http://www.mcafee.com/us/downloads/free-tools/`

- Streams (Windows Sysinternals) : recherche de fichiers ADS.

  `http://technet.microsoft.com/en-us/sysinternals/bb897440.aspx`

- Dislocker (HSC) : lecture de partition bitlocker sous Linux.

  `http://www.hsc.fr/ressources/outils/dislocker/`

- Suites AccessData (payant) : système de fichiers, mémoire...

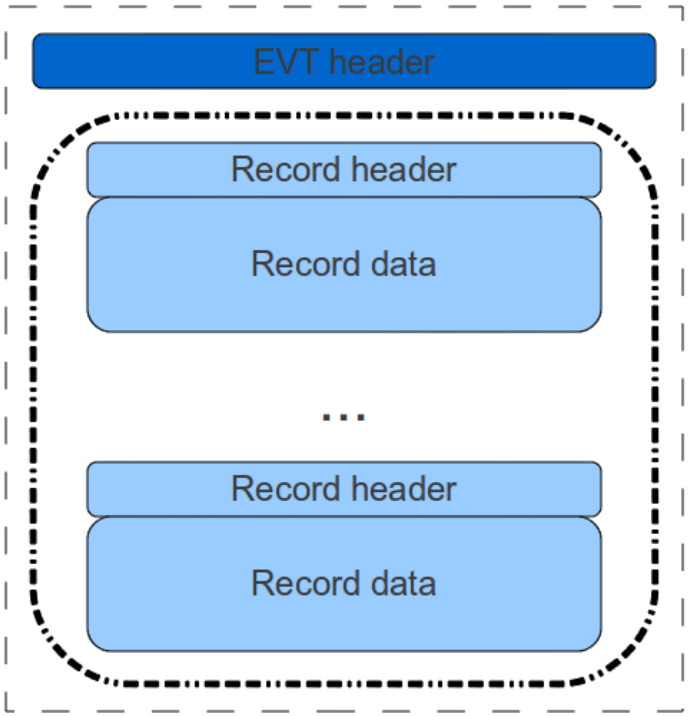
  `http://accessdata.com/products/computer-forensics`

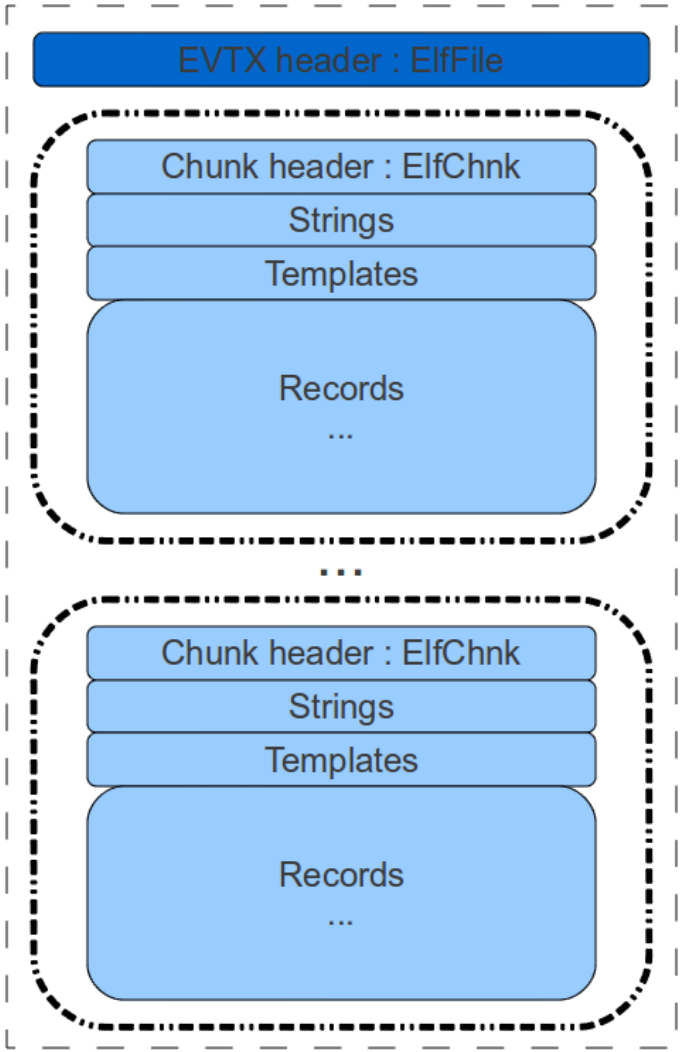
Les journaux d'audit : Formats Evt/Evtx

Evt ($<$ Vista)	Evtx ($\geq$ Vista)
Enregistrements stockés par ordre chronologique	Ordre chronologique par groupe
ID + source d'un évènement = description et format de l'enregistrement	
Plusieurs niveaux d'état/criticité	
Dates d'émission et d'écriture de l'enregistrement (soumis à l'heure système)	
Emplacement par défaut : C:\Windows\system32\config\	Emplacement par défaut : C:\Windows\system32\winevt\logs\
Format de fichier assez simple à exploiter sans les API Windows (séquentiel)	Format de fichier assez complexe à exploiter sans les API Windows (BinXML)

Nécessité d'activer des règles d'audit pour journaliser...

Les journaux d'audit : Formats Evt/Evtx





Les journaux d'audit : Identifiants intéressants

ID	Source	OS	Description
512/513	Security	$<$Vista	Windows start/stop
528/538			User Logon/Logoff
520			The system time was changed
517			The security log was cleared
4608/4609	Microsoft-Windows-Security-Auditing	$\geq$Vista	Windows start/stop
4624/4634			User Logon/Logoff
4616			The system time was changed
1102			The security log was cleared

Les journaux d'audit : Outils

- Evtx Parser : script PERL de conversion Evtx vers XML

  `http://computer.forensikblog.de/en/`

- TZWorks Windows Event Log Viewer : lecteur Evtx avec visualisation binaire

  `http://www.tzworks.net/download_links.php`

- Microsoft wevtutil (à partir de Vista) : conversion Evt vers Evtx

  wevtutil export-log source.evt target.evtx /lf

La base de registre : Présentation

Contient un grand nombre de données :

- Hardware (données non statiques)
- Système : bootkey, GPO et licences...
- Configuration : logiciels, mises à jour, réseau, services et drivers...
- Utilisateurs : liste locale des groupes, utilisateurs, hash des mots de passe
- Historiques utilisateurs : MRU, MUICache, UserAssist...
- Divers : supports externes connectés (USB), applications au démarrage...

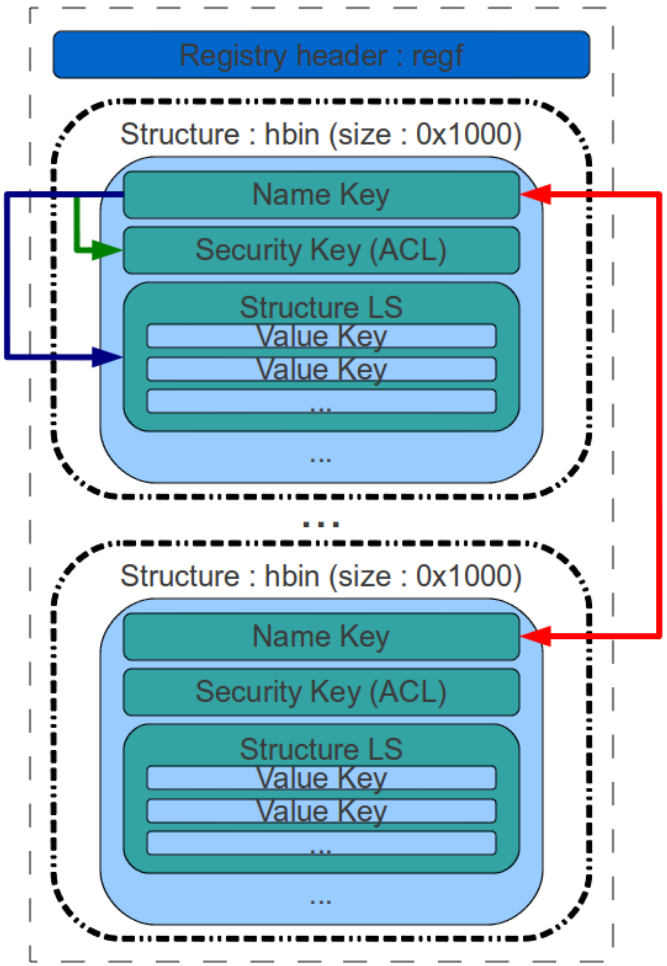
Une mine d'or pour les analyses forensic !

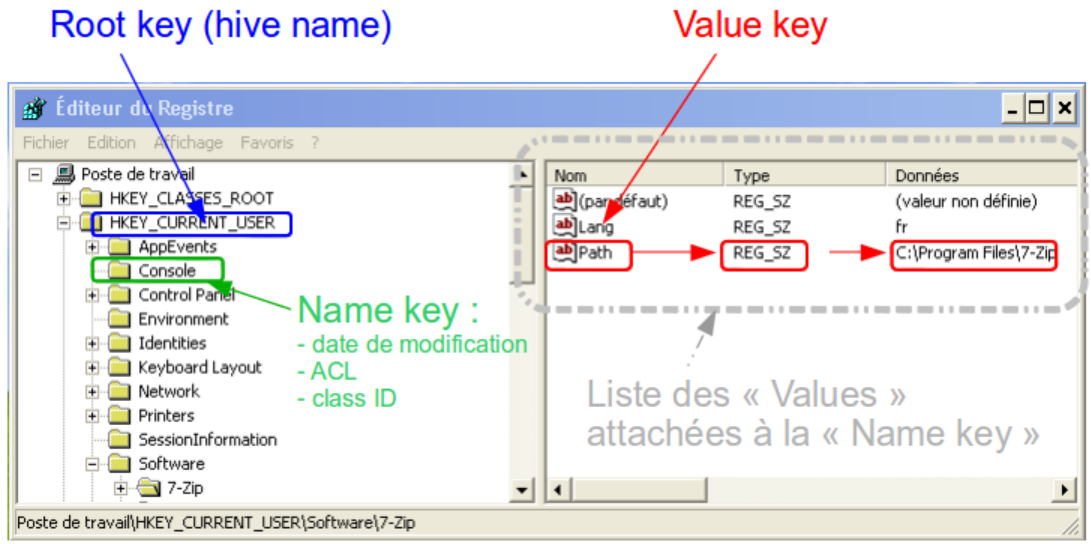
La base de registre : Présentation

Et...

- Le format binaire n'a presque pas évolué, seule la structure a évolué
- Le format binaire est un peu documenté
- Les droits appliqués par défaut sont peu restrictifs
- Droits difficiles à modifier : architecture peu documentée
- L'édition hors ligne est possible en cas de disque non chiffré
- Aucun blocage des API n'existe en GPO (hors ACL), seul Regedit peut être bloqué par une clé de registre (modifiable par tous les utilisateurs)

La base de registre : Le format





La base de registre : Les données

- **Applications au démarrage :** (HKEY_LOCAL_MACHINE et HKEY_CURRENT_USER)
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\, RunOnce, RunOnceEx
  HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Startup\, Logon, Shutdown, Logoff
  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Load\, Run, AppSetup, Shell

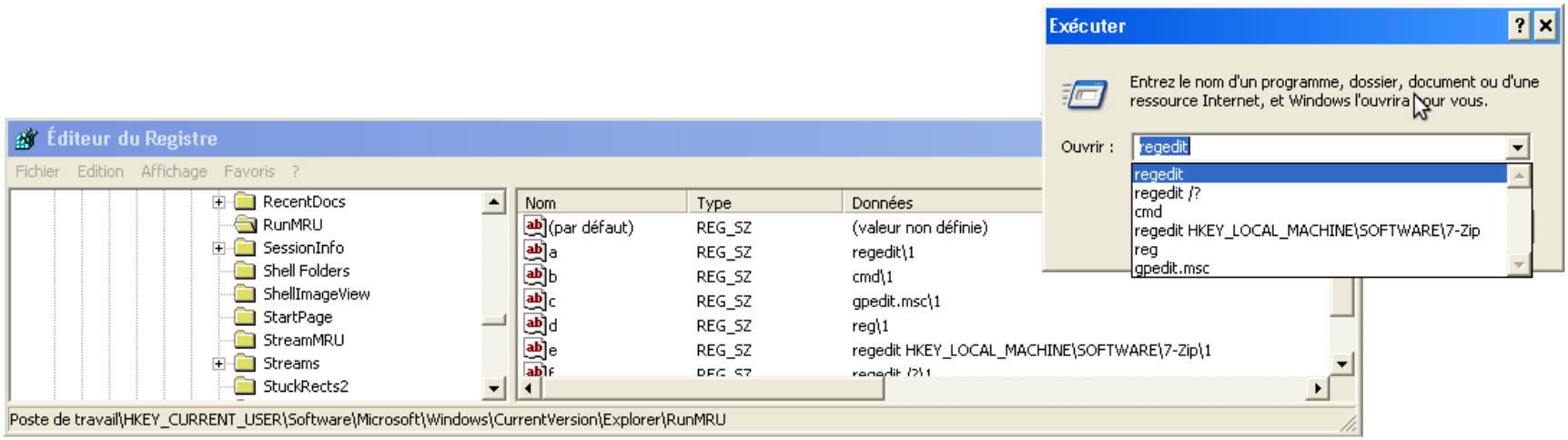
- **Services et drivers :** HKLM\SYSTEM\CurrentControlSet\Services\

- **Logiciels et mises à jour installés :**
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\Packages\
  HKLM\SOFTWARE\Microsoft\Updates\

- **Supports externes déjà connectés :** HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR\

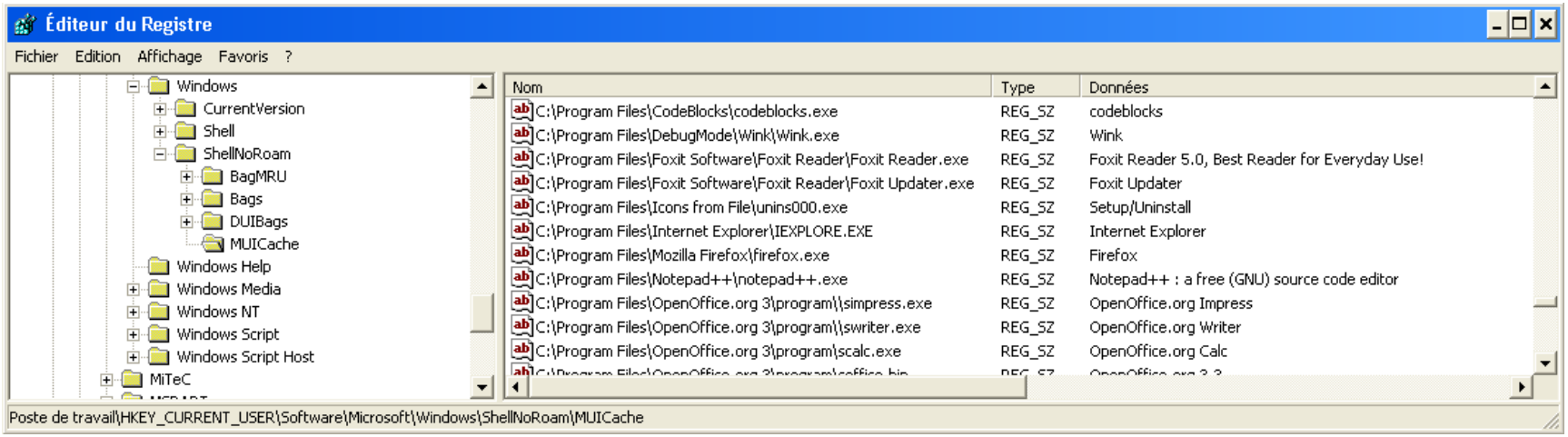
La base de registre : Les données (MRU)

- **MRU (Most Recently Use):**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\, RecentDocs, StreamMRU, ComputerDescriptions, Map Network Drive MRU, ComDlg32\LastVisitedMRU, ComDlg32\OpenSaveMRU
  HKCU\SOFTWARE\Microsoft\Search Assistant\ACMru\
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Applets*\Recent File List\
  HKCU\SOFTWARE\Microsoft\Office**\Recent File List\



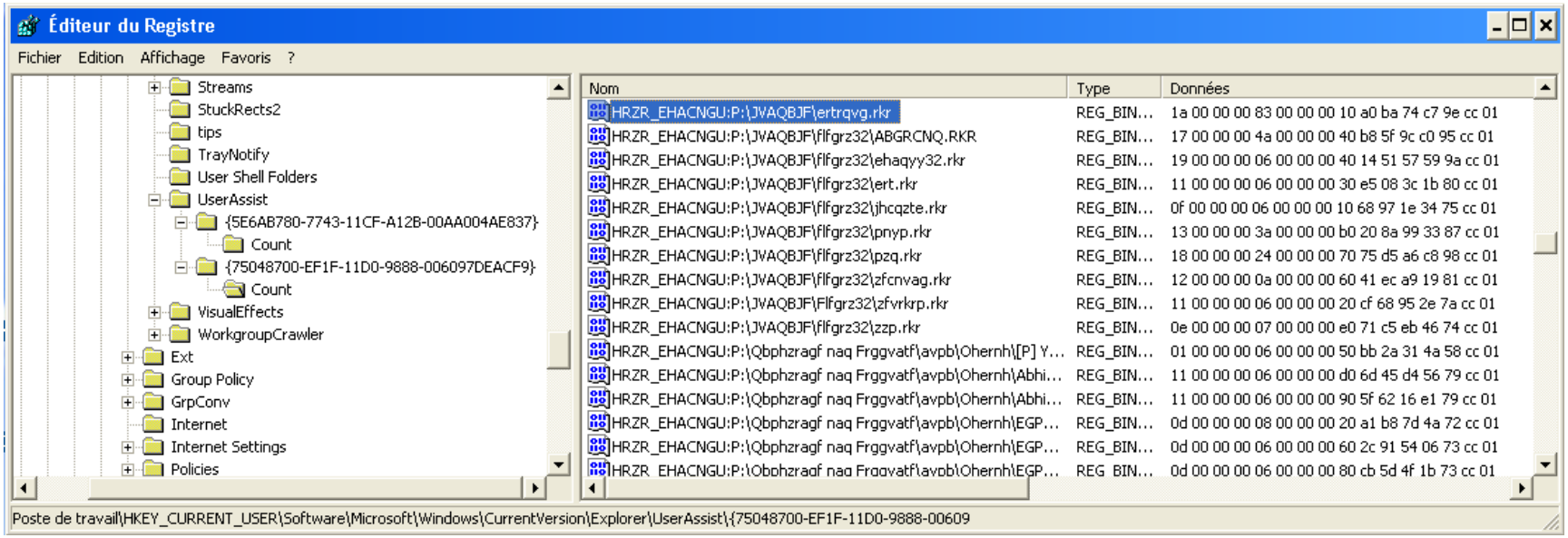
La base de registre : Les données (MUICache)

- **MUICache (Applications déjà exécutées) :**
  HKCU\SOFTWARE\Microsoft\Windows\ShellNoRoam\MUICache\
  HKCU\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MUICache\



La base de registre : Les données (UserAssist)

- **UserAssist (Applications exécutées, codées en ROT13) :**
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist*\



Path	Use count	Last GUID update	User
UEME_RUNPATH:C:\WINDOWS\regedit.exe	0x00000083	2011/11/09-11:04:50	nico ...
UEME_RUNPATH:C:\WINDOWS\system32\NOTEPAD.EXE	0x0000004a	2011/10/28-23:22:16	nico ...
UEME_RUNPATH:C:\WINDOWS\system32\calc.exe	0x0000003a	2011/10/10-10:57:36	nico ...
UEME_RUNPATH:C:\WINDOWS\system32\cmd.exe	0x00000024	2011/11/01-19:56:56	nico ...
UEME_RUNPATH:C:\WINDOWS\system32\mmc.exe	0x00000007	2011/09/16-08:55:48	nico ...
UEME_RUNPATH:C:\WINDOWS\system32\mspaint.exe	0x0000000a	2011/10/02-16:36:22	nico ...
UEME_RUNPATH:C:\WINDOWS\system32\reg.exe	0x00000006	2011/10/01-10:18:14	nico ...
UEME_RUNPATH:C:\WINDOWS\system32\rundll32.exe	0x00000006	2011/11/03-19:47:25	nico ...
UEME_RUNPATH:C:\WINDOWS\system32\wupdmgr.exe	0x00000006	2011/09/17-13:19:33	nico ...

La base de registre : Outils - Windows

Extracteurs/Éditeurs de fichiers de registre brut :

- MiTec Windows Registry Recovery : `http://www.mitec.cz`
- TZWorks Yet Another Registry Utility : `http://www.tzworks.net/download_links.php`
- Digital Forensics Framework : `http://www.digital-forensic.org`
- Regviewer : `http://sourceforge.net/projects/regviewer/`
- Registry decoder : `http://code.google.com/p/registrydecoder/`

Constat : Après plusieures années d'investigation...

- **Peu d'outil libre de corrélation de données :** système de fichiers, journaux d'audit, base de registre et données spécifiques
- **Peu d'outils d'extraction/analyse forensic globale de machine** (et souvent payants)
- **Résultats souvent trop limités**
- Finalement, beaucoup de temps dépensé pour des résultats perfectibles

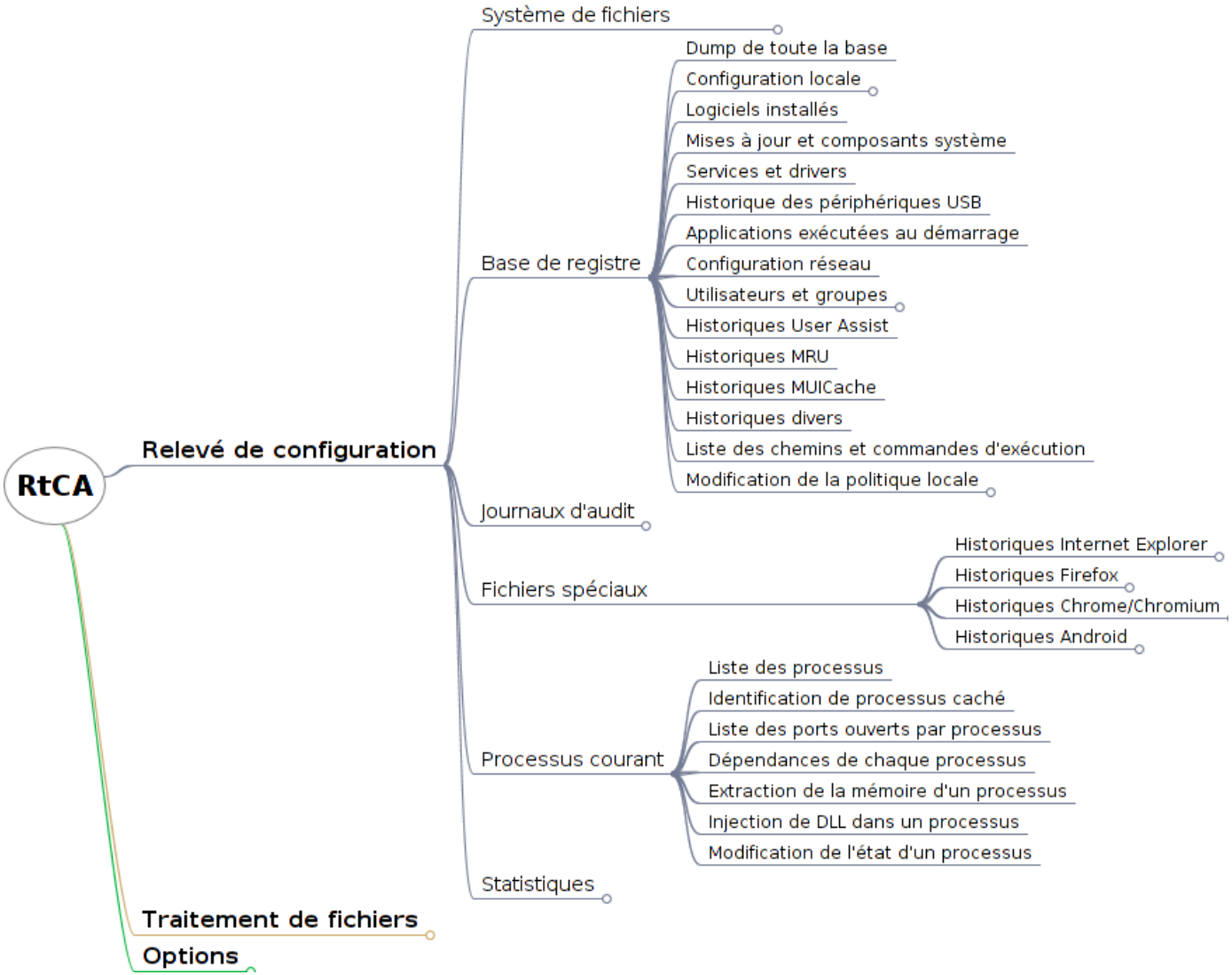
Constat Après plusieures années d'analyses Forensic...

Création d'une boîte à outils d'extraction de configuration et d'analyse forensic : RtCA

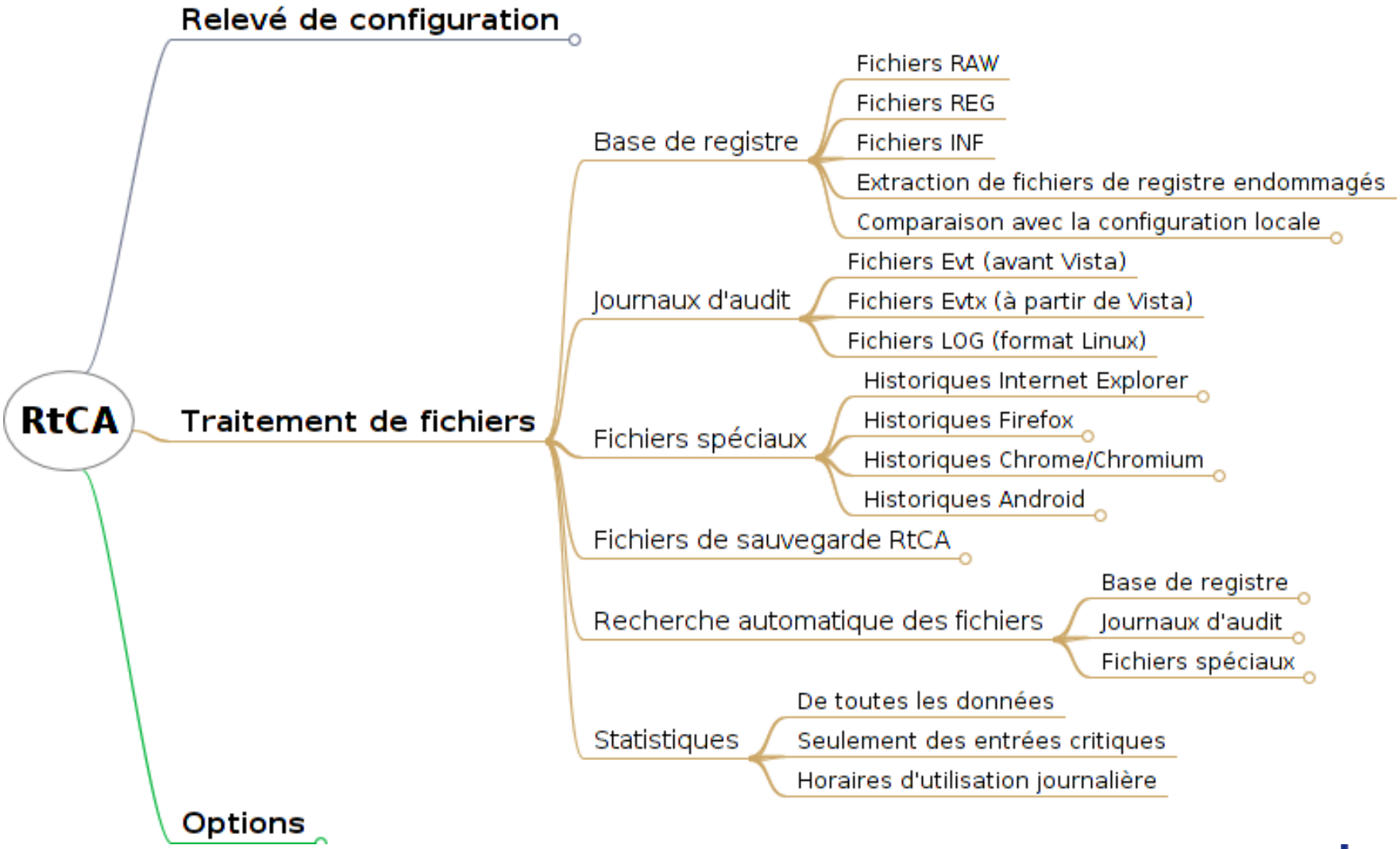
- Projet libre sous licence GPLv3
- Codé en C win32/64 compatible XP/2003/2008/7/8/Wine
- Extraction/Traitement des fichiers, des journaux d'audit, de la base de registre et certains applicatifs (navigateurs, Android...)
- Première publication *testing* en octobre 2011, encore beaucoup de travail...

`http://omni-a.blogspot.com/2011/10/rtca-v01-outil-daide-aux-analyses.html`

RtCA : Fonctionnement

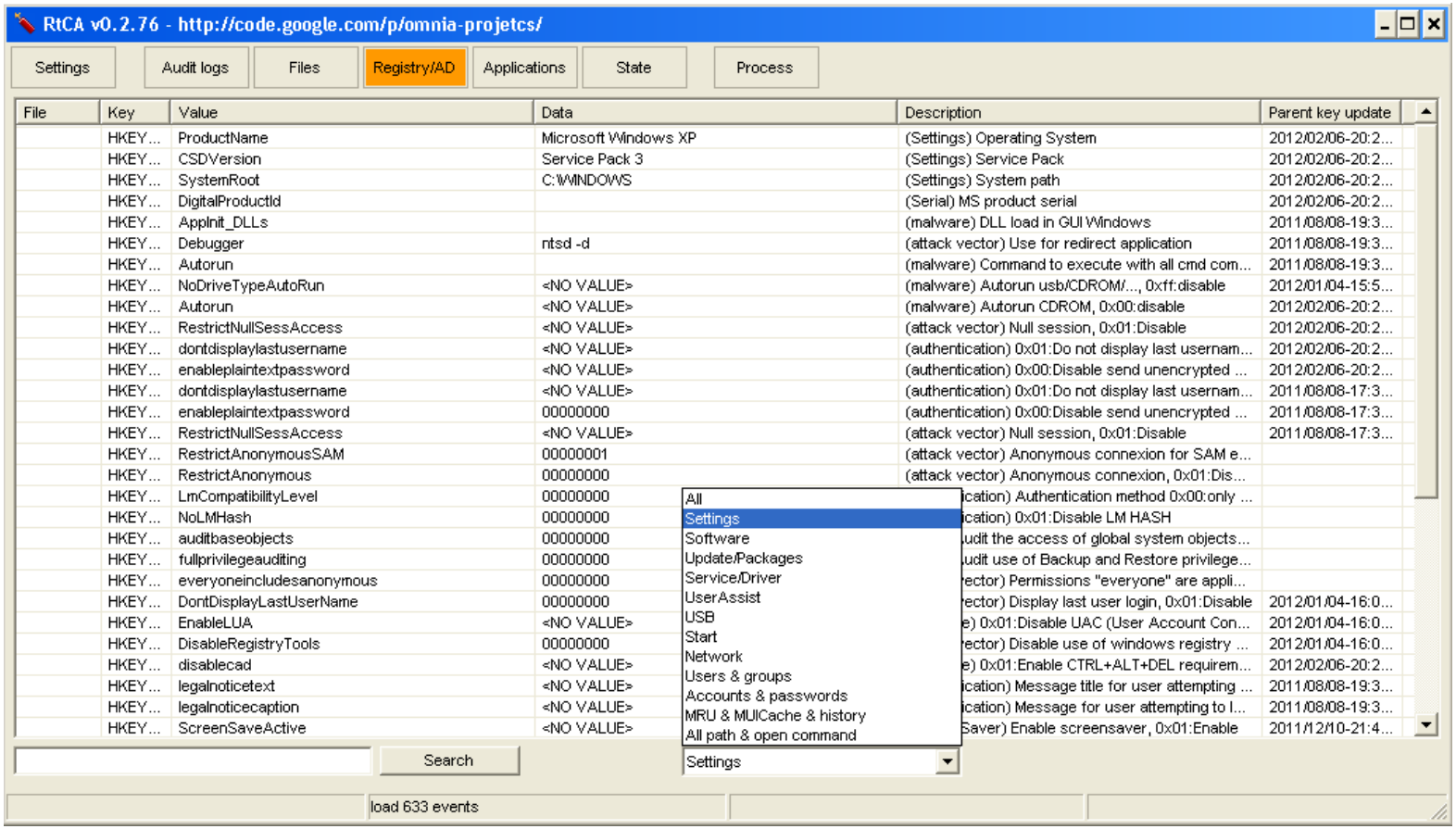


RtCA : Fonctionnement



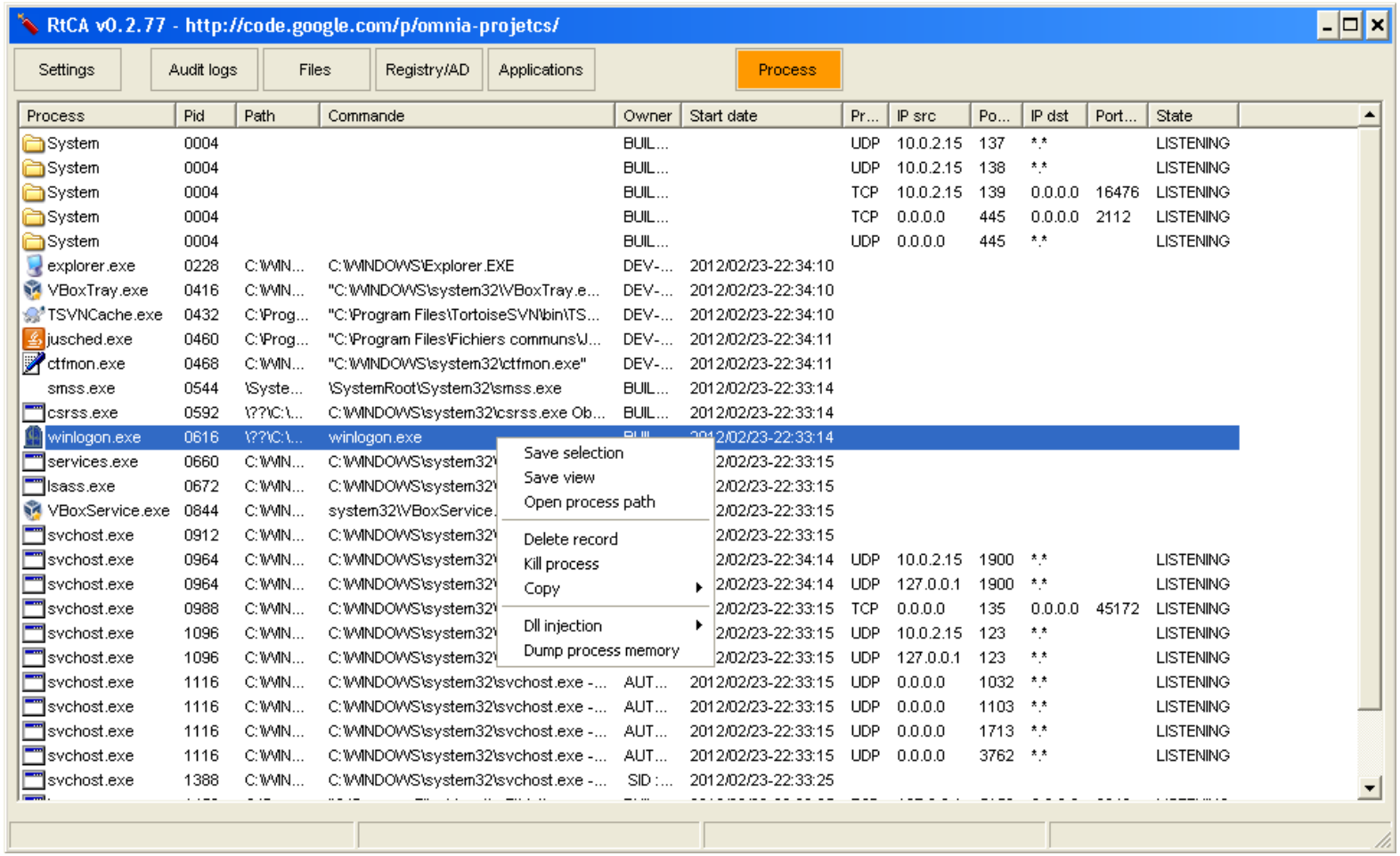
RtCA : Aperçu

Accès rapide aux informations : (outil de relevé de configuration)



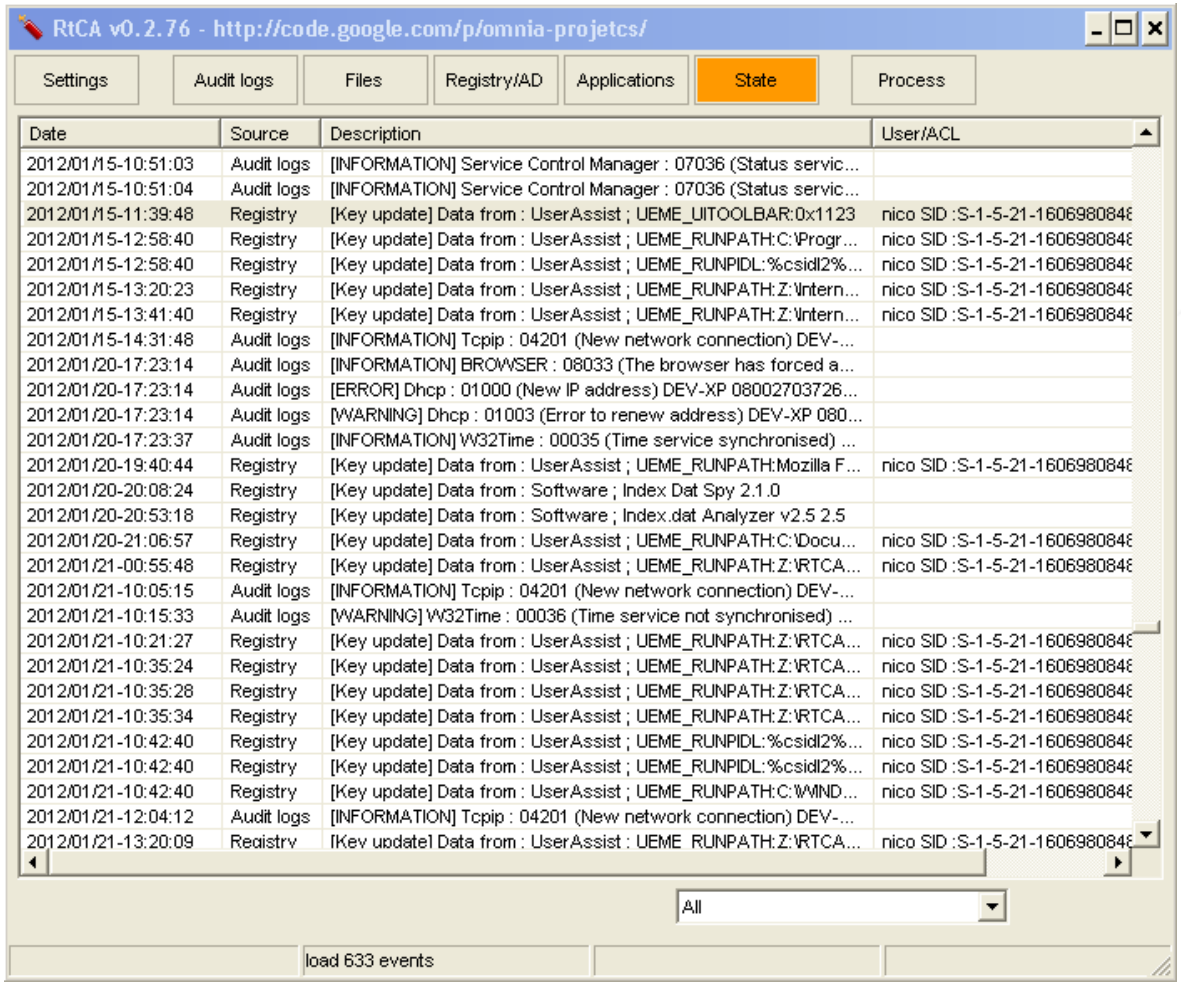
RtCA : Aperçu

État des processus :



RtCA : Aperçu

Corrélation de données :



Références

- **SANS digital forensics :**
  `http://computer-forensics.sans.org/`
- **Andreas Schuster :**
  `http://computer.forensikblog.de/en/`
- **Windows NT Registry File (REGF) format specification :**
  `http://sourceforge.net/projects/libregf/files/Documentation/`
- **Revers of SAM registry :**
  `http://www.beginningtoseethelight.org/ntsecurity/`
- **NTFS Alternate Streams :**
  `http://www.flexhex.com/docs/articles/alternate-streams.phtml`

Des questions ?

Merci d'être resté éveillé jusqu'au bout !

- **Contact :** `nicolas.hanteville(at)devoteam.com`
- **RtCA :** `http://code.google.com/p/omnia-projetcs/`