Les procédures du CERTA pour l'analyse des systèmes d'exploitation Windows

OSSIR-NT

Puteaux, le 07 mars 2005

CERTA http://www.certa.ssi.gouv.fr
Olivier Castan castan@certa.ssi.gouv.fr
certa-svp@certa.ssi.gouv.fr

Plan

- **Contexte**
- **Différences Win32/Unix pour l'analyse**
- **Description interne de NTFS et de la base de registre**
- **Outils que le CERTA développe pour NTFS, les ruches de la base de registre, les “logs” IE et les journaux d'événements**
- **NTFS et la reconstruction de disques RAID-5**
- **Procédures sur un système en fonctionnement**
- **Conclusions**

Contexte

- **Adapter les méthodes de TCT sous Windows**
- **Complexité des règles d'acquisition ⇒**
  - **Outils librement disponibles et développements internes (reactivité et capacité d'adaptation)**
  - **Documentation Internet (souvent non officielle ⇒ problème de validité)**
- **Adhésion aux principes de Brian Carrier sur le besoin de sources ouvertes**
- **Support initial (2001) des versions professionnelles : NT4 avec NTFS**
- **Orienté collecte à chaud**
- **Toujours en cours de validation/développement**

Les spécifités Windows

- **Ce que j'apprécie**
  - **Beaucoup d'objets datés avec une résolution potentielle de 100 ns !**
  - **Dates stockées en UTC**
  - **Beaucoup de structures “connues” avec des offsets prédictibles : aide à la reconstruction**
- **Ce que je déteste**
  - **Fort niveau d'abstraction entre les outils d'administration, le stockage des configurations et ce qui se passe réelement**
  - **Beaucoup de possibilité de lancer du code malveillant (BHO,...) et beaucoup de services qui interagissent (natifs, antivirus,...)**
- **Plus complexe mais plus d'informations**

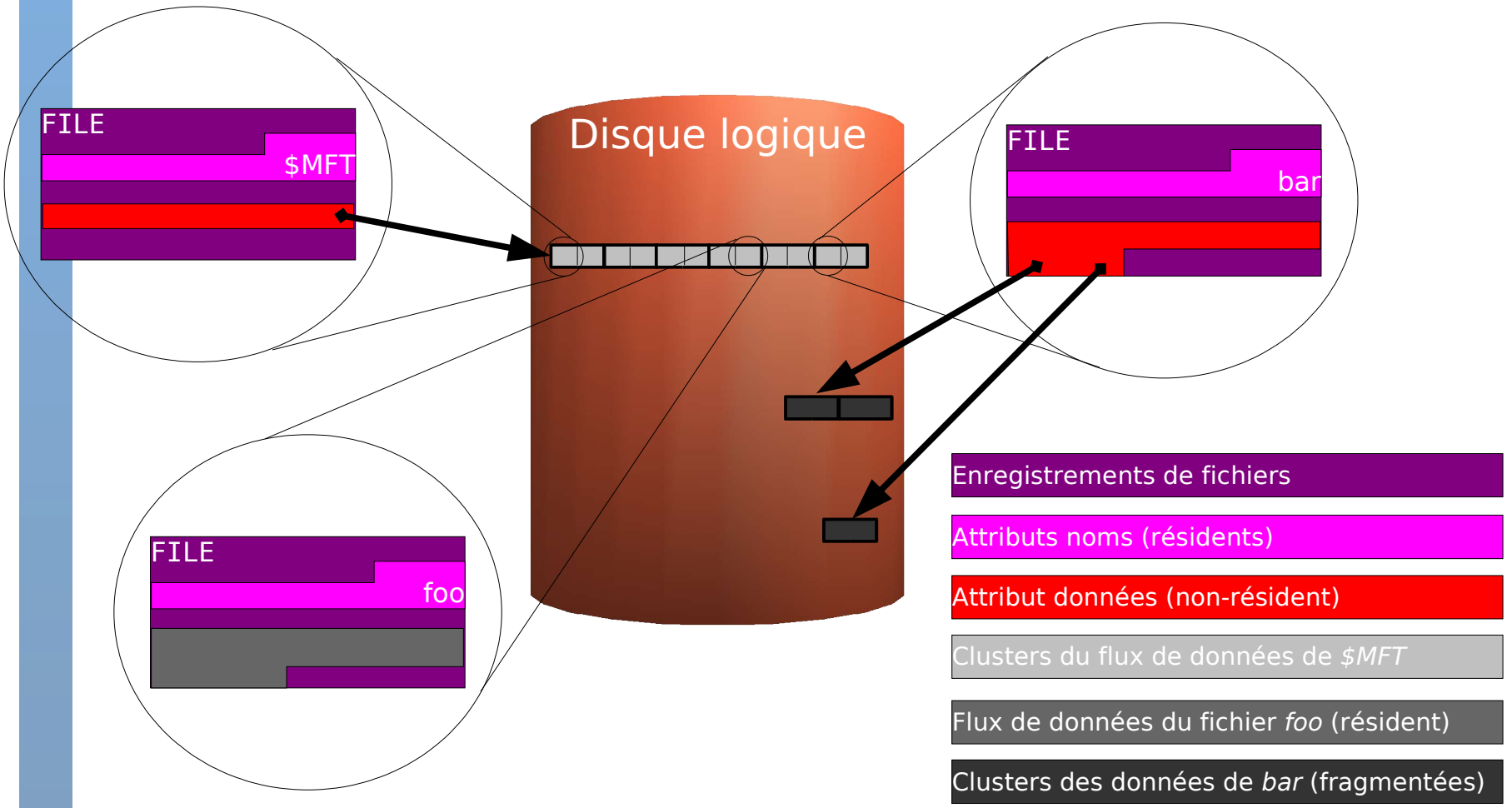
Configurations typiques

- **Serveurs**
  - **NT4 est encore présent (administration limitée à l'installation des Service Packs)**
  - **Audit pauvre par défaut**
  - **Pertes d'événements dues à la “petite” taille maximum des journaux**
- **Particuliers**
  - **Accros de l'installation de programmes...**
- **Souvent plusieurs problèmes (intrusions, “malwares”,...)**
- **Interférences des antivirus : “scans” (dates d'accès), destructions automatiques, créations d'“ADS”...**
- **Souvent des semaines entre l'activité suspecte et la collecte pour analyse**

Structures intéressantes – NTFS 1/3

- **Un fichier NTFS est une collection d'attributs**
  - **Un attribut a un type (nom, “SD”, données,...)**
  - **Plusieurs attributs du même type peuvent coexister (“ADS”, noms pour chaque espace de nommage,...)**
- **Un attribut a un en-tête (description) et un flux (contenu)**
- **Cette collection est décrite dans un enregistrement de taille constante (ou plusieurs si besoin). Le flux d'un attribut est :**
  - **Soit résident (stocké dans l'enregistrement)**
  - **Soit non-résident (l'enregistrement stocke la liste des “clusters” utilisés : “runlists”)**
- **Un enregistrement commence avec 'FILE'**
  - **Tous les enregistrements = les données du fichier *$MFT* ; *$MFT* est toujours le 1er fichier**

Structures intéressantes – NTFS 2/3



Structures intéressantes – NTFS 3/3

- **Documentation**

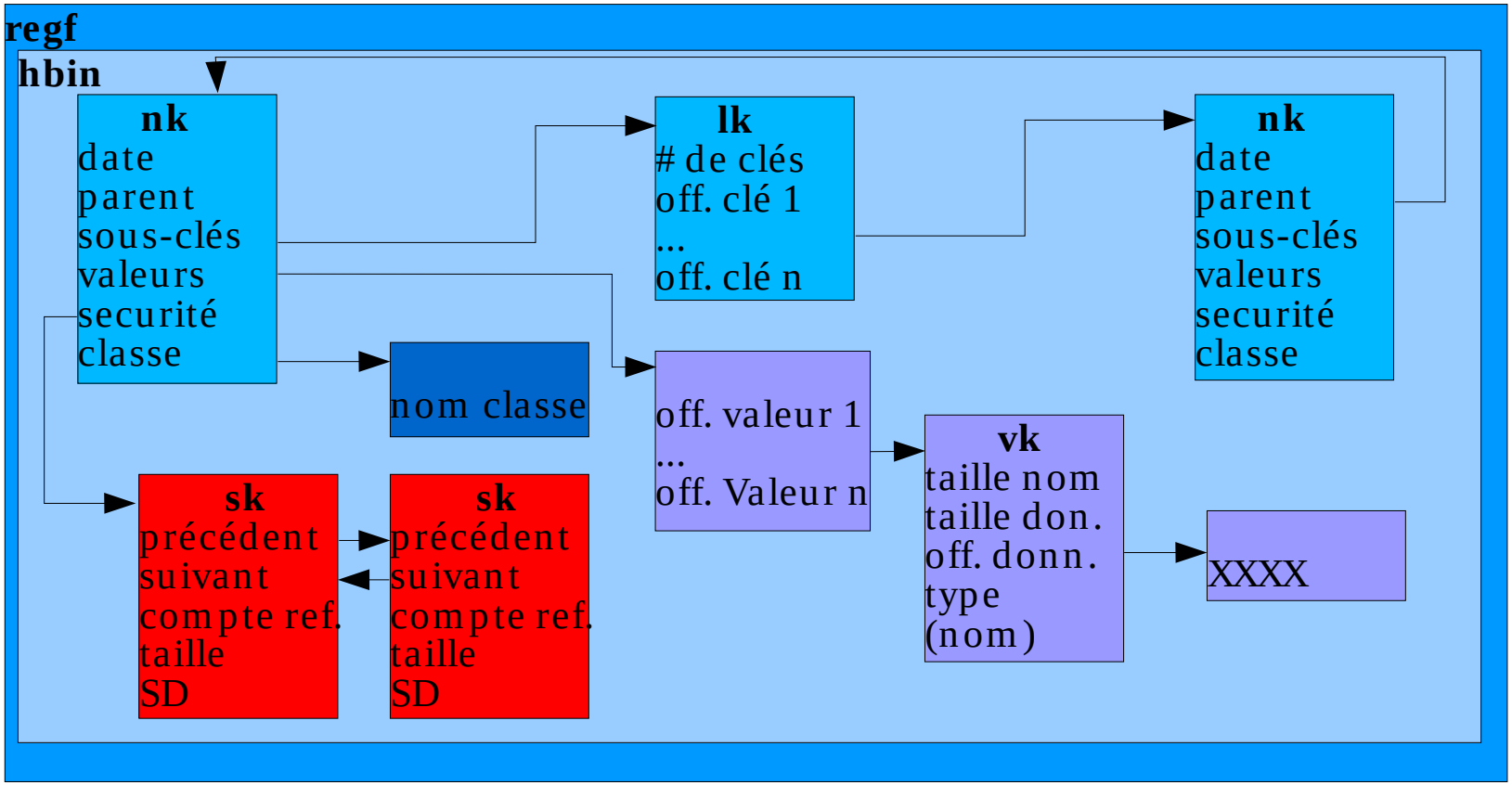
http://linux-ntfs.sf.net/ntfs/index.html

- **4 dates : création, accès, écriture et modification de l'enregistrement (la dernière ne peut être changée avec l'appel SetFileTime de l'API Win32) présentes dans 2 attributs différents (plus encore 4 autres accessibles dans les données du répertoire parent)**
- **La résolution effective peut être différente pour chaque date : aucune abérration n'est apparue en les prenant toutes en compte**

Structures intéressantes – les ruches du registre

- **Documentation**

  http://home.eunet.no/~pnordhal/ntpasswd/WinReg.txt
  http://www.beginningtoseethelight.org/ntsecurity/index.php



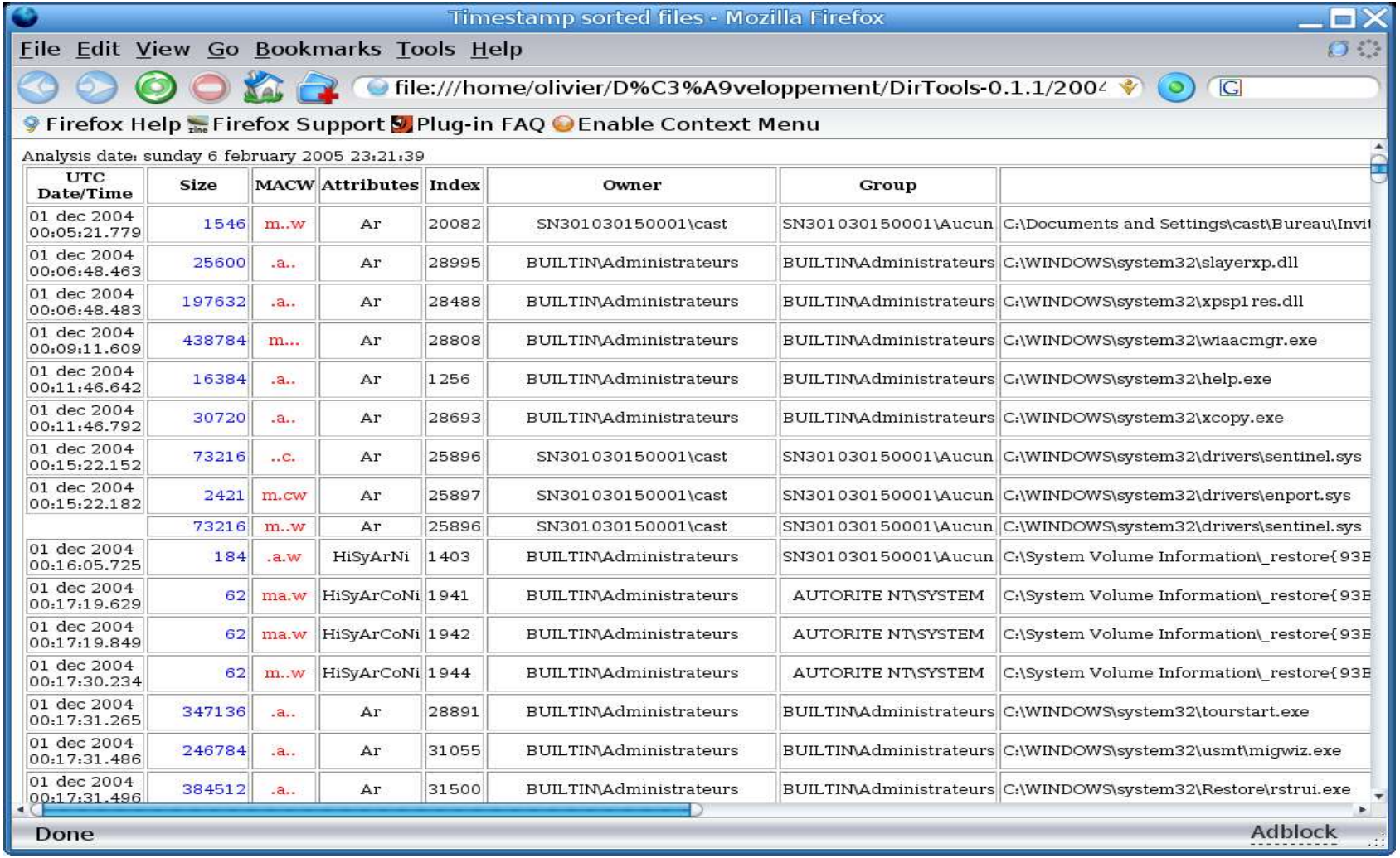
Les outils que le CERTA développe

- **Petits, en ligne de commande, filtre si possible, sortie texte formattée**
- **Dirtools : collecte les informations NT/W2K...**
  - **Lit le disque logique brut et reconstruction NTFS**
  - **Testés sous Linux et Windows (MinGW) x86**
  - **Immunité aux “rootkits” jusqu'à présent**
  - ***Dirmft* : informations sur les fichiers NTFS**
  - ***Dumpstream* : lecture de tout flux de tout fichier**
  - ***Dirhive* : informations sur les clefs des ruches NT**
  - ***Ntdd* (seulement sous Windows) dd+netcat pour NT4 (*dd.exe* de Garner nécessite W2k)**
  - ***WinMac.pl* : tri et formatte (html,...) les sorties de *dirmft* et *dirhive***
- ***Welfr* : décode les fichiers d'événements**
- ***IETraces* : recherche de traces d'activité IE sur un disque brut**

Analyse NTFS : comparaison Sleuthkit/Dirtools

- **Sleuthkit**
  - **Richesse des outils (diverses couches)**
  - **Analyse des répertoires**
  - **Orienté Unix (résolution 1s, pas de “SD”)**
  - **nécessite cygwin.dll sous Windows**
- **Dirtools**
  - **Petite empreinte mémoire (30-50Ko)**
  - **Garde la résolution native des dates**
  - **Décode les descripteurs de sécurité (“SD”)**
  - **Pas d'analyse des répertoires**
  - **Pas d'analyse des espaces libres**
- **Autres outils : ntfsprogs (Unix + Cygwin), WOLF (interne Microsoft), EnCase,...**

Analyse NTFS: *dirmft + WinMac*



UTC Date/Time	Size	MACW	Attributes	Index	Owner	Group	
01 dec 2004 00:05:21.779	1546	m..w	Ar	20082	SN301030150001\cast	SN301030150001\Aucun	C:\Documents and Settings\cast\Bureau\Invi
01 dec 2004 00:06:48.463	25600	.a..	Ar	28995	BUILTIN\Administrateurs	BUILTIN\Administrateurs	C:\WINDOWS\system32\slayerxp.dll
01 dec 2004 00:06:48.483	197632	.a..	Ar	28488	BUILTIN\Administrateurs	BUILTIN\Administrateurs	C:\WINDOWS\system32\xpsp1res.dll
01 dec 2004 00:09:11.609	438784	m...	Ar	28808	BUILTIN\Administrateurs	BUILTIN\Administrateurs	C:\WINDOWS\system32\wiaacmgr.exe
01 dec 2004 00:11:46.642	16384	.a..	Ar	1256	BUILTIN\Administrateurs	BUILTIN\Administrateurs	C:\WINDOWS\system32\help.exe
01 dec 2004 00:11:46.792	30720	.a..	Ar	28693	BUILTIN\Administrateurs	BUILTIN\Administrateurs	C:\WINDOWS\system32\xcopy.exe
01 dec 2004 00:15:22.152	73216	..c.	Ar	25896	SN301030150001\cast	SN301030150001\Aucun	C:\WINDOWS\system32\drivers\sentinel.sys
01 dec 2004 00:15:22.182	2421	m.cw	Ar	25897	SN301030150001\cast	SN301030150001\Aucun	C:\WINDOWS\system32\drivers\enport.sys
	73216	m..w	Ar	25896	SN301030150001\cast	SN301030150001\Aucun	C:\WINDOWS\system32\drivers\sentinel.sys
01 dec 2004 00:16:05.725	184	.a.w	HiSyArNi	1403	BUILTIN\Administrateurs	SN301030150001\Aucun	C:\System Volume Information_restore{93E
01 dec 2004 00:17:19.629	62	ma.w	HiSyArCoNi	1941	BUILTIN\Administrateurs	AUTORITE NT\SYSTEM	C:\System Volume Information_restore{93E
01 dec 2004 00:17:19.849	62	ma.w	HiSyArCoNi	1942	BUILTIN\Administrateurs	AUTORITE NT\SYSTEM	C:\System Volume Information_restore{93E
01 dec 2004 00:17:30.234	62	m..w	HiSyArCoNi	1944	BUILTIN\Administrateurs	AUTORITE NT\SYSTEM	C:\System Volume Information_restore{93E
01 dec 2004 00:17:31.265	347136	.a..	Ar	28891	BUILTIN\Administrateurs	BUILTIN\Administrateurs	C:\WINDOWS\system32\tourstart.exe
01 dec 2004 00:17:31.486	246784	.a..	Ar	31055	BUILTIN\Administrateurs	BUILTIN\Administrateurs	C:\WINDOWS\system32\usmt\migwiz.exe
01 dec 2004 00:17:31.496	384512	.a..	Ar	31500	BUILTIN\Administrateurs	BUILTIN\Administrateurs	C:\WINDOWS\system32\Restore\rstrui.exe

Ruches de la base de registre : Dirtools

- **Collecte les informations sur les clés de la base de registre :**
  - **Nom**
  - **Nom de classe**
  - **Dernière écriture**
  - **Descripteur de sécurité**
  - **Mais les valeurs (noms et données) ne sont pas encore dans la sortie**
- **Exemple :**

Content|Host Name|OS|UTC Time|Local Time|Output Locale|Recorded Filename|Last Modification

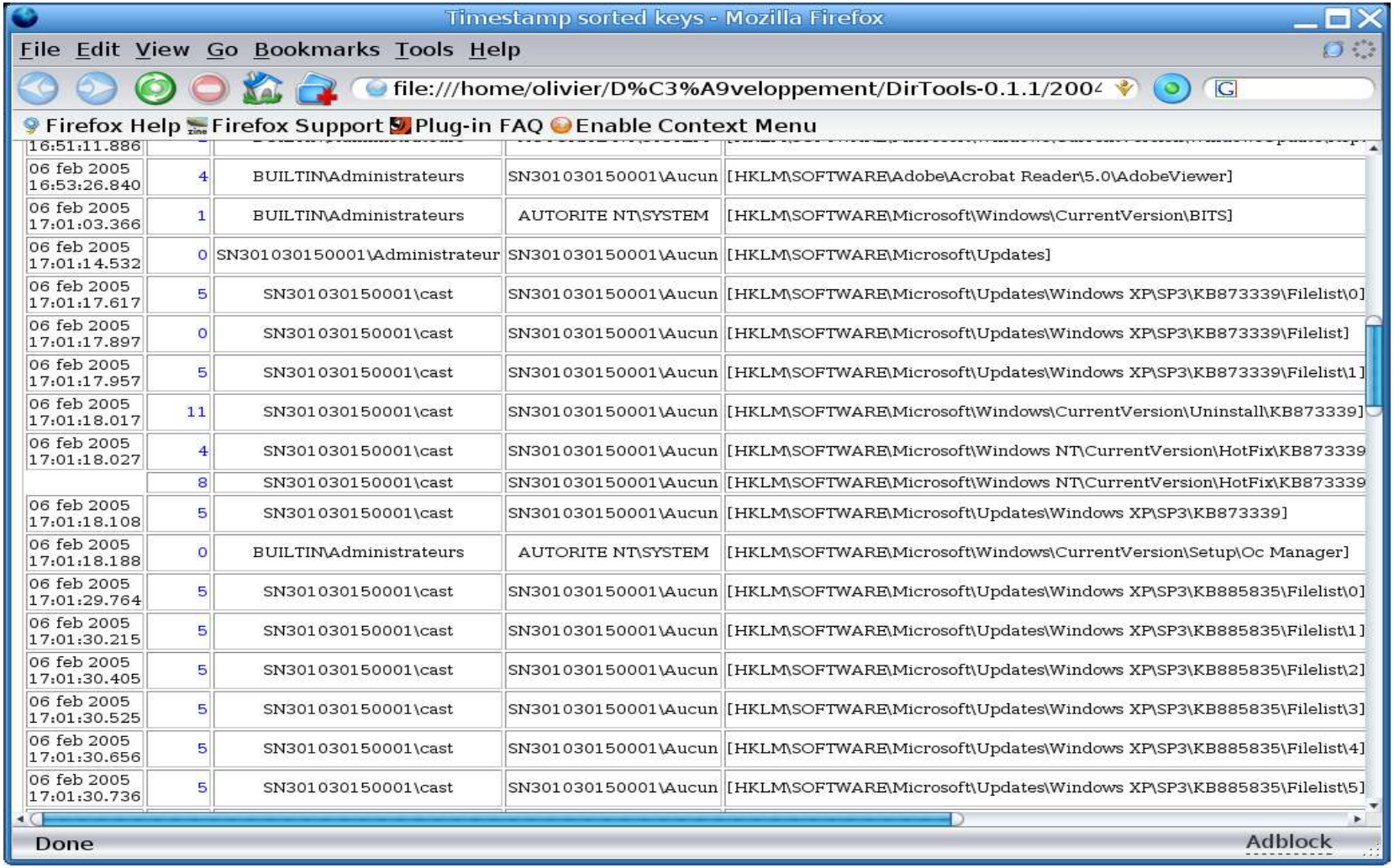
dirhive|SN301030150001|Win XP|06/02/2005 21:16:46.738|06/02/2005 22:16:46.738|"French_France.1252"|emRoot\System32\Config\SOFTWARE|06/02/2005 21:08:28.0818192

Offset|Valid|KeyNode|ClassName|Last Write|# Subkeys|# Values|Owner|Group|# DACE|# SACE|[SID DACE|Rights|...][SID SACE|Audits|...]|

0x1020|1|[HKLM\SOFTWARE]||30/11/2004 23:50:08.4259136|30|0|S-1-5-32-544|S-1-5-18|10|N|S-1-5-32-545|+RdReWeRc|S-1-5-32-545|+Gr|S-1-5-32-547|+RdWdAdReWeDeRc|S-1-5-32-547|+DeGrGw|S-1-5-32-544|+RdWdAdReWeExDeRcWcWo|S-1-5-32-544|+Ga|S-1-5-18|+RdWdAdReWeExDeRcWcWo|S-1-5-18|+Ga|S-1-5-32-544|+RdWdAdReWeExDeRcWcWo|S-1-3-0|+Ga|

0x11b8|1|[HKLM\SOFTWARE\C07ft5Y]||11/10/2002 12:36:43.2652500|1|1|S-1-5-32-544|S-1-5-18|9|N|S-1-5-32-545|+RdReWeRc|S-1-5-32-545|+Gr|S-1-5-32-547|+RdWdAdReWeDeRc|S-1-5-32-547|+DeGrGw|S-1-5-32-544|+RdWdAdReWeExDeRcWcWo|S-1-5-32-544|+Ga|S-1-5-18|+RdWdAdReWeExDeRcWcWo|S-1-5-18|+Ga|S-1-3-0|+Ga|

Ruches de la base de registre : *dirhive* + *WinMac*



Recherche de traces d'activité d' IE

- **Documentation**
  http://prdownloads.sf.net/odessa/IE_Internet_Activity_Reconstruction.pdf
- **Recherche de traces sur un disque complet plutôt que limité aux index.dat**
- **Hypothèses :**
  - **Les structures et l'en-tête des fichiers index.dat sont des multiples de 128 octets**
  - **Les enregistrements pertinents commencent avec 'URL ' 'LEAK' et éventuellement 'REDR'**
- **Algorithme**
  - **Parcours du disque à la recherche des mots clé précédents par pas de 16 octets**
  - **Validité : date et taille de l'enregistrement**
- **Limitations : analyse des structures basée sur index.dat d'IE5, utilisateurs mélangés**

Lecture des fichiers d'évènements

- **Documentation**
  http://msdn.microsoft.com/library/en-us/debug/base/eventlogrecord_str.asp
- **Petit script en Perl pour relire un fichier d'événements abîmé ou sur un autre SE**
- **Sortie :**

  44|2004/01/05-15:35:09|2004/01/05-15:35:09|3221232472|EVENTLOG_ERROR_TYPE|2|0000|0000|00000000|120|0|120|0|142|Service Control Manager|SQLSERV|none|Sev = ERROR (11);C = SYSTEM_CODE (0);R = 0 ;Facility = FACILITY_NULL (0);Code = 7000 |Winsys; %%5|148|

  45|2004/01/05-15:35:15|2004/01/05-15:35:15|1073741850|EVENTLOG_INFORMATION_TYPE|2|0000|0000|00000000|108|0|108|0|538|Application Popup|SQLSERV|none|Sev = INFORMATIONAL (10);C = SYSTEM_CODE (0);R = 0 ;Facility = FACILITY_NULL (0);Code = 26 |Gestionnaire de contrôle des services ; Au moins un service ou pilote n'a pas pu démarrer au démarrage du système. Veuillez consulter le journal des événements dans l'Observateur d'événements pour plus de détails.^M;|544|

- **Amélioration possible : interrogation automatique de http://www.eventid.net ou http://www.evtcatalog.com**

Recréer des disques RAID-5 à l'aide de NTFS

- **Structures prédictibles**
  - **Les 10-11 premiers fichiers ont des noms connus**
  - **Un enregistrement commence avec 'FILE'**
  - **Fragmentation peu problable au début de la MFT (sauf les mauvais secteurs marqués 'BAAD')**
  - **Le secteur de “boot” commence avec 'NTFS '**
  - **La taille des “chunks” est un multiple de celle des enregistrements MFT et celle des clusters, elles-mêmes multiples de la taille des secteurs**
- **Algorithme**
  - **Lecture de chaque secteur de chaque disque physique (+ reconstruction XOR si l'un manque)**
  - **Recherche de 'FILE' ou 'NTFS ' au début**
    - **Si enregistrement MFT extraire le nom fichier**
    - **Si secteur de boot, extraire l'“offset” de la MFT**
- **Déduire alors la taille des “chunks” et l'entrelacement**

Dates : autres sources possibles

- **drwatson.log : peut donner des informations sur les processus dans le passé (Unicode, utiliser 'recode UTF16' les autres SE)**
- **Historique des modification des ruches grâce aux “snapshots” (640 ruches trouvées dans un cas récent)**
  - **%windir%/REPAIR**
  - **System Volume Information/_repair{...}/ RP*/Snapshot/**
- **Les documents OLE sont des “structured storage” : un système de fichier dans un fichier. Les “répertoires” ont des dates (tests préliminaires avec Ole::Storage)**
- **4 dates par utilisateur dans la ruche SAM**

Enfin, la procédure du CERTA...

- ***dd.exe* (Garner) : copie mémoire (> W2k)**
- ***Fport*, *tcpview* et *netstat* (/o) pour les connexions réseau**
- **Collecter les informations NTFS (*dirmft*) et copier le fichier d'échange, les ruches principales et les journaux (*dumpstream*)**
- ***Pslist*, *listdlls*, *handle* pour les processus**
- **Script appelant les outils en mode console**
- **Copie des disques physiques et/ou logiques avec *dd.exe* ou *ntdd.exe***
- **Monter les images avec *filedisk* - Windows (!!! journalisation $\Rightarrow$ écriture) ou Linux**
- **Analyse habituelle : historique, *sorter*, *strings* ('-e l' ou version Sysinternals)...**

Futur/Conclusions

- **Retour d'expérience souhaité**
- **Réécrire *dirmft*, *dumpstream* avec la *libntfs* (compression, répertoires, spécification de chemins pour *dumpstream*) + respecter le modèle Microsoft pour les descripteurs de sécurité au format texte**
- **Développer un pilote pour avoir une image disque dans un état cohérent ?**
- **Peut-on conduire une analyse plus sophistiquée que la recherche de chaînes dans la mémoire et le “swap” copiés ?**
- **Il semble que WinFS (Yukon) sera différent de NTFS**
- **Des questions ?**