2012

Forensics Recherche d'informations à froid

Acquisition de preuves et analyse à froid d'un système sous Windows

Cédric BERTRAND bertrandcedricc@hotmail.fr
http://lepouvoirclapratique.blogspot.fr/
08/04/2012

Table des illustrations

Résumé

De plus en plus utilisée dans le cadre d'enquête ou de l'expertise légale, l'analyse forensique qui consiste à effectuer des recherches sur une machine, nécessite méthodologie et outils afin d'être menée à bien. Au cours de ce document, nous verrons la méthodologie et les outils utilisés afin d'effectuer et d'analyser la copie d'un ordinateur sous Windows.

Introduction

Le terme anglais Forensics (lien) désigne les recherches effectuées sur une machine suite à sa compromission par exemple, afin d'en déterminer les causes et de juger de l'étendue des dommages. [1]

La définition de Wikipédia : « *On désigne par informatique légale ou investigation numérique légale l'application de techniques et de protocoles d'investigation numériques respectant les procédures légales et destinée à apporter des preuves numériques à la demande d'une institution de type judiciaire par réquisition, ordonnance ou jugement. Ce concept, construit sur le modèle plus ancien de médecine légale, correspond à l'anglais « computer forensics ». »*

Une définition plus formelle pourrait être : l'action d'acquérir, de recouvrer, de préserver, et de présenter des informations traitées par le système d'information et stockées sur des supports informatiques.

Ces investigations suivent généralement 3 grandes étapes :
- L'acquisition de données : Cette étape consiste à récupérer les données d'une machine dans le but de les analyser. Il faut évidemment éviter toute modification du système et des informations elles-mêmes. L'approche sera différente suivant que le système est en cours d'exécution ou arrêté.

- Le recouvrement de données : Un fichier effacé sur un disque dur l'est rarement de façon sécurisée. Les informations concernant ce fichier y restent souvent physiquement. Il est donc généralement possible de recouvrer ces fichiers à partir de l'image d'un disque dur. On emploiera par exemple la technique de "file carving" (lien) qui consiste à faire une recherche sur l'image disque par rapport au type des fichiers.

- L'analyse de données : Une fois les données récupérées, il faut les analyser ; la facilité de l'analyse est étroitement liée aux compétences du pirate. Certains ne tenteront pas de se dissimuler, laissant des traces voyantes un peu partout sur le système (dans les journaux systèmes, les fichiers de traces applicatives, etc. …). D'autres auront pris soin d'effacer un maximum d'éléments pouvant trahir leur présence ou leur identité jusqu'à ne rien écrire sur le disque (intrusion par *Meterpreter* par exemple - lien).

[11] http://www.secuobs.com/news/02082007-forensic_lexfo.shtml

Dans quels cas utiliser l'analyse forensique ?

Lors d'un incident de sécurité au sein d'un SI, il est nécessaire de comprendre le mode opératoire de l'attaquant afin de retracer ses actions, mais également de pouvoir collecter assez de preuves pour pouvoir porter plainte (pédo-criminalité, intrusion, etc.). L'analyse forensique peut être par exemple utilisée dans le cas de :

- Analyse de malwares
- Récupération de preuves en vue d'une plainte (intrusion, pédocriminalité, procès, etc.)
- Test d'intrusion
- Récupération de données
- Etc.

Pour cela, plusieurs techniques sont utilisées [2]:

- Récupération de fichiers effacés
- Analyse des logs
- Analyse des fichiers infectés
- Analyse de la mémoire
- Extraction des informations pertinentes
- Etc.

Dans le cas d'une plainte, il faudra néanmoins veiller à assurer l'intégrité des données, celles-ci ayant vocation à être présentées devant la justice.

Les différentes approches

Trois types de collecte peuvent alors être détaillés, à savoir le "*dead*" forensics (système éteint - analyse de disque), le "*live*" forensics (système allumé - analyse de la mémoire vive) et le "mixed" forensics (analyse de la mémoire vive & analyse du disque). Dans le cas présent, nous limiterons nos investigations à l'approche à froid (*dead forensics*).

La méthodologie

L'analyse forensique exige de la méthodologie. Il va s'agir de collecter et de préserver les preuves. Il est donc recommandé de suivre un guide des bonnes pratiques afin de pas altérer/modifier les données analysées. Un point essentiel de l'analyse forensique est **la documentation et l'horodatage des actions effectuées**.

Voici un exemple de méthodologie d'analyse forensique sous Windows :

1. Colliger (collecte)
    a. Déconnecter le poste du réseau
    b. Sauvegarde / analyse de la mémoire vive
    c. Effectuer un clone du disque dur
    d. Effectuer un calcul de l'empreinte de l'image afin de s'assurer de l'intégrité des

[2] http://www.lestutosdenico.com/outils/analyse-forensique-completement-sick

données (calcul hash SHA-1[3])

2. Examiner
    a. Récupérer les fichiers effacés
    b. Analyser la base de registre
    c. Analyser les logs / journaux d'événements
    d. Analyser les traces de connexion Internet
    e. Extraire les comptes utilisateurs de la machine
    f. Extraire les informations pertinentes avec l'évènement

3. Analyser
    a. Interprétation des informations obtenues (source de l'incident)

4. Signaler
    a. Dépôt d'une plainte

Pour plus d'informations sur la méthodologie, vous pouvez consulter le document suivant : Analyse forensique – Règles et méthodes à suivre.

Les outils

Au cours de ce document, je citerais de nombreux outils et les liens où nous pouvons les télécharger. Parmi ceux que j'ai le plus utilisés, je peux citer :

- *Access FTK Imager*[4]
- *OSForensics*[5]
- *Forensic Toolkit*[6]

Il existe bien sûr des outils beaucoup plus puissants tels qu'*Encase*[7], néanmoins ce type d'outil est bien souvent payant et de par le prix des licences, celles-ci se trouvent difficilement accessibles aux particuliers. Dans ce document, l'accent sera donc mis sur les outils gratuits ou open-source.

[3] http://fr.wikipedia.org/wiki/Fonction_de_hachage
[4] http://accessdata.com/
[5] http://www.osforensics.com/
[6] http://accessdata.com/
[7] http://www.guidancesoftware.com/forensic.htm

L'étude

Concernant le poste à analyser, j'ai hésité à mettre à disposition un lien vers une image. Néanmoins ceci ne me semblait pas ni utile, ni très pertinent (taille de l'image, données personnelles). Le plus simple que je puisse conseiller est l'installation d'une machine virtuelle avec un logiciel du type *Vmware*[8], *Virtual Box* [9]ou encore *Virtual PC*[10] puis d'utiliser ce poste un certain temps afin d'accumuler quelques données intéressantes à récupérer (installation d'un navigateur, logiciels de messagerie/lecteur pdf, enregistrement des mots de passe, navigation web, création de fichiers protégés par mot de passe, etc.). Puis de créer une copie de ce disque afin d'y effectuer les manipulations décrites dans ce document.

Une fois votre poste installé, configuré et utilisé un certain temps, nous pourrons passer à la première étape à savoir l'acquisition des données.

1) L'acquisition des données

Cette étape consiste à récupérer les données d'une machine dans le but de les analyser. Il faut évidemment éviter toute modification du système et des informations elles-mêmes (analyse du système en lecture seule).

a) La copie du disque

L'acquisition c'est lorsque vous faites une copie bit par bit des données stockées sur le matériel saisi (avec la commande DD où d'autres outils…) Concernant la copie d'un disque, de nombreux outils sont disponibles dont :

- *Helix* (tutorial ici[11])
- *Dd* (http://www.ossir.org/resist/supports/cr/20070925/Roukine-Forensiques.pdf)
- *Encase*[12]

Un excellent article de *Zythom* sur ce thème est disponible ici : Récupération des données, faites la vous-même. D'autres outils sont aussi décrits sur cette page.

Voyons la démarche avec FTK Imager, qui lui permet aussi la copie d'un disque dur.

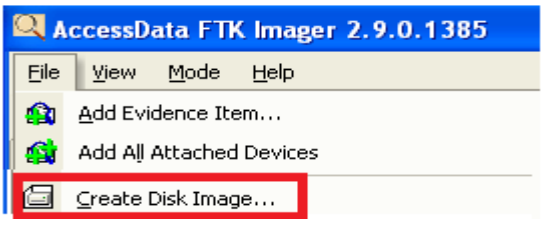
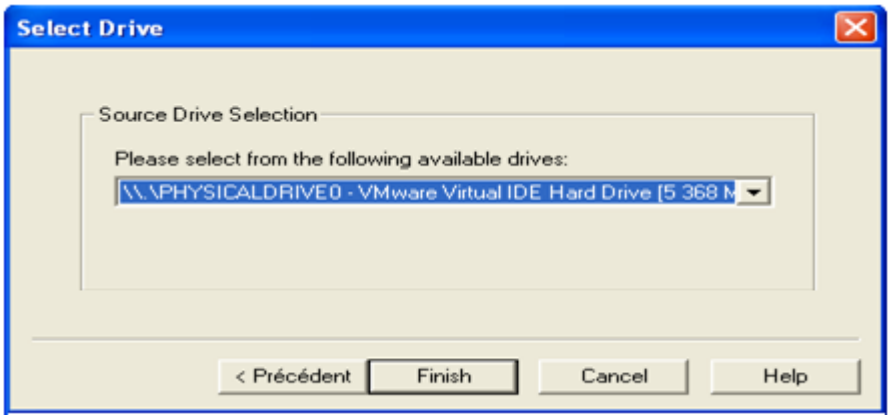
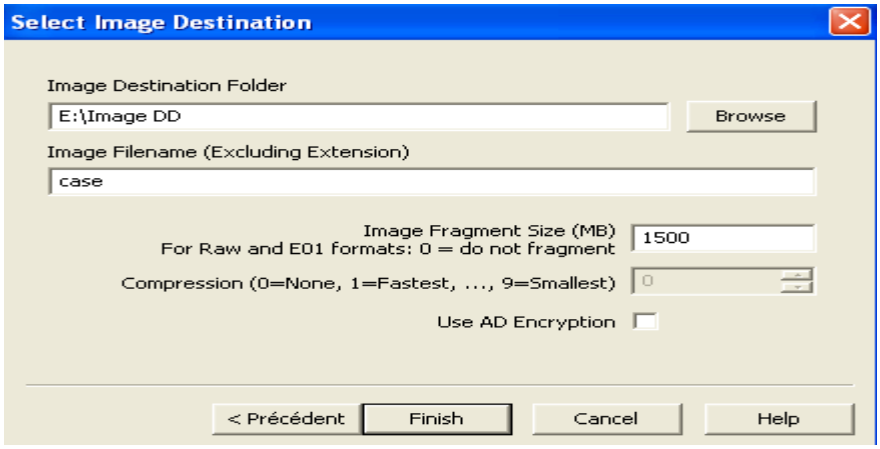


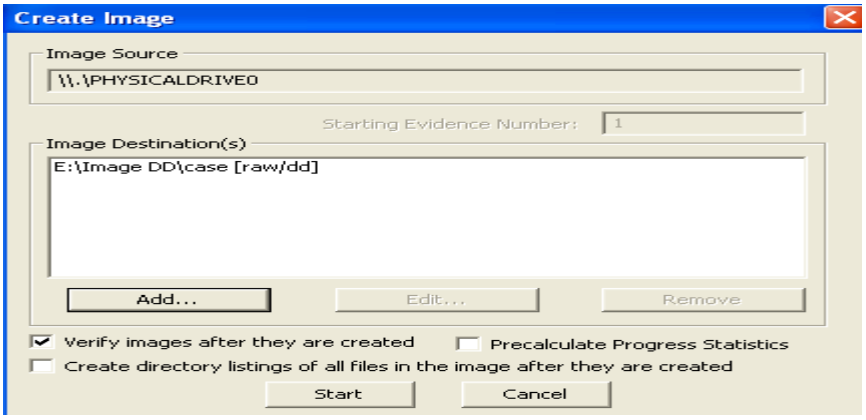
Figure 1 Création d'une image disque avec FTK imager

[8] http://www.vmware.com/fr/
[9] https://www.virtualbox.org/
[10] http://www.microsoft.com/windows/virtual-pc/default.aspx
[11] http://www.creativeo.net/ii-forensique-lacquisition-de-donnees-ewfacquire/
[12] http://www.forensicswiki.org/wiki/EnCase

On sélectionne ensuite la partition ou le disque dur que l'on souhaite sauvegarder (ici un disque sous *Vmware*) et la destination de notre sauvegarde.







Après la copie du disque, un *hash*[13] de l'image est réalisé afin de pouvoir vérifier l'intégrité de notre image.

[13] http://fr.wikipedia.org/wiki/Fonction_de_hachage

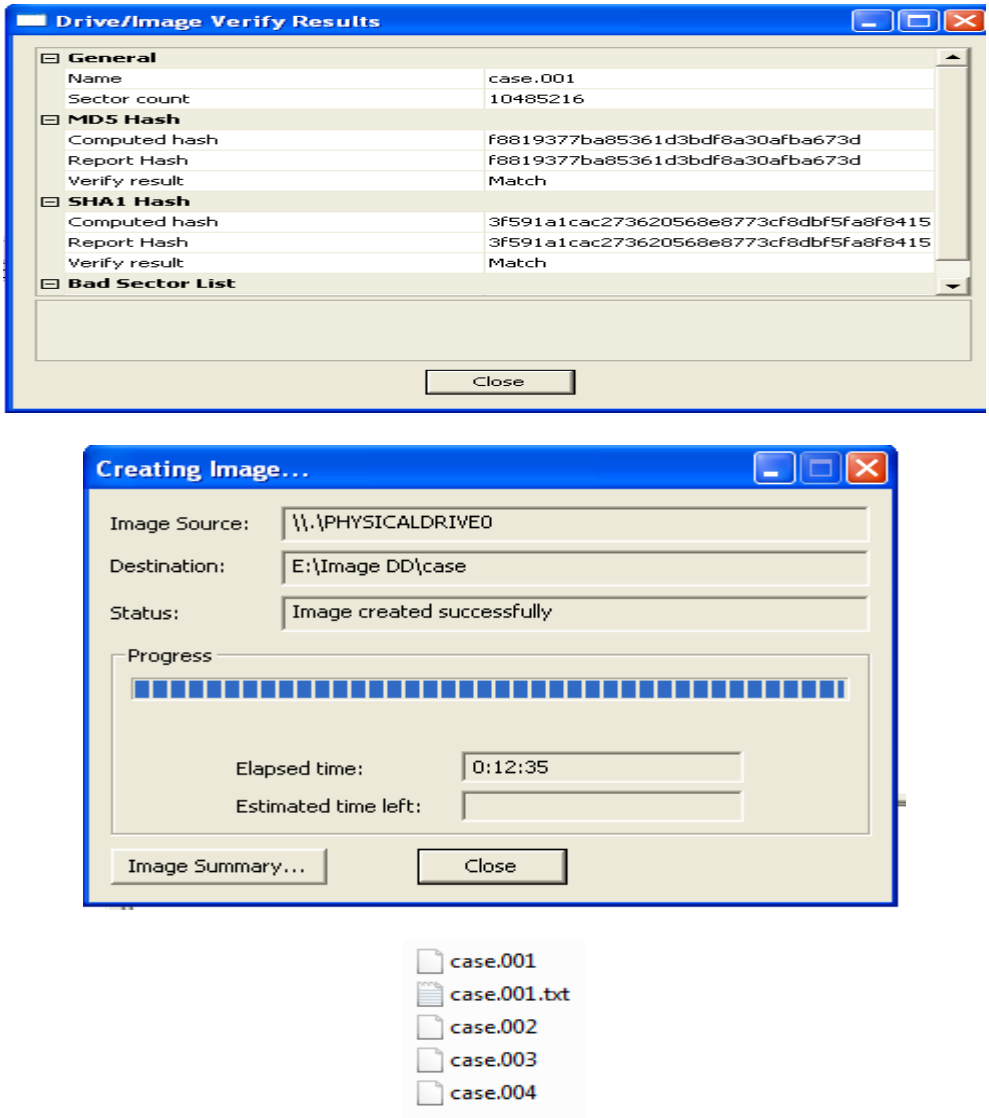


Figure 2 Copie du disque réalisée

Par souci de sécurité, ne pas hésiter à faire une copie de sauvegarde du fichier image.

b) Le montage de l'image

Une fois la copie réalisée, il va falloir monter celle-ci sur un autre poste afin de pouvoir l'analyser. Pour se faire, il existe les outils suivants :

- *Lmdisk*[14] (émuler un ou plusieurs lecteurs de disques)
- *FTK imager*
- *Encase*

Par exemple, dans le cadre d'un travail pratique dans mon cursus professionnel, nous avions à notre disposition un fichier zip représentant partiellement un disque dur.

[14] http://www.ltr-data.se/opencode.html/

Figure 3 Fichier image sous forme de fichier zip

Pour monter ce fichier zip, nous allons utiliser l'outil *Access FTK Imager*[15].

Monter une image avec FTK imager

Cet outil va nous permettre de monter notre fichier image comme un disque. Ne pas oublier de réaliser une copie de sauvegarde de l'image avant tout travail.

On sélectionne notre image puis on la monte. On choisit de la monter en lecture seule (*read only*) afin de ne pas modifier les fichiers et ainsi ne pas fausser notre analyse.

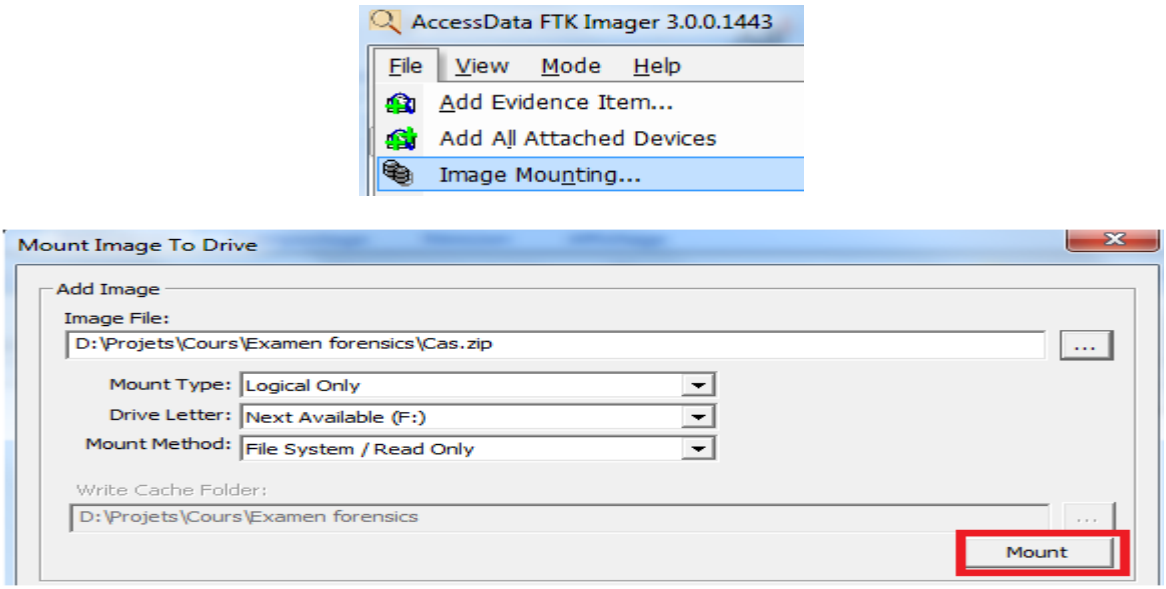
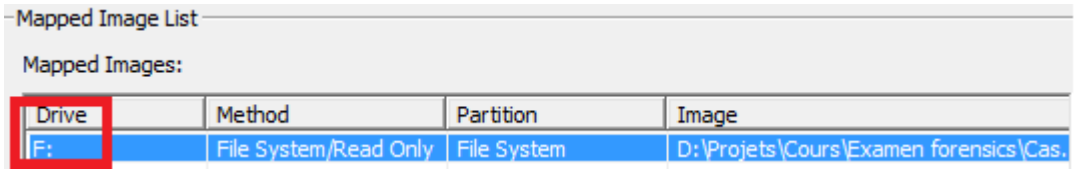


Figure 4 Montage de l'image avec FTK imager

Notre image devient ainsi accessible via un explorateur de fichiers.



[15] http://accessdata.com/products/computer-forensics/ftk

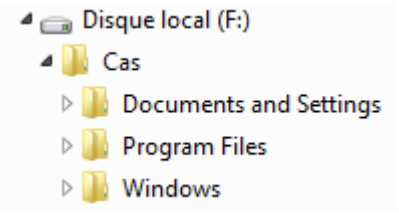


Figure 5 Image accessible par gestionnaire de fichiers

Monter une image avec OSForensics

Dans le cas de la sauvegarde du disque réalisée précédemment, on peut aussi utiliser l'outil *OSForensics*.

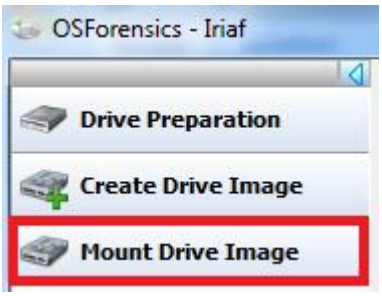
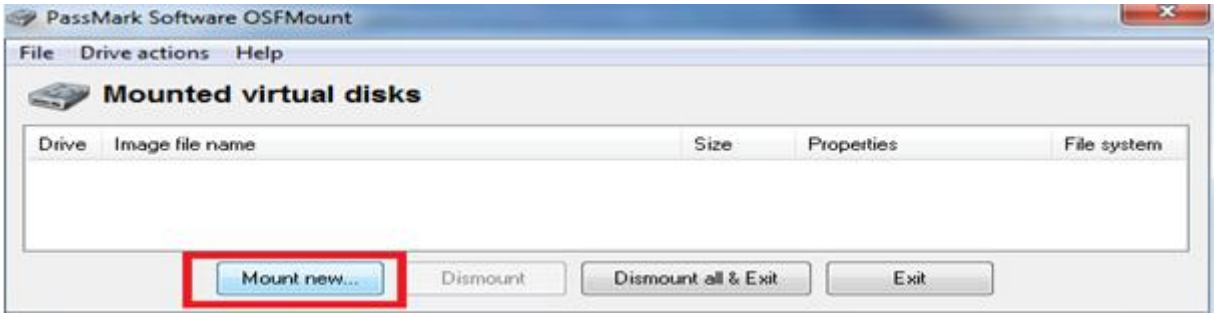
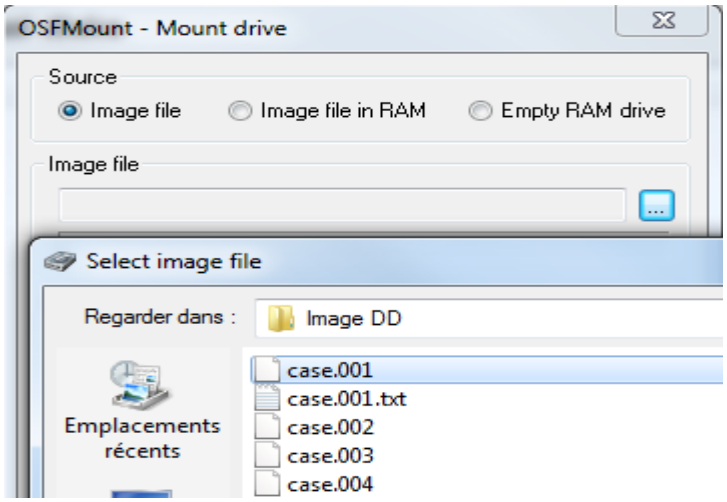
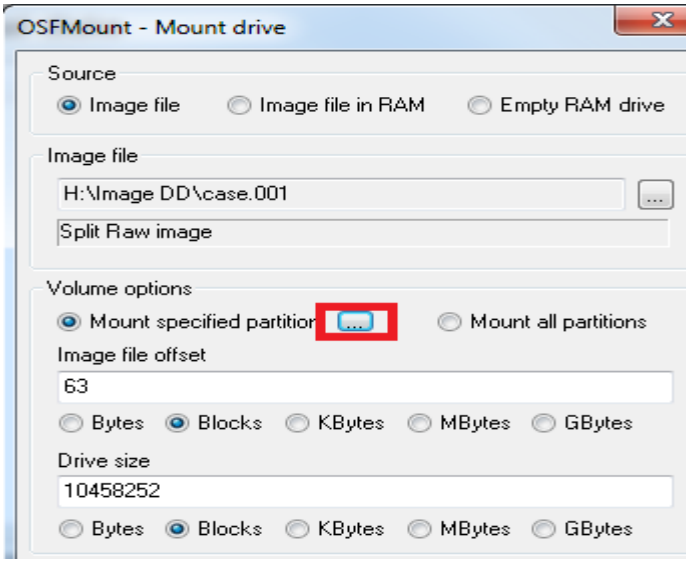


Figure 6 Monter une image avec OSForensics

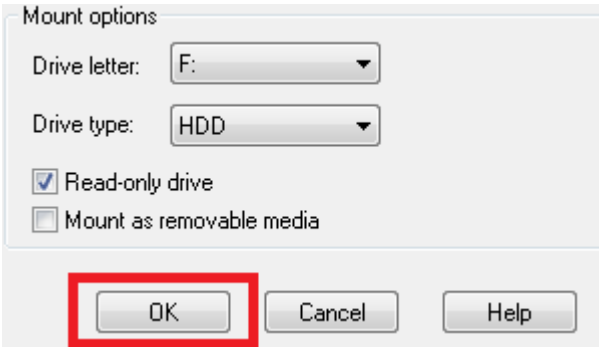
On clique sur « Mount New » et on sélectionne notre fichier image.







N’oublions pas de cocher le montage en lecture seule afin de sauvegarder l’intégrité de notre fichier image.



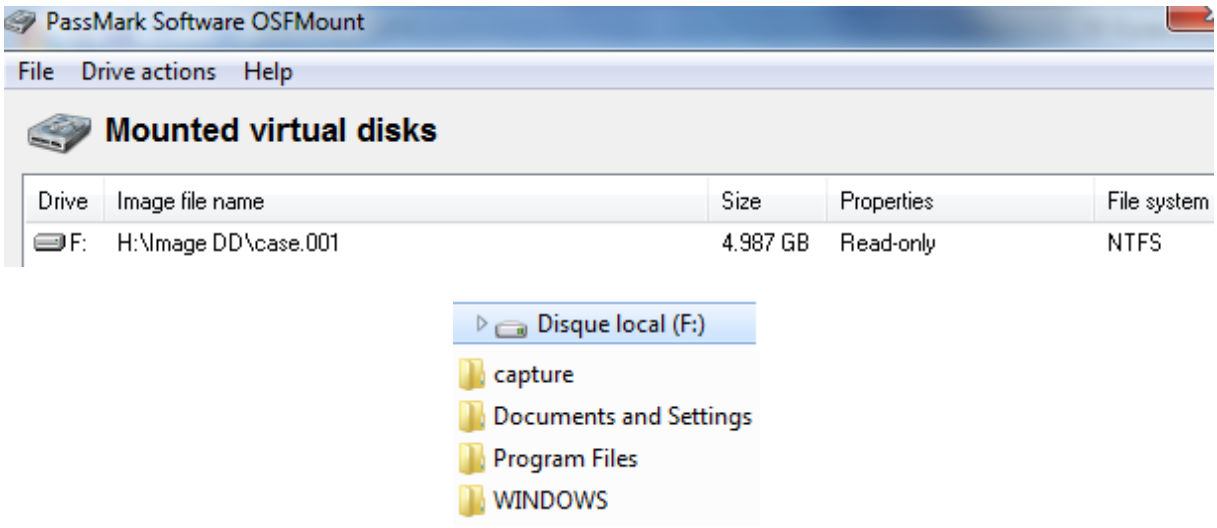
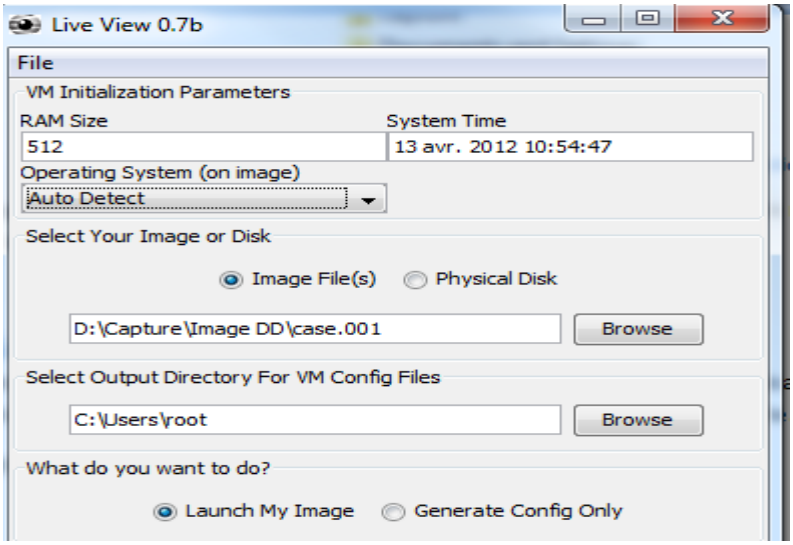


Figure 7 Image montée et accessible via un explorateur de fichiers

Notre image est maintenant accessible et ne pas être modifiée.

c) Convertir une image en machine virtuelle

Il peut être parfois intéressant de convertir une image en machine virtuelle afin de pouvoir démarrer celle-ci. Pour cela, il existe le logiciel *LiveView*[16] qui se charge de cette tâche. Il suffit d'indiquer l'emplacement de notre image et cet outil se charge de la convertir en image *Vmware.* Nous pouvons ensuite démarrer l'image convertie avec *Vmware*.



Pour plus d'informations, vous pouvez consulter le lien suivant : « How to Create a Virtual Machine from a Raw Hard Drive Image ».

2) L'analyse du disque

Il va s'agir maintenant d'analyser le disque afin d'y extraire des informations pertinentes : identification du système, récupération des fichiers effacés, analyse des logs, récupération d'informations sensibles, etc.

d) L'identification du système

La première étape de l'analyse est de déterminer le système d'exploitation utilisé, pour cela nous avons plusieurs moyens à notre disposition[17].

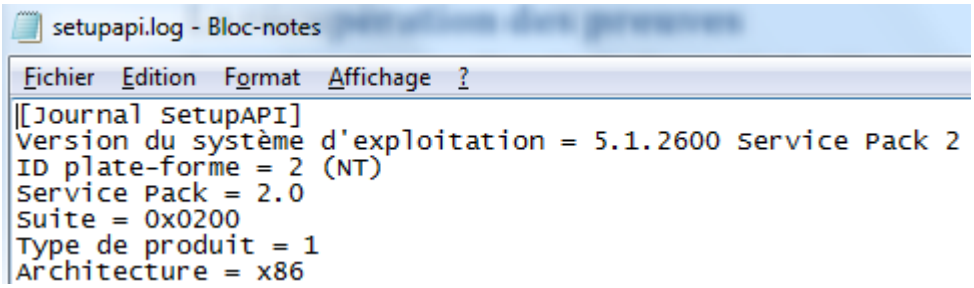
Sous les systèmes *Windows 95/98/Me*, il existe la présence d'un fichier \MSDOS.SYS. Il suffit d'ouvrir ce fichier et d'examiner la ligne [Options]WinVer parameter.

Pour les systèmes *NT/Vista/XP/Seven*, il y a déjà le nom du répertoire : « c:\Winnt » pour les NT, « C:\Wndows » pour les XP.

Il est possible de retrouver ces informations dans la base de registre à la ruche *Microsoft\Windows NT\CurrentVersion* key (*ProductName, CSDVersion, ProductId, BuildLab,* et sur *Vista, BuildLabEx*).

[16] http://liveview.sourceforge.net/
[17] http://www.forensicswiki.org/wiki/Determining_OS_version_from_an_evidence_image

La consultation du fichier « *setupapi.log* » dans le répertoire Windows permet aussi d'obtenir le même genre d'informations.



Sous Linux, on peut consulter les fichiers */etc/issue* et */etc/issue.net* pour connaitre la version du système. Le document suivant donne aussi d'autres pistes : « How To Know Which Linux Distribution You Are Using ».

e) La récupération des fichiers effacés

Quand un document est effacé, seule la référence dans l'index du disque dur est modifiée. Le fichier est toujours là, mais inaccessible pour le commun des mortels. Nous avons plusieurs outils à disposition pour récupérer les fichiers effacés :

- Foremost
- Dd_rescue
- NTFS undelete
- Fatback
- Sleuth Kit
- Etc.

On peut aussi utiliser *Osforensics* qui permet de réaliser facilement cette opération.

Figure 8 Récupération des fichiers effacés

Un disque dur ne dispose pas de fonction d'effacement : une fois une donnée écrite, la seule façon de l'effacer est donc d'écrire d'autres données par-dessus les données existantes. Il existe de

nombreux outils permettant un effacement sécurisé des données[18]. Citons le cas par exemple de *Ccleaner* (logiciel gratuit destiné à nettoyer un ordinateur) qui propose de telles options :

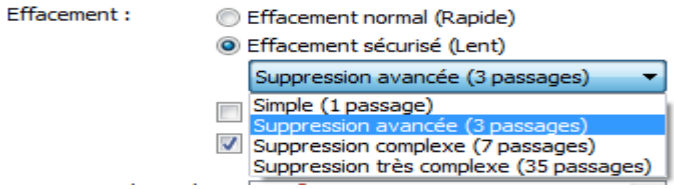


Figure 9 Effacement sécurisé avec Ccleaner

Pour plus d'informations sur l'effacement des disques durs, le document suivant est accessible en ligne : Effacement sécurisé des disques durs.

f) L'analyse de la base de registre

La base de registre contient une multitude d'informations très intéressantes à analyser. Pour rappel, celle-ci se présente sous forme de différentes « ruches » (fichiers) qui sont stockées dans :

- *C:\Windows\System32\Config*
- *C:\Document and Settings\#utilisateur#\NTUSER.dat*
- *C:\Windows\repair*

Pour analyser une base de registre offline, il existe de nombreux outils gratuits :

- *Autoruns*[19] de *sysinternals*
- *RegRipper*[20]
- *Rip*
- *RipXP*
- *RegSlack*
- *Mitec Windows Registry*[21]

Commençons par exemple par analyser le fichier NTUSER.dat avec *regripper*.

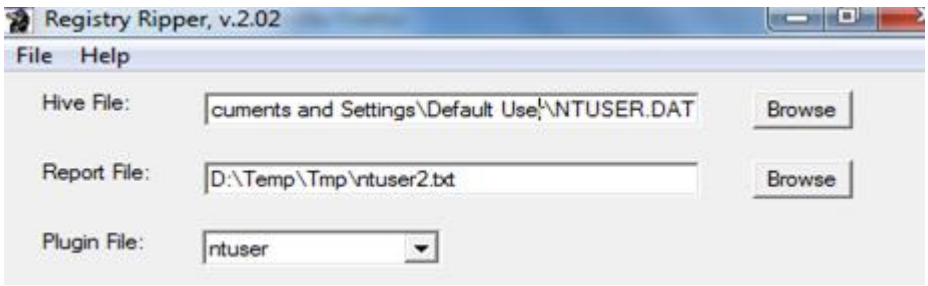


Figure 10 Analyse de la base de registre avec RegRipper

Parmi les informations récupérées, nous avons tout ce qui concerne la version de Windows :

[18] http://www.espacefr.com/winouti/secu8.php
[19] http://technet.microsoft.com/en-us/sysinternals/bb963902
[20] http://regripper.wordpress.com/
[21] http://mitec.cz/wrr.html

```
WinNT_CV
Microsoft\Windows NT\CurrentVersion
LastWrite Time Mon Mar  7 20:39:37 2011 (UTC)

  SubVersionNumber :
  RegDone :
  RegisteredOrganization :
  CurrentVersion : 5.1
  CurrentBuildNumber : 2600
  SoftwareType : SYSTEM
  SourcePath : A:\I386
  SystemRoot : C:\WINDOWS
  PathName : C:\WINDOWS
  RegisteredOwner : autodiagprog
  CSDVersion : Service Pack 2
  CurrentType : Uniprocessor Free
  ProductName : Microsoft Windows XP
  ProductId : 76413[redacted]
  BuildLab : 2600.xpsp_sp2_gdr.100216-1441
  InstallDate : Sun Jul 20 20:45:34 2008 (UTC)
```

Figure 11 Informations extraites sur la version de Windows utilisée

Nous pouvons aussi obtenir tous les fichiers qui ont été exécutés sur la machine[22].

```
MUICache
Software\Microsoft\Windows\ShellNoRoam\MUICache
LastWrite Time Sun Jul 20 20:38:59 2008 (UTC)
      C:\WINDOWS\system32\igfxtray.exe (igfxTray Module)
      C:\WINDOWS\system32\hkcmd.exe (hkcmd Module)
      C:\WINDOWS\system32\igfxpers.exe (persistence Module)
      D:\Program Files\Adobe\Reader 8.0\Reader\Reader_sl.exe
(Adobe Acrobat SpeedLauncher)
      C:\Program Files\Java\jre1.6.0_03\bin\jusched.exe (Java(TM)
Platform SE binary)
      C:\WINDOWS\RTHDCPL.EXE (Realtek HD Audio Control Panel)
      C:\WINDOWS\ALCMTR.EXE (Realtek Azalia Audio - Event Monitor)
      C:\Program Files\Asus\EeePC ACPI\AsTray.exe (Eee PC Tray
Utility)
      C:\Program Files\Asus\EeePC ACPI\AsAcpiSvr.exe (Asus Eee PC
ACPI Service)
      C:\Program Files\Elantech\ETDCtrl.exe (ETD Ware TSR |
Enhancements)
      C:\sysprep\factory.exe (Factory pre-installation utility)
```

Figure 12 Fichiers exécutés sur la machine

Volumes montés

Autre information intéressante : les points de montage. Utile pour savoir si un disque dur chiffré (avec *TrueCrypt* [23]par exemple) a été monté :

```
MountPoints2
Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
LastWrite Time Sun Jul 20 20:38:59 2008 (UTC)

Remote Drives:

Volumes:
Sun Jul 20 20:38:59 2008 (UTC)
  {10563ec0-0b5b-11dd-a142-806d6172696f}
  {10563ec1-0b5b-11dd-a142-806d6172696f}
  {10563ec2-0b5b-11dd-a142-806d6172696f}
  {278aa040-054d-11dd-8eee-806d6172696f}
  {70f29240-0ca7-11dd-aa20-806d6172696f}
```

Figure 13 Volumes montés sur le poste

Une autre information intéressante à récupérer concerne les documents récemment ouverts[24].

[22] http://www.nirsoft.net/utils/muicache_view.html
[23] http://www.truecrypt.org/

Liste des documents récemment ouverts

La liste se trouve dans à la clé *NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs*

```
RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Wed Apr 11 12:23:07 2012 (UTC)
  29 = COFEE ORIGINAL TORRENT
  28 = READ ME FIRST!.txt
  27 = Passware Kit Forensic 10.1
  26 = Working Serial.txt
  25 = SourceDir
  24 = User Guide for COFEE v112.pdf
```

Figure 14 Documents récemment ouverts

Idem avec les fichiers *pdf*.

```
Adoberdr v.20100218
Adobe Acrobat Reader version 9.0 located.
Software\Adobe\Acrobat Reader\9.0\AVGeneral\cRecentFiles

Most recent PDF opened: Thu Apr  5 09:03:51 2012 (UTC)
  c1   /C/Documents and Settings/Ced/Mes
documents/COFEE/SourceDir/User Guide for COFEE v112.pdf
```

Figure 15 Fichiers pdf récemment ouverts

Il est aussi possible de récupérer ces informations avec *OsForensics*.

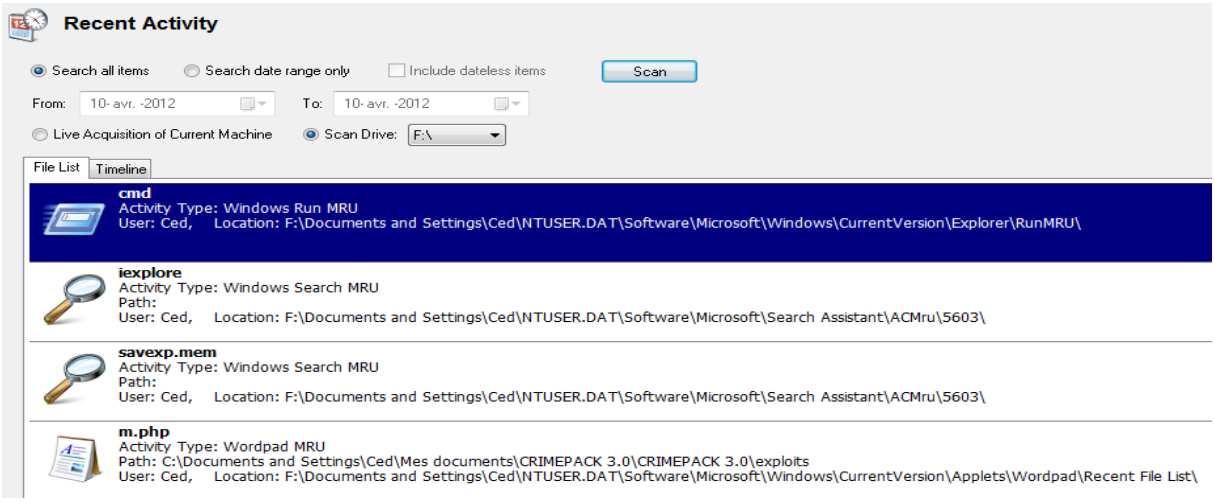


Figure 16 Récupération des documents récemment ouverts

[24] http://forensicartifacts.com/2011/02/recentdocs/

Programmes qui se lancent avec Windows

Utile dans le cas d'analyse de malwares, la plupart des programmes se lançant au démarrage de la machine utilisent souvent ce biais. Les informations se trouvent dans la ruche *Software\Microsoft\Windows\CurrentVersion\Run*

```
Software\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Sat Apr  5 19:07:43 2008 (UTC)
      CTFMON.EXE -> C:\WINDOWS\system32\CTFMON.EXE
```

Figure 17 Programmes qui démarrent avec Windows

Nom de la machine et utilisateur

Pour récupérer le nom de la machine ainsi que l'utilisateur, on peut utiliser l'utilitaire rip avec le plug-in "system" :

```
D:\Attaque\Forensics\Tools\Base de registre\rr_tools>rip.exe -r F:\Cas\Windows\S
ystem32\config\system -f system
Parsed Plugins file.
Launching compname v.20090727
ComputerName    = YOUR-9BC5H1JIWR
```

```
D:\Attaque\Forensics\Tools\Base de registre\rr_tools>rip.exe -r D:\Temp\Tmp\NTUS
ER.dat -p logonusername
Launching logonusername v.20080324
Logon User Name
Software\Microsoft\Windows\CurrentVersion\Explorer
LastWrite Time [Sun Jul 20 20:38:59 2008 (UTC)]
Logon User Name = Propri├®taire
```

Figure 18 Récupération du nom de la machine

Paramètres du proxy

Récupérer des informations sur le proxy utilisé peut aussi s'avérer une démarche intéressante (présence parfois d'un compte utilisateur)

```
D:\Attaque\Forensics\Tools\Base de registre\rr_tools>rip.exe -r D:\Temp\Tmp\NTUS
ER.dat -p proxysettings
Launching proxysettings v.20081224
ProxySettings
Software\Microsoft\Windows\CurrentVersion\Internet Settings
LastWrite Time Sun Jul 20 20:38:59 2008 (UTC)
  AutoConfigProxy               wininet.dll
  EmailName                     IEUser@
  EnableHttp1_1                 1
  EnableNegotiate               1
  IE5_UA_Backup_Flag            5.0
  MigrateProxy                  1
  MimeExclusionListForCache     multipart/mixed multipart/x-mixed-replace multi
part/x-byteranges
  NoNetAutodial                 0
  PrivacyAdvanced               0
  ProxyEnable                   0
  UseSchannelDirectly           1
  User Agent                    Mozilla/4.0 (compatible; MSIE 6.0; Win32)
  WarnOnPost                    1
```

Figure 19 Récupération des paramètres du proxy

Liste des URL tapées dans internet Explorer

La liste des adresses tapées dans internet Explorer est aussi accessible.

```
TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Fri Apr  6 14:53:50 2012 (UTC)
  url1 -> http://rennes.onvasortir.com/
  url2 -> http://google.fr/
  url3 -> http://gmail.com/
  url4 -> http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6
&ar=msnhome
```

Figure 20 URL tapées dans Internet Explorer

Il existe encore de nombreuses informations intéressantes à explorer, pour plus d'informations, vous pouvez consulter ce document.

g) Analyses des fichiers logs / évènements

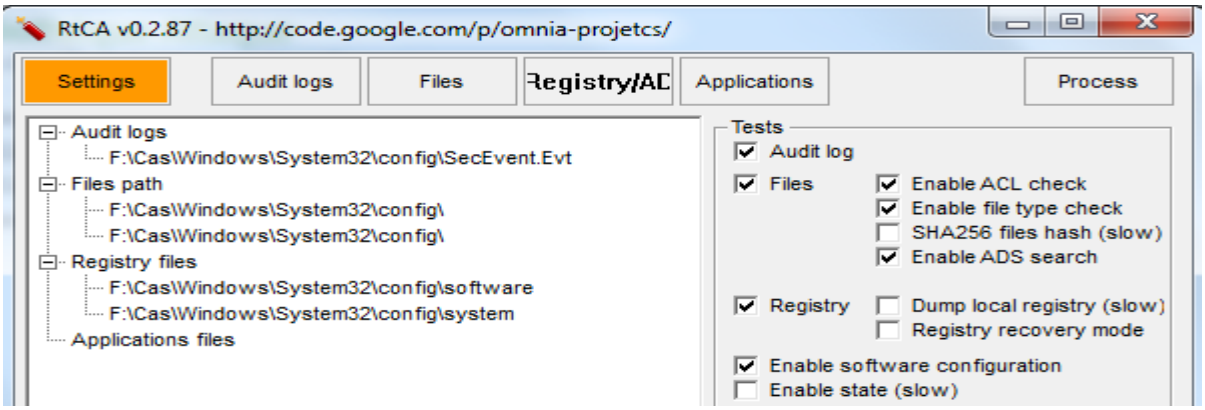
Tout comme la base de registre, les journaux d'enregistrement peuvent être une source d'informations très riches. Ceux-ci localisés dans le répertoire « *Windows\System32\Config* », sont activés par défaut sur la plupart des systèmes Windows (application, sécurité, system).

En analysant ces fichiers, on peut trouver rapidement un évènement répétitif (tentatives multiples de login par exemple qui peut traduire une tentative d'intrusion ou un malware par exemple) qui peut donner des pistes.

Concernant l'analyse des fichiers logs, événements, il existe :

- *Log Parser*[25](outil qui permet un accès universel aux fichiers journaux)
- *Evtrpt.pl*[26] (script perl permettant d'établir des statistiques)
- *RtCA*[27] *(outil d'aide aux analyses)*

Avec ce dernier outil, on peut analyser de manière simple et détaillée un fichier log.



[25] http://technet.microsoft.com/fr-fr/scriptcenter/dd919274
[26] http://windowsir.blogspot.fr/2009/03/eventlog-parsing.html
[27] http://omni-a.blogspot.fr/2011/10/rtca-v01-outil-daide-aux-analyses.html

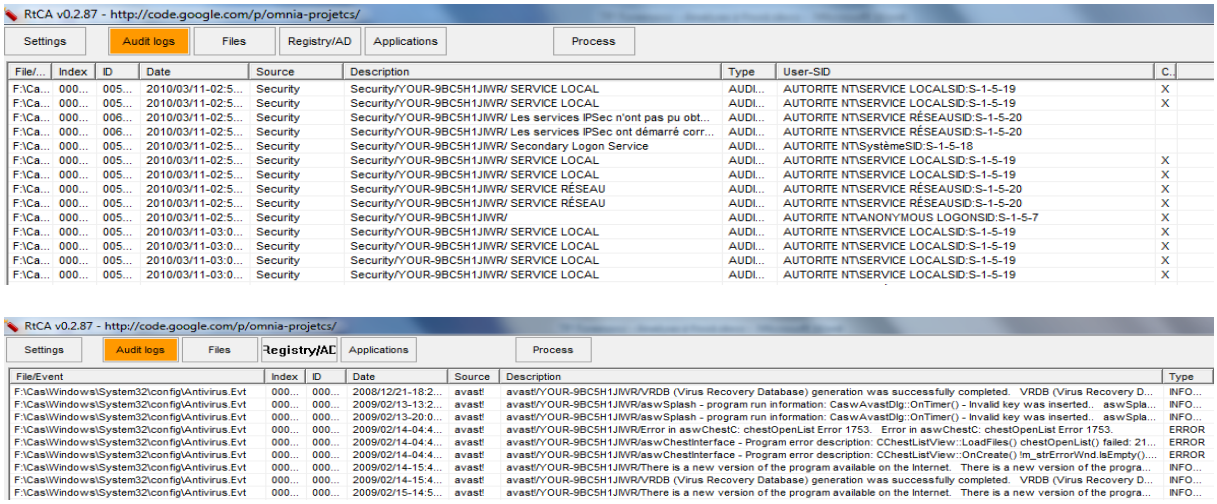


Figure 21 Analyse de fichier log avec l'outil rtCA

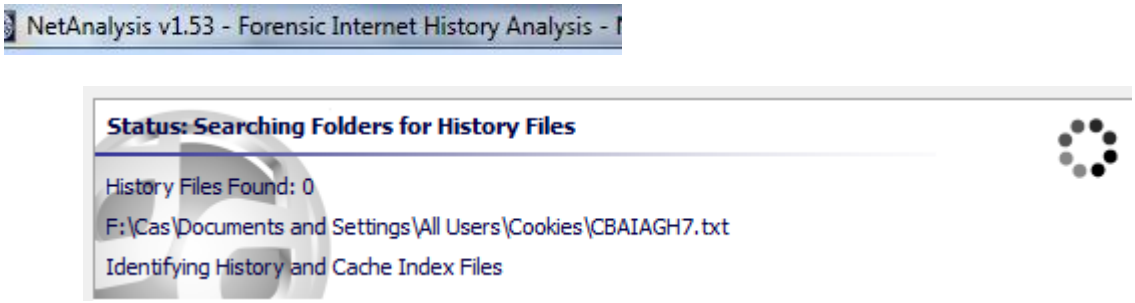
Pour avoir plus d'informations sur l'emplacement des fichiers logs, il est possible de consulter ce document : [Liste des fichiers logs].

h) L'analyse des traces de connexion Internet

Il peut être judicieux d'analyser les navigations web effectuées à partir du poste. Pour cela, il existe de nombreux utilitaires :

- *ProDiscover*[28]
- *NetAnalysis*[29]
- *Web Historian*[30]
- *IEHistoryView, etc.*[31]

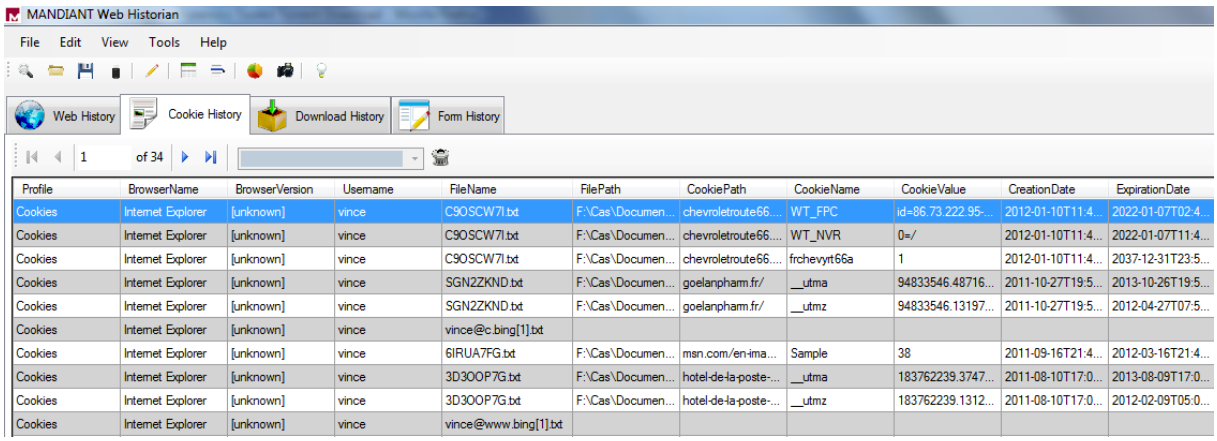
Ci-dessous une analyse de la navigation Internet avec l'outil *NetAnalysis* ainsi que *Web Historian*. En général ces outils analysent le fichier « index.dat » présents dans « *document and settings\#user#\Cookies* »



[28] http://www.techpathways.com/prodiscoverdft.htm
[29] http://www.digital-detective.co.uk/
[30] http://www.mandiant.com/products/free_software/web_historian/
[31] http://www.nirsoft.net/computer_forensic_software.html

Type		Last Visited [UTC]	Last Visited [Local]	Hits	User	URL	Host
cookie		15/03/2012 21:48:29 jeu.	15/03/2012 22:48:29 jeu.	20	v	Cookie: @www.dailymotion.com/	www.dailymotion.com
cookie		15/03/2012 21:48:29 jeu.	15/03/2012 22:48:29 jeu.	59	v	Cookie: @fr.a2dfp.net/	fr.a2dfp.net
cookie		15/03/2012 21:48:03 jeu.	15/03/2012 22:48:03 jeu.	2	v	Cookie: @numerama.com/	numerama.com
cookie		15/03/2012 21:47:49 jeu.	15/03/2012 22:47:49 jeu.	7	v	Cookie: @darksite.ch/	darksite.ch
cookie		15/03/2012 21:47:43 jeu.	15/03/2012 22:47:43 jeu.	3	v	Cookie: @www.darksite.ch/	www.darksite.ch
cookie		15/03/2012 21:47:36 jeu.	15/03/2012 22:47:36 jeu.	322	v	Cookie: @google.fr/	google.fr
cookie		15/03/2012 21:47:18 jeu.	15/03/2012 22:47:18 jeu.	330	v	Cookie: @weborama.fr/	weborama.fr
cookie		15/03/2012 21:47:18 jeu.	15/03/2012 22:47:18 jeu.	5117	v	Cookie: @criteo.com/	criteo.com
cookie		15/03/2012 21:47:17 jeu.	15/03/2012 22:47:17 jeu.	58	v	Cookie: @fr.a2dfp.net/	fr.a2dfp.net

Figure 22 Analyse web avec NetAnalysis



Profile	BrowserName	BrowserVersion	Username	FileName	FilePath	CookiePath	CookieName	CookieValue	CreationDate	ExpirationDate
Cookies	Internet Explorer	[unknown]	vince	C9OSCW7I.txt	F:\Cas\Documen...	chevroletroute66....	WT_FPC	id=86.73.222.95-...	2012-01-10T11:4...	2022-01-07T02:4...
Cookies	Internet Explorer	[unknown]	vince	C9OSCW7I.txt	F:\Cas\Documen...	chevroletroute66....	WT_NVR	0=/	2012-01-10T11:4...	2022-01-07T11:4...
Cookies	Internet Explorer	[unknown]	vince	C9OSCW7I.txt	F:\Cas\Documen...	chevroletroute66....	frchevyrt66a	1	2012-01-10T11:4...	2037-12-31T23:5...
Cookies	Internet Explorer	[unknown]	vince	SGN2ZKND.txt	F:\Cas\Documen...	goelanpharm.fr/	__utma	94833546.48716...	2011-10-27T19:5...	2013-10-26T19:5...
Cookies	Internet Explorer	[unknown]	vince	SGN2ZKND.txt	F:\Cas\Documen...	goelanpharm.fr/	__utmz	94833546.13197...	2011-10-27T19:5...	2012-04-27T07:5...
Cookies	Internet Explorer	[unknown]	vince	vince@c.bing[1].txt						
Cookies	Internet Explorer	[unknown]	vince	6IRUA7FG.txt	F:\Cas\Documen...	msn.com/en-ima...	Sample	38	2011-09-16T21:4...	2012-03-16T21:4...
Cookies	Internet Explorer	[unknown]	vince	3D3OOP7G.txt	F:\Cas\Documen...	hotel-de-la-poste-...	__utma	183762239.3747...	2011-08-10T17:0...	2013-08-09T17:0...
Cookies	Internet Explorer	[unknown]	vince	3D3OOP7G.txt	F:\Cas\Documen...	hotel-de-la-poste-...	__utmz	183762239.1312...	2011-08-10T17:0...	2012-02-09T05:0...
Cookies	Internet Explorer	[unknown]	vince	vince@www.bing[1].txt						

Figure 23 Analyse web avec Web Historian

Pour ceux que le sujet intéresse, voici une liste d'autres liens :

- http://www.symantec.com/connect/articles/web-browser-forensics-part-1
- http://www.forensicswiki.org/wiki/Internet_Explorer_History_File_Format

i) La recherche de fichiers

Il peut être parfois fastidieux d'effectuer des recherches de fichiers sur un disque dur, de par la multitude des fichiers existants. Heureusement il existe des outils pour nous aider dans cette tâche. Parmi eux, nous pouvons citer :

- *Access Forensic Toolkit*[32]
- *OSForensics*
- *Scalpel*[33]
- *Sleuth Kit*

Par exemple avec l'outil *Forensic Toolkit*, nous pouvons facilement créer un index des fichiers, ce qui permet d'avoir un tri selon le type de fichier et leur extension.

[32] http://accessdata.com/products/computer-forensics/ftk
[33] http://www.digitalforensicssolutions.com/Scalpel/

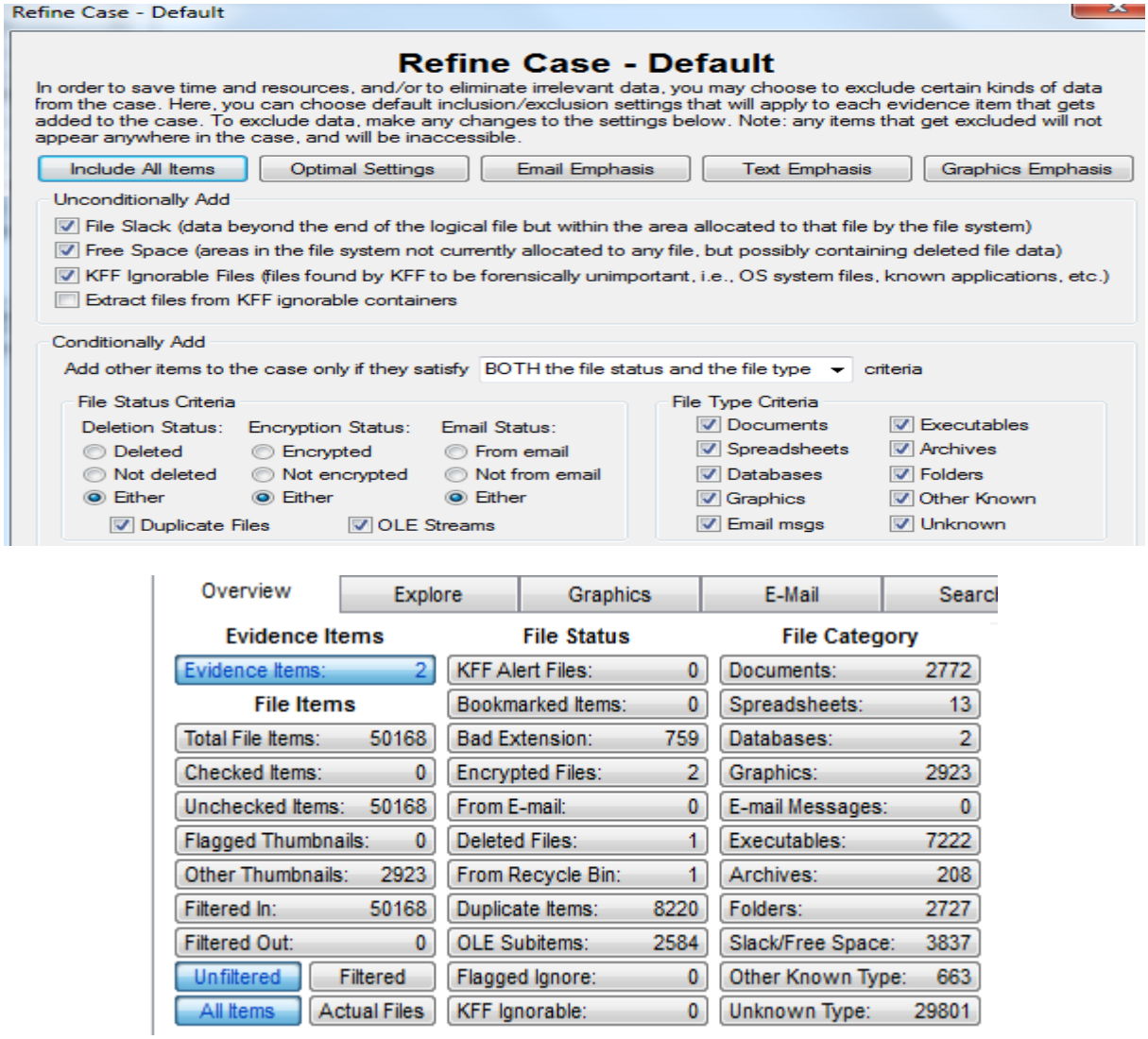
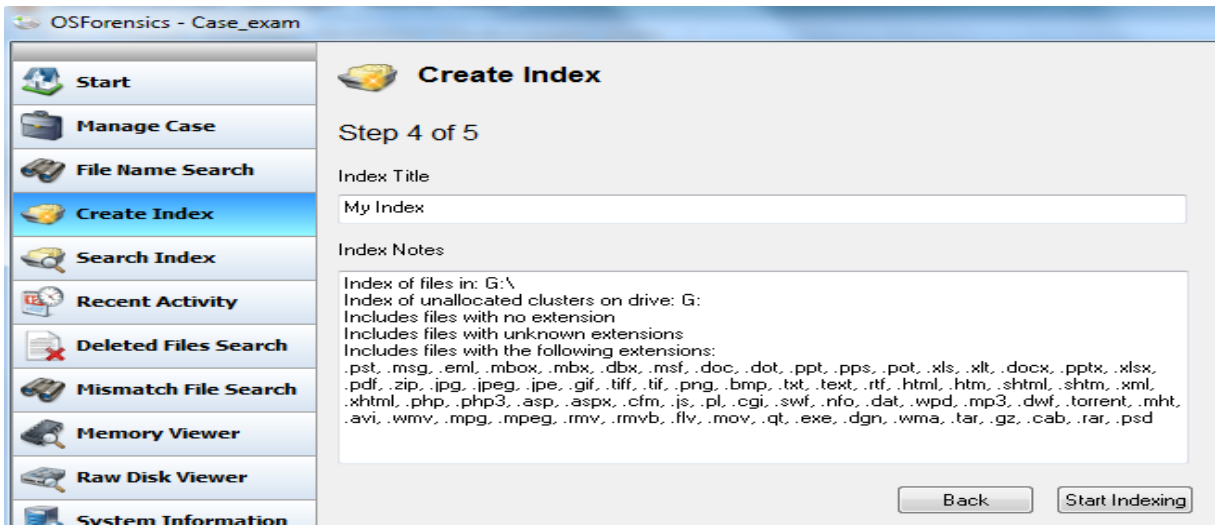


Figure 24 Création d'un index avec *Forensic Toolkit*

L'outil *OSForensics* permet lui aussi de créer un index des fichiers sur le disque analysé afin de simplifier les recherches.



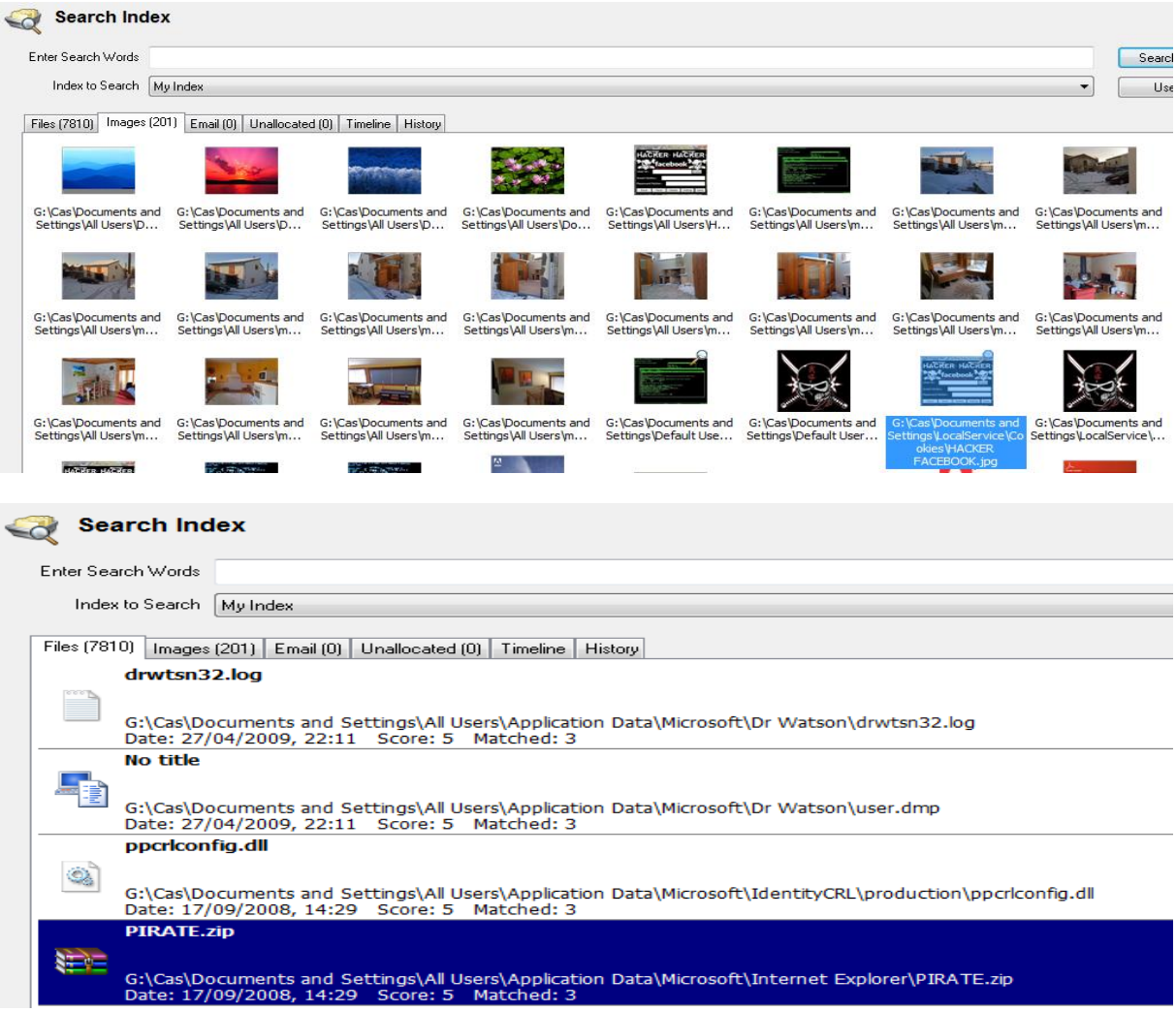


Figure 25 Création d'un index avec OSForensics

Ces outils permettent de faciliter les recherches et les investigations éventuelles (récupération des emails, images, fichiers exécutables, etc.)

j) La récupération d'informations sensibles

Peut-être une partie les plus intéressantes d'une analyse forensique : la récupération d'informations sensibles. Il y a beaucoup de types différents : mots de passe des utilisateurs de la machine, mots de passe enregistrés dans le navigateur, mots de passe des logiciels tiers… Voyons ensemble comment extraire ce type d'informations.

L'extraction des comptes utilisateurs de la machine

Toujours utile de savoir comment extraire les comptes utilisateurs d'un système Windows. Pour plus d'informations sur la manière dont Windows stocke les mots de passe des utilisateurs, le lien suivant est accessible : « Comment faire pour utiliser l'utilitaire SysKey pour sécuriser la base de données du gestionnaire des comptes de sécurité de Windows ».

Il existe de nombreux outils tels que *pwdump*[34] pour extraire les comptes utilisateurs d'un système Windows. Le souci est que ces outils ne fonctionnent que sur les systèmes on-line. Dans notre cas, nous allons devoir récupérer la clé de chiffrement système stockée localement. Pour cela, nous allons l'outil *HashDumper* [35]de *Cain*[36], outil qui permet d'effectuer des attaques réseau et de cracker des mots de passe.

Cette clé se trouve dans la ruche « *system* » du répertoire système de Windows. On ouvre *Cain* et on utilise l'utilitaire « *syskey decoder* ».

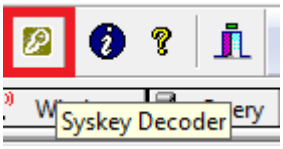


Figure 26 Syskey Decoder

Ne souhaitant pas récupérer la clé stockée localement sur notre système, on indique l'emplacement du fichier « *system* » de notre image présente dans « \Windows\System32\config » :

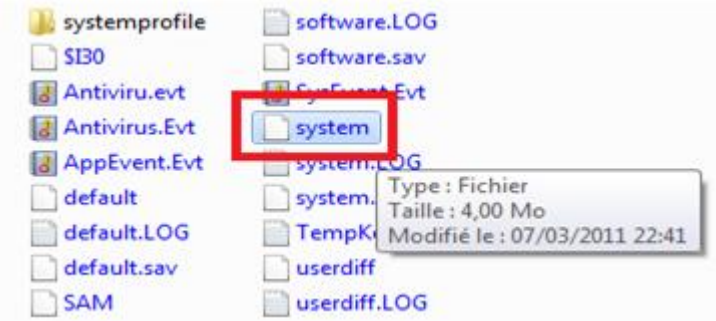


Figure 27 Emplacement de la ruche system

Cain extrait alors de manière automatique la clé de chiffrement.

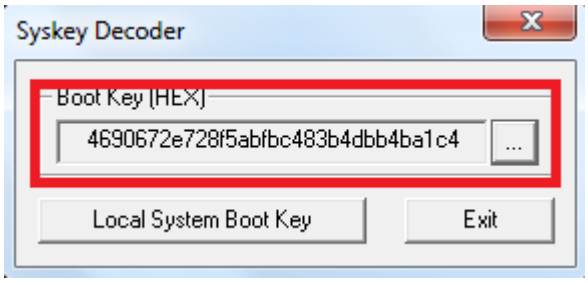


Figure 28 Extraction de la clé de chiffrement

Cette clé de chiffrement récupérée, nous allons pouvoir extraire les comptes utilisateurs de la SAM. On se rend dans l'onglet « cracking » et on clique sur la case « + ».

[34] http://syskb.com/telecharger-pwdump/
[35] http://www.oxid.it/ca_um/topics/nt_hashes_dumper.htm
[36] http://www.oxid.it/cain.html

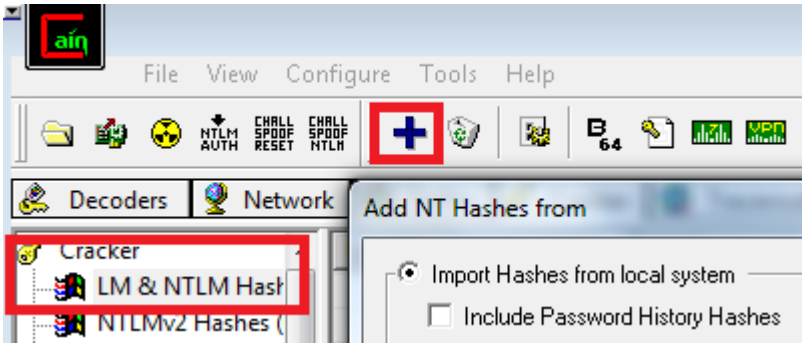
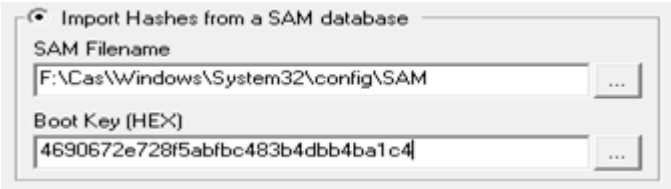


Figure 29 Extraction des comptes utilisateurs de la machine

On indique ensuite l'emplacement de la base SAM de notre image (*Windows**System32**config*) et la clé de chiffrement que nous avons récupéré précédemment.



Après avoir cliqué sur le bouton « *next* », on obtient alors l'ensemble des comptes utilisateurs du système analysé.

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type
Administrateur	* empty *		* empty *				
Invité	* empty *		* empty *				
SUPPORT_388945a0	* empty *	*		AAD3B435B51...	594BDAB2ED8...		LM & NTLM
ASPNET				FCBDBC080AB...	421F380284C5...		LM & NTLM
HelpAssistant				9FB76119A144...	32844305A9A9...		LM & NTLM
autodiagprog	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16...		LM & NTLM

Figure 30 Comptes utilisateurs extraits

Le compte administrateur a un mot de passe vide, mais si ce n'est pas le cas, *Cain* propose des méthodes pour casser le mot de passe. Un simple clic droit sur le compte permet de choisir sa méthode.

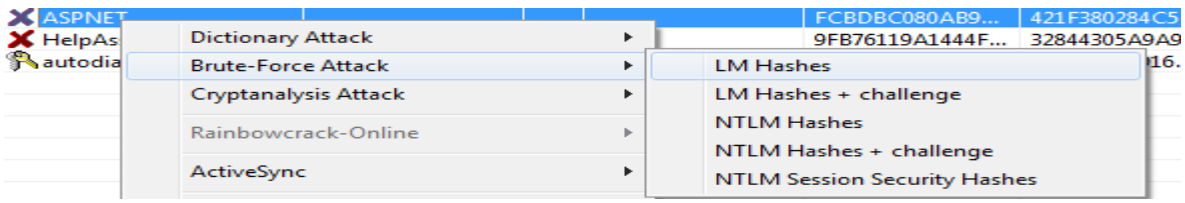


Figure 31 Cassage des mots de passe

On peut aussi obtenir le même résultat avec *OSForensics*.

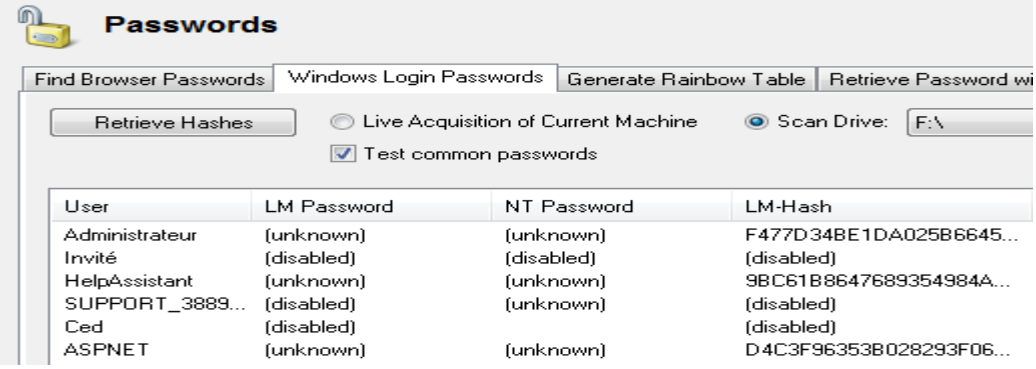


Figure 32 Récupération des hash avec OSForensics

Extraction des mots de passe des navigateurs

Pour une liste des emplacements ou Windows stocke les différents mots de passe, le document suivant est consultable en ligne : [Password Storage Locations For Popular Windows Applications]

Toujours avec *OSForensics*, il est possible de scanner une machine afin d'y récupérer les mots de passe des différents navigateurs.

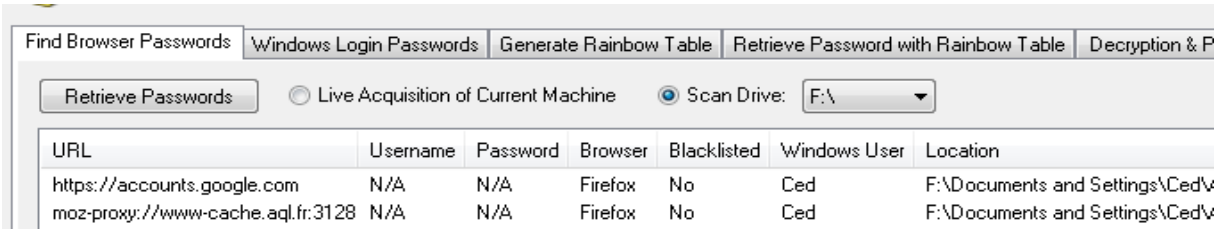
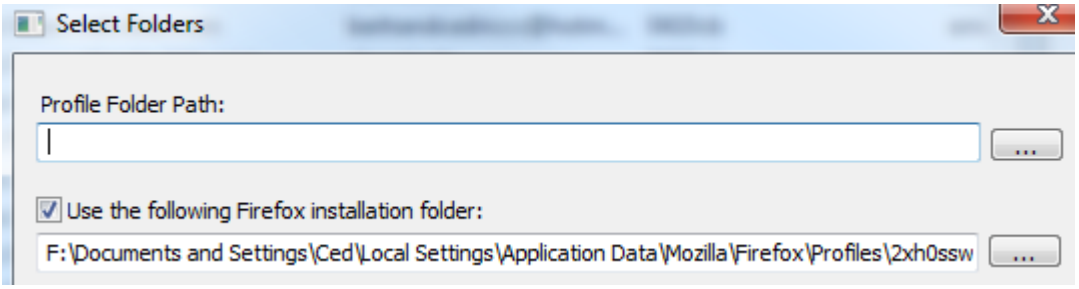


Figure 33 Récupération des mots de passe du navigateur

Néanmoins ceci ne semble pas fonctionner avec la version gratuite de cet outil, nous pouvons donc utiliser certains outils *nirsoft* afin de réaliser ces opérations. Prenons par exemple l'extraction des mots de passe de *Firefox* avec l'outil *PasswordFox*[37]. Cet outil permet d'extraire les mots de passe localement ou situé sur un disque externe. (*File -> Select folders*)



[37] http://www.nirsoft.net/utils/passwordfox.html

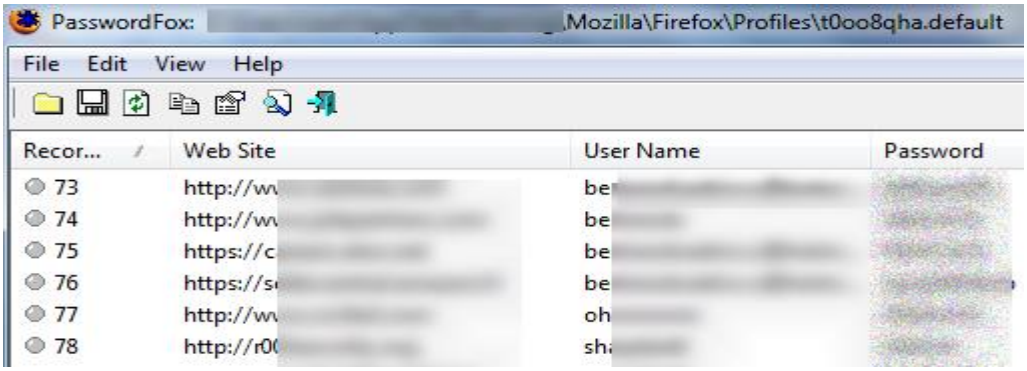
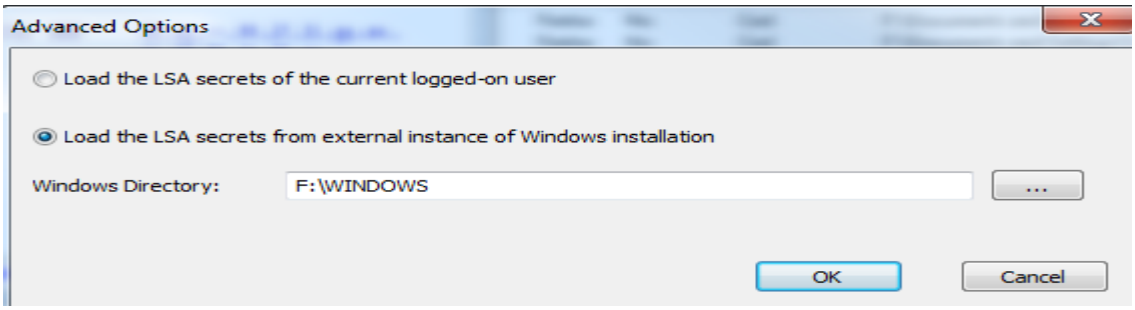


Figure 34 Récupération des mots de passe stockés par Firefox

Sur le même site, des outils existent pour les différents navigateurs : *Internet Explorer, Google Chrome, Opéra et Safari*.

Extraction des secrets LSA

LSA pour *Local Security Autority* [38]est un espace de stockage des informations tel que les mots de passe utilisés pour démarrer certains services. Pour extraire les mots de passe LSA, on peut utiliser l'outil *LSASecretsView*[39] de *Nirsoft*. Cet outil permet aussi de retrouver les mots de passe d'une machine externe.



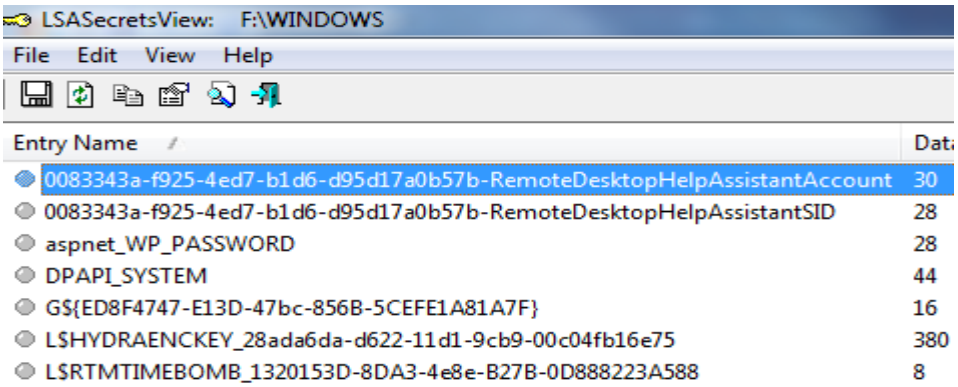


Figure 35 Extraction des secrets LSA

[38] http://www.windowsnetworking.com/kbase/WindowsTips/WindowsNT/RegistryTips/Miscellaneous/LSASecrets.html
[39] http://www.nirsoft.net/utils/lsa_secrets_view.html

Récupération du mot de passe VNC

Si le logiciel VNC est installé sur le poste analysé, il est possible d'extraire la clé de registre correspondante et de retrouver le mot de passe. Pour cela, nous pouvons utiliser l'outil *vncpwdump*[40].

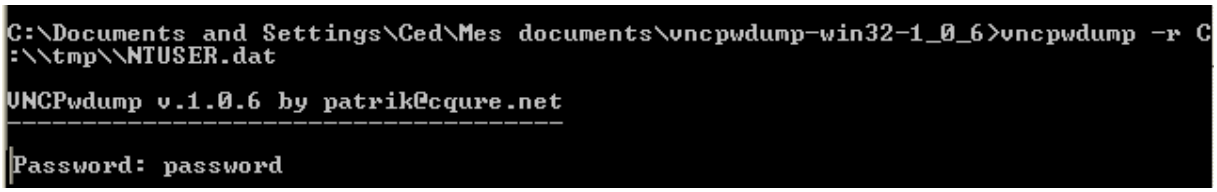


Figure 36 Récupération du mot de passe VNC

Recherche de fichiers protégés

On appelle par « fichier protégé », les fichiers qui nécessitent un mot de passe (exemple : fichier zip protégé par un mot de passe). Pour rechercher ce type de fichiers sur un poste, nous pouvons par exemple utiliser l'outil « *Password Recovery Toolkit Forensic* [41]». C'est un outil offrant de nombreuses fonctions dont le déchiffrement de conteneurs *truecrypt*, la récupération de mots de passe, le crackage de fichiers protégés, etc.

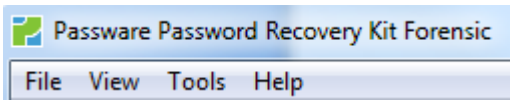


Figure 37 Password Recovery Toolkit Forensic

Pour la recherche de fichiers protégés, on choisit l'option appropriée.

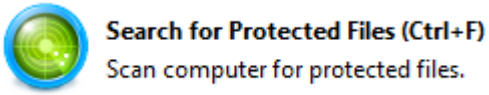
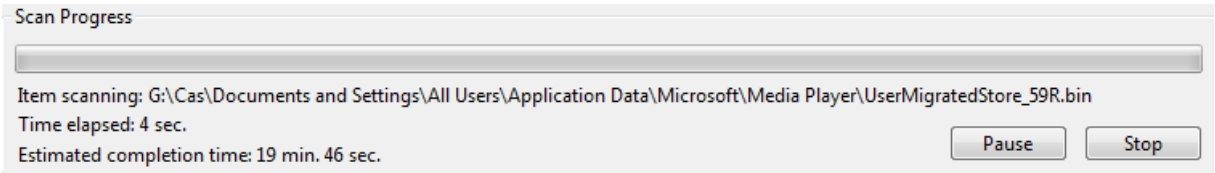
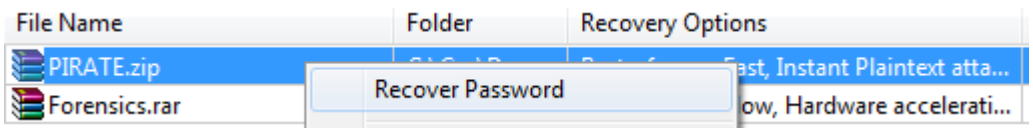


Figure 38 Recherche de fichiers protégés



Une fois qu'un fichier protégé a été trouvé, il est aussi possible de chercher le mot de passe.



De nombreuses options sont disponibles afin de retrouver le mot de passe.

[40] http://www.cqure.net/wp/vncpwdump/
[41] http://www.tracip.fr/password-recovery-toolkit.html

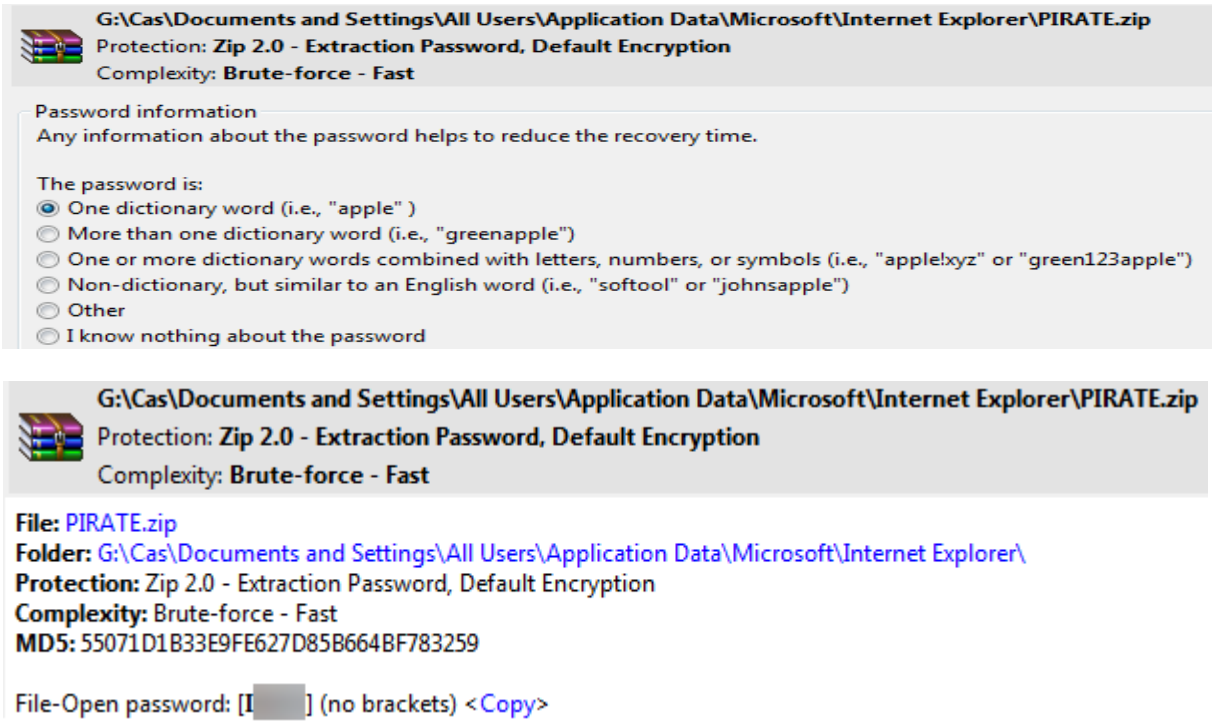


Figure 39 Crackage du mot de passe d'un fichier protégé

L'outil *OSForensics* propose aussi le même genre d'attaque.

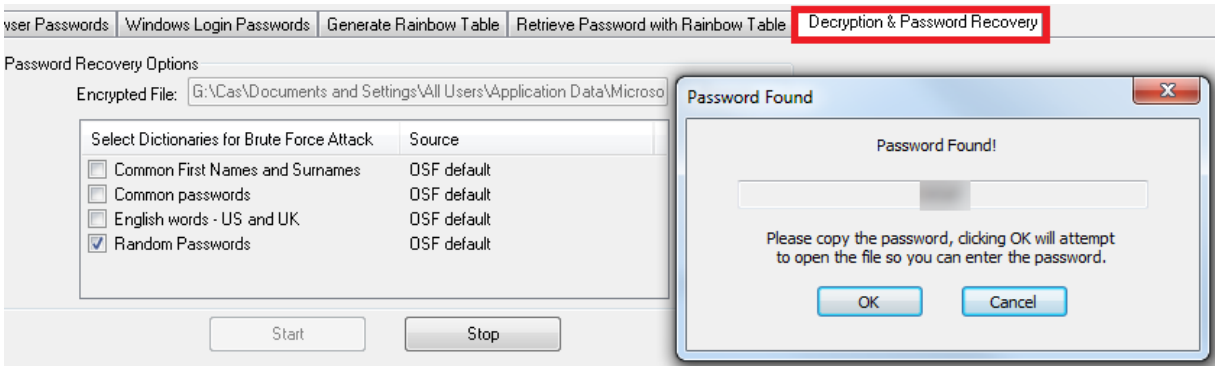


Figure 40 Cassage de mots de passe avec OSForensics

Déchiffrement de containers TrueCrypt

Une option intéressante de « *Password Recovery Toolkit Forensic* « est la possibilité de lancer une attaque pour trouver les mots de passe de containers *truecrypt*[42]. *TrueCrypt* est un outil permettant de créer des disques durs virtuels chiffrés.

[42] http://www.truecrypt.org/

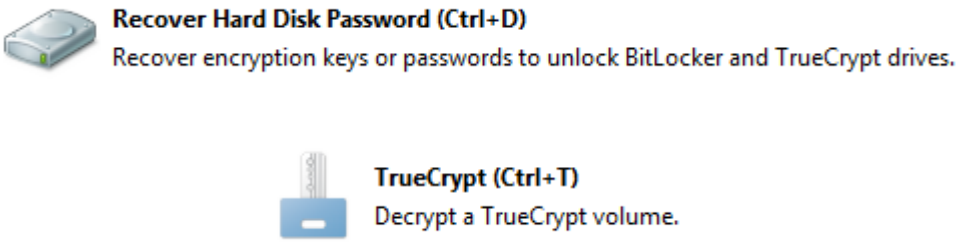
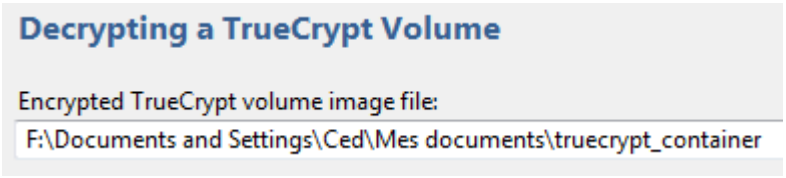
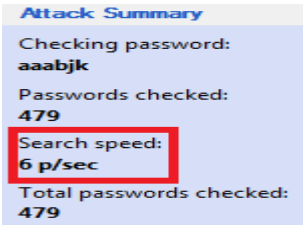


Figure 41 Crackage de containers Truecrypt

Une fois l'emplacement du container *TrueCrypt* indiqué, nous lançons une attaque de recherche de mots de passe.



Par contre la vitesse de calcul est tellement basse que sans indication du mot de passe, il est illusoire d'espérer le trouver.



Néanmoins une option de l'outil est de permettre de rechercher la trace de clé de chiffrement *aes*[43] dans la mémoire vive, ce qui permet le déchiffrement rapide d'un container TrueCrypt.

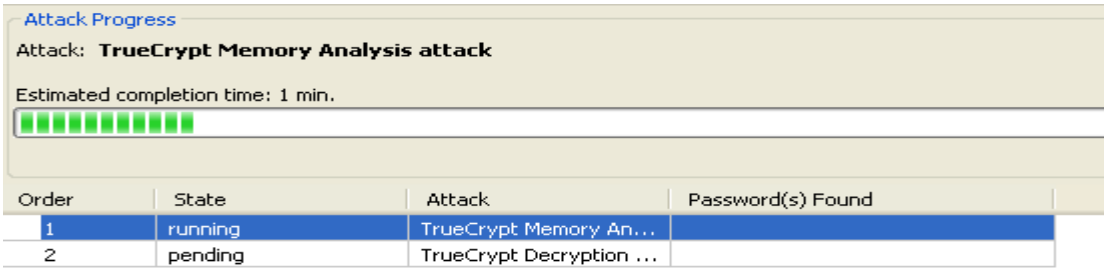
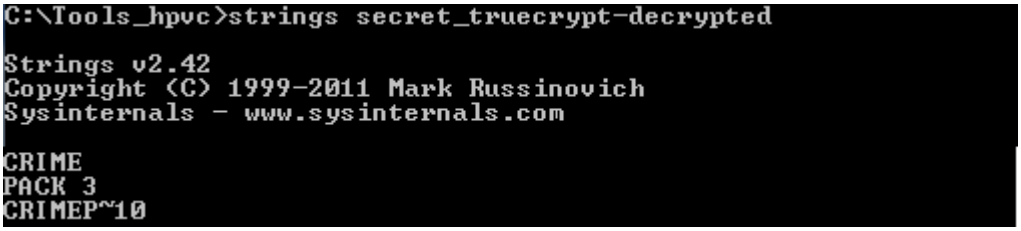


Figure 42 Cassage d'un container TrueCrypt par analyse de la mémoire vive

Volume image file: secret_truecrypt
Folder: C:\Documents and Settings\Ced\Mes documents\
Physical memory image file: memdump_xp.mem
Folder: C:\Documents and Settings\Ced\Mes documents\Capture\
Protection: TrueCrypt Volume - Open Password, TrueCrypt AES Encryption
Complexity: Instant Unprotection

Unprotected file: secret_truecrypt-decrypted

[43] http://fr.wikipedia.org/wiki/Advanced_Encryption_Standard



Malgré tout il faut rester réaliste, car cette méthode nécessite de faire une capture de la mémoire vive pendant que le container *TrueCrypt* est ouvert, ce qui est assez peu probable en situation réelle.

Récupération d'autres mots de passe

La machine analysée peut contenir de nombreux autres logiciels tiers installés dont la récupération d'informations sensibles est possible. Réaliser leur liste exhaustive étant impossible, je me contenterais d'en citer quelques uns, je laisse le soin aux lecteurs motivés d'effectuer leurs propres recherches :

- *FileZilla*[44] (serveur FTP) : "*Password Recovery for FileZilla*[45]"
- *Remote Desktop* [46]: "*Remote Desktop Passview*[47]"
- Mot de passes VPN, RAS, dialup *: dialupass*[48]

Pour savoir quels sont les logiciels installés sur le poste, la chose la plus simple à faire est de consulter le répertoire « \program files » et de faire une liste des logiciels qui pourraient contenir des informations intéressantes à récupérer.

[44] http://filezilla.fr/
[45] http://www.reactive-software.com/filezilla-password-recovery.html
[46] http://fr.wikipedia.org/wiki/Remote_Desktop_Protocol
[47] http://www.nirsoft.net/utils/remote_desktop_password.html
[48] http://www.nirsoft.net/utils/dialupass.html

Conclusion

Ce document a uniquement traité de l'analyse forensique à froid c'est-à-dire quand le système est éteint. Nous avons pu constater que nombreux sont les outils qui permettent d'analyser et d'aider à l'analyse de ce type de système. Il n'est bien sûr pas exhaustif et de nombreux points tels que la recherche de *malwares*[49], l'expertise judiciaire, la détection d'une intrusion n'ont pas été abordés. Ces points nécessitent souvent d'autres connaissances techniques que je n'ai pas souhaité détailler dans ce document.

Une autre approche intéressante et qui offre de nombreuses possibilités concerne l'analyse de la mémoire vive. Si le thème vous intéresse, je ne peux que vous suggérer de vous initier au framework *Volatility*[50]. Un excellent document réalisé par *Devoteam* traite de l'analyse de la mémoire vive : Livre blanc Devoteam – H@ckRAM, attaques contre la mémoire.

Si le domaine de l'analyse forensique du point de vue expertise judiciaire vous intéresse, je vous suggère aussi l'excellent blog de *Zythom* qui contient de très nombreux articles intéressants sur le thème :

- Comment devenir un expert judiciaire
- Demande d'informations
- Le rapport d'expertise
- Récupération d'images et plus encore
- La récupération des données, faites la vous-même

Un document pdf regroupant l'ensemble de ces posts est d'ailleurs disponible : « Dans la peau d'un informaticien expert judiciaire T1 ».

Je ne puis aussi que vous conseiller l'excellent magazine *MISC* qui traite bien souvent des problématiques liées à l'analyse forensique. Le numéro 56 y est d'ailleurs consacré.

Vous trouverez aussi dans la partie bibliographie dans de nombreux liens pour aller plus loin.

En cas de suggestions, critiques ou autres, vous pouvez toujours m'écrire à bertrandcedricc@hotmail.fr

[49] http://fr.wikipedia.org/wiki/Logiciel_malveillant
[50] https://www.volatilesystems.com/default/volatility

Challenges

Ci-joint une liste de challenges afin de tester ses connaissances dans le domaine de l'analyse forensique.

Digital Forensic Challenge

The Forensic Challenge

Rooted

Forensic Challenge

DFRWS 2005 Forensics Challenge

Test Images and Forensic Challenges

Forensic Contest

Live-Cd forensics

Il existe de nombreuses distributions dédiées à l'analyse forensique. En voici quelques-unes.

Helix

Helix est une distribution GNU/Linux Ubuntu customisée intégrant un ensemble d'outils destinés à attaquer, évaluer la sécurité et la compromission d'une machine ou d'un réseau.

http://www.e-fense.com/products.php

Caine (Computer Aided INvestigative Environment Digital Forensics)

CAINE est une solution Live[CD|USB] d'interopérabilité qui regroupe, en tant que modules, un grand nombre d'outils Open Source pour faciliter, via une interface graphique homogène, la collecte de données et la recherche légale de preuves numériques sur un ordinateur compromis.

http://www.caine-live.net/

Deft

DEFT Linux est un live-CD désormais basé sur Ubuntu et intégrant une panoplie d'applications open-source spécialement destinées aux enquêtes de criminalité informatique.

http://www.deftlinux.net/

Backtrack 5

Basée sur Ubuntu depuis la version 4, son objectif est de fournir une distribution contenant l'ensemble des outils nécessaires aux tests de sécurité d'un réseau. Elle contient aussi de nombreux outils consacrés à l'analyse forensique.

http://www.backtrack-linux.org/

COFEE (*Computer Online Forensic Evidence Extractor*)

Outil relativement privé et confidentiel fourni par Microsoft aux services de police. Contient plus de 150 outils destinés à récupérer des preuves sur un ordinateur. Disponible sur Internet suite à une fuite.

Bibliographie

Criminalités numériques

http://blog.crimenumerique.fr

Blog d 'un informaticien expert judiciaire

http://zythom.blogspot.fr/

Wiki Forensics

http://www.forensicswiki.org/

Analyse forensique d'un système Windows

http://devloop.users.sourceforge.net/index.php?article29/analyse-forensique-d-un-systeme-windows-partie-1

Analyse complètement sick – Les tutos de nicos

http://www.lestutosdenico.com/outils/analyse-forensique-completement-sick

Détection d'une intrusion et réalisation d'un audit post-mortem

http://stankiewicz.free.fr/Wikka/wikka.php?wakka=HowtoForensic

Misc - Recherche de malwares à froid

Misc n°56 – Forensics : Les nouveaux enjeux