Techniques d'enquête et outils

HackerSpace

23 juillet 2015

Nadia Vigneault
Claude Charest

Bureau de sécurité de l'information
Université Laval

La confiance règne. **Ensemble,** nous y veillons.

bsi.ulaval.ca

UNIVERSITÉ LAVAL
Bureau de sécurité de l'information

Qui sommes-nous?

Nadia Vigneault
Conseillère en sécurité de l'information
Claude Charest
Conseiller en sécurité de l'information

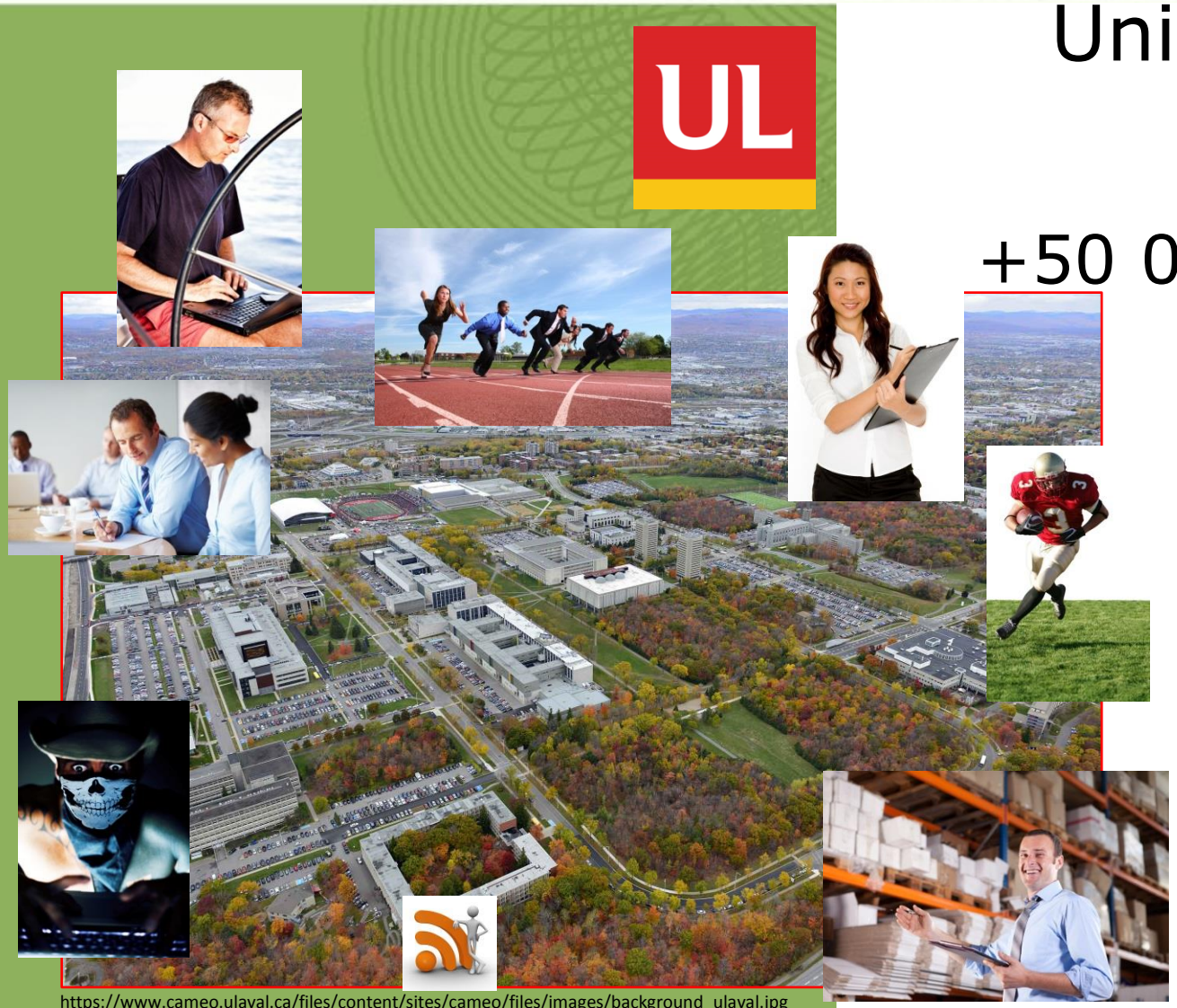
Nos responsabilités :

1- Gestion des incidents de sécurité de l'information;
2- Soutient informatique aux enquêtes touchant à la sécurité de l'information;
3- Gestion des vulnérabilités.

Bureau de sécurité de l'information de l'Université Laval
bsi.ulaval.ca

UNIVERSITÉ LAVAL
Bureau de sécurité de l'information

Première partie



https://www.cameo.ulaval.ca/files/content/sites/cameo/files/images/background_ulaval.jpg

Université Laval

-> 1852

+50 000 utilisateurs

étudiants &
employés

57 unités &
17 facultés qui
couvrent tous
les domaines du
savoir

Première partie

BSI :

Nous visons à être reconnu par l'Université Laval :
- comme le centre d'expertise en matière de sécurité de l'information (SDI) et comme un agent de promotion et de développement d'une **saine culture de gestion du risque**;
- comme un joueur important en SDI auprès des organismes publics et privés du Québec.

Sous la responsabilité du Vice-rectorat exécutif et au développement, nous avons pour mandat d'assurer la sécurité de l'information (SDI) de l'ensemble des unités d'enseignement, de recherche et d'administration de l'Université Laval.

Ce mandat repose sur le maintien des trois propriétés essentielles à l'information :

- son intégrité : propriété d'une information de n'être détruite ou altérée de quelque façon, sans autorisation;
- sa disponibilité : propriété d'une information d'être accessible en temps voulu et de la manière requise par une entité ou une personne autorisée;
- sa confidentialité : propriété d'une information de n'être accessible qu'aux seules entités ou personnes autorisées.

Un total de 11 employés

Directeur : Douglas Doyer

UNIVERSITÉ LAVAL
Bureau de sécurité de l'information

Sujet de la présentation d'aujourd'hui

Enquêtes, Processus, Outils & Techniques utilisées pour collecter des **preuves numériques** d'une utilisation non autorisée des équipements, de vol de temps, de téléchargements illégaux, etc... à l'Université Laval.

Le Bureau de sécurité de l'information (BSI) a la responsabilité de répondre aux incidents de sécurité, de surveiller le réseau et d'enquêter sous mandat.

Lors de notre présentation, nous vous présenterons nos techniques d'enquêtes, nos mandats, nos défis et nos outils.

On verra que faire des enquêtes informatiques est un travail passionnant... les outils sont de plus en plus performants, souvent gratuits, parfois complexes, mais le « forensic » est un monde fascinant.

Plan de la présentation

1- Université Laval & BSI ✓
2- Partenaires
3- Mandats & portée
4- Enquête & types
5- Processus d'enquête & normes
6- Techniques & outils d'enquête
7- Extra – Bonus!

Principaux partenaires :

Internes :

DTI : +200 employés

SSP : +15 employés

https://www.dti.ulaval.ca/
http://www.ssp.ulaval.ca/

Externes :

CCRIC & Cert/AQ

http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-fra.aspx
http://www.cspq.gouv.qc.ca/faire-affaire-avec-le-cspq/famille-de-services/sous-famille-de-services/services/service/gestion-des-incidents-gouvernementaux-certaq/?no_cache=1

Mandats & portée :

Mandats d'enquête proviennent du SSP

Techniques et outils d'enquête proviennent du BSI

Support technologique provient de la DTI

BSI :

Pas d'enquêtes criminelles

Types d’enquête :

Enquêtes administratives

Utilisation non-autorisé des équipements

Téléchargements illégaux

Réponse à un incident de sécurité

Peu importe le média sur lequel les preuves se retrouvent, les étapes d'enquête vont exiger un protocole légal d'investigation :

- identifier la source ;
- acquisition de l'image du média;
- respecter l'intégrité des données récoltées;
- restaurer et extraire les données de ces médias ;
- analyser le tout ;
- rédiger le rapport final.

Enquête informatique

On peut définir celle-ci en disant simplement que c'est l'application de différentes techniques d'investigation respectant les procédures légales pour recueillir la preuve numérique.

L'investigation regroupe plusieurs méthodes qui permettent de cueillir, identifier, restaurer, extraire, analyser la preuve numérique pour reconstruire un événement/incident dans le cadre de la production d'un rapport qui sera remis à un enquêteur.

Ces techniques et méthodes viennent soutenir celles plus traditionnelles pour compléter le dossier de la preuve (entrevue de témoins, etc.).

Cinquième partie

ISO/IEC27037

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

5.4.2 Identification
5.4.3 Collection
5.4.4 Acquisition
5.4.5 Preservation

Normes internationales:

NIST SP800-86

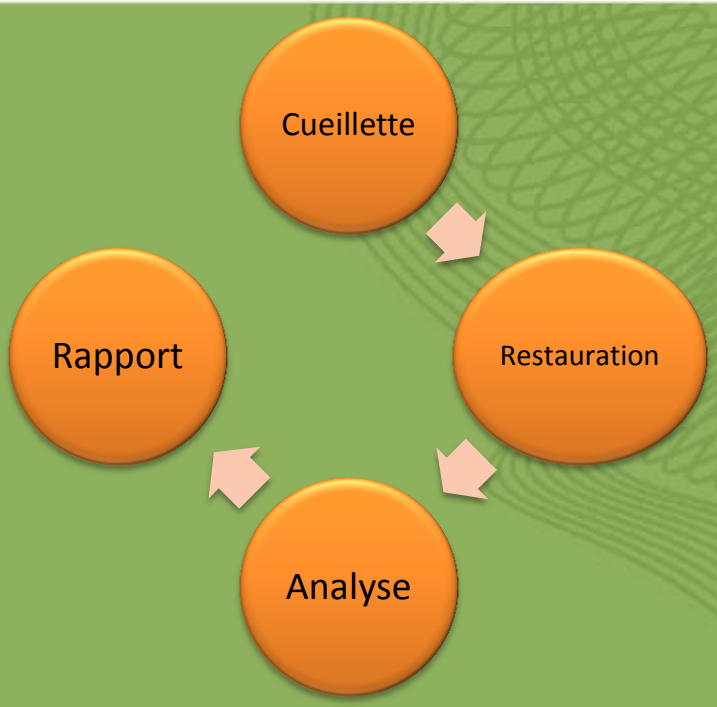
Guide to Integrating Forensic Techniques into Incident Response

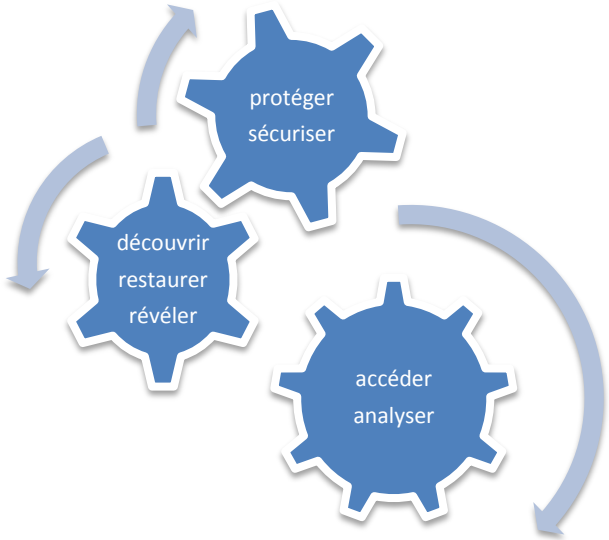
3.1 Data Collection
3.2 Examination
3.3 Analysis
3.4 Reporting
3.5 Recommendations

UNIVERSITÉ LAVAL
Bureau de sécurité de l'information

Cinquième partie

Processus :





Cueillette - média (contexte physique)

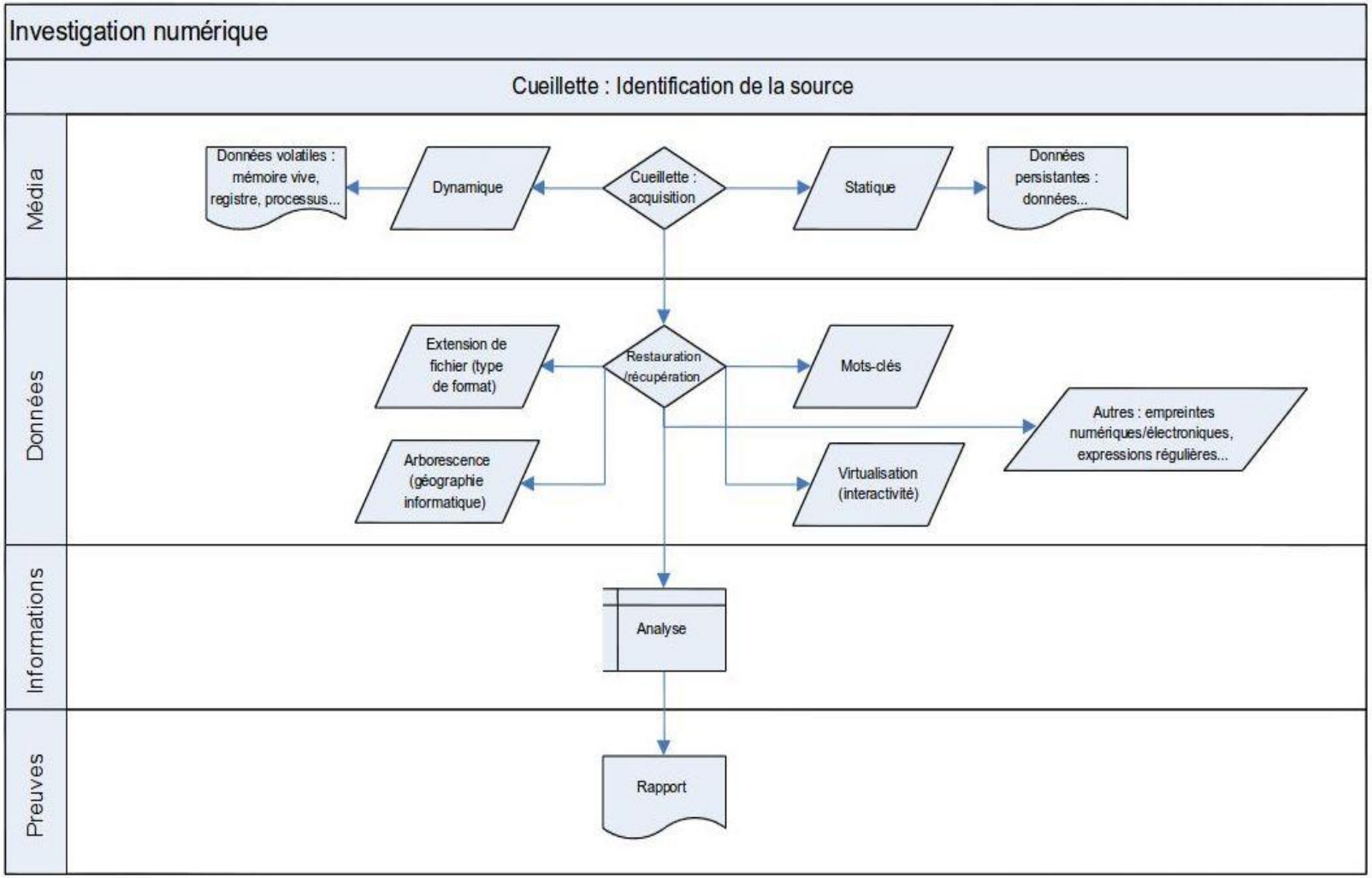
Restauration - données (contexte logique)

Analyse - informations (contexte légal)

Rapport - preuves (contexte légal)

http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
http://www.digitalevidencepro.com/Resources/Approach.pdf
http://www.forensicfocus.com/computer-forensic-tools-investigation

Processus :



Cinquième partie

Physique : les sources peuvent être localisées dans différents médias physiques, comme des disques durs, dvd, clé USB;

Local : les sources d'informations devront être identifiées à travers, par exemple, le réseau;

Distant / virtuel : les sources peuvent être géolocalisées physiquement dans différents endroits, comme auprès des fournisseurs de services Internet, hébergeurs ou fournisseurs de services infonuagiques. Plusieurs informations de surveillance devront être identifiées (pour la corrélation de preuves) comme les fichiers journaux des différents serveurs, etc.

Nadia Vigneault 2014-2015 : INVESTIGATION DE SYSTÈMES VIRTUELS ET NON-CONVENTIONNELS : TRACES ET PREUVES

L'identification des sources se retrouve face à divers types de potentialités :

Une enquête peut être étendue sur plusieurs semaines / mois!

Patience!!!!!!

Processus d'enquête au BSI :

On reçoit une demande de la part du SSP

On précise la portée du mandat

On établit notre stratégie d'enquête

On teste des logiciels et notre technique

On passe à l'action!

Sixième partie

Peu importe la technique choisie parmis les 4 premières, nous aurons toujours :

- Une étape de restauration/extraction des données
- Une étape d'analyse des données cueillies
- Un rapport final

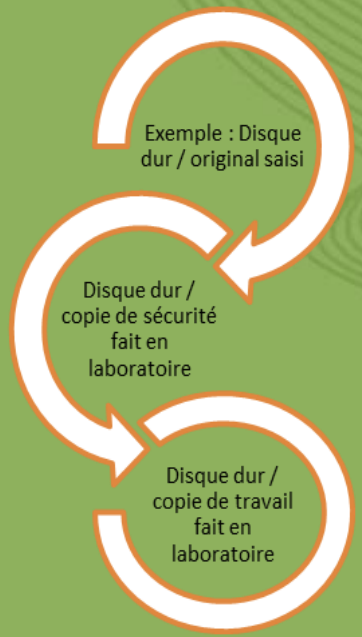
Techniques d'enquête :

"Computer forensic"
"Live forensic"
"Network forensic"
"Remote forensic"
…Cyber-intelligence

Sixième partie

Faire une image bit-a-bit d'un média (disque dur, clé USB…) avec un matériel et un logiciel spécialisés

Toujours travailler sur une copie de travail!



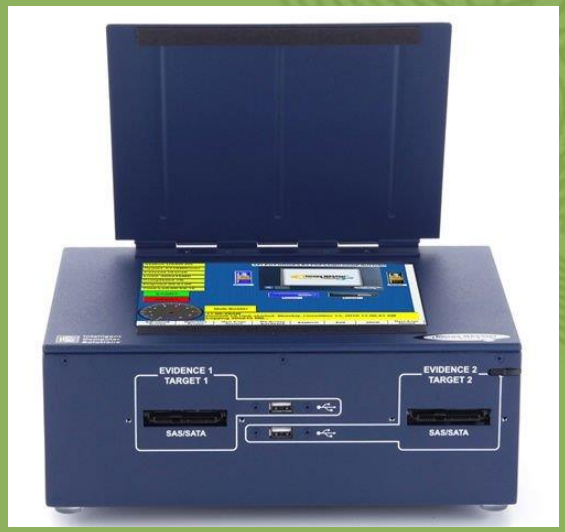
Nadia Vigneault 2014-2015 : INVESTIGATION DE SYSTÈMES VIRTUELS ET NON-CONVENTIONNELS : TRACES ET PREUVES

"Computer forensic"

Acquisition statique d'un média

Ordinateur est fermé!

Acquisition :



Ics Solo 4 Forensic

http://www.ics-iq.com/

Matériel: Protecteur d'écriture

Tableau

https://www.guidancesoftware.com/products/Pages/tableau/products/forensic-bridges.aspx

Outils intéressants :

* AccessData : FTKToolkit, MPE+, Triage, FTKImager & Registry Viewer
* Get Data : Forensic Explorer, Forensic Imager
* Belkasoft Evidence Center

Autopsy (version Windows ou Linux TSK)
DFF
OSForensics
USB device forensics
Winhex
Dd
Bulk extractor
Registry Decoder
GuyMager
Cyclone

Plates-formes : Deft-Linux – Kali-Linux

* Produits commerciaux

"Computer forensic"

Recherches :

- utilisation de métadonnées :
signature de fichiers;
extensions de fichiers;
autres propriétés de fichiers (date MAC, nom, taille).
- utilisation des données :
empreintes numériques (valeur de hachage);
mots-clés / phrases-clés;
expressions régulières.
- exploration du contenu :
arborescence (géographie informatique du système de fichiers);
informations résiduelles (fichiers effacés, orphelins, balances de fichiers et de partitions, secteurs non-alloués).

Nadia Vigneault 2014-2015 : INVESTIGATION DE SYSTÈMES VIRTUELS ET NON-CONVENTIONNELS : TRACES ET PREUVES

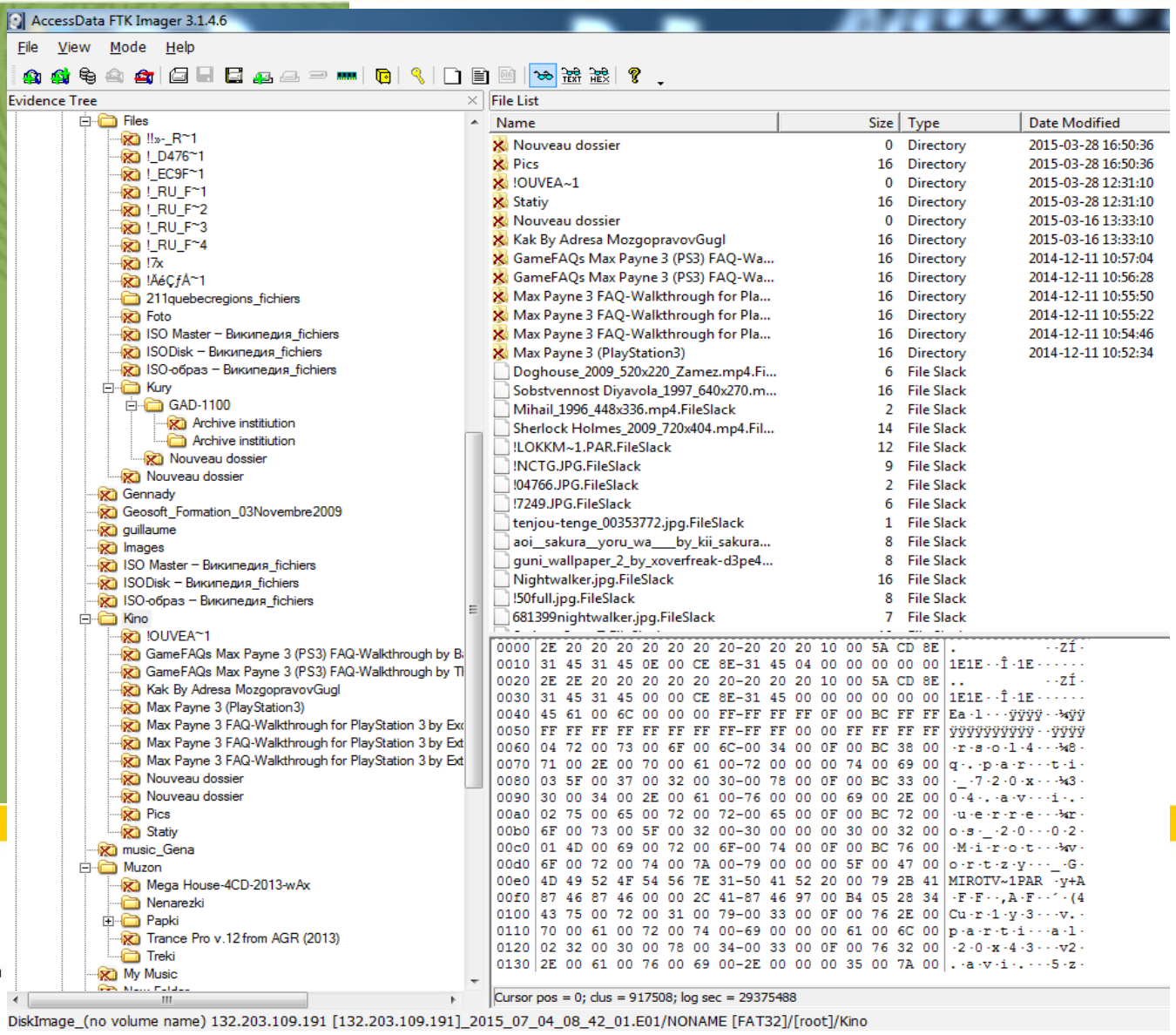
"Computer forensic"

Recherche de preuves

Sixième partie

Arborescence des fichiers :

FTK Imager



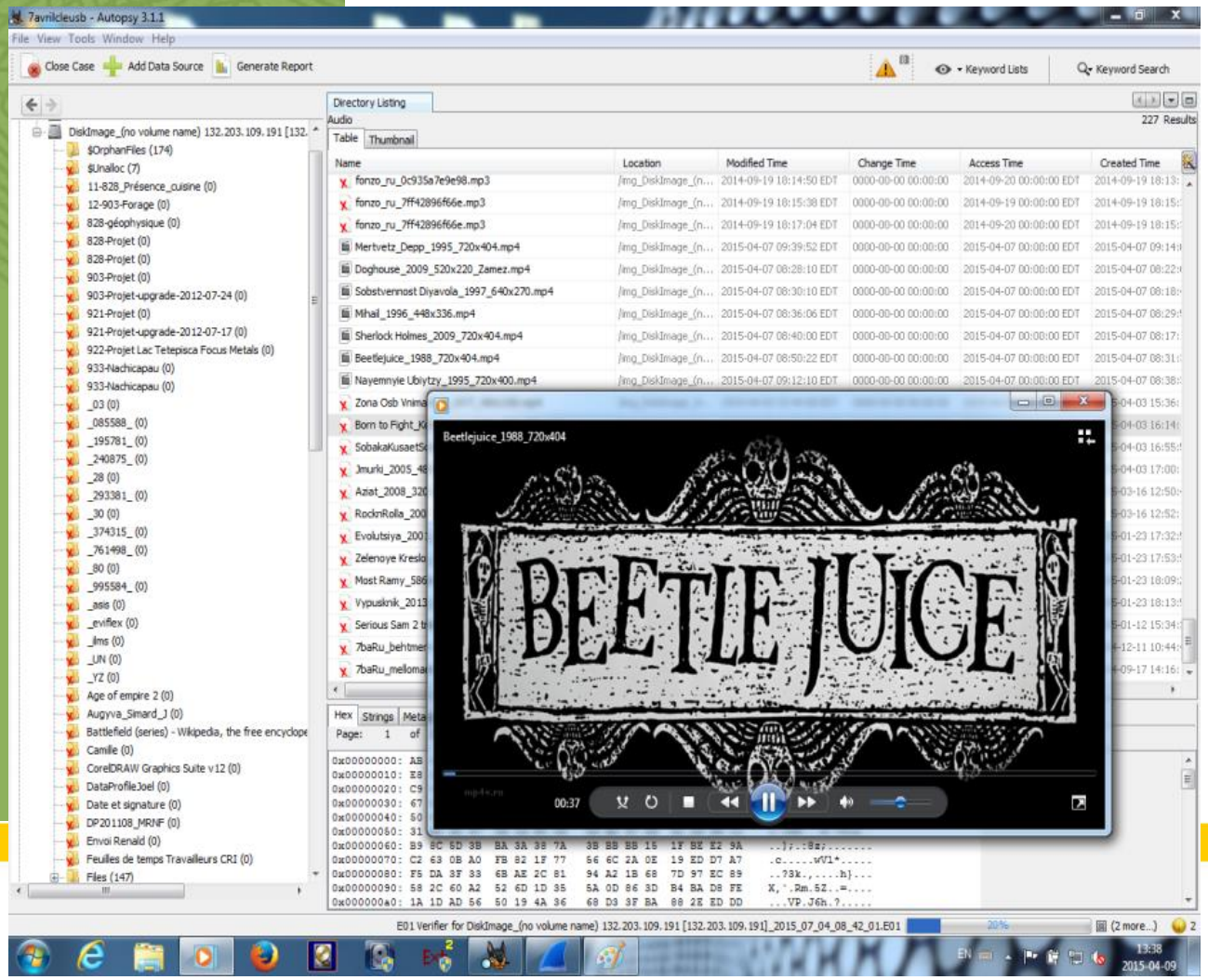
UNIVERSITÉ LAVAL

Bureau de sécurité de l'information

Sixième partie

Fichiers actifs & supprimés :

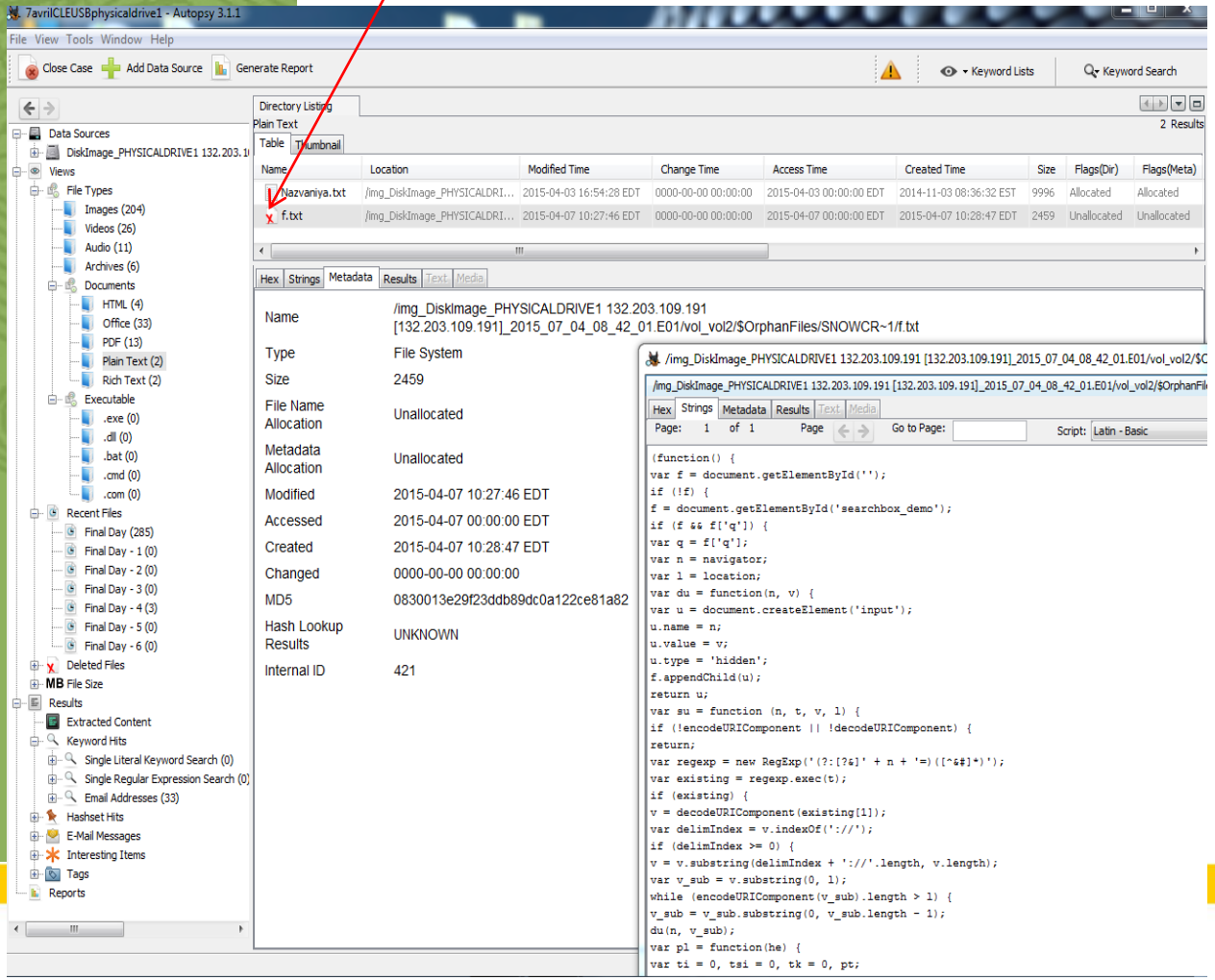
Autopsy



Sixième partie

Visualiser le contenu d'un fichier supprimé :

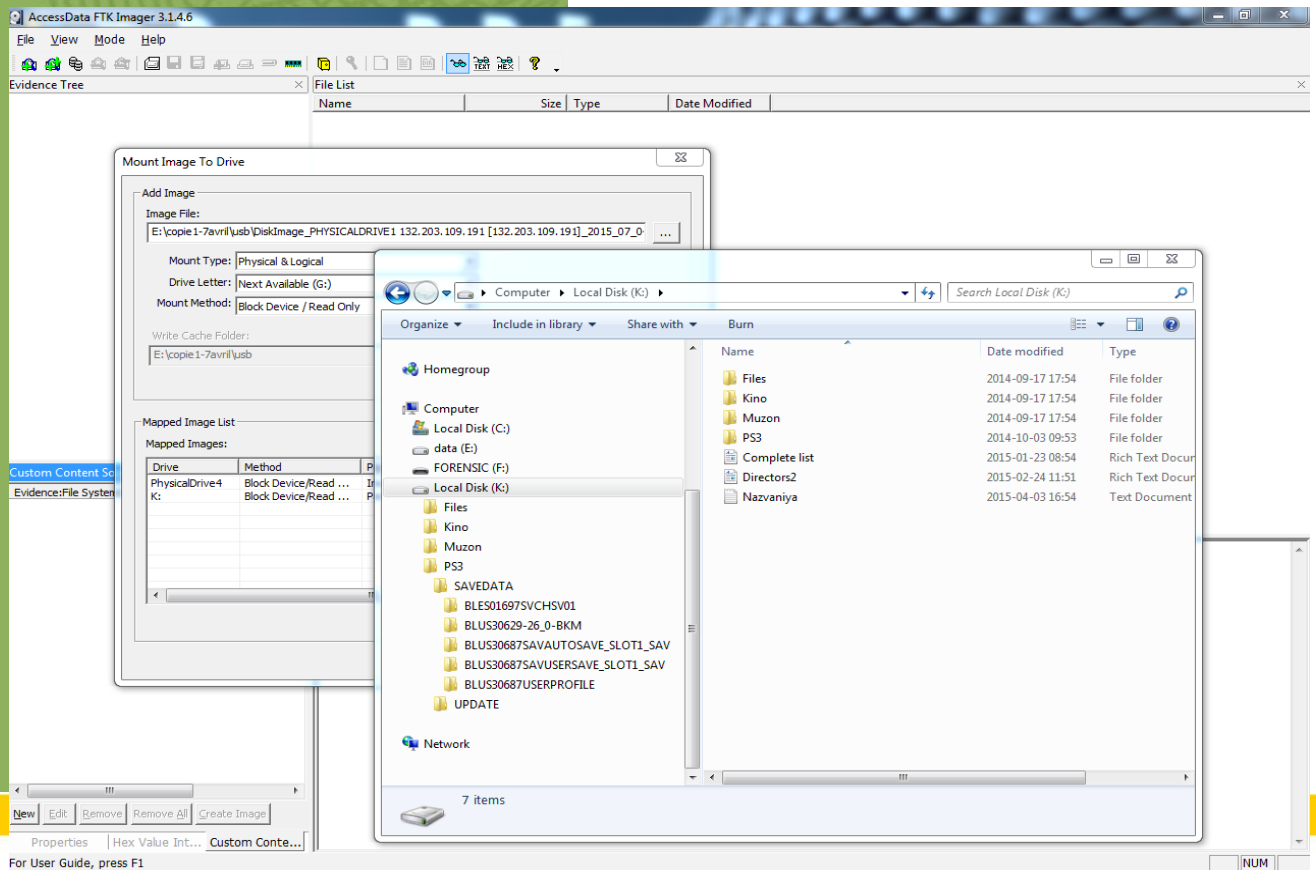
Autopsy



Bureau de sécurité de l'information

Montage d'une clé USB :

FTK Imager

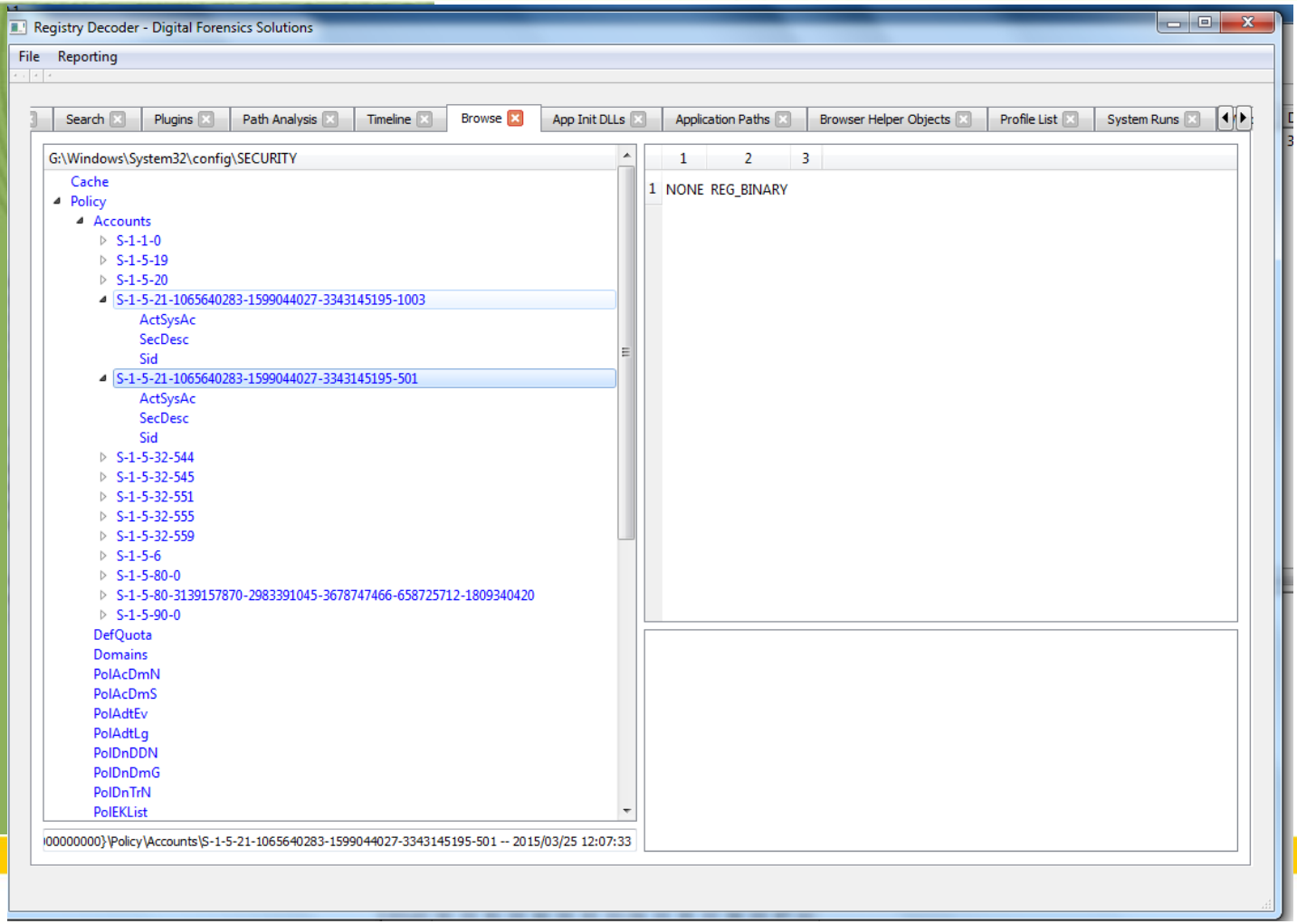


UNIVERSITÉ LAVAL
Bureau de sécurité de l'information

Sixième partie

Analyse du registre Windows :

Registry Decoder

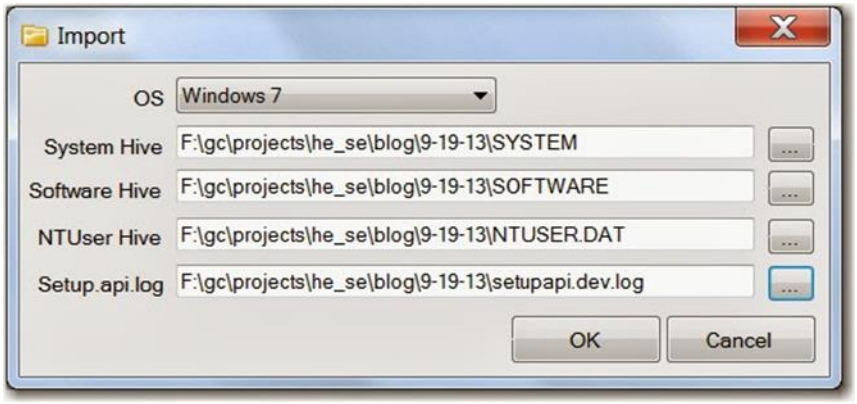


UNIVERSITÉ LAVAL
Bureau de sécurité de l'information

Croisement de 4 fichiers du registre Windows :

System
Sofware
NTUSER.dat
SetUpAPI

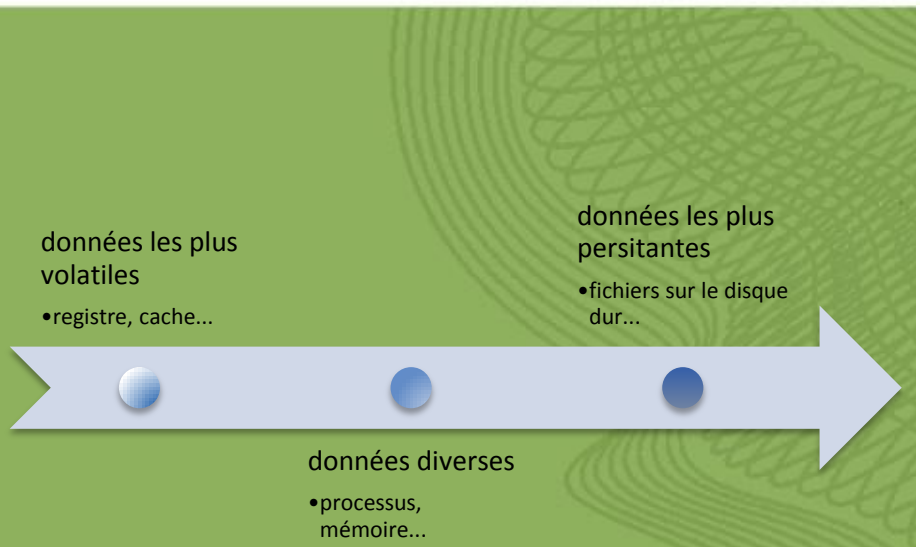
USBDeviceForensics



http://www.hecfblog.com/2013_09_01_archive.html

Vendor	Product	Version	Serial No	VID	PID	ParentIdPrefix	Drive Letter	Volume Name	GUID
Ven_	Prod_USB_Flash_Memory	Rev_5.00	0DE15280E2D1C89F	VID_0930	PID_6545				7037e1cc-ee5e-11e4-827e-e839355c0918
Ven_Kingston	Prod_DataTraveler_2.0	Rev_1.00	08606E6D3FDAFE7047062957	VID_0951	PID_1665				a574a44e-fedf-11e4-828d-e839355c0918
Ven_Kingston	Prod_DataTraveler_3.0	Rev_PMAP	00190F0C02ADBE50D96784C9	VID_0951	PID_1666		E:		ea3bffe1-084c-11e5-8296-e839355c0918
Ven_Staples	Prod_Relay_UFD	Rev_1.10	20044320330A41B1FFC9	VID_0781	PID_5202				a36e8e10-045f-11e5-8294-e839355c0918
Ven_USB	Prod_Flash_Disk	Rev_1100	FBA1004150005484	VID_090C	PID_1000				

Sixième partie



"Live forensic"

Acquisition dynamique et la capture des données volatiles

Ordinateur est ouvert!

Outils intéressants :

Capture :
AccessData : FTKToolkit, FTKImager
RamCapturer
SysinternalsSuite
NirSoft
UserDump
Mandiant RedLine

Extraction / Analyse :
Volatily Framework
Belkasoft Evidence Center

Plates-formes : Deft-Linux – Kali-Linux

"Live forensic"

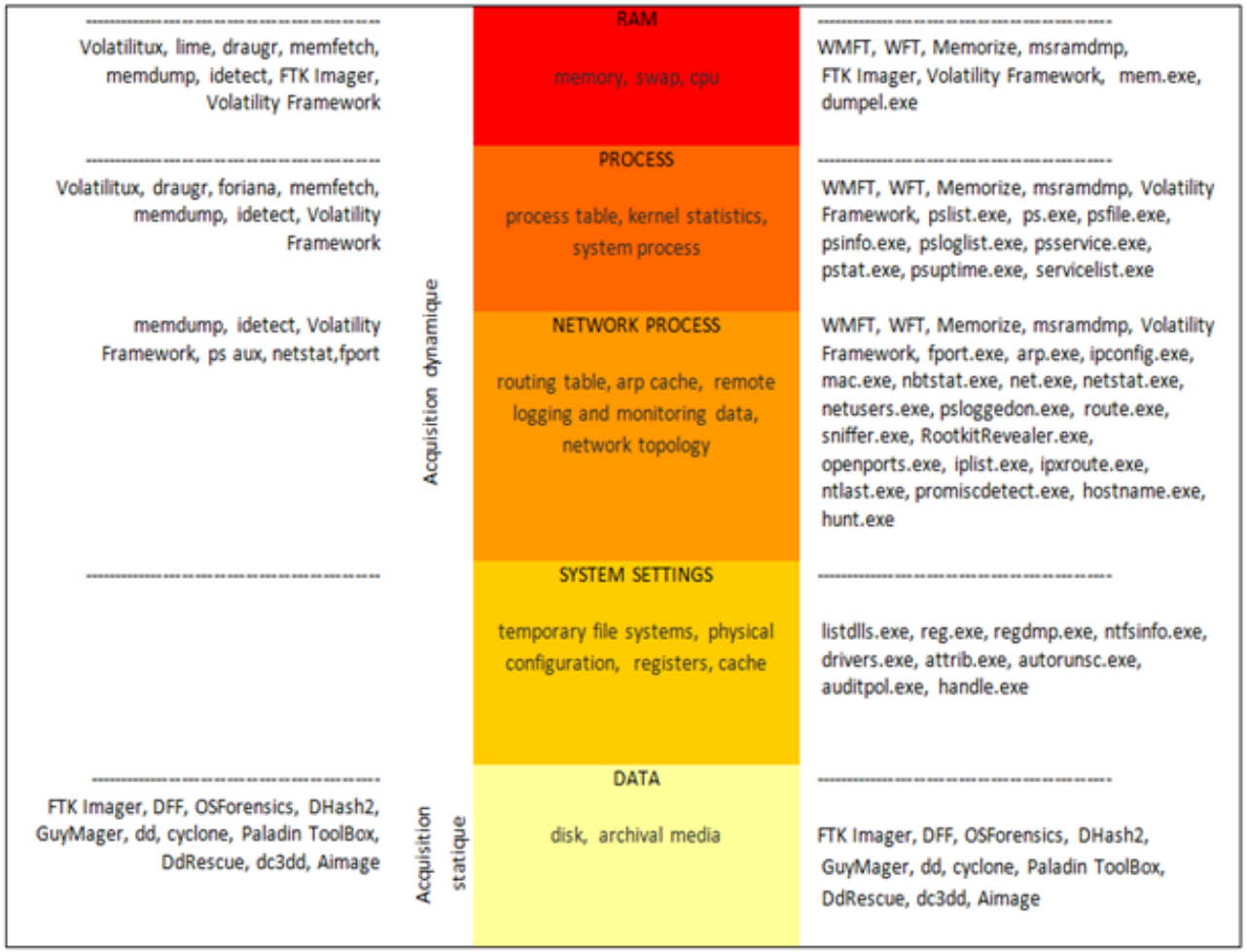
Capture de données volatiles :

RFC 3227 chapitre 2.1 : Order of volatility

rfc3227.txt

https://tools.ietf.org/html/rfc3227#section-2.1

Volatilité des données



Sixième partie

volatility
An advanced memory forensics framework

vol.py --profile=Win7SP1x64 -f “nom_img” filescan > filescan.txt

0x000000021bc6e9e0 16 0 R—rw \Device\HarddiskVolume3\Nazvaniya.txt
0x000000021bef7bc0 1 1 R--rw- \Device\HarddiskVolume3\Kino\ZolotoyVek_II_2012_720x304.avi.lb4b6t3.partial

vol.py --profile=Win7SP1x64 -f “nom_img” hivedump -o 0xfffff8a00000d010 > hivedumpsystem.txt

2015-03-18 12:02:54 UTC+0000 \CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661}\##?#WpdBusEnumRoot#UMB#2&37c186b&1&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_STAPLES&PROD_RELAY_UFD&REV_1.10#20044320330A41B1FFC9&0##{10497b1b-ba51-44e5-8318-a65c837b6661}\#

dlllist

To display a process's loaded DLLs, use the dlllist command. It walks the doubly-linked list of LDR_DATA_TABLE_ENTRY structures which is pointed to by the PEB's InLoadOrderModuleList. DLLs are automatically added to this list when a process calls LoadLibrary (or some derivative such as LdrLoadDll) and they aren't removed until FreeLibrary is called and the reference count reaches zero.

```
$ python vol.py --profile=Win7SP0x86 -f win7.dmp dlllist

[snip]

************************************************************************
services.exe pid:    492
Command line : C:\Windows\system32\services.exe

Base             Size             Path
0x00a50000       0x041000         C:\Windows\system32\services.exe
0x778a0000       0x13c000         C:\Windows\SYSTEM32\ntdll.dll
0x779f0000       0x0d4000         C:\Windows\system32\kernel32.dll
0x75ca0000       0x04a000         C:\Windows\system32\KERNELBASE.dll
0x75e40000       0x0ac000         C:\Windows\system32\msvcrt.dll
0x76650000       0x0a1000         C:\Windows\system32\RPCRT4.dll
0x758d0000       0x01a000         C:\Windows\system32\SspiCli.dll
0x759f0000       0x00b000         C:\Windows\system32\profapi.dll
0x75d80000       0x019000         C:\Windows\SYSTEM32\sechost.dll
0x75940000       0x00c000         C:\Windows\system32\CRYPTBASE.dll
0x758c0000       0x00f000         C:\Windows\system32\scext.dll
0x764a0000       0x0c9000         C:\Windows\system32\USER32.dll
0x765b0000       0x04e000         C:\Windows\system32\GDI32.dll
0x76330000       0x00a000         C:\Windows\system32\LPK.dll
[snip]
```

connections

To view the active connections, use the connections command. This walks the singly-linked list of connection structures pointed to by a non-exported symbol in the tcpip.sys module. This command is for Windows XP and Windows 2003 Server only.

```
$ python vol.py -f Bob.vmem connections
Volatile Systems Volatility Framework 2.0
 Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ------
0x81c6a9f0 192.168.0.176:1176       212.150.164.203:80         888
0x82123008 192.168.0.176:1184       193.104.22.71:80           880
0x81cd4270 192.168.0.176:2869       192.168.0.1:30379         1244
0x81cd4270 127.0.0.1:1168           127.0.0.1:1169             888
0x81e41108 127.0.0.1:1169           127.0.0.1:1168             888
0x82108890 192.168.0.176:1178       212.150.164.203:80        1752
0x82210440 192.168.0.176:1185       193.104.22.71:80           880
0x8207ac58 192.168.0.176:1171       66.249.90.104:80           888
0x81cef808 192.168.0.176:2869       192.168.0.1:30380            4
0x81cc57c0 192.168.0.176:1189       192.168.0.1:9393          1244
0x8205a448 192.168.0.176:1172       66.249.91.104:80           888
```

Selon le guide: https://code.google.com/p/volatility/wiki/CommandReference
Voir aussi : http://volatilityfoundation.github.io/volatility/index.html
Ainsi que : http://resources.infosecinstitute.com/the-hunt-for-memory-malwares/

UNIVERSITÉ LAVAL
Bureau de sécurité de l'information

Outils intéressants :

Wireshark
Tshark
TCPdump
Network Miner
Xplico

Plates-formes : Kali-Linux – Deft-Linux

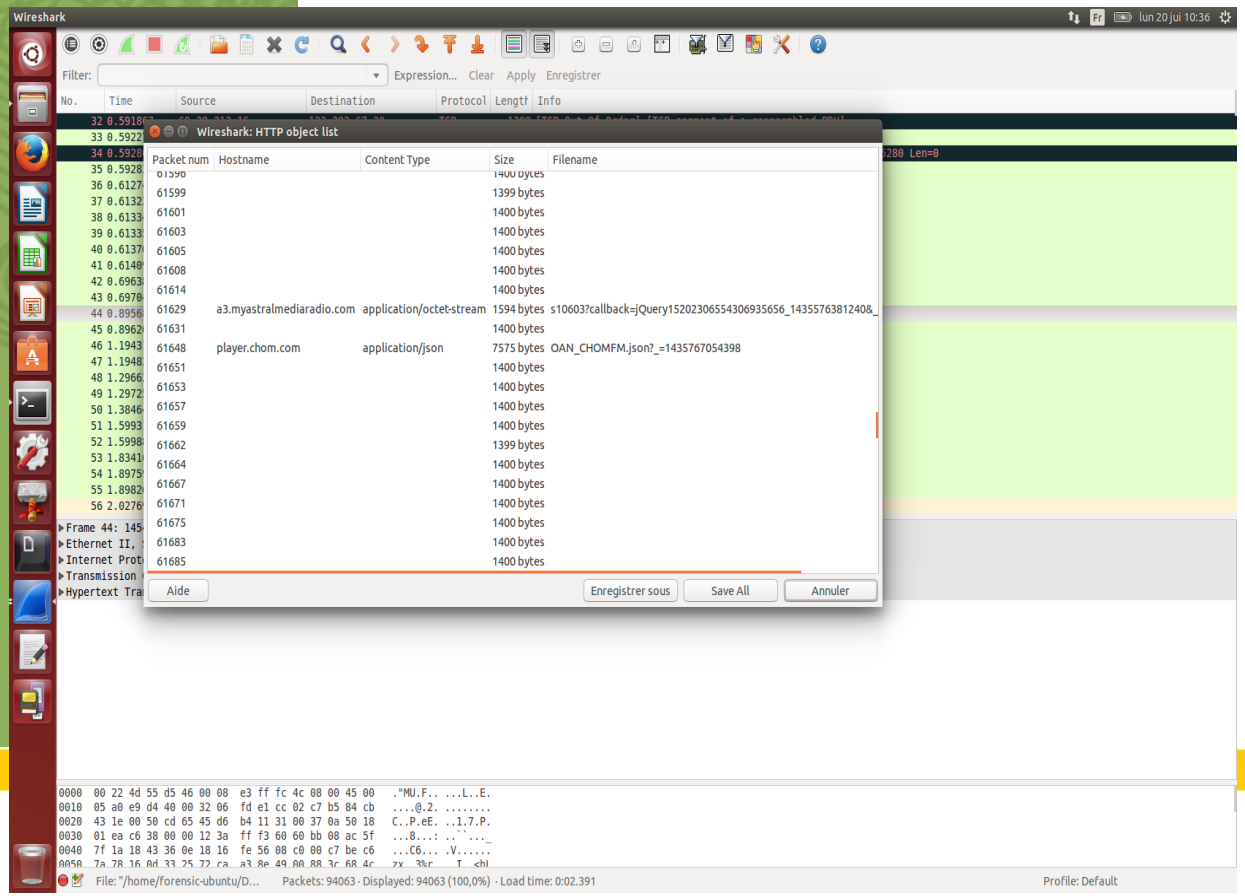
"Network forensic"

Surveillance du trafic
Fichiers journaux

Exportation des objets d'une capture de trafic :

"Network forensic"

Wireshark



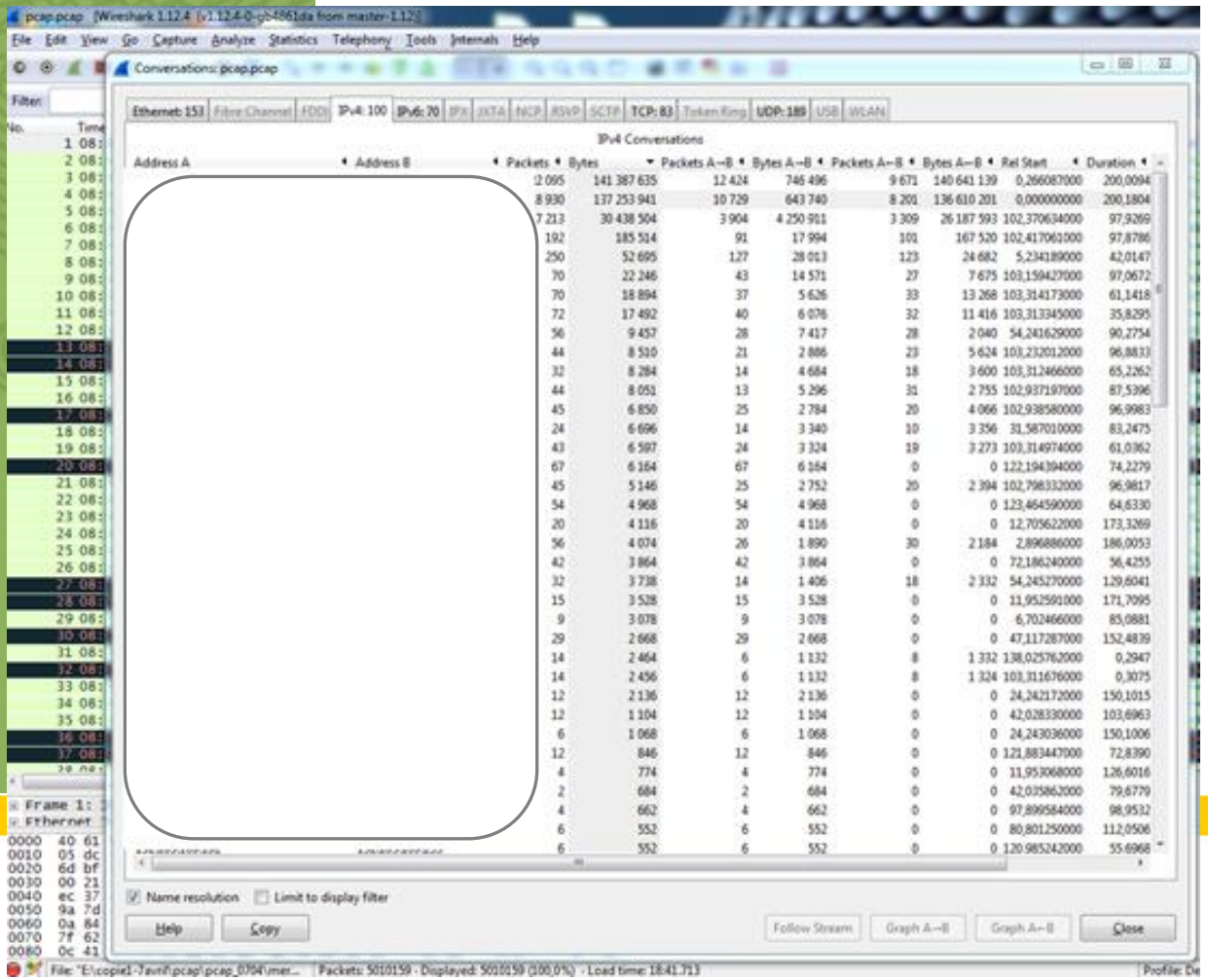
Bureau de sécurité de l'information

Conversations TCP :

"Network forensic"

Trafic entre deux “endpoints” spécifiques

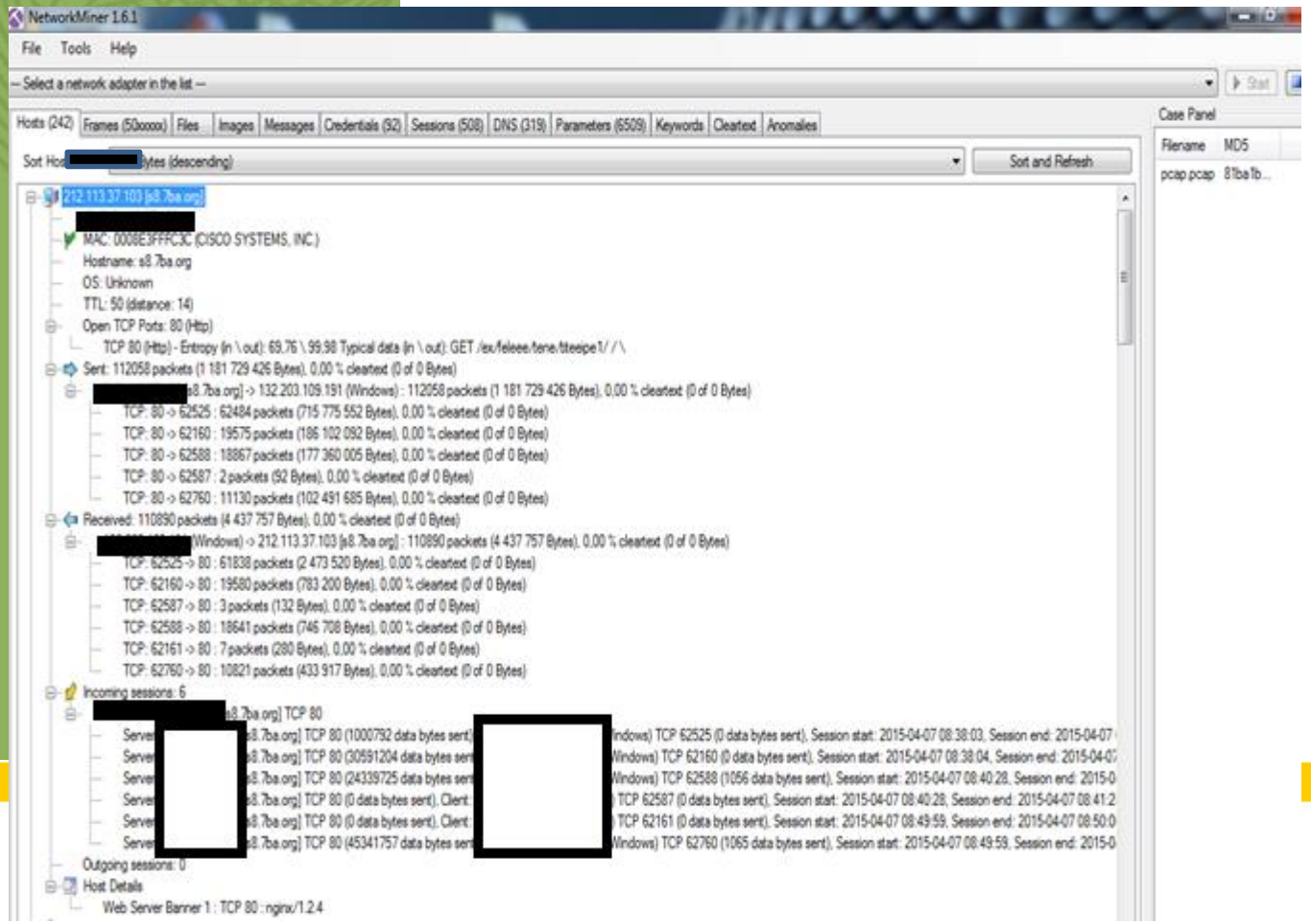
Wireshark



Analyse d'une capture de trafic :

"Network forensic"

Network Miner

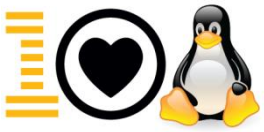


Sixième partie

Pour les passionné(e)s de Linux voici quelques commandes intéressantes:

```
tcpdump -i eth0 dst IP -w "/.../ dump.pcap"

tshark -r dump.pcap -Y rtp -T fields -e rtp.payload -w rtp.out

cat logs/*.log | grep -o 'xxx.xxx.[0-9]\{1,3\.[0-]\{1,3\}' |uniq -c|sort > list_ip.txt

egrep "HackerSpace" logs/*.log > ip_hack.txt

cat ip_conn_ftp.txt | awk '{print $2}' | sort -nr > unique.txt
```

Un conseil pour réaliser des enquêtes informatiques :



-> avoir des connaissances en Linux

Sixième partie

"Remote forensic"

Acquisition statique & dynamique

… à distance!

UNIVERSITÉ LAVAL

Bureau de sécurité de l'information

Outil intéressant :

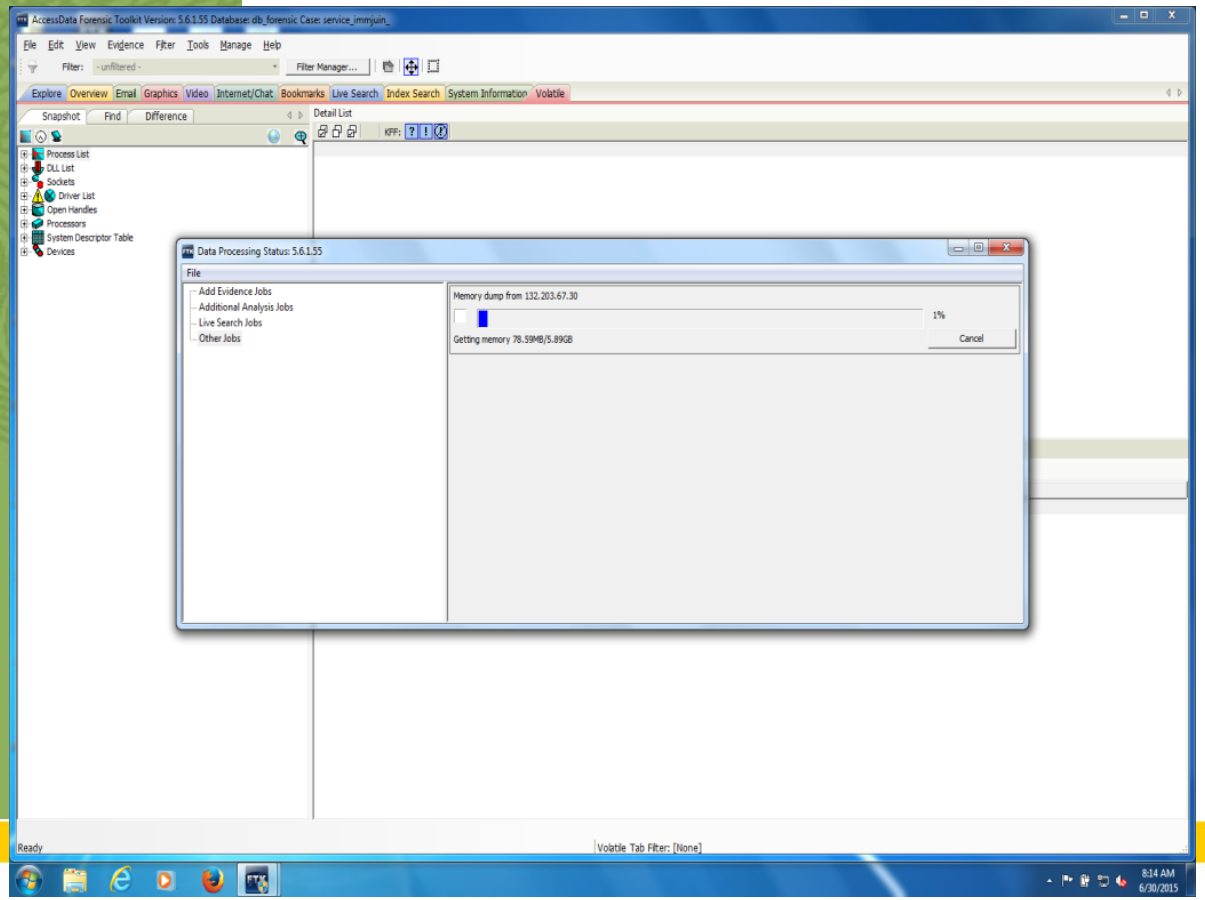
"Remote forensic"

AccessData : FTKToolkit

Avoir l'IP de la machine à distance & avoir un profil "admin" sur cette machine

FTK pousse un agent temporaire

On fait l'acquisition de la mémoire volatile du média désiré, et même, l'image du disque dur!



UNIVERSITÉ LAVAL
Bureau de sécurité de l'information

Outils intéressants :

Maltego
Metagoofil
DNSmap
URLcrazy
TheHarvester
DomainTools
Wayback Machine
Google operators
Nslookup
Whois

Cyber-Intelligence

Collecte d'information sur le web, bases de données "whois", etc

Sixième partie

Log : IP destination 207.82.69.109

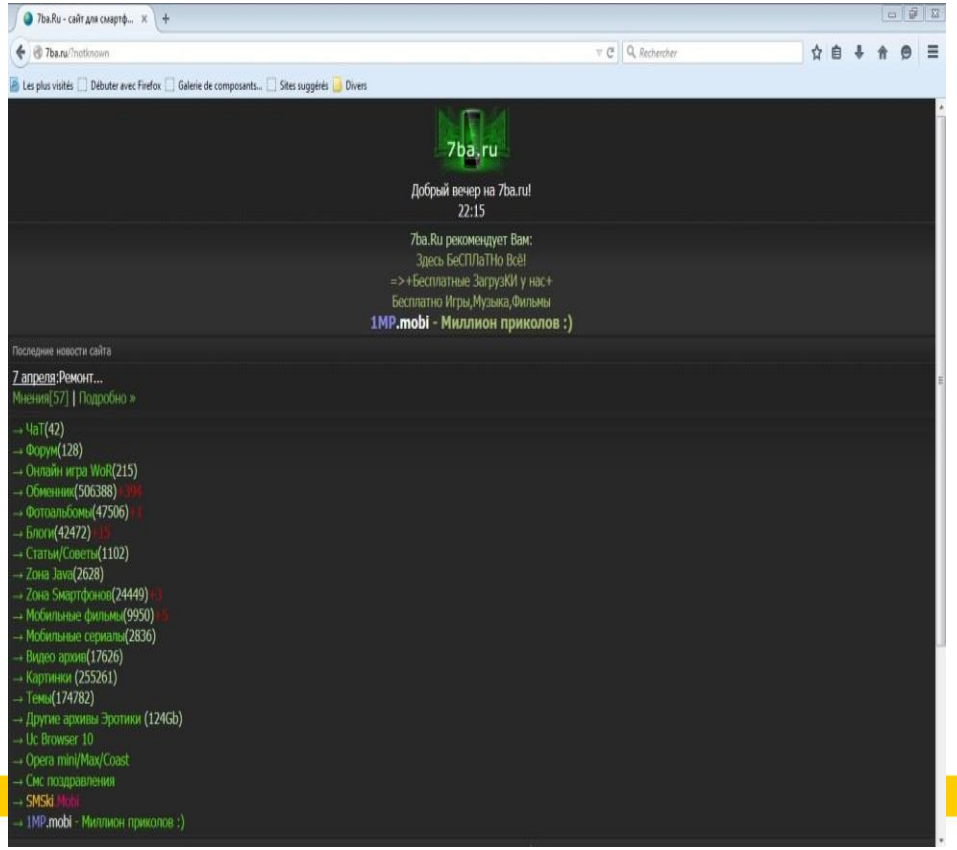
DomainTools:

207.82.69.109 : AS3561 SAVVIS – Savvis
United States Grapevine Gamestop Inc

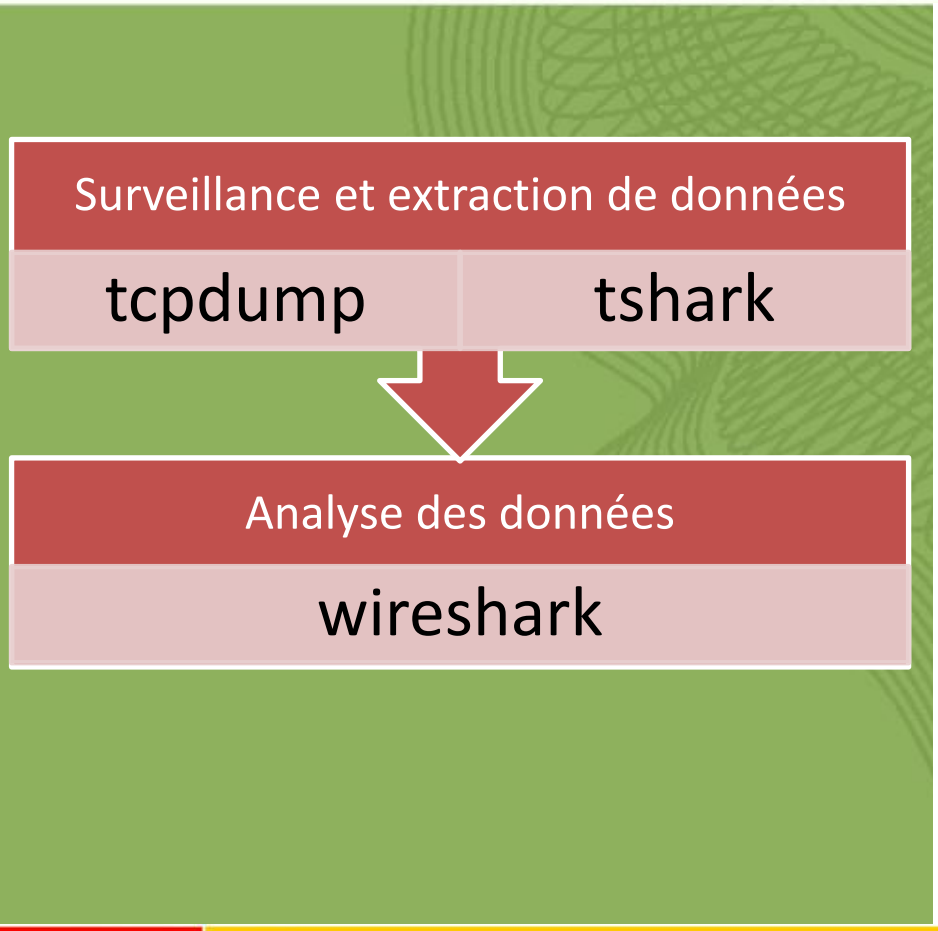
212.113.37.103 : AS6849 UKRTELNET JSC UKRTELECOM
Ukraine Kiev Utel Internet Services

Truc : Utilisé Sandboxie pour ouvrir le lien!

Cyber-Intelligence



UNIVERSITÉ LAVAL
Bureau de sécurité de l'information



Rapport final

Truc :

Historique de vos actions, des outils utilisés, des techniques utilisées, des intervenants, des preuves trouvées… Il faut TOUT écrire… au jour le jour… de votre enquête. Faites des captures d'écran!!!!

La rapport est extrêmement important pour l'enquêteur, mais aussi pour nous et aussi dans la cas d'une poursuite ou d'une présence à la cour comme témoin expert !

Sandboxing

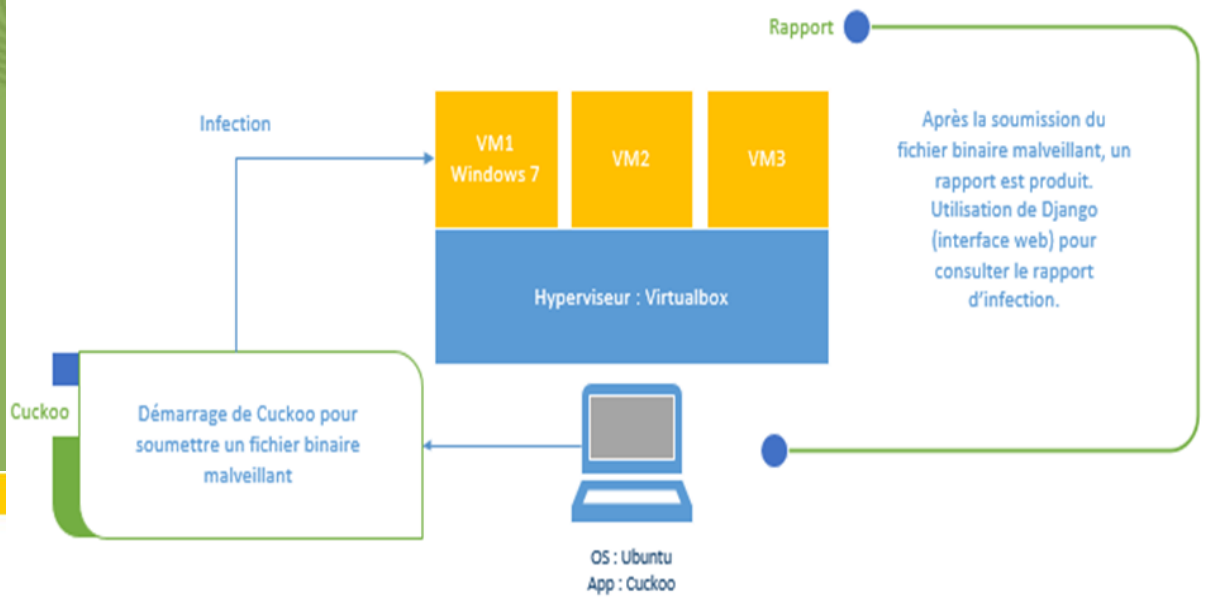
Un besoin important dans la gestion des incidents et des enquêtes informatiques est celui d'avoir une plate-forme de travail pour analyser un « malware » (fichier malveillant). Un environnement sécuritaire pour réaliser une analyse et en faire un rapport : un « sandbox » !

Ce dernier permet d'isoler un environnement non sécuritaire pour y analyser une application ou un fichier malveillant. C'est une approche dynamique d'une analyse de fichier malveillant au lieu d'une analyse statique.

Outil : Cuckoo

Une tâche importante en enquête - réponse à un incident de sécurité :

Analyse de malware!!!



Machines virtuelles

Dans le domaine de l'investigation numérique, la virtualisation est une technologie qui permet aux informaticiens judiciaires l'interactivité entre eux et le média analysé lors de leur investigation. La virtualisation est alors utilisée comme un outil de travail en informatique judiciaire (enquêtes informatiques).

Exemple : pendant l'analyse, un technicien peut rapidement visualiser les applications installées dans le système d'exploitation du média perquisitionné. En utilisant un hyperviseur de type 2, il peut virtuellement naviguer dans le système ayant maintenant accès au mode graphique que lui permet la virtualisation.

Outils :

LiveView / VMWare
Dd2vmdk

Une autre technique d'enquête importante :

"virtual forensic"

Anti-forensic

Que ce soit par des techniques de chiffrement, de stéganographie, d'effacement irréversible ou soit par des dispositifs d'anonymat comme Tor, il y a plusieurs outils pour cacher ou effacer des données.

Un défi :

Un « ennemi » des informaticiens judiciaires est l'utilisation des outils du domaine « *anti-forensic* » par les utilisateurs malveillants (fraudeurs, pirates, criminels, etc). Ces outils ont comme buts d'empêcher (ou du moins retarder) quiconque de parvenir à retrouver l'information sur le média, ou de prévenir la cueillette d'information et de prévenir la détection de crimes informatiques.

« Data carving »

Pour illustrer le tout, voici un exemple :

une clé USB Kingston 8 GB
FS : FAT32
Ne contient pas de fichiers actifs/supprimés!

Un autre défi :

Qu'est-ce que le "data carving" ?

C'est l'dentification et l'extraction de fichiers qui sont situés dans des zones de clusters non alloués.

Cette technique utilise la signature du fichier ("magic number").

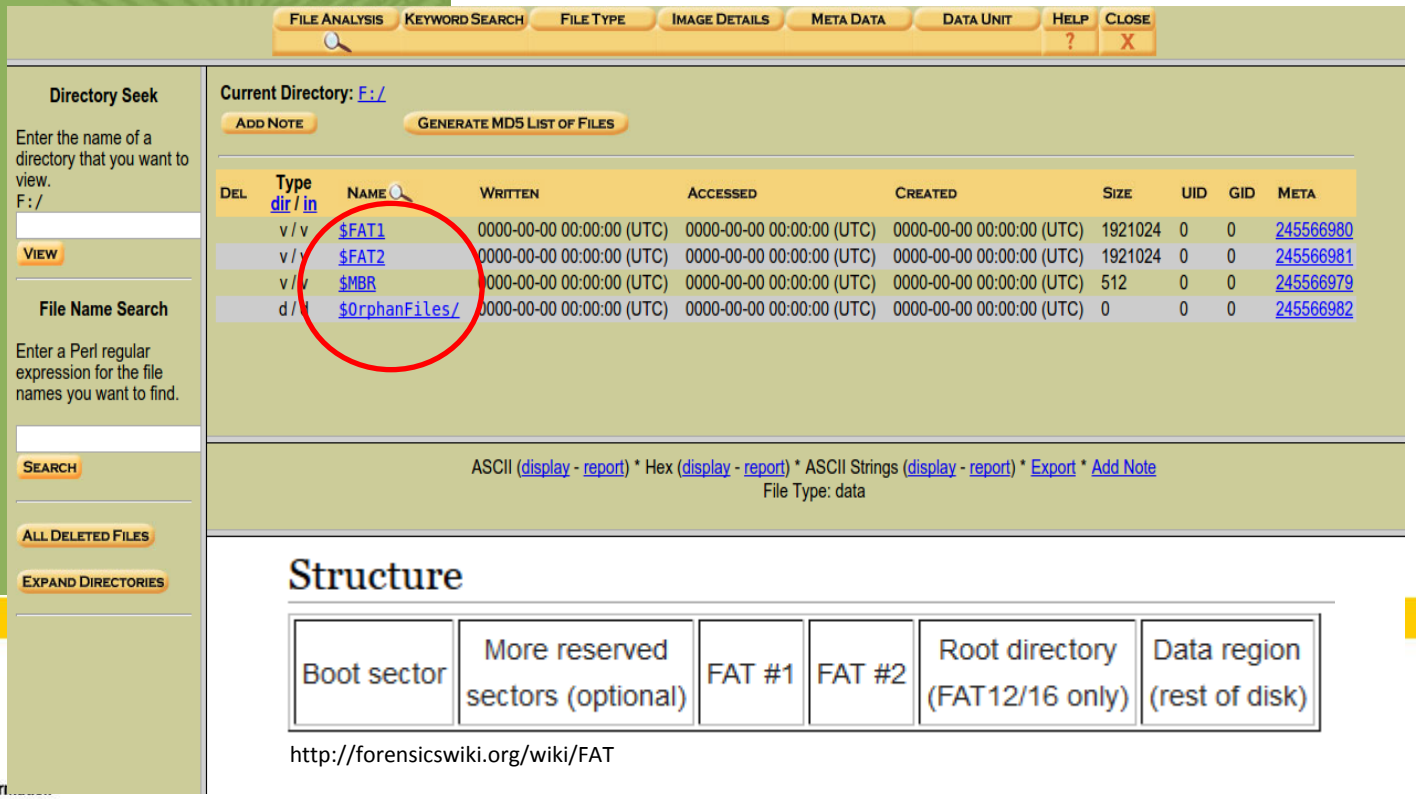
Septième partie

FAT32 : $FAT1 & $FAT2
$MBR
$OrphanFiles

MBR :
MasterBootRecord
Zone d'amorcage

OrphanFiles :
Fichiers supprimés qui ont encore des metadata dans le FS mais ne sont pas accessibles par le "root directory"

```
deftlinux-vm ~/evidence/sylvain % mmls nadvig.aff - calculate offset 512
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000008063   0000008064   Unallocated
02:  00:00   0000008064   0015364415   0015356352   Win95 FAT32 (0x0c)
```

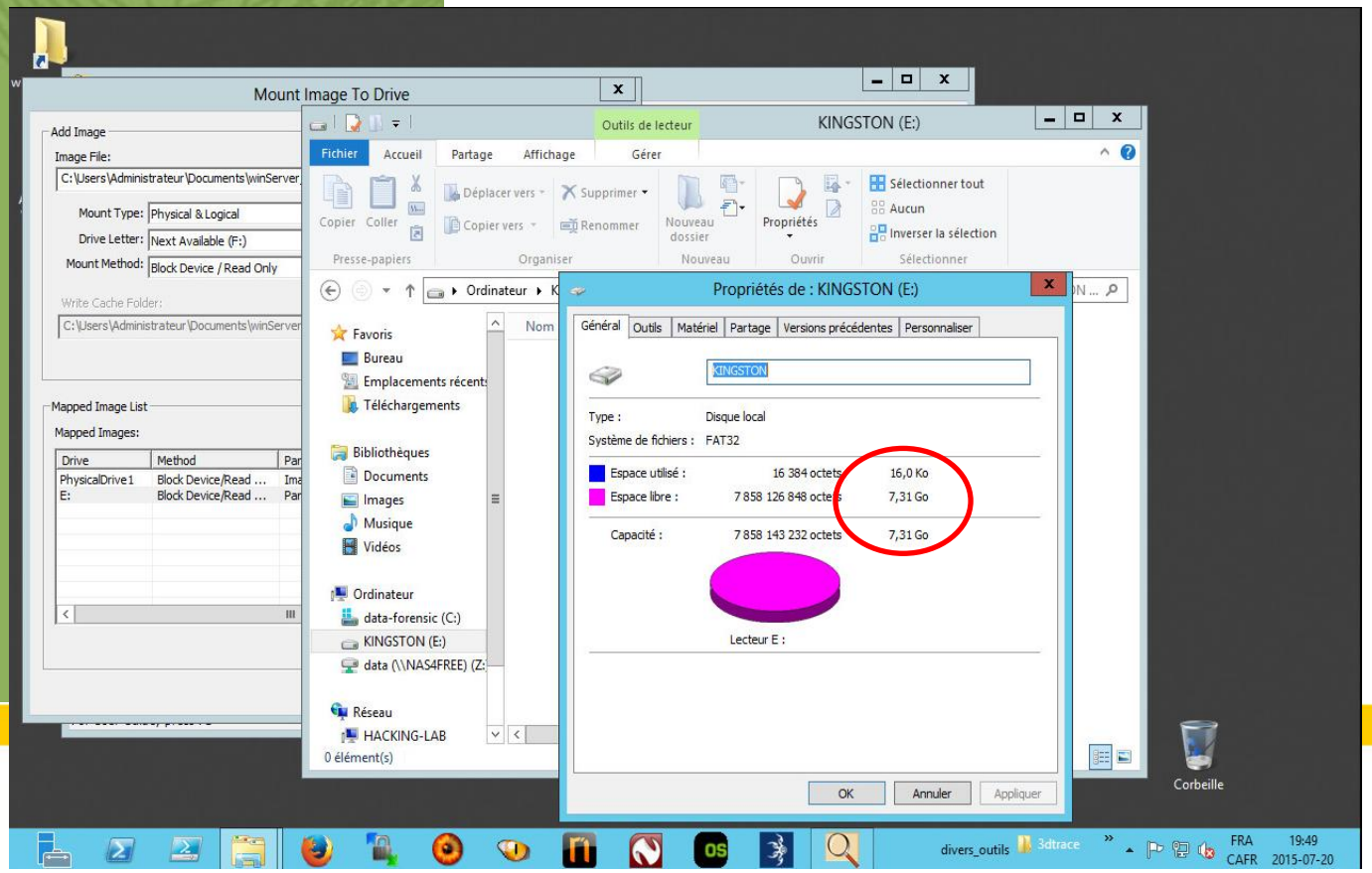


Autopsy TSK

http://forensicswiki.org/wiki/FAT

Septième partie

L’image de la clé USB peut être « montée » : pas de fichiers actifs !



FTKImager

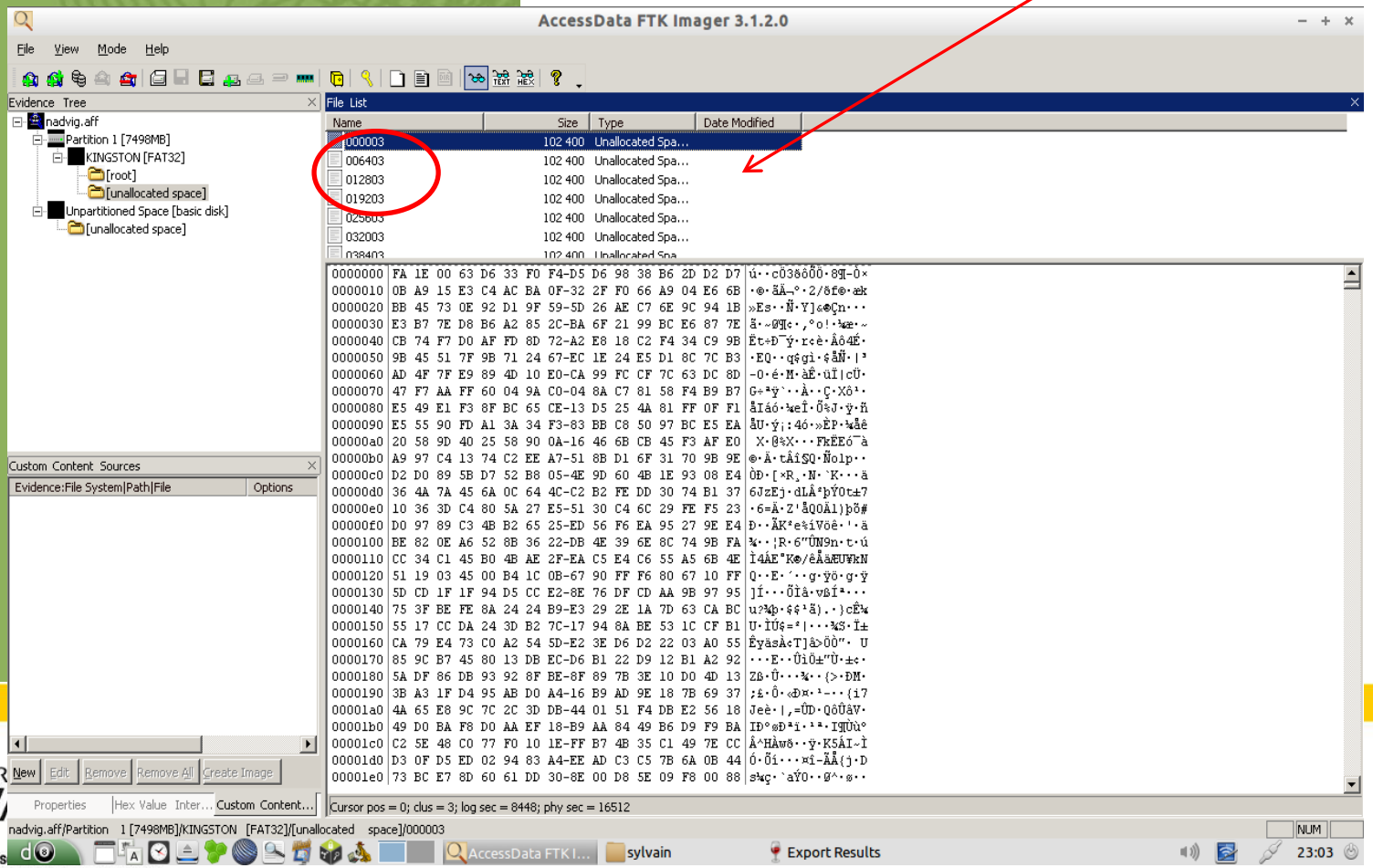
UNIVERSITÉ LAVAL

Bureau de sécurité de l'information

Septième partie

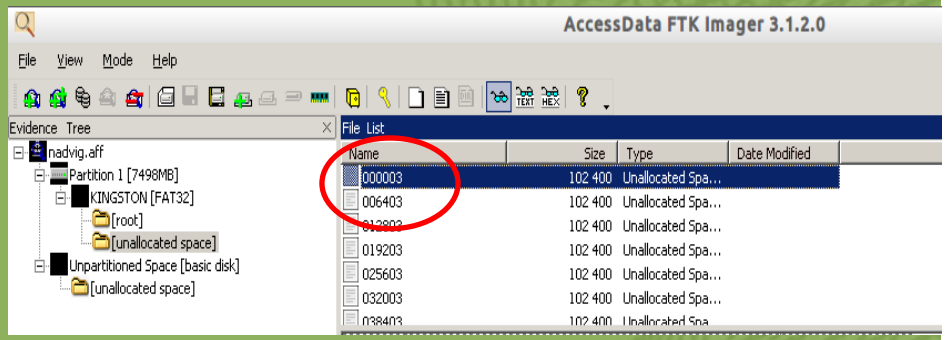
Ces deux fichiers sont situés dans la zone :
« Unallocated space »

Espace non alloué



FTKImager

Quoi faire avec les fichiers?



FTKImager

Foremost vient à la rescousse!

Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
Foremost started at Tue Jul 21 23:01:39 2015
Invocation: foremost -av /home/deftlinux/evidence/sylvain/000003 -T
Output directory: /home/deftlinux/output_Tue_Jul_21_23_01_39_2015
Configuration file: /etc/foremost.conf

File: /home/deftlinux/evidence/sylvain/000003
Start: Tue Jul 21 23:01:39 2015
Length: 100 MB (104857600 bytes)

Num	Name (bs=512)	Size	File Offset	Comment
0:	00135493.jpg	20 MB	69372516	(Header dump)
1:	00000232.bmp	2 MB	118903	(Header dump)
2:	00001191.bmp	2 MB	610196	(Header dump)
3:	00001194.bmp	2 MB	611760	(Header dump)
4:	00001427.bmp	2 MB	731070	(Header dump)

...
Finish: Tue Jul 21 23:02:04 2015

991 FILES EXTRACTED

jpg:= 1
bmp:= 466
exe:= 524

Foremost finished at Tue Jul 21 23:02:04 2015

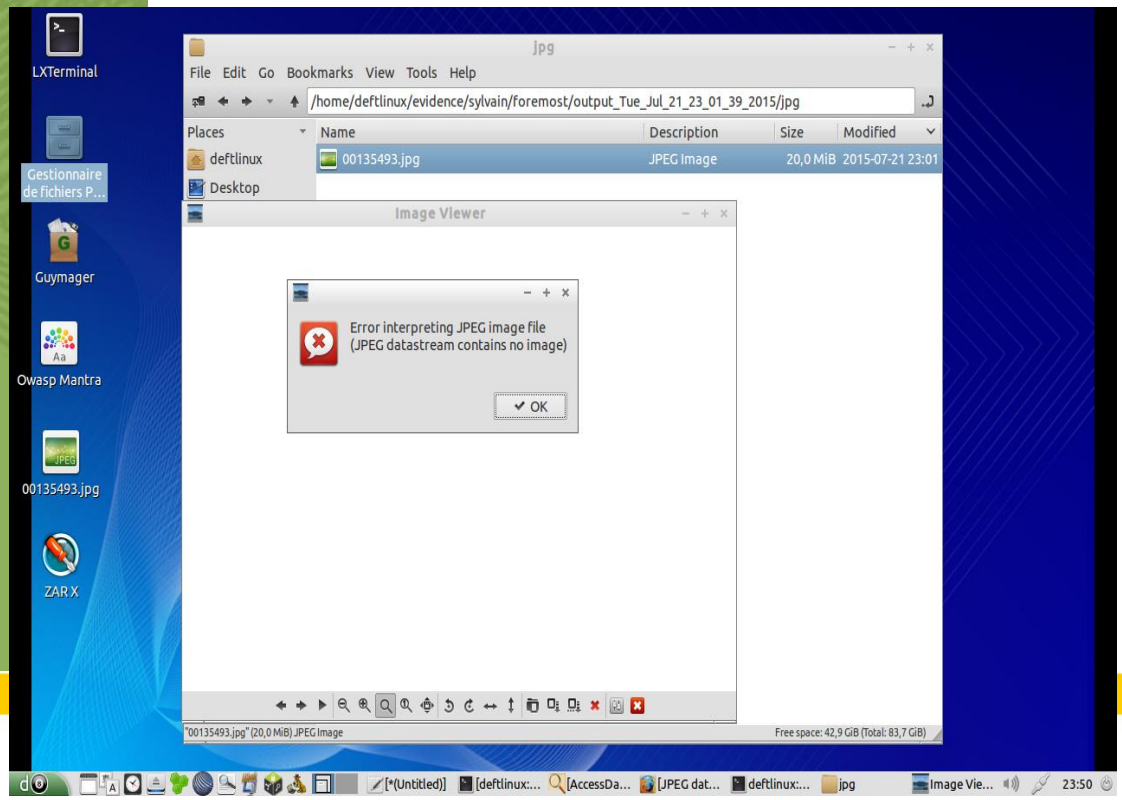
Septième partie

Aucun de ces fichiers jpeg, bmp ou exe ne peut s'ouvrir « a la normale ». Les fichiers images sont de fausses images : JPEG datastream contains no image!

Les fichiers « carvés » a partir du fichier 000003 ont tous la même taille : presque tous a 2 MB pour les .bmp, 1024 k pour les .exe et 20 MB pour le seul jpeg

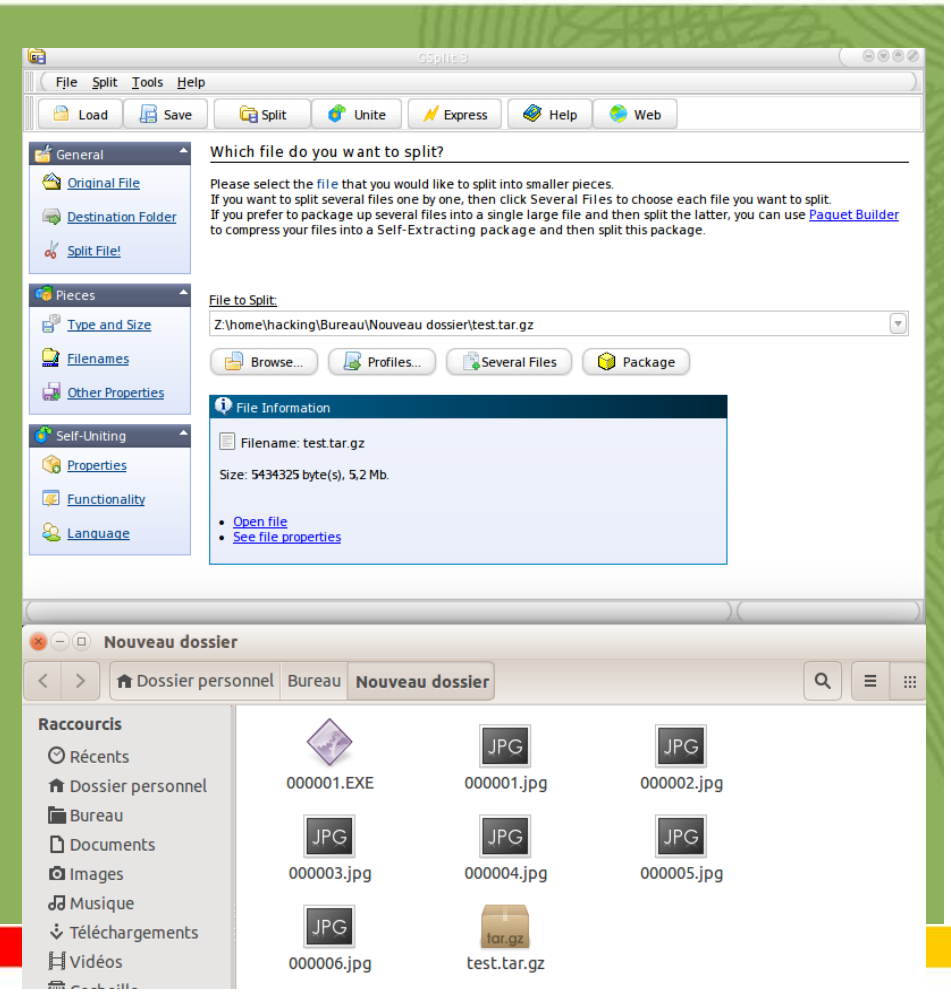
deftlinux-vm ~/Desktop % identify 00135493.jpg
identify.im6: JPEG datastream contains no image `00135493.jpg' @ error/jpeg.c/JPEGErrorHandler/316.

deftlinux-vm ~/Desktop % exif 00135493.jpg
Corrupt data
The data provided does not follow the specification.
ExifLoader: The data supplied does not seem to contain EXIF data.



UNIVERSITÉ LAVAL
Bureau de sécurité de l'information

Septième partie



Intuition!!

Les fichiers bmp, jpg et exe se ressemblent (taille, nom de fichier…)… pourquoi ces petits fichiers?

gsplit.exe est un exemple d'une application qui permet de « splitter » un gros fichier en plusieurs petits fichiers.

Il « split » un fichier dans des fichiers de taille désirée avec l'extension désirée et avec un nom de fichier désiré qui peut être incrémenté.

UNIVERSITÉ LAVAL
Bureau de sécurité de l'information

Septième partie

Exemple pour regrouper les multiples fichiers en un seul :

```
cat 00* > new_exe
file new_exe
    new_exe: MS-DOS executable, MZ for MS-DOS
ls -l new_exe
-rw-rw-r-- 1 hacking hacking 542872646 jui 22 19:18
new_exe
```

Donc le fichier qui regroupe l'ensemble des multiples fichiers bmp en un seul, donne 964 MB. L'autre, c-a-d, le regroupement de tous les fichiers exe : 542 MB.

La suite ? Regrouper le tout pour créer le fichier de format original!

Intuition!!

Est-ce réellement ce qui a été fait ?

Utilitaires intéressants :

rsync
bash script
crontab
tmux
sandboxie
keepnotes
winmerge
…

Tout au long de votre enquête…

Septième partie

Commandes Linux/Windows:

cat /proc/buddyinfo	lsof
cat /proc/cpuinfo	lsusb
cat /proc/diskstats	md5sum nom_fichier > nom_fichier.txt
cat /proc/dma	mount /dev/mapper/loop0p3 /mnt/ -o loop,ro
cat /proc/iomem	mount –o loop,ro nom_fichier /mnt/
cat /proc/meminfo	netstat
cat /proc/mounts	ntfsfix nom_fichier.dd
cat /proc/swaps	ovftool –st=OVA –tt=OVF nom_fichier
cat /proc/version	parted nom_fichier
cat /proc/vmstat	ps aux
cat /proc/zoneinfo	psinfo.exe
date	pslist.exe no_processus -x
dd2vmdk –i nom__fichier.dd nom_fichier.vmdk	qemu-img –convert –o vmdk nom_fichier.dd nom_fichier.vmdk
df –h	sha256.exe nom_fichier
df –i	sha256sum nom_fichier > nom_fichier.txt
dmidecode	stat /etc/passwd
fdisk -l /dev/sdX	tree /f
fdisk –v	tree /f > nom_fichier.txt
file	tree -L 1
free	uname –a
hdparm –g	uptime
hdparm –i	userdump.exe –k –w no_processus nom_fichier.dump
hdparm –V	vboxManage internalcommands createrawvmdk -filename «C:\Users\labo\VirtualBox VMs\usb_mint.vmdk» -rawdisk \\.\PhysicalDrive5
history	vboxManage internalcommands listpartitions -rawdisk \\.\PhysicalDrive5
hostname	vmware-vdiskmanager -r J:\source\nom_fichier.vmdk -t 0 J:\destination\nom_fichier.vmdk
ifconfig	vol.py -f ...\nom_fichier.mem imageinfo
java –jar raw2vmdk.jar nom_fichier	volume_dump.exe > nom_fichier.txt
kpartx -a nom_fichier	whoami
kpartx -l nom_fichier	winpmem-1.4.exe > nom_fichier.raw
last	winunhide-1.4.exe –l
last -f /var/log/wtmp	winunhide-1.4.exe sys > nom_fichier.txt
last -f utmp	*wipe -r -q -Q 1 data_Ext*
ls -i /etc/passwd	wmic.exe
ls –l	wmic:root\cli>diskdrive list

Quoi mettre dans votre boîte à outils pour réaliser des enquêtes ?

De la passion

De la persévérance

Un(e) bon(ne) collègue

De bons outils

Merci de votre participation

Nadia Vigneault
Conseillère en sécurité de l'information
Gestion des incidents de sécurité de l'information, participation aux enquêtes touchant à la sécurité de l'information, Gestion des vulnérabilités
nadia.vigneault@bsi.ulaval.ca
Bureau de sécurité de l'information
418 656-2131, poste 4019

Claude Charest
Conseiller en sécurité de l'information
Gestion des incidents de sécurité de l'information, participation aux enquêtes touchant à la sécurité de l'information, Gestion des vulnérabilités
claude.charest@bsi.ulaval.ca
Bureau de sécurité de l'information
418 656-2131, poste 11396

Bureau de sécurité de l'information de l'Université Laval
bsi.ulaval.ca