

# 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](http://bsi.ulaval.ca)



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](http://bsi.ulaval.ca)



Bureau de sécurité de l'information



## Première partie

# Université Laval

-> 1852

+50 000 utilisateurs

étudiants &  
employés

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



[https://www.cameo.ulaval.ca/files/content/sites/cameo/files/images/background\\_ulaval.jpg](https://www.cameo.ulaval.ca/files/content/sites/cameo/files/images/background_ulaval.jpg)



# 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





# 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!





## Seconde partie



# 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-scr/cbr-scr/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](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)

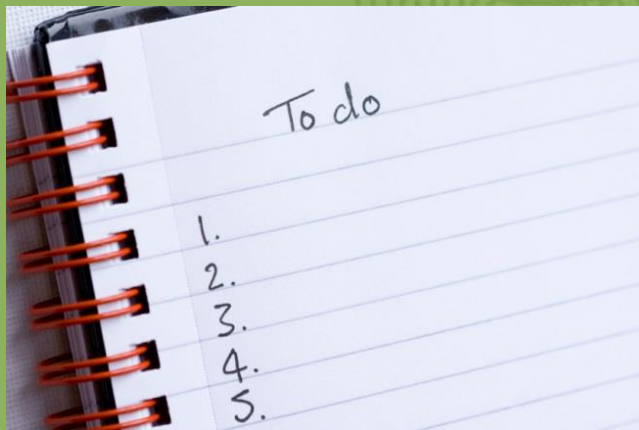


UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



## Troisième partie



# Mandats & portée :

Mandats d'enquête proviennent du SSP

Techniques et outils d'enquête proviennent du BSI

Support technologique provient de la DTI



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information





## Quatrième partie

BSI :

Pas d'enquêtes criminelles

## Types d'enquête :

Enquêtes administratives

Utilisation non-autorisé des équipements

Téléchargements illégaux

Réponse à un incident de sécurité



## Quatrième partie

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.

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



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information

# 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

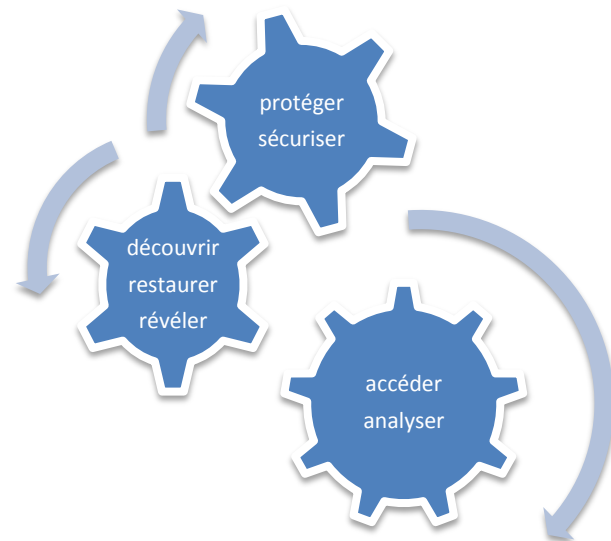
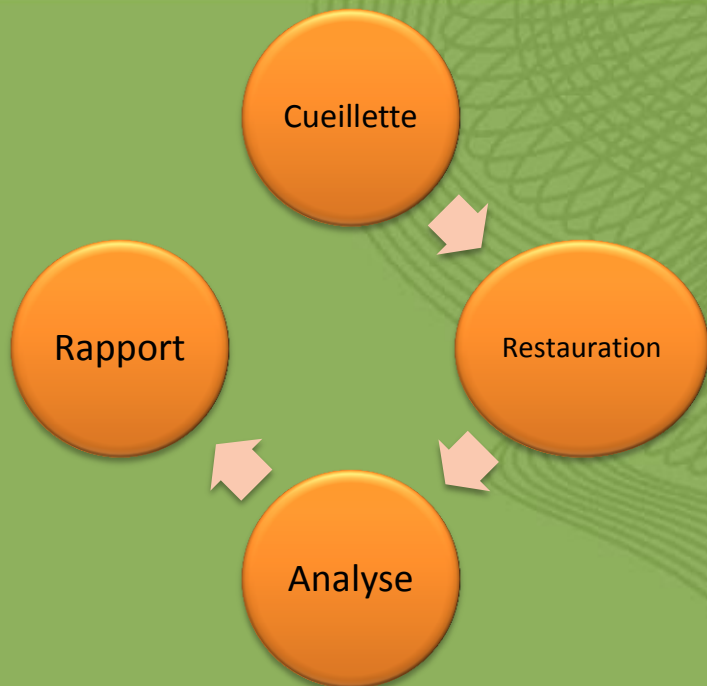


Bureau de sécurité de l'information



## Cinquième partie

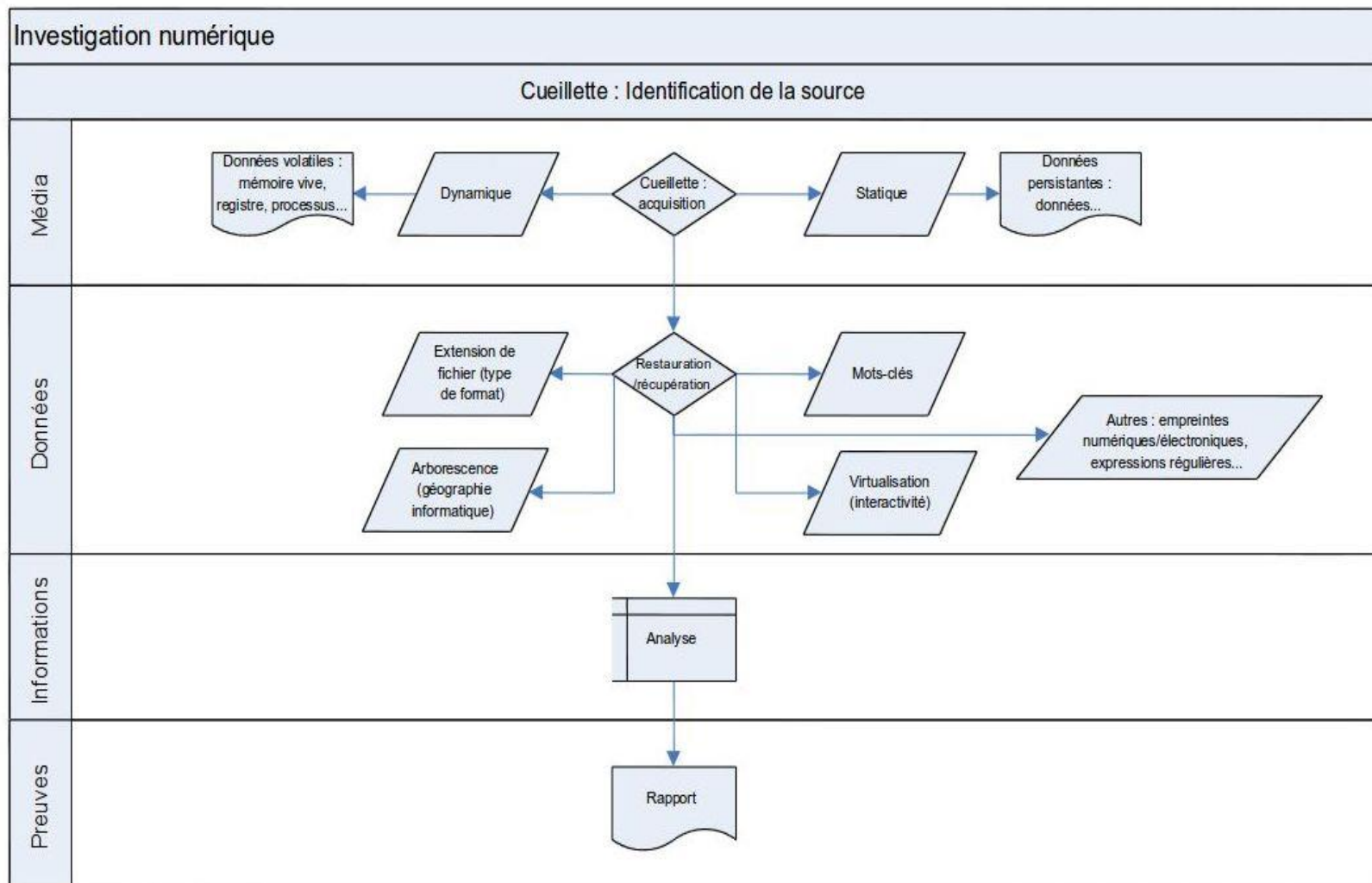
### Processus :





## Cinquième partie

# 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 :



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information





## Cinquième partie

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!



Bureau de sécurité de l'information



## Sixième partie

Peu importe la technique choisie parmi 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



UNIVERSITÉ  
LAVAL

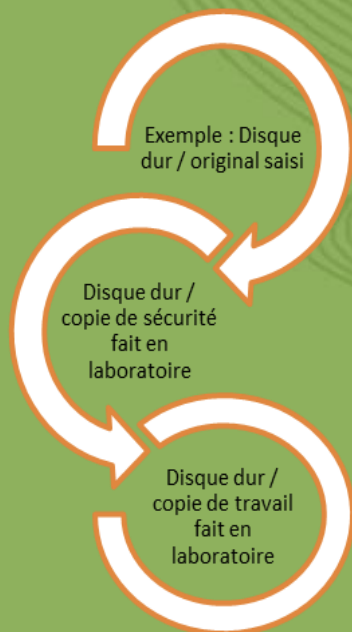
Bureau de sécurité de l'information



## 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!



## Sixième partie

### 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>



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



## Sixième partie

### 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"



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



## Sixième partie

### 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



Bureau de sécurité de l'information





# Sixième partie

## Arborescence des fichiers :

FTK Imager



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information

AccessData FTK Imager 3.1.4.6

File View Mode Help

Evidence Tree

- Files
  - !a~\_R~1
  - I\_D476~1
  - I\_EC9F~1
  - I\_RU\_F~1
  - I\_RU\_F~2
  - I\_RU\_F~3
  - I\_RU\_F~4
  - I7x
  - IA6CfA~1
  - 211quebecregions\_fichiers
  - Foto
  - ISO Master - Википедия\_fichiers
  - ISODisk - Википедия\_fichiers
  - ISO-образ - Википедия\_fichiers
  - Kury
    - GAD-1100
      - Archive institution
      - Archive institution
      - Nouveau dossier
      - Nouveau dossier
    - Gennady
    - Geosoft\_Formation\_03Novembre2009
    - guillaume
    - Images
    - ISO Master - Википедия\_fichiers
    - ISODisk - Википедия\_fichiers
    - ISO-образ - Википедия\_fichiers
  - Kino
    - IOUVEA~1
    - GameFAQs Max Payne 3 (PS3) FAQ-Walkthrough by B...
    - GameFAQs Max Payne 3 (PS3) FAQ-Walkthrough by T...
    - Kak By Adresa MozgopravovGugl
    - Max Payne 3 (PlayStation3)
    - Max Payne 3 FAQ-Walkthrough for PlayStation 3 by E...
    - Max Payne 3 FAQ-Walkthrough for PlayStation 3 by Ext...
    - Nouveau dossier
    - Nouveau dossier
    - Pics
    - Statiy
    - music\_Gena
  - Muzon
    - Mega House-4CD-2013-wAx
    - Nenarezki
    - Papki
    - Trance Pro v.12 from AGR (2013)
    - Treki
    - My Music

File List

Name	Size	Type	Date Modified
Nouveau dossier	0	Directory	2015-03-28 16:50:36
Pics	16	Directory	2015-03-28 16:50:36
IOUVEA~1	0	Directory	2015-03-28 12:31:10
Statiy	16	Directory	2015-03-28 12:31:10
Nouveau dossier	0	Directory	2015-03-16 13:33:10
Kak By Adresa MozgopravovGugl	16	Directory	2015-03-16 13:33:10
GameFAQs Max Payne 3 (PS3) FAQ-Wa...	16	Directory	2014-12-11 10:57:04
GameFAQs Max Payne 3 (PS3) FAQ-Wa...	16	Directory	2014-12-11 10:56:28
Max Payne 3 FAQ-Walkthrough for Pla...	16	Directory	2014-12-11 10:55:50
Max Payne 3 FAQ-Walkthrough for Pla...	16	Directory	2014-12-11 10:55:22
Max Payne 3 FAQ-Walkthrough for Pla...	16	Directory	2014-12-11 10:54:46
Max Payne 3 (PlayStation3)	16	Directory	2014-12-11 10:52:34
Doghouse_2009_520x220_Zamez.mp4.Fi...	6	File Slack	
Sobstvennost Diyavola_1997_640x270.m...	16	File Slack	
Mihail_1996_448x336.mp4.FileSlack	2	File Slack	
Sherlock Holmes_2009_720x404.mp4.Fil...	14	File Slack	
!LOKKM~1.PAR.FileSlack	12	File Slack	
!NCTG.JPG.FileSlack	9	File Slack	
!04766.JPG.FileSlack	2	File Slack	
!7249.JPG.FileSlack	6	File Slack	
tenjou-tenge_00353772.jpg.FileSlack	1	File Slack	
aoi_sakura_yoru_wa_by_kii_sakura...	8	File Slack	
guni_wallpaper_2_by_xoverfreak-d3pe4...	8	File Slack	
Nightwalker.jpg.FileSlack	16	File Slack	
!50full.jpg.FileSlack	8	File Slack	
681399nightwalker.jpg.FileSlack	7	File Slack	

0000 2E 20 20 20 20 20 20 20~20 20 20 10 00 5A CD 8E . . . . . ZI .  
0010 31 45 31 45 0E 00 CE 8E~31 45 04 00 00 00 00 00 1E1E . . i . 1E . . . . .  
0020 2E 2E 20 20 20 20 20 20 20~20 20 20 10 00 5A CD 8E . . . . .  
0030 31 45 31 45 00 00 CE 8E~31 45 00 00 00 00 00 00 1E1E . . i . 1E . . . . .  
0040 45 61 00 6C 00 00 00 00~FF FF FF FF 0F 0F BC FF FF E a . . . . . YYY Y  
0050 FF FF FF FF FF FF FF~FF FF 0F 0F FF FF FF YYY YYY YYY YYY YYY YYY  
0060 04 72 00 73 00 6F 00 6C~00 34 0F 0F BC 38 00 . r . s . o . l . 4 . . . 48 .  
0070 71 00 2E 00 70 00 61 00~72 00 00 00 74 00 69 00 q . . p . a . r . . . . t . i .  
0080 03 5F 00 37 00 32 00 30~00 78 00 0F 00 BC 33 00 . . 7 . 2 . 0 . x . . . 43 .  
0090 30 00 34 00 2E 00 61 00~76 00 00 69 00 2E 00 0 4 . . . a . v . . . i . .  
00a0 02 75 00 65 00 72 00 72~00 65 0F 00 BC 72 00 . u . e . r . r . e . . . 4r .  
00b0 6F 00 73 00 5F 00 32 00~30 00 00 30 00 32 00 o . s . . . 2 . 0 . . . . 0 . 2 .  
00c0 01 4D 00 69 00 72 00 6F~00 74 0F 0F BC 76 00 . M . i . r . o . t . . . . 4v .  
00d0 6F 00 72 00 74 00 7A 00~79 00 00 5F 00 47 00 o . r . t . z . y . . . . G .  
00e0 4D 49 52 4F 54 56 7E 31~50 41 52 20 00 79 2B 41 MIROTV-1PAR . y + A  
00f0 87 46 87 46 00 00 2C 41~87 46 97 00 B4 05 28 34 . F . F . . . A . F . . . . ( 4  
0100 43 75 00 72 00 31 00 79~00 33 0F 00 76 2E 00 C u . x . l . y . 3 . . . . v .  
0110 70 00 61 00 72 00 74 00~69 00 00 61 00 6C 00 p . a . r . t . i . . . . a . l .  
0120 02 32 00 30 00 78 00 34~00 33 0F 00 76 32 00 . 2 . 0 . x . 4 . 3 . . . . v 2 .  
0130 2E 00 61 00 76 00 69 00~2E 00 00 35 00 7A 00 . . a . v . i . . . . 5 . z .

Cursor pos = 0; clus = 917508; log sec = 29375488

DiskImage\_(no volume name) 132.203.109.191 [132.203.109.191]\_2015\_07\_04\_08\_42\_01.E01/NONAME [FAT32]/[root]/Kino



## Sixième partie

# Fichiers actifs & supprimés :

Autopsy

7avnicleusb - Autopsy 3.1.1

File View Tools Window Help

Close Case Add Data Source Generate Report

Keyword Lists Keyword Search

227 Results

Directory Listing

Audio

Name	Location	Modified Time	Change Time	Access Time	Created Time
fonzo_nu_0c935a7e9e98.mp3	/img_DiskImage_(n...	2014-09-19 18:14:50 EDT	0000-00-00 00:00:00	2014-09-20 00:00:00 EDT	2014-09-19 18:13:...
fonzo_nu_7ff42896f66e.mp3	/img_DiskImage_(n...	2014-09-19 18:15:38 EDT	0000-00-00 00:00:00	2014-09-19 00:00:00 EDT	2014-09-19 18:15:...
fonzo_nu_7ff42896f66e.mp3	/img_DiskImage_(n...	2014-09-19 18:17:04 EDT	0000-00-00 00:00:00	2014-09-20 00:00:00 EDT	2014-09-19 18:15:...
Mertvretz_Depp_1995_720x404.mp4	/img_DiskImage_(n...	2015-04-07 09:39:52 EDT	0000-00-00 00:00:00	2015-04-07 00:00:00 EDT	2015-04-07 09:14:...
Doghouse_2009_520x220_Zamez.mp4	/img_DiskImage_(n...	2015-04-07 08:28:10 EDT	0000-00-00 00:00:00	2015-04-07 00:00:00 EDT	2015-04-07 08:22:...
Sobstvennost_Diyavola_1997_640x270.mp4	/img_DiskImage_(n...	2015-04-07 08:30:10 EDT	0000-00-00 00:00:00	2015-04-07 00:00:00 EDT	2015-04-07 08:18:...
Mhal_1996_448x336.mp4	/img_DiskImage_(n...	2015-04-07 08:36:06 EDT	0000-00-00 00:00:00	2015-04-07 00:00:00 EDT	2015-04-07 08:29:...
Sherlock Holmes_2009_720x404.mp4	/img_DiskImage_(n...	2015-04-07 08:40:00 EDT	0000-00-00 00:00:00	2015-04-07 00:00:00 EDT	2015-04-07 08:17:...
Beetlejuice_1988_720x404.mp4	/img_DiskImage_(n...	2015-04-07 08:50:22 EDT	0000-00-00 00:00:00	2015-04-07 00:00:00 EDT	2015-04-07 08:31:...
Nayemmyie_Ubiytrzy_1995_720x400.mp4	/img_DiskImage_(n...	2015-04-07 09:12:10 EDT	0000-00-00 00:00:00	2015-04-07 00:00:00 EDT	2015-04-07 08:38:...
Zona Osb Vnima					2014-03-15:36:...
Born to Fight_Ki					2014-03-16:14:...
SobakakusaetS					2014-03-16:55:...
Jmurki_2005_48					2014-03-17:00:...
Aziet_2008_320					2014-03-16:12:50:...
RocknRolla_200					2014-03-16:12:52:...
Evolutsiya_200					2014-01-23 17:32:...
Zelenoye Kreslo					2014-01-23 17:53:...
Most Ramy_586					2014-01-23 18:09:...
Vypusknik_2013					2014-01-23 18:13:...
Serious Sam 2 b					2014-01-12 15:34:...
7baRu_behtme					2012-11 10:44:...
7baRu_melloma					2014-09-17 14:16:...

Hex Strings Meta

Page: 1 of

0x00000000: AB  
0x00000001: E8  
0x00000002: C9  
0x00000003: 67  
0x00000004: 60  
0x00000005: 31  
0x00000006: B9 5C 5D 3B BA 3A 38 7A 3B 8B 5B 15 1F 5E E2 5A .....:8ap.....  
0x00000007: C2 63 0B A0 FB 82 17 7F 56 6C 2A 0E 19 2D D7 A7 .....:v71\*.....  
0x00000008: F5 DA 3F 33 6B AE 2C 81 94 A2 1B 68 7D 97 EC 89 .....:73k.....h)...  
0x00000009: 58 2C 6D A2 52 6D 1D 35 5A 0D 86 3D B4 BA D8 FE X\* 2m.5Z. ....  
0x0000000A: 1A 1D AD 56 50 19 4A 36 68 D3 3F BA 88 2E ED DD ...VP.J6h. ?....

Beetlejuice\_1988\_720x404

00:37

E01 Verifier for DiskImage\_(no volume name) 132.203.109.191 [132.203.109.191]\_2015\_07\_04\_08\_42\_01.E01

20%

EN 13:38 2015-04-09



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



## Sixième partie

Visualiser le contenu d'un fichier supprimé :

Autopsy

Autopsy 3.1.1 interface showing a deleted file.

**File List:**

Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
lazvaniya.txt	/img_DiskImage_PHYSICALDRIVE1...	2015-04-03 16:54:28 EDT	0000-00-00 00:00:00	2015-04-03 00:00:00 EDT	2014-11-03 08:36:32 EST	9996	Allocated	Allocated
x.f.txt	/img_DiskImage_PHYSICALDRIVE1...	2015-04-07 10:27:46 EDT	0000-00-00 00:00:00	2015-04-07 00:00:00 EDT	2015-04-07 10:28:47 EDT	2459	Unallocated	Unallocated

**File Details (x.f.txt):**

Property	Value
Name	/img_DiskImage_PHYSICALDRIVE1 132.203.109.191 [132.203.109.191]_2015_07_04_08_42_01.E01/vol2/\$OrphanFiles/SNOWCR~1/f.txt
Type	File System
Size	2459
File Name	Unallocated
Allocation	Unallocated
Modified	2015-04-07 10:27:46 EDT
Accessed	2015-04-07 00:00:00 EDT
Created	2015-04-07 10:28:47 EDT
Changed	0000-00-00 00:00:00
MD5	0830013e29f23ddb89dc0a122ce81a82
Hash Lookup Results	UNKNOWN
Internal ID	421

**File Content (Text View):**

```
(function() {  
  var f = document.getElementById('');  
  if (!f) {  
    f = document.getElementById('searchbox_demo');  
    if (f && f['q']) {  
      var q = f['q'];  
      var n = navigator;  
      var l = location;  
      var du = function(n, v) {  
        var u = document.createElement('input');  
        u.name = n;  
        u.value = v;  
        u.type = 'hidden';  
        f.appendChild(u);  
        return u;  
      };  
      var su = function(n, t, v, l) {  
        if (!encodeURIComponent || !decodeURIComponent) {  
          return;  
        }  
        var regexp = new RegExp('(?:[?&])' + n + '=' + ([^&]*));  
        var existing = regexp.exec(t);  
        if (existing) {  
          v = decodeURIComponent(existing[1]);  
          var delimIndex = v.indexOf('://');  
          if (delimIndex >= 0) {  
            v = v.substring(delimIndex + '://'.length, v.length);  
            var v_sub = v.substring(0, 1);  
            while (encodeURIComponent(v_sub).length > 1) {  
              v_sub = v_sub.substring(0, v_sub.length - 1);  
            }  
            du(n, v_sub);  
          }  
          var pl = function(h) {  
            var ti = 0, tsi = 0, tk = 0, pt;
```



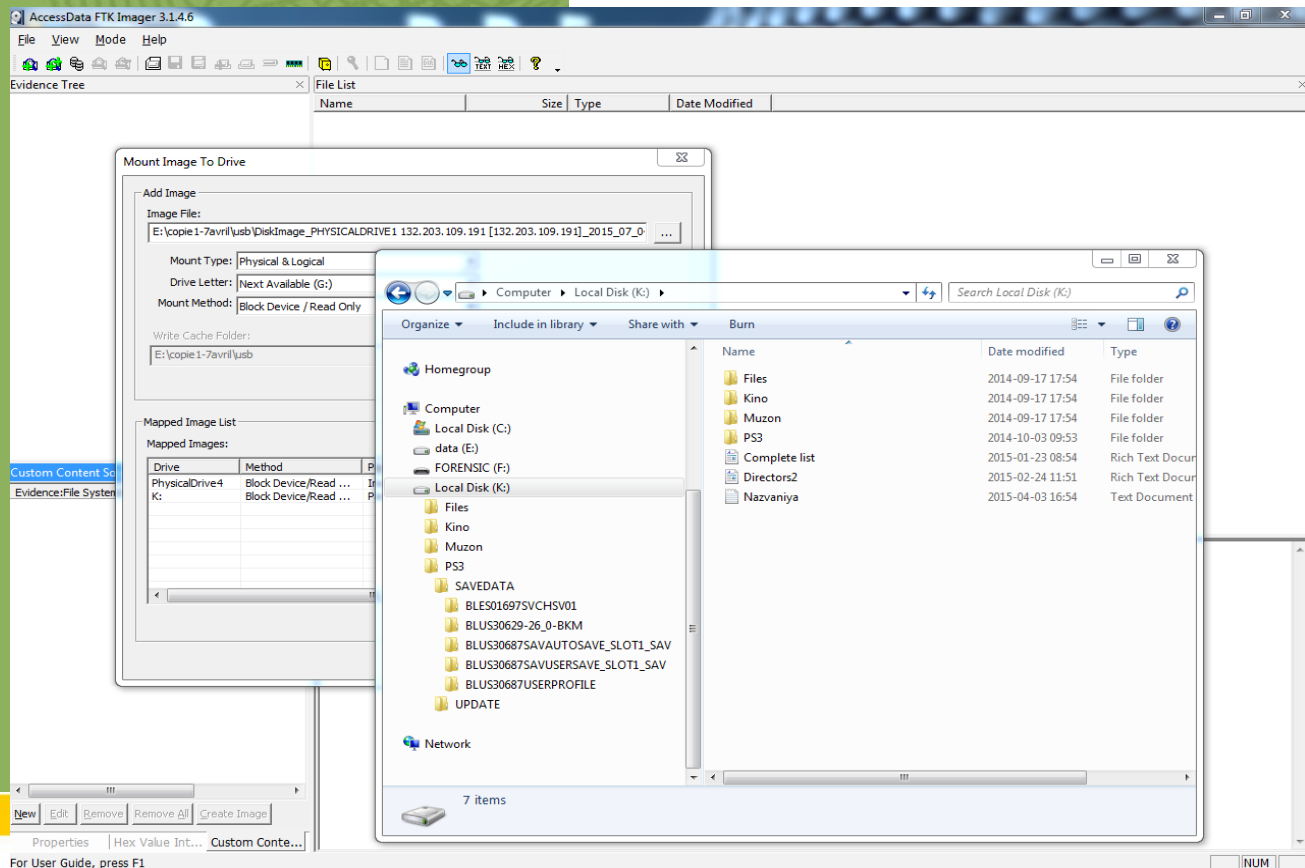
Bureau de sécurité de l'information



## Sixième partie

# Montage d'une clé USB :

FTK Imager



UNIVERSITÉ  
LAVAL

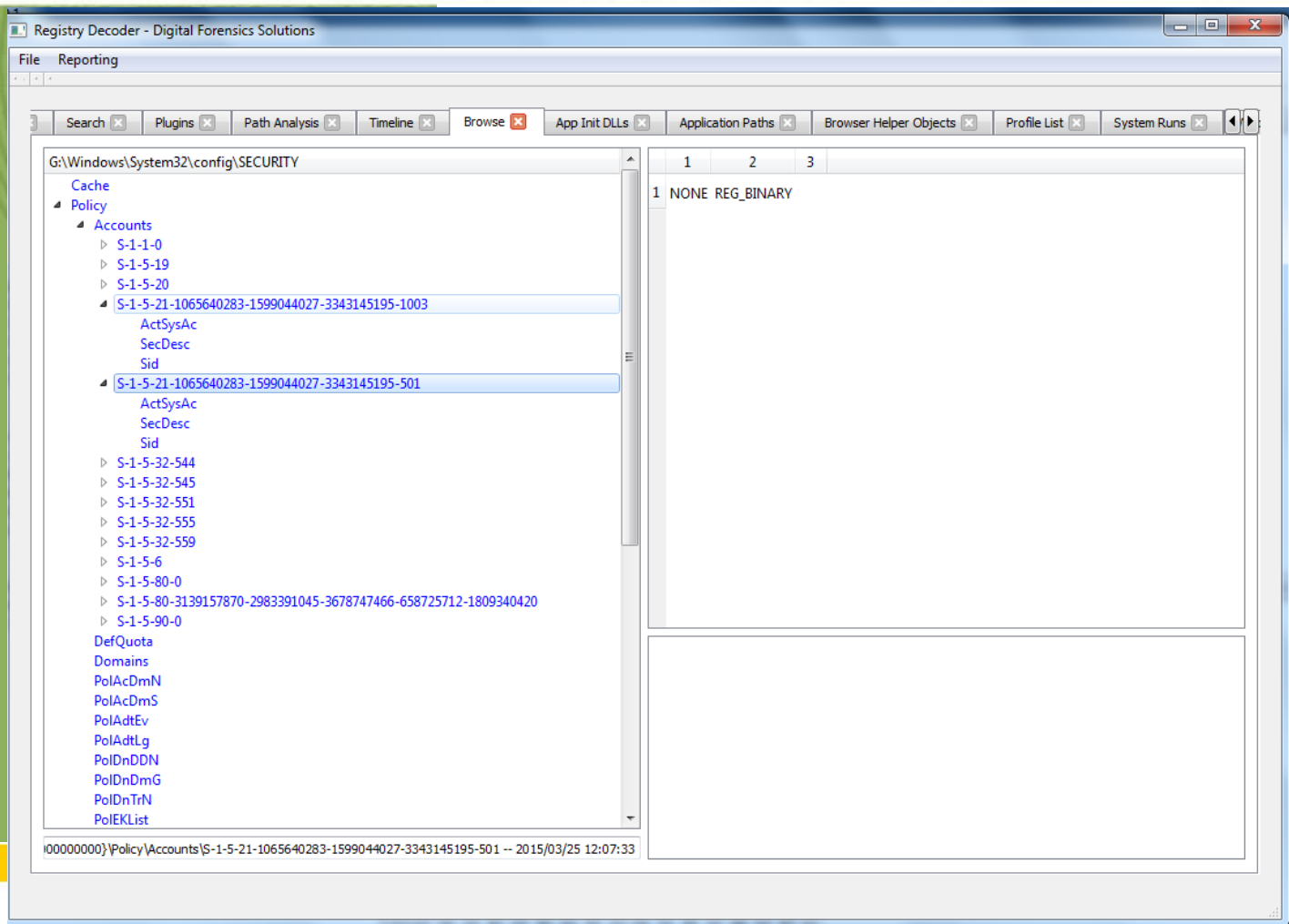
Bureau de sécurité de l'information



## Sixième partie

# Analyse du registre Windows :

Registry Decoder



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information





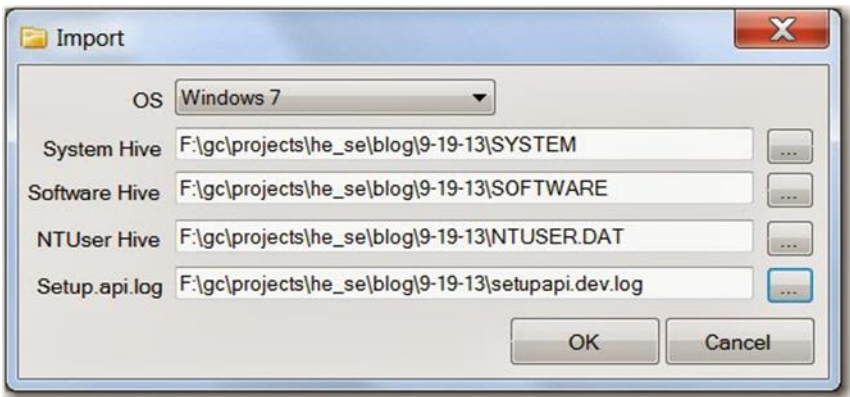
## Sixième partie

# Croisement de 4 fichiers du registre Windows :

System  
Software  
NTUSER.dat  
SetupAPI

USBDeviceForensics

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				

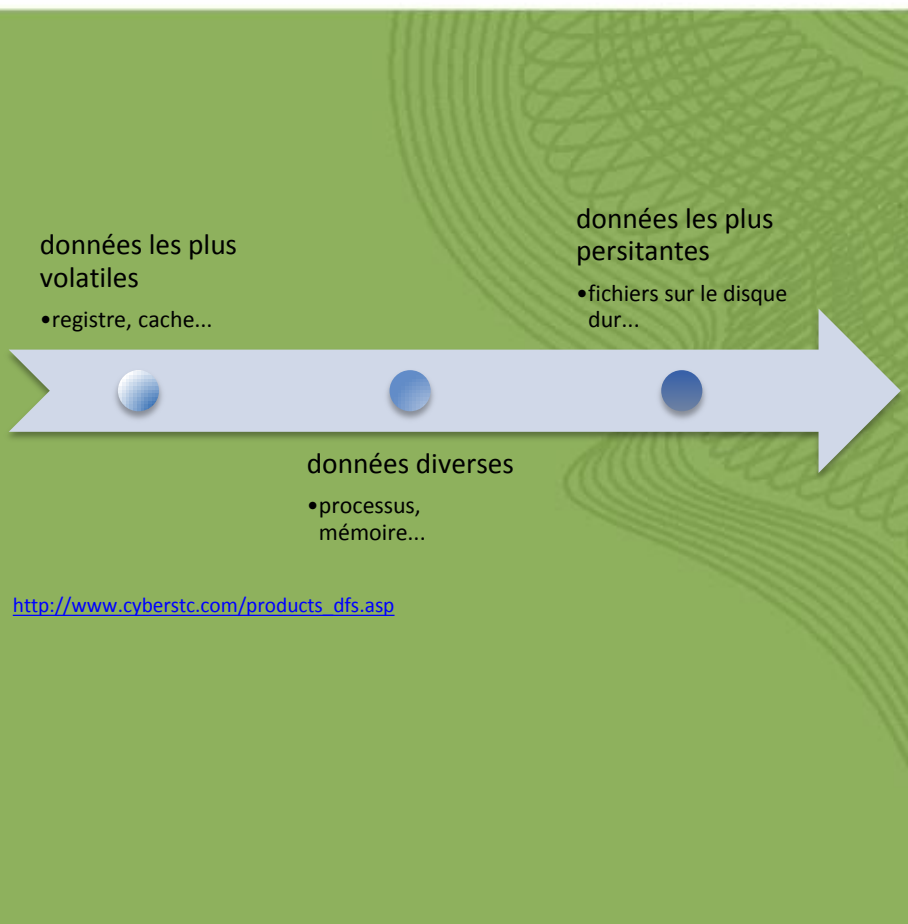


[http://www.hecfblog.com/2013\\_09\\_01\\_archive.html](http://www.hecfblog.com/2013_09_01_archive.html)





## Sixième partie



# "Live forensic"

Acquisition dynamique  
et la capture des  
données volatiles

Ordinateur est ouvert!



## Sixième partie

### Outils intéressants :

Capture :

AccessData : FTKToolkit, FTKImager

RamCapturer

SysinternalsSuite

NirSoft

UserDump

Mandiant RedLine

Extraction / Analyse :

Volatility Framework

Belkasoft Evidence Center

Plates-formes : Deft-Linux – Kali-Linux

### "Live forensic"



Bureau de sécurité de l'information



## Sixième partie

# Capture de données volatiles :

RFC 3227 chapitre 2.1 : Order of volatility



rfc3227.txt

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



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information

## Volatilité des données

Volatilitux, lime, draugr, memfetch, memdump, idetect, FTK Imager, Volatility Framework	Acquisition dynamique	<b>RAM</b> memory, swap, cpu	WMFT, WFT, Memorize, msrmdmp, FTK Imager, Volatility Framework, mem.exe, dumpel.exe
Volatilitux, draugr, foriana, memfetch, memdump, idetect, Volatility Framework		<b>PROCESS</b> process table, kernel statistics, system process	WMFT, WFT, Memorize, msrmdmp, Volatility Framework, pslist.exe, ps.exe, psfile.exe, psinfo.exe, psloglist.exe, psservice.exe, pstat.exe, psuptime.exe, servicelist.exe
memdump, idetect, Volatility Framework, ps aux, netstat, fport		<b>NETWORK PROCESS</b> routing table, arp cache, remote logging and monitoring data, network topology	WMFT, WFT, Memorize, msrmdmp, Volatility Framework, fport.exe, arp.exe, ipconfig.exe, mac.exe, nbtstat.exe, net.exe, netstat.exe, netusers.exe, psloggedon.exe, route.exe, sniffer.exe, RootkitRevealer.exe, openports.exe, iplist.exe, ipxroute.exe, ntlast.exe, promiscdetect.exe, hostname.exe, hunt.exe
		<b>SYSTEM SETTINGS</b> temporary file systems, physical configuration, registers, cache	listdlls.exe, reg.exe, regdmp.exe, ntfsinfo.exe, drivers.exe, attrib.exe, autorunsc.exe, auditpol.exe, handle.exe
FTK Imager, DFF, OSForensics, DHash2, GuyMager, dd, cyclone, Paladin ToolBox, DdRescue, dc3dd, Aimage	Acquisition statique	<b>DATA</b> disk, archival media	FTK Imager, DFF, OSForensics, DHash2, GuyMager, dd, cyclone, Paladin ToolBox, DdRescue, dc3dd, Aimage

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



## 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.lb  
4b6t3.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&STOR  
AGE#VOLUME#_??_USBSTOR#DISK&VEN_STAPLES&PROD_RELAY_UF  
D&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  
Volatility 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



## Sixième partie

### Outils intéressants :

Wireshark  
Tshark  
TCPdump  
Network Miner  
Xplico

Plates-formes : Kali-Linux – Deft-Linux

## "Network forensic"

Surveillance du trafic  
Fichiers journaux



Bureau de sécurité de l'information

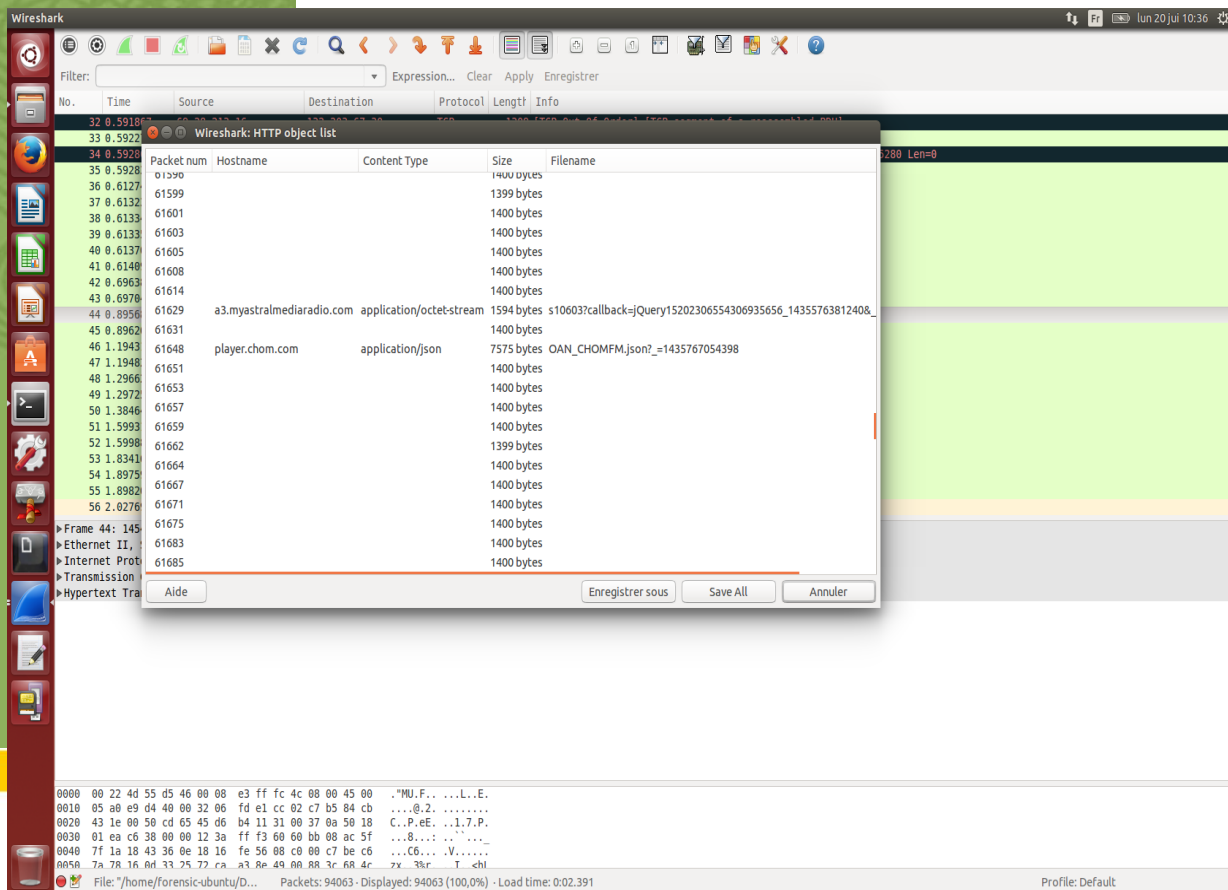


## Sixième partie

Exportation des objets  
d'une capture de  
trafic :

"Network forensic"

Wireshark



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information





## Sixième partie

# Conversations TCP :

Trafic entre deux "endpoints" spécifiques

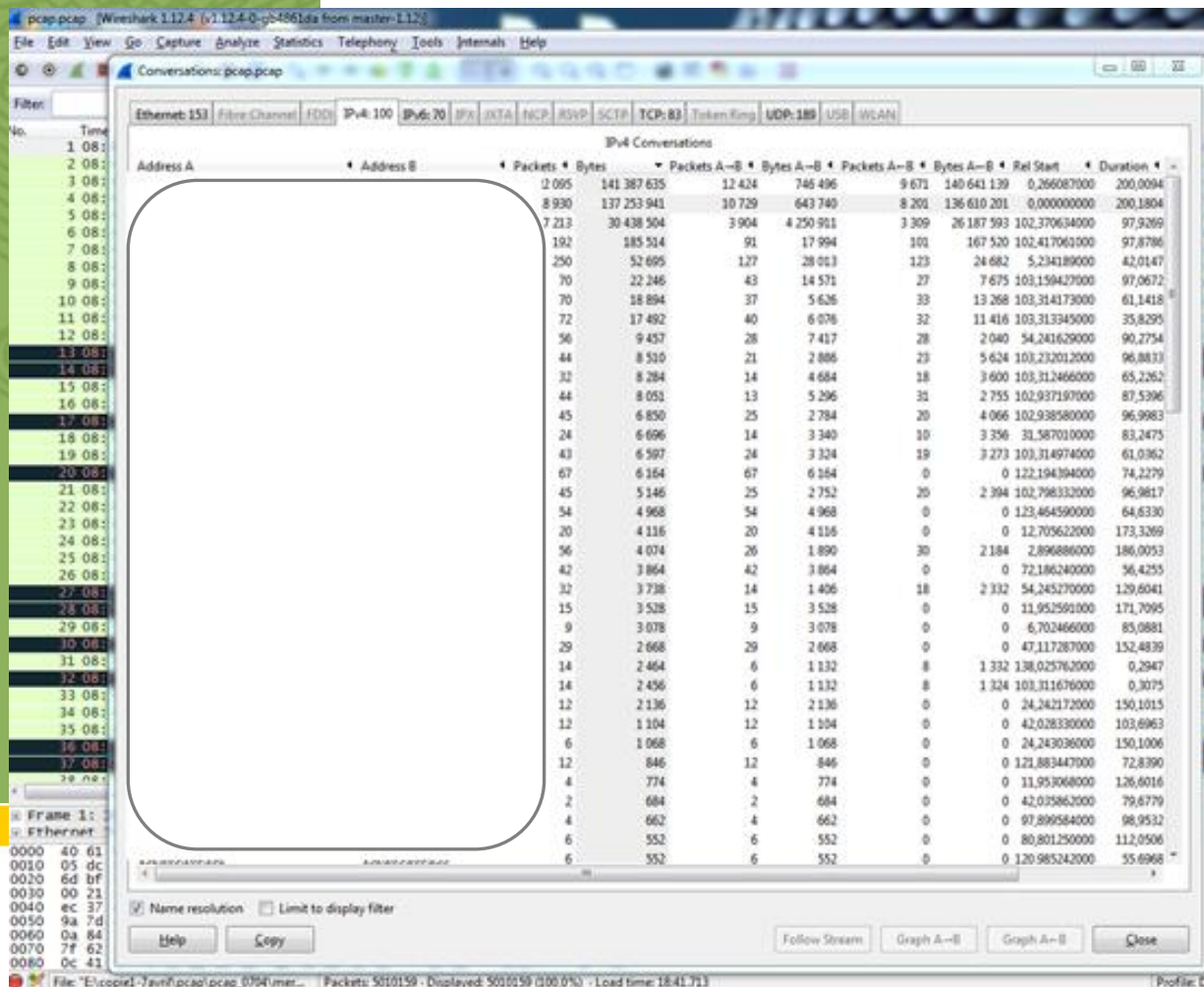
Wireshark



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information

# "Network forensic"



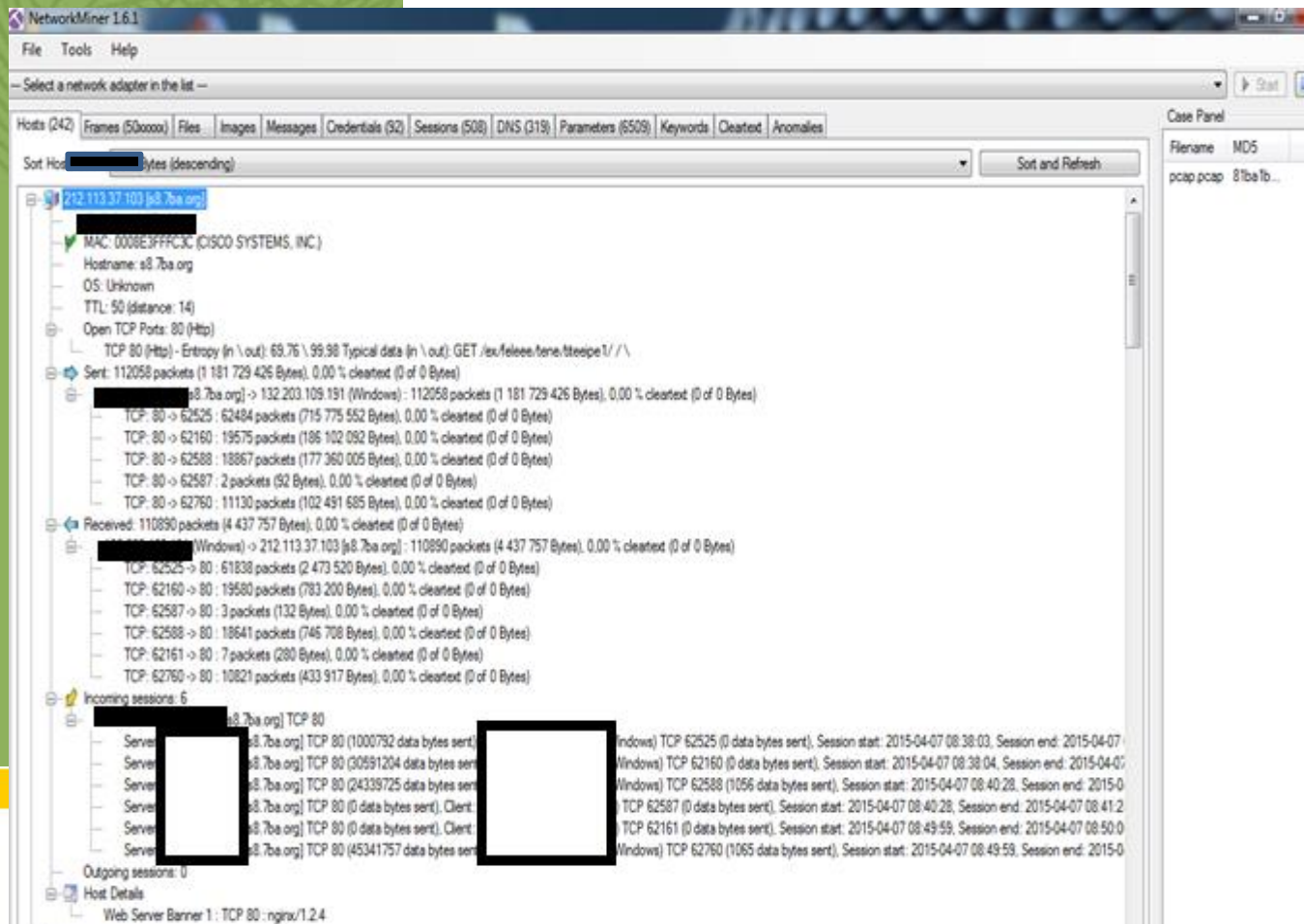


## Sixième partie

# Analyse d'une capture de trafic :

## "Network forensic"

Network Miner



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



## 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!



## Sixième partie

### Outil intéressant :

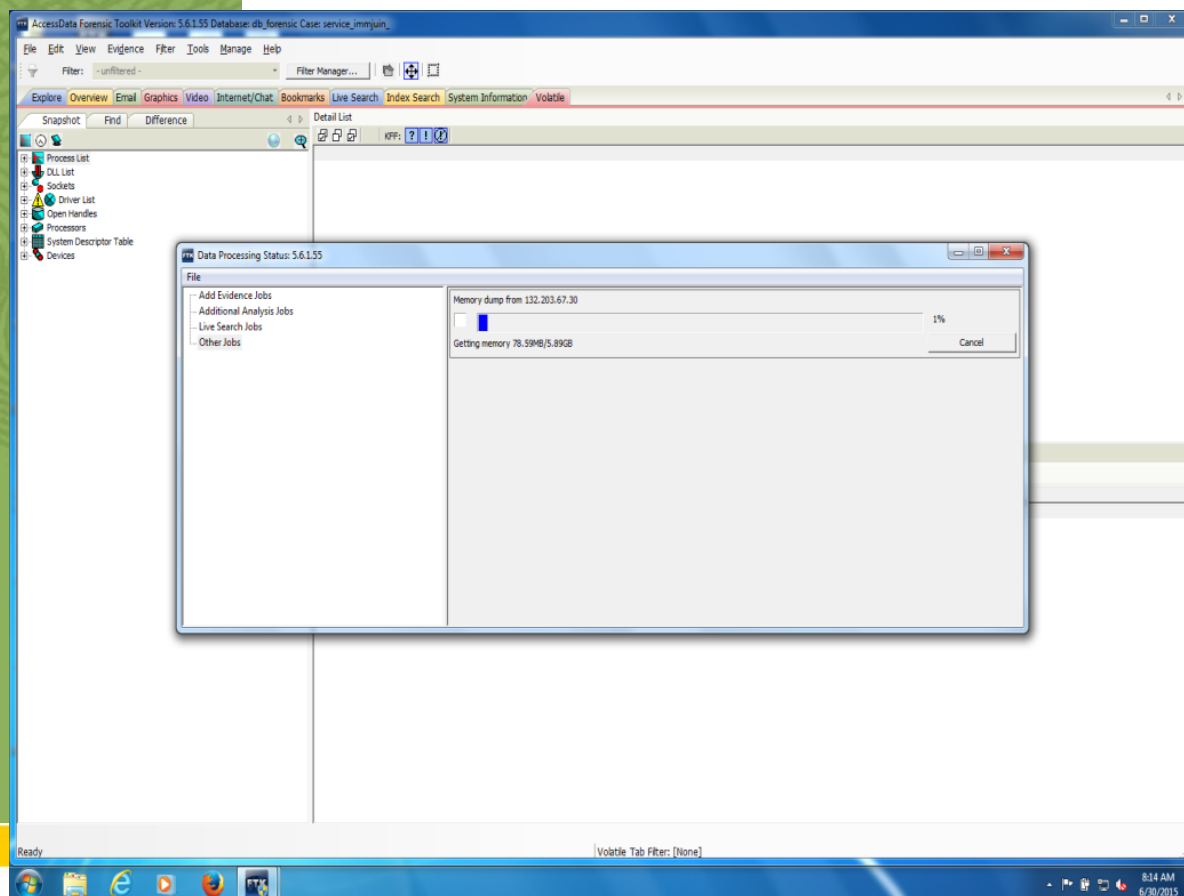
AccessData : FTKToolkit

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!

## "Remote forensic"



Bureau de sécurité de l'information



## Sixième partie

### 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

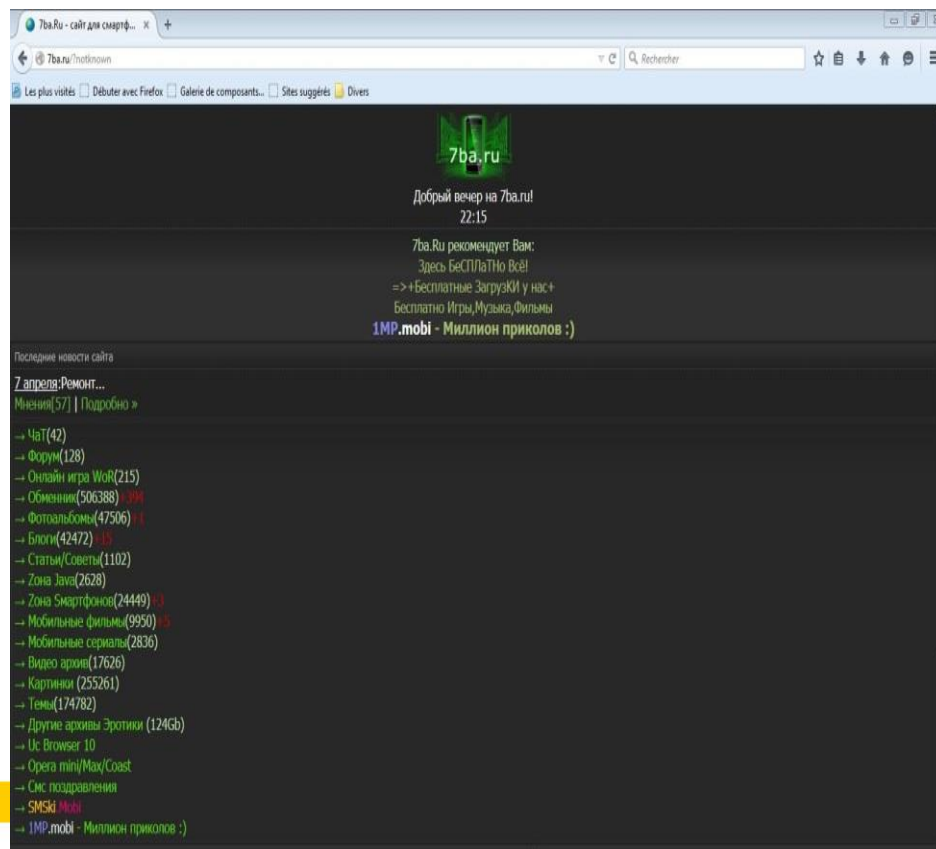
DomainTools:

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



Bureau de sécurité de l'information



## Sixième partie

Surveillance et extraction de données

tcpdump

tshark



Analyse des données

wireshark

## 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 !



## Septième partie

# 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

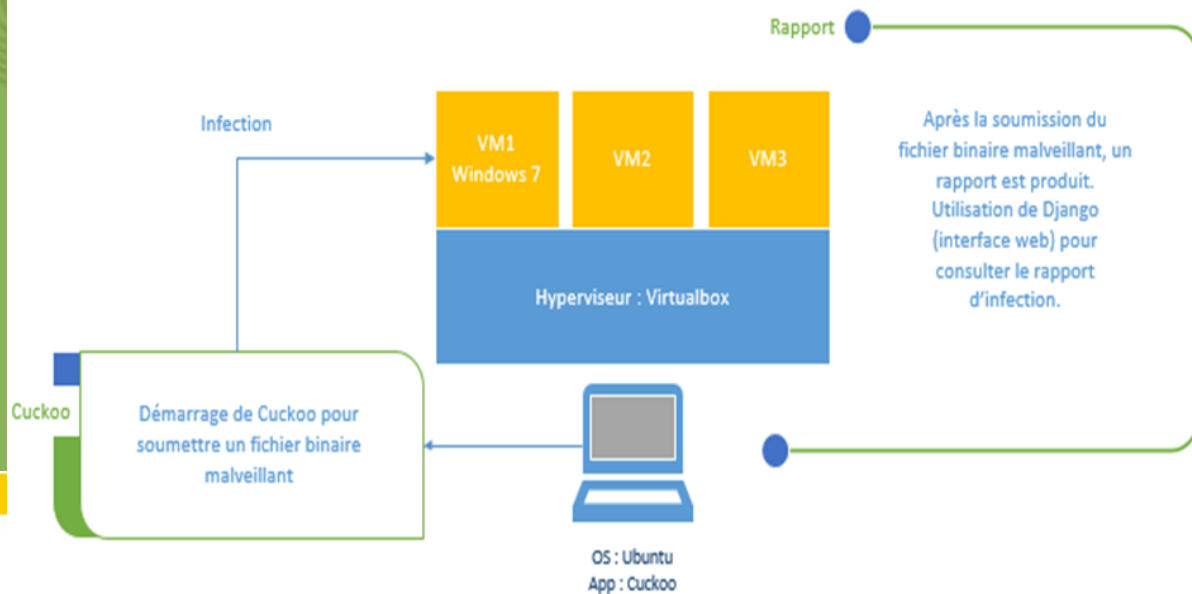


UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information

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

## Analyse de malware!!!





## Septième partie

### 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"



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



### 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'identification 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'amorçage

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)

Directory Seek

Enter the name of a directory that you want to view.  
F: /

**VIEW**

File Name Search

Enter a Perl regular expression for the file names you want to find.

**SEARCH**

**ALL DELETED FILES**

**EXPAND DIRECTORIES**

Current Directory: F: /

**ADD NOTE** **GENERATE MD5 LIST OF FILES**

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	v / v	<u>\$FAT1</u>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	1921024	0	0	<a href="#">245566980</a>
	v / v	<u>\$FAT2</u>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	1921024	0	0	<a href="#">245566981</a>
	v / v	<u>\$MBR</u>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	<a href="#">245566979</a>
	d /	<u>\$OrphanFiles/</u>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	<a href="#">245566982</a>

ASCII ([display](#) - [report](#)) \* Hex ([display](#) - [report](#)) \* ASCII Strings ([display](#) - [report](#)) \* [Export](#) \* [Add Note](#)

File Type: data

**Structure**

Boot sector	More reserved sectors (optional)	FAT #1	FAT #2	Root directory (FAT12/16 only)	Data region (rest of disk)
-------------	----------------------------------	--------	--------	--------------------------------	----------------------------

<http://forensicswiki.org/wiki/FAT>



Bureau de sécurité de l'information

Autopsy TSK



## Septième partie

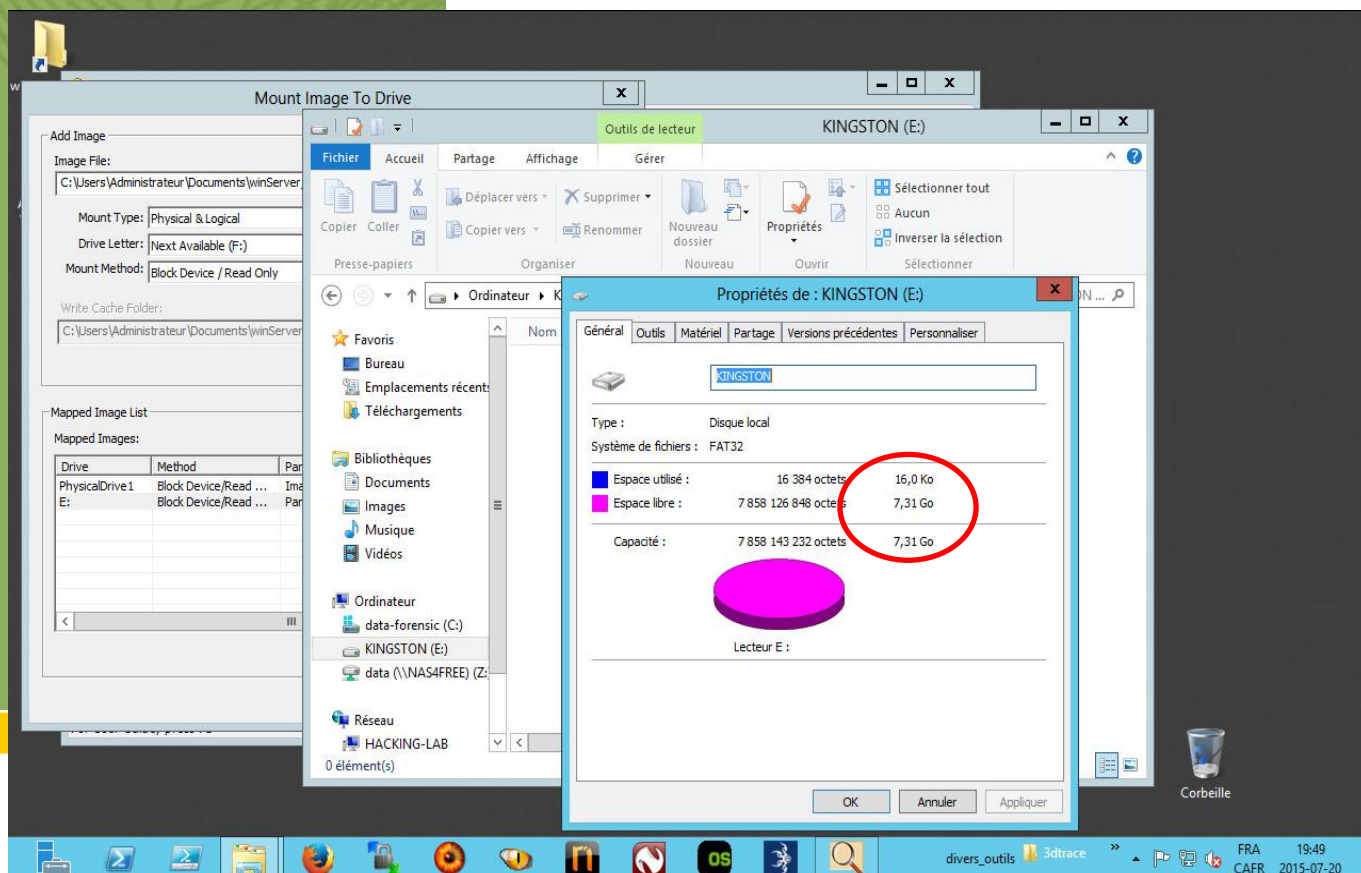
L'image de la clé USB peut être « montée » : pas de fichiers actifs !

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



UNIVERSITY OF LAMON

Bureau de s

AccessData FTK Imager 3.1.2.0

File View Mode Help

Evidence Tree

- navig.aff
- Partition 1 [7498MB]
- KINGSTON [FAT32]
- [root]
- [unallocated space]
- Unpartitioned Space [basic disk]
- [unallocated space]

File List

Name	Size	Type	Date Modified
000003	102 400	Unallocated Spa...	
006403	102 400	Unallocated Spa...	
012803	102 400	Unallocated Spa...	
019203	102 400	Unallocated Spa...	
025803	102 400	Unallocated Spa...	
032003	102 400	Unallocated Spa...	
038403	102 400	Unallocated Spa...	

Custom Content Sources

Evidence:File System[Path]File Options

Properties Hex Value Inter... Custom Content...

Cursor pos = 0; clus = 3; log sec = 8448; phy sec = 16512

navig.aff/Partition 1 [7498MB]/KINGSTON [FAT32]/[unallocated space]/000003

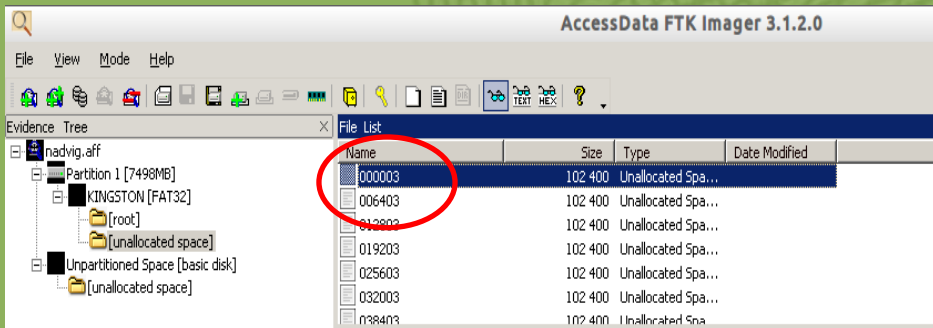
AccessData FTK I... sylvain Export Results

NUM 23:03



## Septième partie

### 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`



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information

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



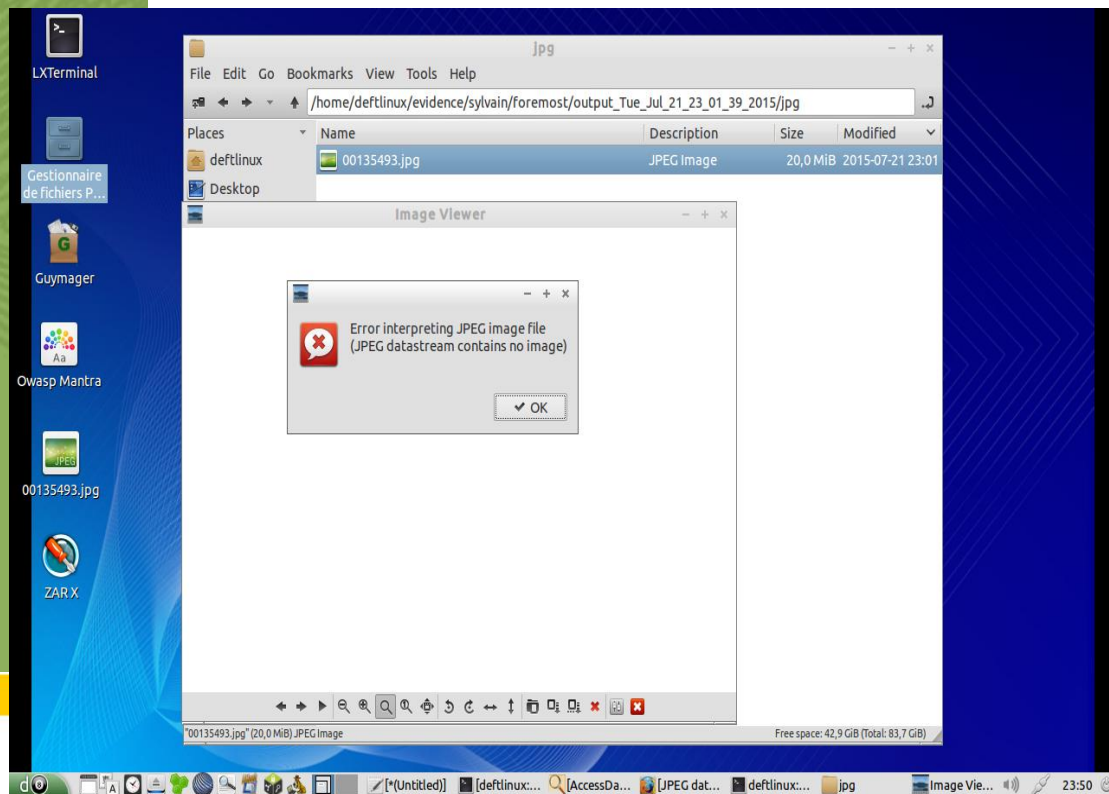
## Septième partie

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





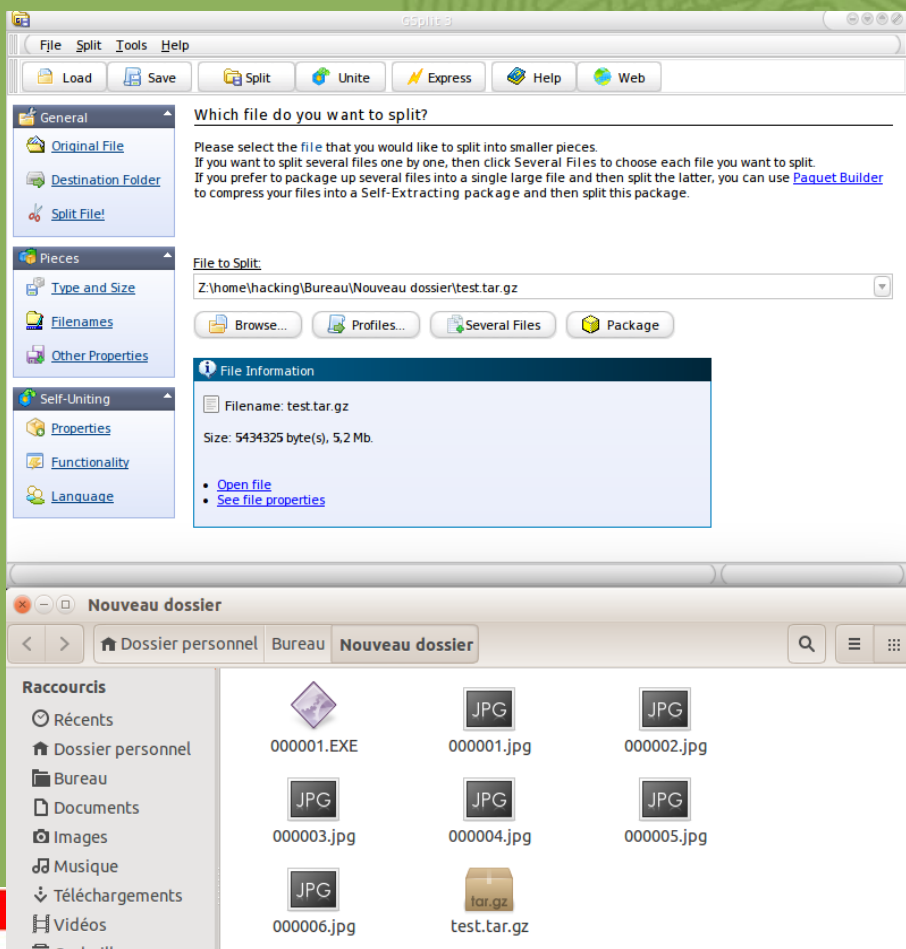
## Septième partie

# 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 ?



## Septième partie

### Utilitaires intéressants :

rsync  
bash script  
crontab  
tmux  
sandboxie  
keepnotes  
winmerge  
...

Tout au long de  
votre enquête...



## Septième partie

### Commandes Linux/Windows:

cat /proc/buddyinfo	lsuf
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



## Septième partie



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

Merci!



## **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](mailto: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

[claudc.charest@bsi.ulaval.ca](mailto:claudc.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](http://bsi.ulaval.ca)