

# 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- Soutien 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)



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



## Première partie

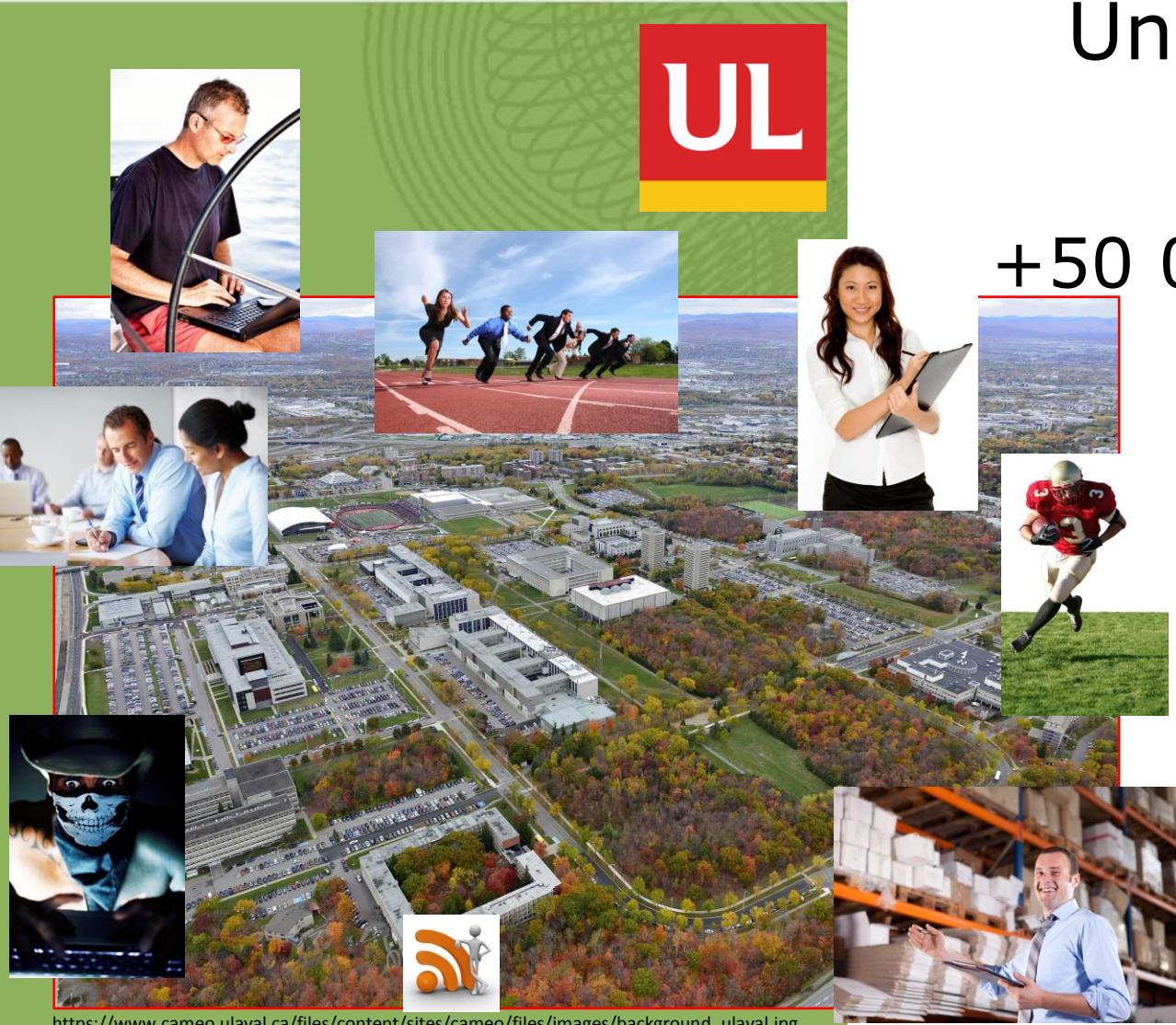


# Université Laval

-> 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



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.



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



# 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!



Bureau de sécurité de l'information



## 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-scrf/cbr-scrf/ccirc-ccric-fra.aspx>

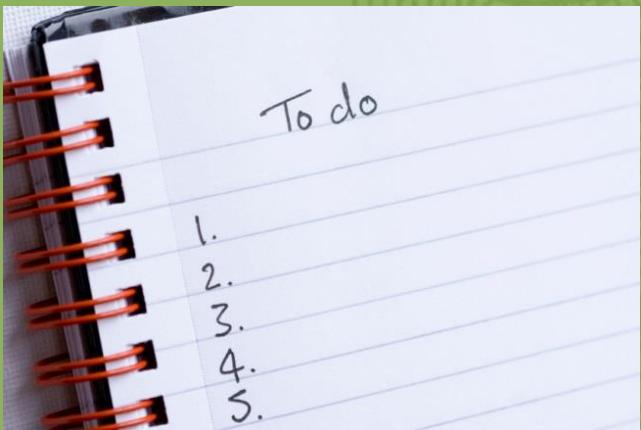
[http://www.cspq.gouv.qc.ca/faire-affaire-avec-le-cspq/famille-de-services/sous-famille-de-services/service/gestion-des-incident-gouvernementaux-certaq/?no\\_cache=1](http://www.cspq.gouv.qc.ca/faire-affaire-avec-le-cspq/famille-de-services/sous-famille-de-services/service/gestion-des-incident-gouvernementaux-certaq/?no_cache=1)



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



UNIVERSITÉ  
Laval

Bureau de sécurité de l'information



## 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.

# 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

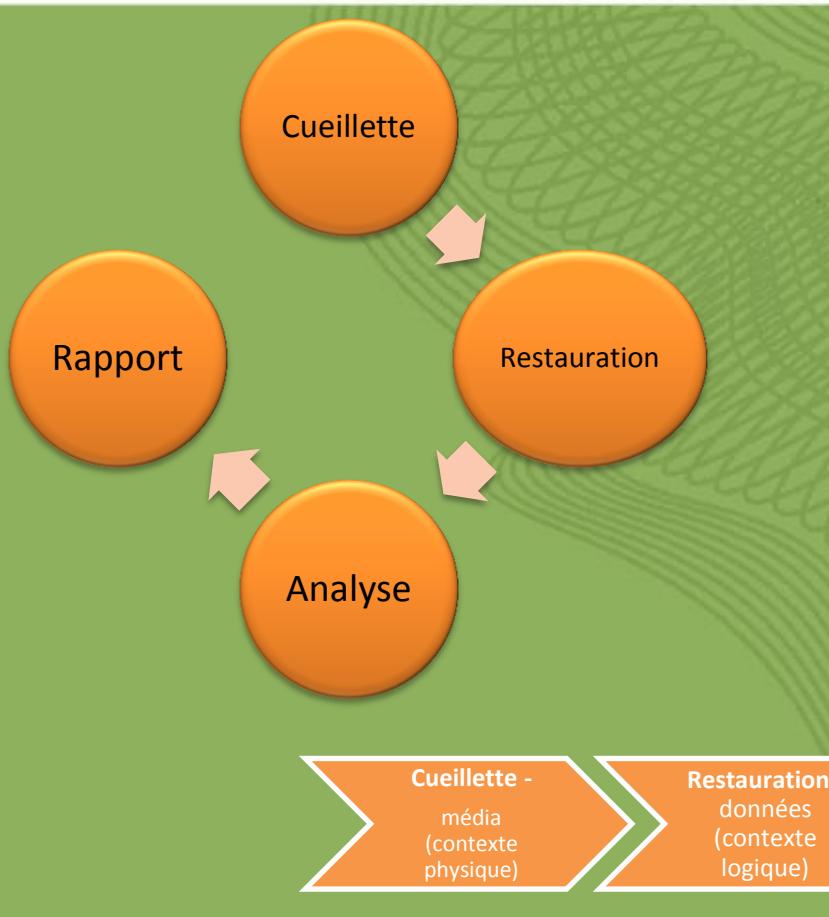
3.5 Recommendations



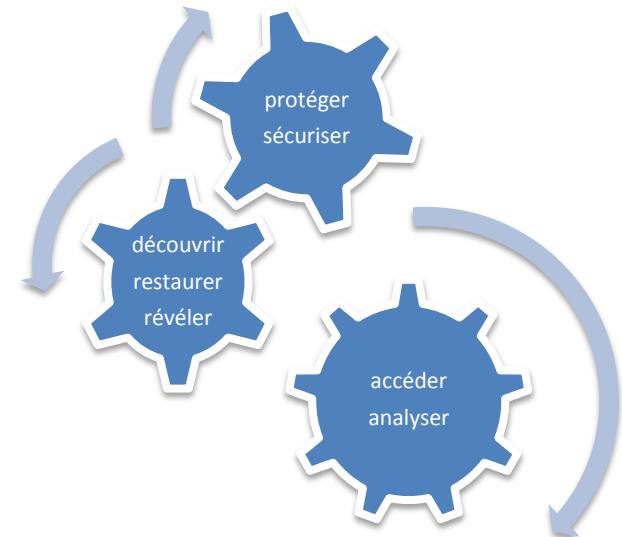
Bureau de sécurité de l'information



## Cinquième partie



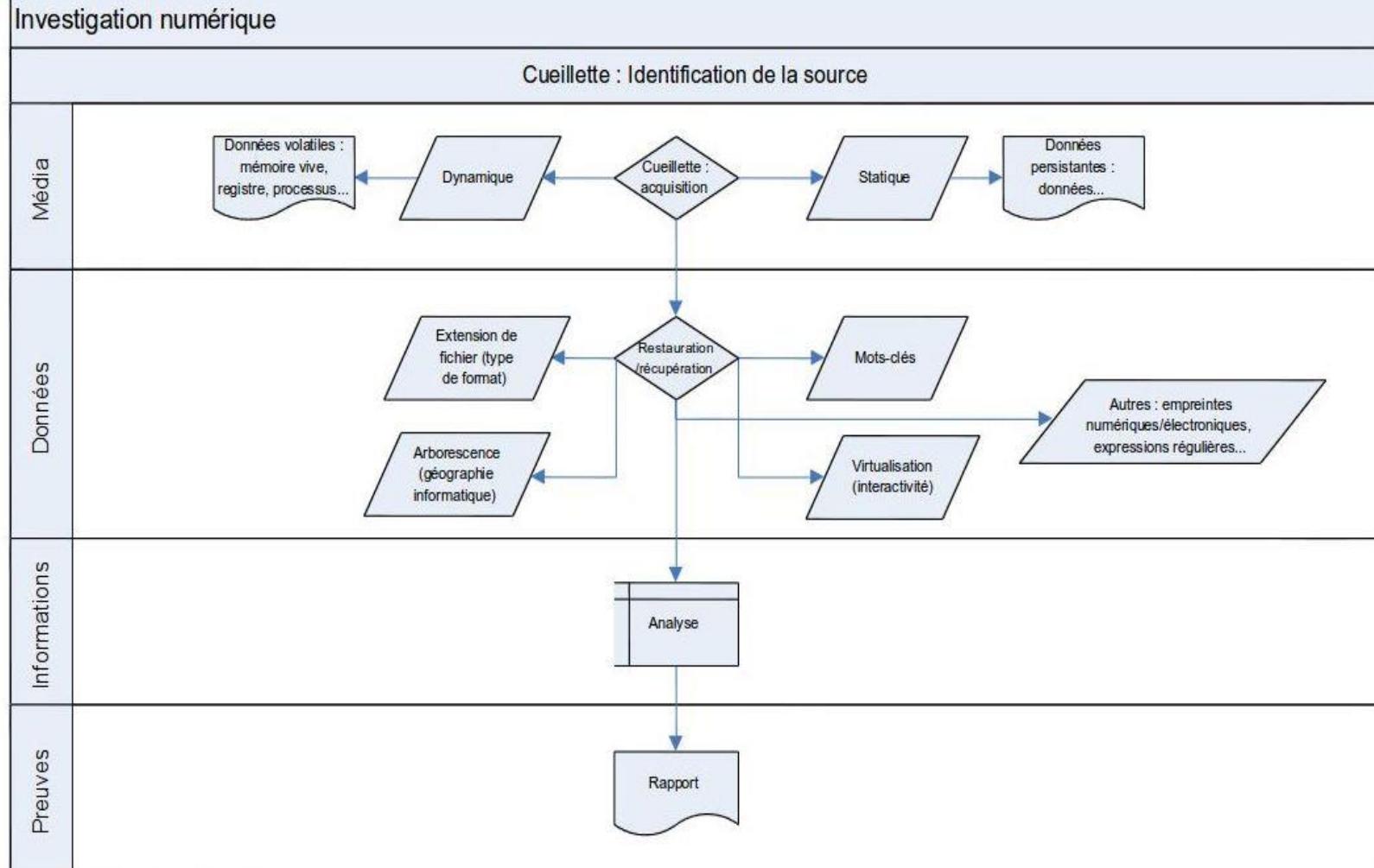
## Processus :





## 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.

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



## 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



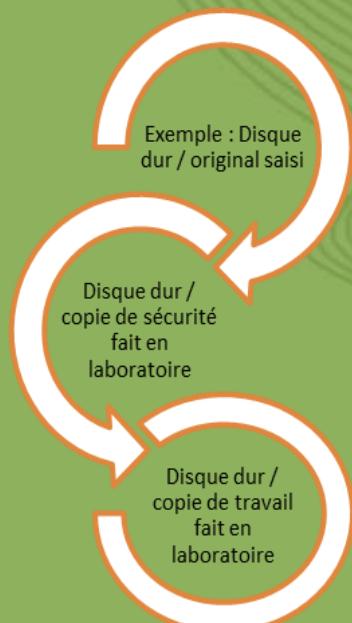
Bureau de sécurité de l'information



## 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>



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"



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



# Sixième partie

## Fichiers actifs & supprimés :

Autopsy

The screenshot shows the Autopsy 3.1.1 interface. The main window displays a 'Directory Listing' for a disk image. The listing includes columns for Name, Location, Modified Time, Change Time, Access Time, and Created Time. A thumbnail view is also present. A specific file, 'Beetlejuice\_1988\_720x404.mp4', is selected and shown in a preview window. The preview window displays the title 'BEETLE JUICE' from the movie. Below the preview are hex dump, strings, and meta data tabs. The bottom of the screen shows the Windows taskbar with various icons.



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



## Sixième partie

# Visualiser le contenu d'un fichier supprimé :

Autopsy

The screenshot shows the Autopsy interface with a red arrow pointing from the title 'Sixième partie' to the 'Deleted Files' section of the left sidebar.

**Deleted Files** (highlighted by a red arrow)

- Final Day (285)
- Final Day - 1 (0)
- Final Day - 2 (0)
- Final Day - 3 (0)
- Final Day - 4 (3)
- Final Day - 5 (0)
- Final Day - 6 (0)
- f.txt

**f.txt** (highlighted by a red arrow)

Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
Jazvaniya.txt	/img_DiskImage_PHYSICALDRIVE1 132.203.109.191 [132.203.109.191]_2015_07_04_08_42_01.E01/vol_vo1/\$OrphanFiles/SNOWCR~1/f.txt	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
f.txt	/img_DiskImage_PHYSICALDRIVE1 132.203.109.191 [132.203.109.191]_2015_07_04_08_42_01.E01/vol_vo1/\$OrphanFiles/SNOWCR~1/f.txt	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 System**

Name	Type	Size	File Name Allocation	Metadata Allocation	Modified	Accessed	Created	Changed	MD5	Hash Lookup Results	Internal ID
/img_DiskImage_PHYSICALDRIVE1 132.203.109.191 [132.203.109.191]_2015_07_04_08_42_01.E01/vol_vo1/\$OrphanFiles/SNOWCR~1/f.txt	File System	2459	Unallocated	Unallocated	2015-04-07 10:27:46 EDT	2015-04-07 00:00:00 EDT	2015-04-07 10:28:47 EDT	0000-00-00 00:00:00	0830013e29f23ddb89dc0a122ce81a82	UNKNOWN	421

**Text**

```
(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 pi = function(he) {
                var ti = 0, ts = 0, tk = 0, pt;
            }
        }
    }
})()
```



UNIVERSITÉ  
LAVAL

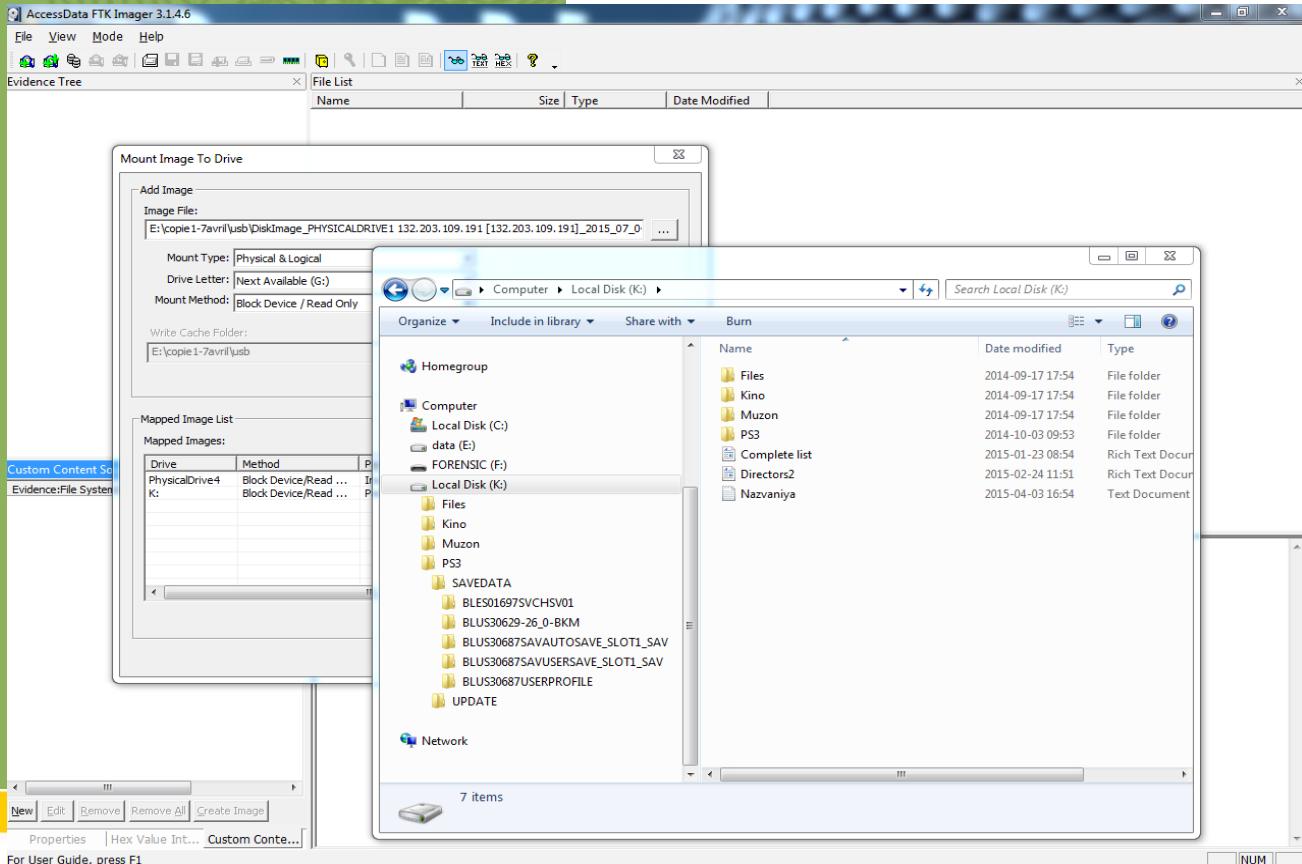
Bureau de sécurité de l'information



## 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

A screenshot of the Registry Decoder application window. The title bar reads "Registry Decoder - Digital Forensics Solutions". The menu bar includes "File" and "Reporting". The toolbar contains buttons for "Search", "Plugins", "Path Analysis", "Timeline", "Browse", "App Init DLLs", "Application Paths", "Browser Helper Objects", "Profile List", and "System Runs". The main pane shows the registry structure under "G:\Windows\System32\config\SECURITY". The "Policy" key is expanded, showing subkeys like "Accounts", "ActSysAc", "SecDesc", "Sid", and several SIDs (e.g., S-1-5-21-1065640283-1599044027-3343145195-1003, S-1-5-21-1065640283-1599044027-3343145195-501). Other keys visible include "DefQuota", "Domains", "PolAcDmN", "PolAcDmS", "PolAdtEv", "PolAdtLg", "PolDnDDN", "PolDnDmG", "PolDnTrN", and "PolEKList". A status bar at the bottom indicates the path "00000000\Policy\Accounts\S-1-5-21-1065640283-1599044027-3343145195-501 -- 2015/03/25 12:07:33".

1 2 3  
1 NONE REG\_BINARY



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information

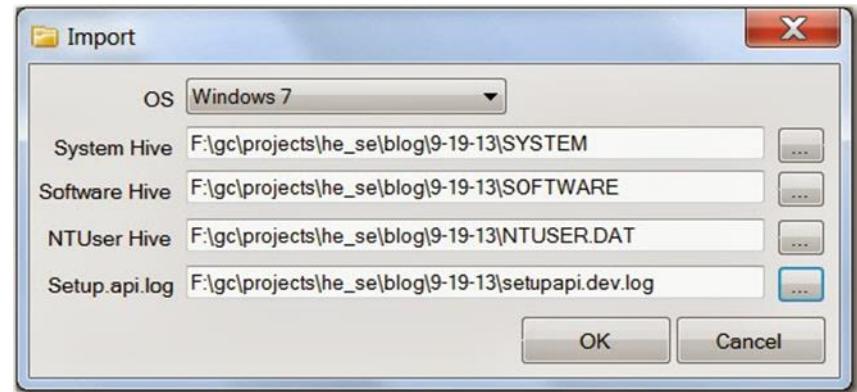


## Sixième partie

# Croisement de 4 fichiers du registre Windows :

System  
Software  
NTUSER.dat  
SetUpAPI

## USBDeviceForensics



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

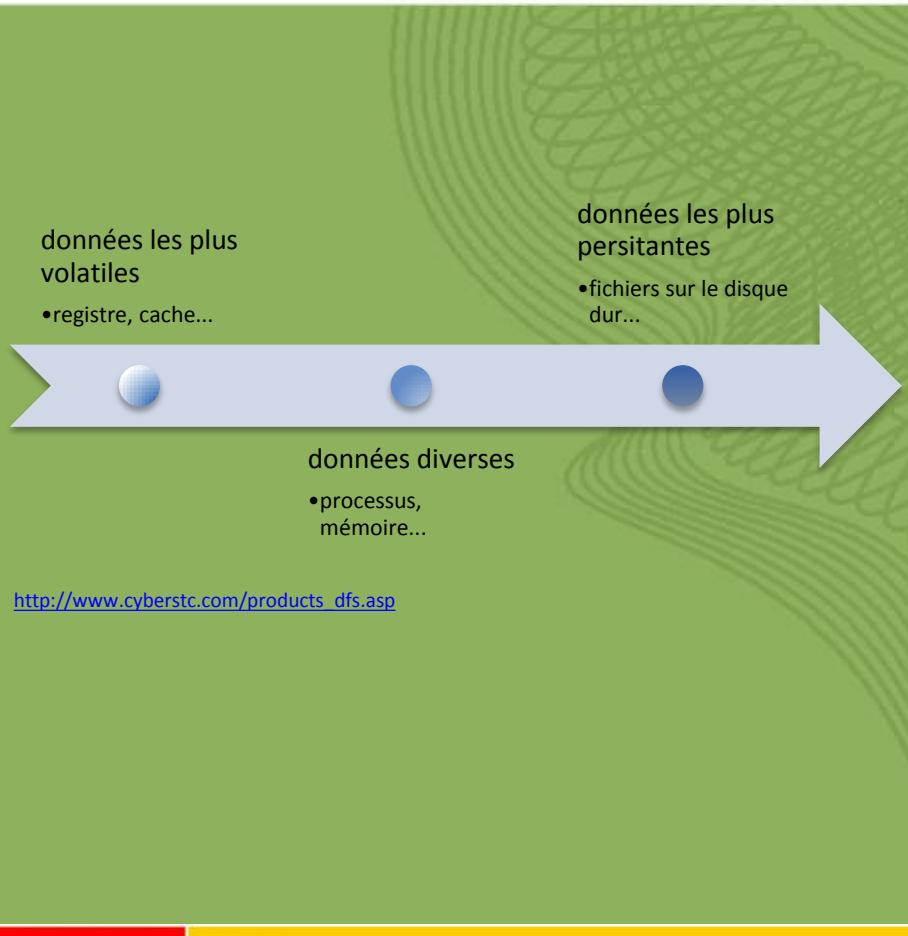
Vendor	Product	Version	Serial No	VID	PID	ParentIdPrefix	Drive Letter	Volume Name	GUID
Ven_	Prod_USB_Flash_Memory	Rev_5.00	ODE15280E2D1C89F	VID_0930	PID_6545				7037e1cc-ee5e-11e4-827e-e839355c0918
Ven_Kingston	Prod_DataTraveler_2.0	Rev_1.00	08606E6D3FDAFE7047062957	VID_0951	PID_1665				a574a44e-fedf-11e4-828d-e839355c0918
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				



Bureau de sécurité de l'information



## Sixième partie



### "Live forensic"

Acquisition dynamique  
et la capture des  
données volatiles

Ordinateur est ouvert!



Bureau de sécurité de l'information



## Sixième partie

### Outils intéressants :

Capture :

AccessData : FTKToolkit, FTKImager

RamCapturer

SysinternalsSuite

NirSoft

UserDump

Mandiant RedLine

Extraction / Analyse :

Volatile 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



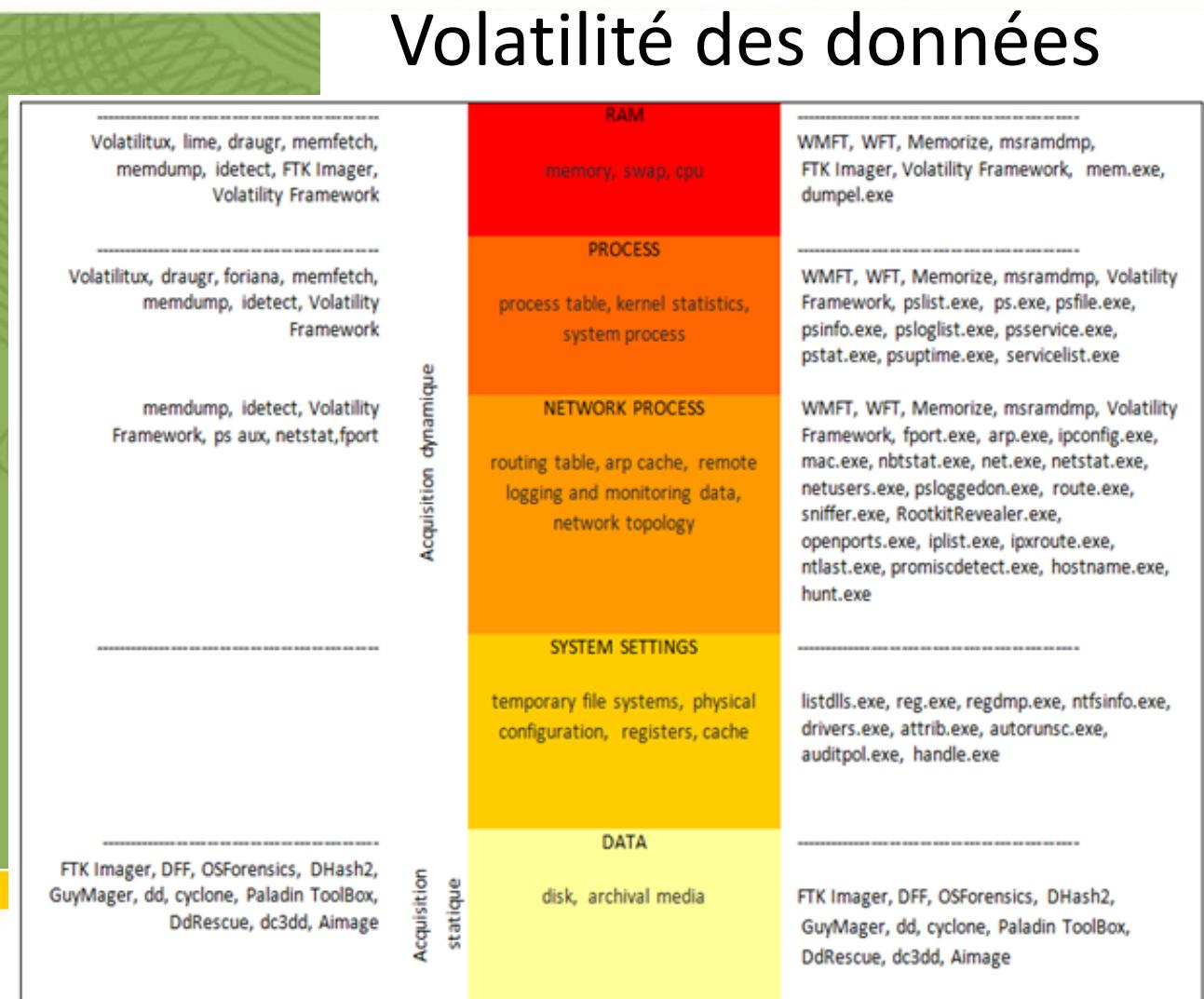
rfc3227.txt

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



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



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



# Sixième partie

```
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 dllist 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 0x13e000  C:\Windows\SYSTEM32\ntdll.dll
0x779f0000 0xd4000   C:\Windows\SYSTEM32\kernel32.dll
0x75ca0000 0x04a000  C:\Windows\SYSTEM32\KERNELBASE.dll
0x75440000 0x0ac000  C:\Windows\SYSTEM32\msvcrt.dll
0x76550000 0x01e000  C:\Windows\SYSTEM32\RPCRT4.dll
0x758d0000 0x016000  C:\Windows\SYSTEM32\SplC1.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\seext.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
0x81cef08 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/>



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



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information

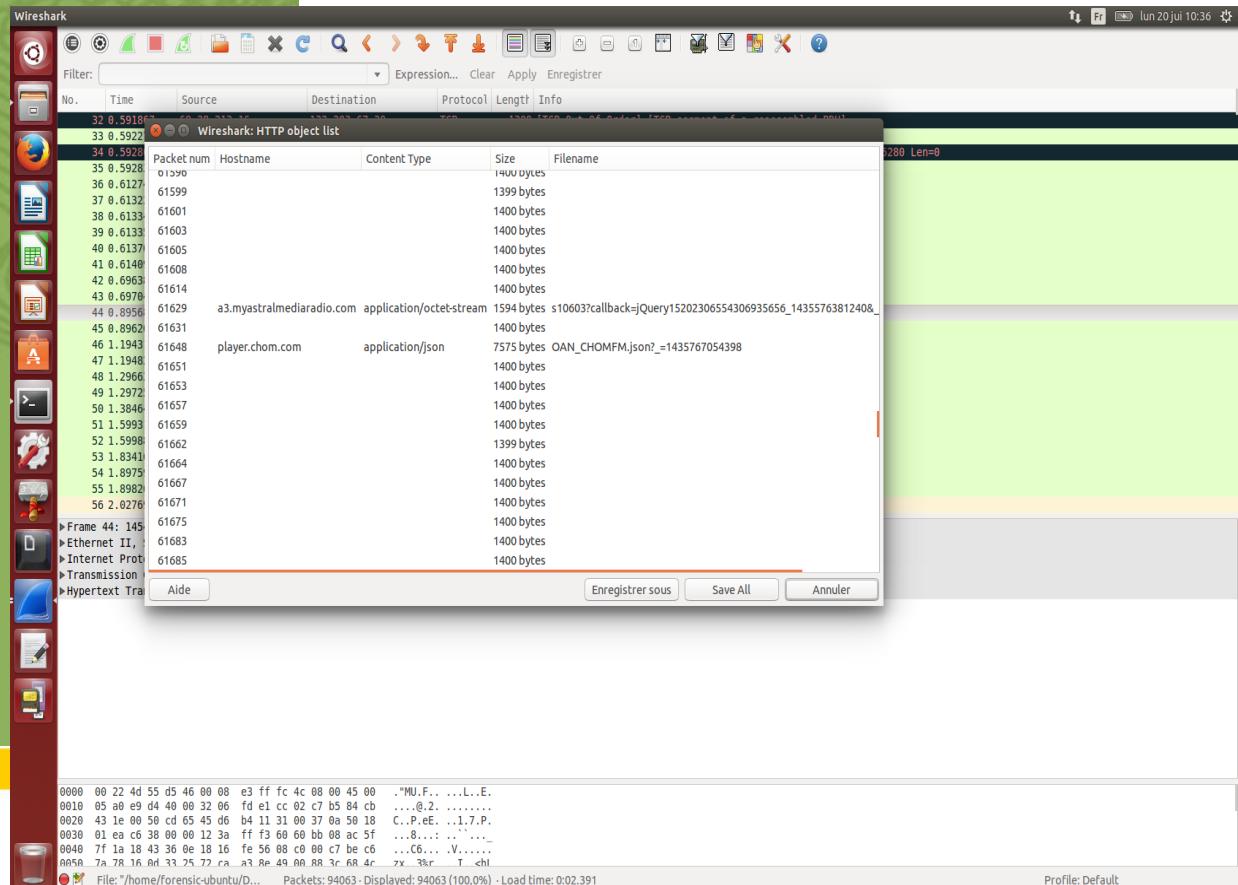


## Sixième partie

# Exportation des objets d'une capture de trafic :

Wireshark

## "Network forensic"



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



## Sixième partie

### Conversations TCP :

Trafic entre deux “endpoints” spécifiques

The screenshot shows the Wireshark interface with a list of TCP conversations. A specific conversation is highlighted with a large black oval. The conversation details show Address A and Address B, along with various statistics for each packet exchange.

No.	Time	Address A	Address B	Packets	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration
1	08:12:44.000000000	192.168.1.100	192.168.1.101	12095	141387635	12424	746496	9671	140641139	0.266087000
2	08:12:44.000000000	192.168.1.100	192.168.1.101	8930	137253943	10729	643749	8201	136610201	0.000000000
3	08:12:44.000000000	192.168.1.100	192.168.1.101	7213	30438504	3904	4250911	3309	26187593102370634000	97.9269
4	08:12:44.000000000	192.168.1.100	192.168.1.101	192	185504	91	17994	101	167520102417063000	97.8786
5	08:12:44.000000000	192.168.1.100	192.168.1.101	250	52695	127	28013	123	246825234189000	42.0147
6	08:12:44.000000000	192.168.1.100	192.168.1.101	70	22246	43	14571	27	7675101159427000	97.0672
7	08:12:44.000000000	192.168.1.100	192.168.1.101	70	18894	37	5626	33	13268103314173000	61.1418
8	08:12:44.000000000	192.168.1.100	192.168.1.101	72	17492	40	6076	32	11416103313345000	35.8295
9	08:12:44.000000000	192.168.1.100	192.168.1.101	56	9437	28	7417	28	204054241629000	90.7754
10	08:12:44.000000000	192.168.1.100	192.168.1.101	44	8510	21	2886	23	5624101232012000	96.8833
11	08:12:44.000000000	192.168.1.100	192.168.1.101	32	8284	14	4684	18	36001033124666000	65.2262
12	08:12:44.000000000	192.168.1.100	192.168.1.101	44	8053	13	5296	31	2755101937197000	87.5396
13	08:12:44.000000000	192.168.1.100	192.168.1.101	45	6850	25	2784	20	4066102938580000	96.9983
14	08:12:44.000000000	192.168.1.100	192.168.1.101	24	6696	14	3340	19	3336313587010000	83.2475
15	08:12:44.000000000	192.168.1.100	192.168.1.101	43	6597	24	3324	19	3273101314974000	61.0362
16	08:12:44.000000000	192.168.1.100	192.168.1.101	67	6164	67	6164	0	0122194394000	74.2279
17	08:12:44.000000000	192.168.1.100	192.168.1.101	45	5146	25	2752	26	2394102798332000	96.9817
18	08:12:44.000000000	192.168.1.100	192.168.1.101	54	4968	54	4968	0	01234645590000	64.6330
19	08:12:44.000000000	192.168.1.100	192.168.1.101	20	4116	20	4116	0	012705622000	173.3269
20	08:12:44.000000000	192.168.1.100	192.168.1.101	56	4074	26	1890	30	2184289686000	186.0953
21	08:12:44.000000000	192.168.1.100	192.168.1.101	42	3864	42	3864	0	032186240000	56.4255
22	08:12:44.000000000	192.168.1.100	192.168.1.101	32	3738	14	1406	18	233254245270000	129.6041
23	08:12:44.000000000	192.168.1.100	192.168.1.101	15	3528	15	3528	0	011952591000	171.7095
24	08:12:44.000000000	192.168.1.100	192.168.1.101	9	3078	9	3078	0	067024666000	85.0881
25	08:12:44.000000000	192.168.1.100	192.168.1.101	29	2668	29	2668	0	047117287000	152.4839
26	08:12:44.000000000	192.168.1.100	192.168.1.101	14	2464	6	1132	8	1332138025762000	0.2947
27	08:12:44.000000000	192.168.1.100	192.168.1.101	14	2456	6	1132	8	1324101311676000	0.3075
28	08:12:44.000000000	192.168.1.100	192.168.1.101	12	2136	12	2136	0	024242172000	150.1015
29	08:12:44.000000000	192.168.1.100	192.168.1.101	12	1104	12	1104	0	042028330000	103.6963
30	08:12:44.000000000	192.168.1.100	192.168.1.101	6	1068	6	1068	0	024243036000	150.1006
31	08:12:44.000000000	192.168.1.100	192.168.1.101	12	846	12	846	0	0121883447000	72.8390
32	08:12:44.000000000	192.168.1.100	192.168.1.101	4	774	4	774	0	011953068000	126.6016
33	08:12:44.000000000	192.168.1.100	192.168.1.101	2	684	2	684	0	04202862000	79.6779
34	08:12:44.000000000	192.168.1.100	192.168.1.101	4	662	4	662	0	097899584000	98.9532
35	08:12:44.000000000	192.168.1.100	192.168.1.101	6	552	6	552	0	080801250000	112.0506
36	08:12:44.000000000	192.168.1.100	192.168.1.101	6	552	6	552	0	0120985242000	55.6966



UNIVERSITÉ  
LAVAL

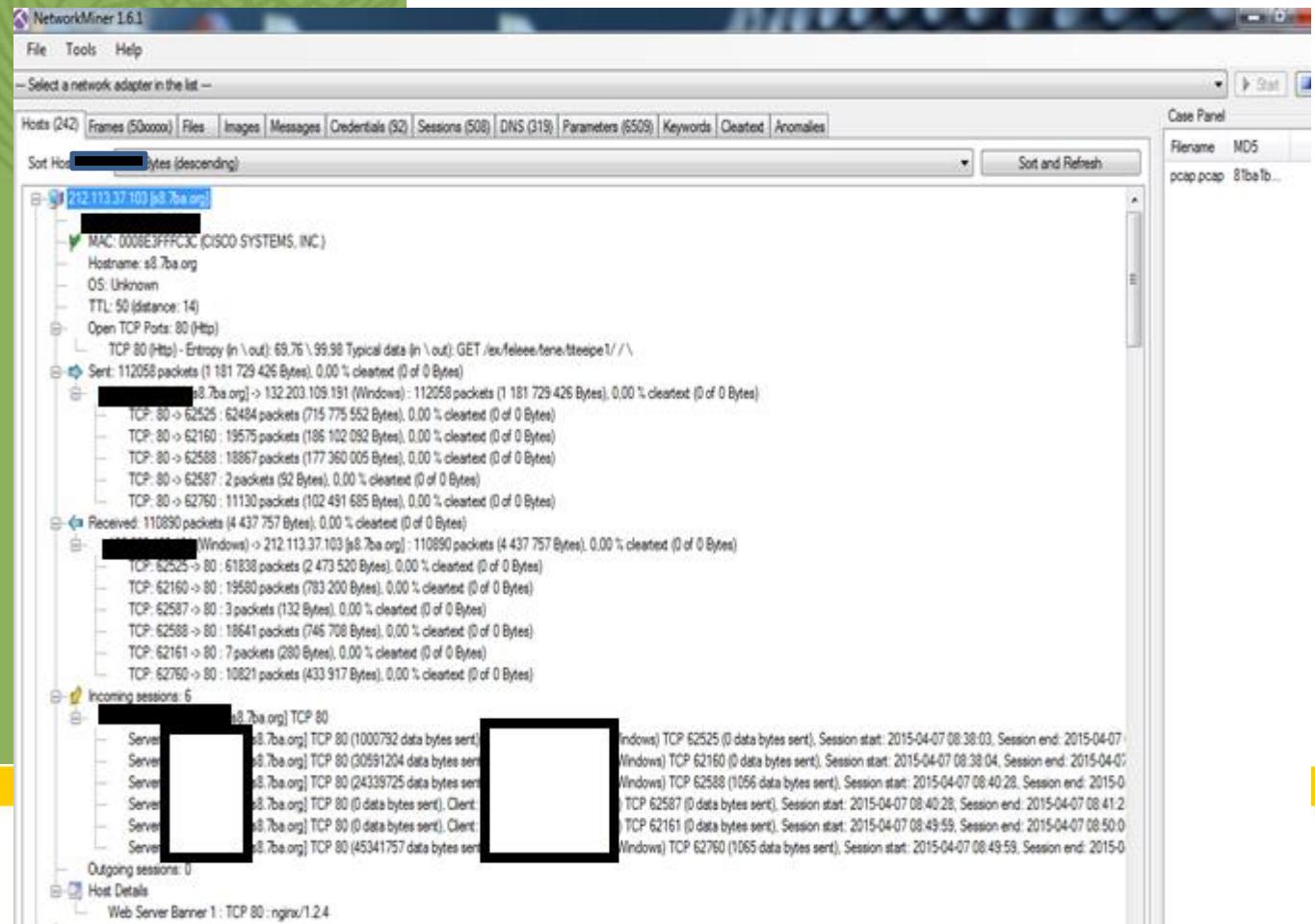
Bureau de sécurité de l'information



## 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



Bureau de sécurité de l'information



## Sixième partie

# "Remote forensic"

Acquisition statique & dynamique

... à distance!



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



## Sixième partie

### Outil intéressant :

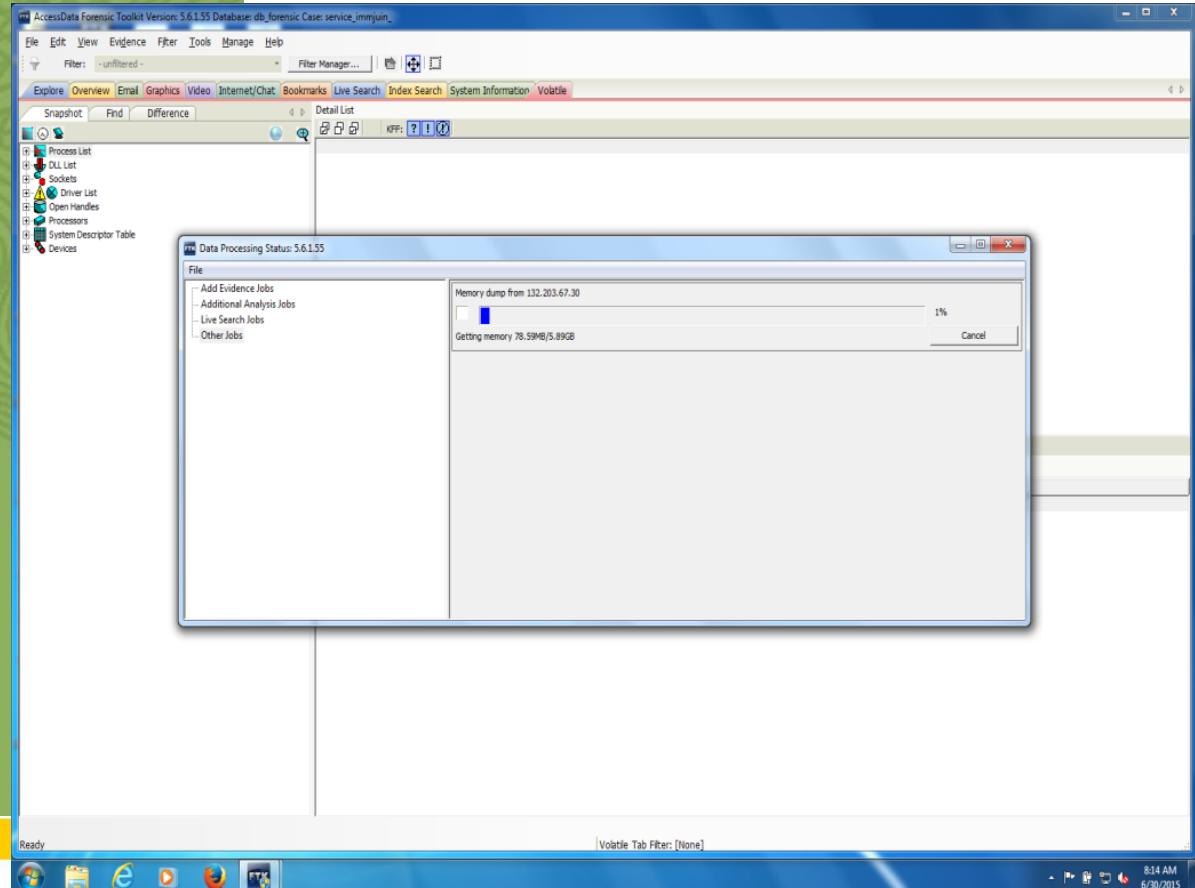
AccessData : FTKToolkit

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



Bureau de sécurité de l'information



## 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

The screenshot shows a Firefox browser window with the URL [7ba.ru/notknown](http://7ba.ru/notknown). The page is in Russian and features a dark background with green and white text. At the top, it says "Добрый вечер на 7ba.ru! 22:15". Below that, it says "7ba.Ru рекомендует Вам: Здравствуйте всем! => +Бесплатные Загрузки у нас+ Бесплатно Игры, Музыка, Фильмы IMP.mobi - Миллион приковов :)".

On the left, there's a sidebar with "Последние новости сайта" and a list of links:

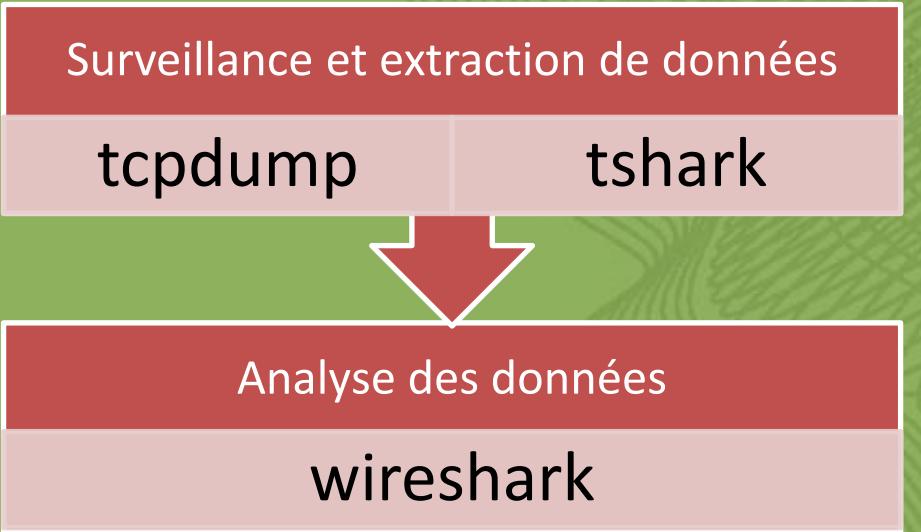
- 7 запрещающих Ремонт...
- Мнения(57) | Подробно »
- Чат(42)
- Форум(128)
- Онлайн игра Warcraft(215)
- Обменник(506388) ↗
- Фотогалерея(47506) ↗
- Блоги(42472) ↗
- Статьи/Советы(1102)
- Zona Java(2628)
- Zona Smartphone(24449) ↗
- Мобильные фильмы(9950) ↗
- Мобильные сериалы(2836)
- Видео архив(17626)
- Картинки(255261)
- Темы(174782)
- Другие архивы Эротики(124Gb)
- Us Browser 10
- Опера mini/Max/Coast
- SMS поздравления
- SMS Mobi
- IMP.mobi - Миллион приковов :)



Bureau de sécurité de l'information



## Sixième partie



# 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!!!!

Le rapport est extrêmement important pour l'enquêteur, mais aussi pour nous et aussi dans le 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.

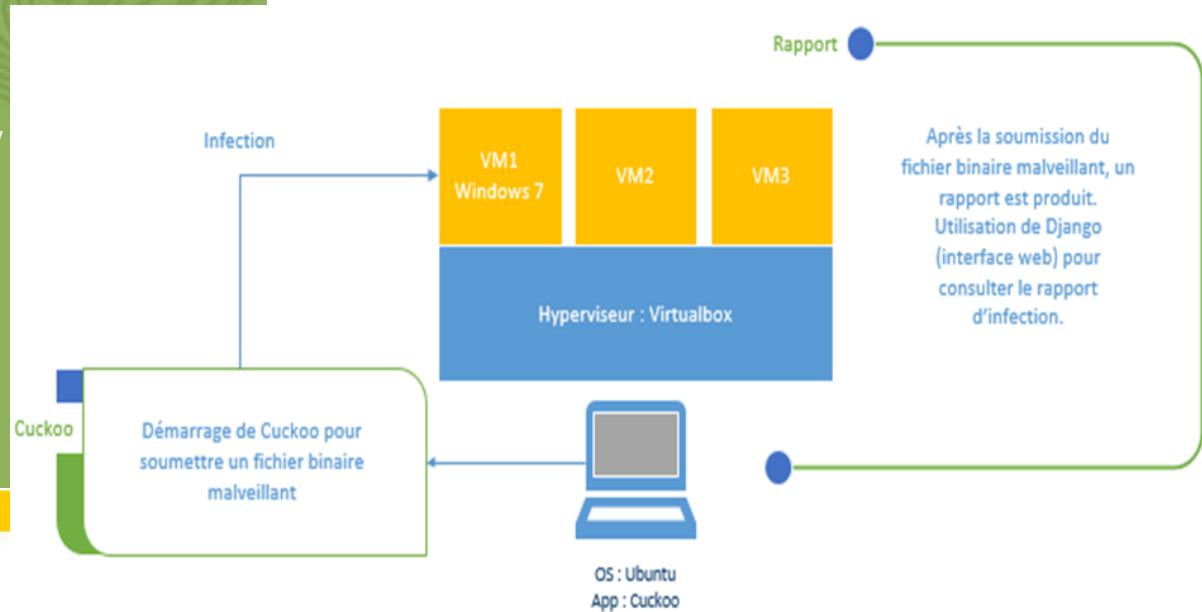
Outil : Cuckoo



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”



Bureau de sécurité de l'information



## Septième partie

### 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.



Bureau de sécurité de l'information



## Septième partie

### « 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”).



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



## 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”



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'info

Autopsy TSK

```
deftlinux-vm ~/evidence/sylvain % mmcls 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)
----	-------	------------	------------	-------------------------------

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	dir / in	\$FAT1	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	\$FAT2	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	\$MBR	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 / l	\$OrphanFiles/	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

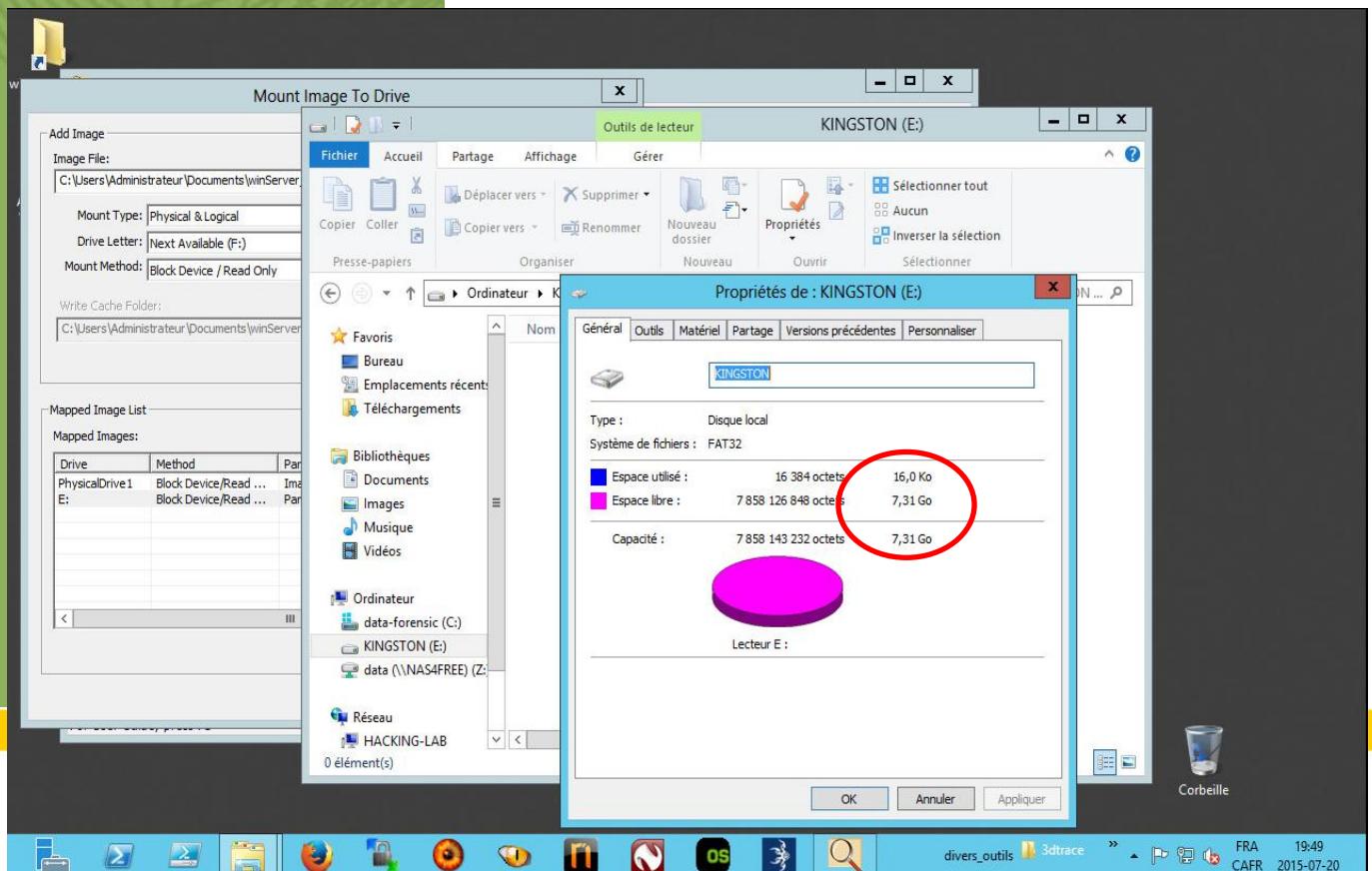


<http://forensicswiki.org/wiki/FAT>



## Septième partie

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



FTKImager



Bureau de sécurité de l'information



## Septième partie

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

# Espace non alloué

The screenshot shows the AccessData FTK Imager interface. On the left, the Evidence Tree pane shows a partition labeled 'navig.aff' containing a 'KINGSTON [FAT32]' volume. Within this volume, there is a '[root]' folder and a '[unallocated space]' folder. The '[unallocated space]' folder is circled in red. The main window, titled 'File List', displays several files with names starting with '000003', '006403', '012803', '019203', '025603', '032003', and '038403'. A red arrow points from the text 'Espace non alloué' to the circled '[unallocated space]' folder in the Evidence Tree.

AccessData FTK Imager 3.1.2.0

Evidence Tree

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...  
025603 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...

Bureau de s... d@ Bureau de s... A Bureau de s... sylvain Bureau de s... Export Results

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

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

NUM 23:03



## Septième partie

### Quoi faire avec les fichiers?

AccessData FTK Imager 3.1.2.0

Evidence Tree

File List

Name	Size	Type
000003	102 400	Unallocated Spa...
006403	102 400	Unallocated Spa...
012803	102 400	Unallocated Spa...
019203	102 400	Unallocated Spa...
025603	102 400	Unallocated Spa...
032003	102 400	Unallocated Spa...
038403	102 400	Unallocated Spa...

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



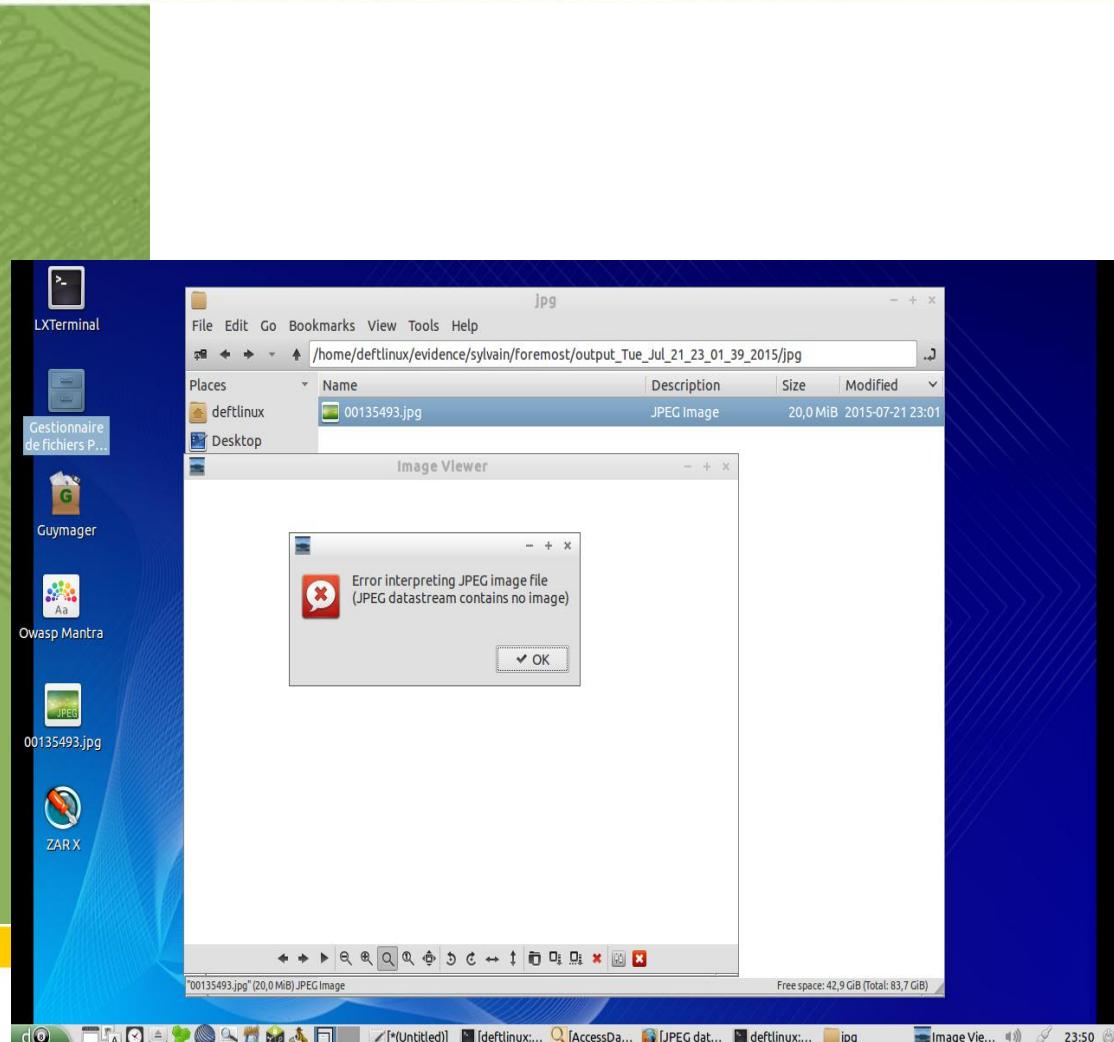
## Septième partie

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.
```

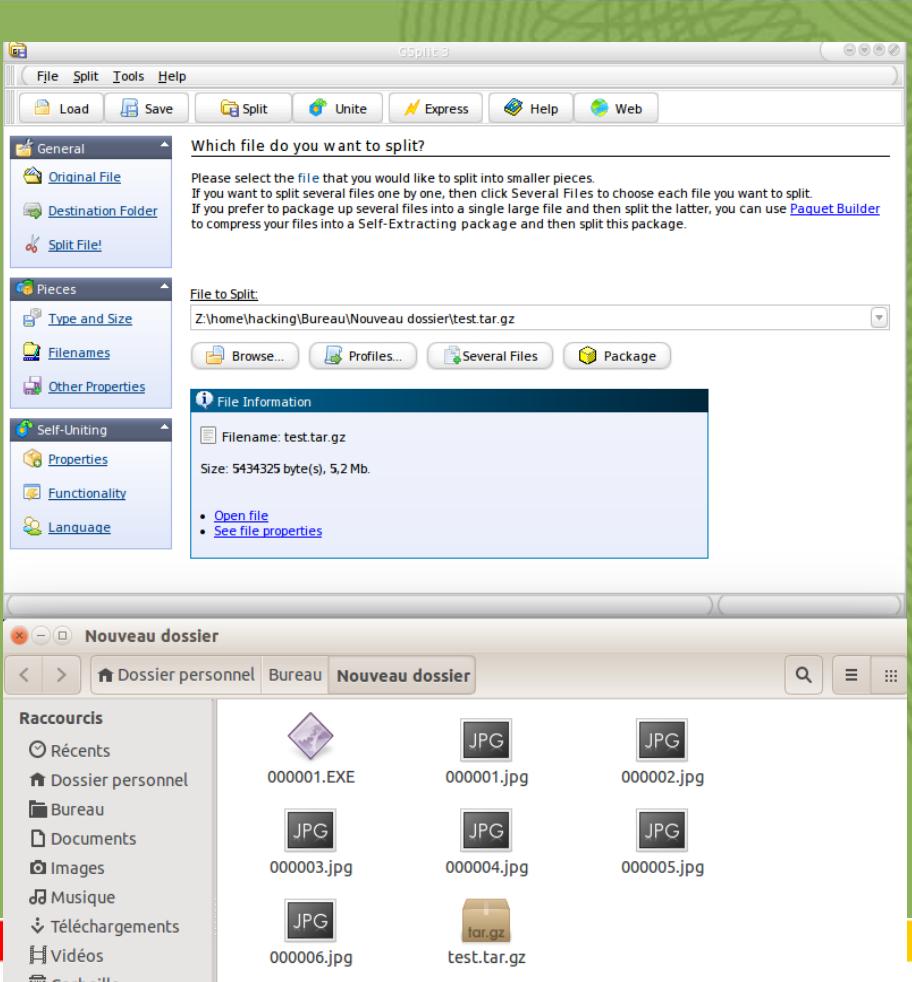
```
deftlinux-vm ~/Desktop % exif 00135493.jpg
Corrupt data
The data provided does not follow the specification.
ExifLoader: The data supplied does not seem to
contain EXIF data.
```



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.



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 ?



Bureau de sécurité de l'information



## Septième partie

### Utilitaires intéressants :

rsync  
bash script  
crontab  
tmux  
sandboxie  
keepnotes  
winmerge  
...

Tout au long de  
votre enquête...



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



# Septième partie

## Commandes Linux/Windows:

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



## 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



UNIVERSITÉ  
LAVAL

Bureau de sécurité de l'information



# 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

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