

squad



MIX YOUR  
**TALENT**

Étude de cas



## L'affaire Megacorp



1

## L'affaire Megacorp

27 Novembre 2018 : Mme Lecomte, PDG de Megacorp, une entreprise faisant du business consulting, passe une mauvaise journée. Tous ses directeurs-rices démissionnent, l'un-e après l'autre, déclinant ses contre-propositions salariales. C'est comme si le principal concurrent de Megacorp, UltraVenture, proposait des offres toujours au-dessus de celles de Megacorp.

Le seul endroit où sont écrits les propositions salariales et la marge associée est le fichier *leads.xlsx* stocké sur l'intranet de Megacorp. Il y a seulement 3 personnes qui ont accès à ce fichier : Mr Dupond, Mr Durand et la PDG elle-même.



1

## L'affaire Megacorp

Mr Dupond est le directeur adjoint. Il a rejoint Megacorp il y a plus de 10 ans. Il travaille dur pour négocier des contrats dans le monde entier. Durant son dernier voyage à Miami, il a gagné un contrat très lucratif qui permet à Megacorp d'être serein pour les 5 prochaines années.

Mr Durand est le nouveau directeur de l'IT. Il reporte directement ses KPI à Mr Dupond. Il a rejoint Megacorp récemment mais il a négocié pour déjà avoir des vacances ce mois-ci.

Mme Lecomte n'a pas confiance en Mr Durand. Elle pense qu'il est fainéant et qu'il devrait travailler plus au lieu de partir déjà en vacances. Elle a essayé sans succès de savoir ce qu'il avait prévu pour ses vacances, que ce soit en lui demandant à lui ou à ses collègues.





1

## L'affaire Megacorp

Mme Lecomte a sommé Mr Durand de lui dire ce qu'il a fait durant ses vacances mais il a persisté en disant que c'était sa vie privée. La coïncidence est trop grande et Mme Lecomte est persuadée que c'est lui le coupable. Elle voudrait le licencier et l'assigner en justice. Elle contacte votre entreprise afin d'effectuer une analyse pour tenter de comprendre ce qu'il s'est passé et avoir des preuves à produire en justice.

Evidemment, Mr Durand proclame son innocence, il n'avait pas accès à l'intranet pendant ses vacances, car il avait laissé son ordinateur portable dans l'entreprise. Cet argument est réfuté par Mr Martin, le technicien de surface, qui nettoie le bureau chaque jour. Il n'a pas vu d'ordinateur durant cette période dans le bureau de Mr Durand.

Vous êtes l'expert-e inforensique devant traiter cette affaire.



## L'affaire Megacorp

### Le matériel

Le matériel saisi :

- L'ordinateur portable de Mr Durand
  - Un disque dur de 32 Go
  - 8 Go de RAM
  - L'ordinateur est éteint
- La clé USB pro de Mr Durand
  - 4 Go

Ni la clé USB, ni le disque dur sont chiffrés.



## L'affaire Megacorp

Ce que nous savons

L'existence du fichier *leads.x/sx* sur le site de l'intranet <https://intranet.megacorp.com>

- La sauvegarde de l'intranet est chiffrée
- La configuration des logs est mauvaise et aucune trace intéressante est récupérable à ce niveau-là

D'après l'enchaînement des événements, si le fichier Excel a été volé et vendu au concurrent UltraVenture, ça a dû se passer entre le 10 et le 20 novembre 2018

- Mr Dupond n'a été informé d'aucun signalement suspect durant cette période
- Mr Durand était en vacances



## L'affaire Megacorp

### L'acquisition

Malheureusement le disque dur est soudé à l'ordinateur portable. Le retirer est compliqué et pourrait endommager les preuves.

- L'acquisition est effectuée avec une clé USB *bootable* contenant une distribution Linux Kali
- Le disque dur n'est pas monté une fois que la distribution a démarré
- La copie du disque dur est effectuée bit à bit avec dd :
  - `dd if=/dev/sda1 of=partition2_28G.img conv=noerror,sync bs=4k`

La copie et l'ordinateur portable sont stockés en lieu sûr et on travaille sur une copie de la copie.





## L'affaire Megacorp

### Montage de l'image disque

L'analyse inforensique est effectuée sur une distribution Linux Kali

- De nombreux outils open-source sont disponibles

L'image disque est montée dans /mnt/partition2 en mode lecture seule afin de ne pas altérer l'image disque

Le disque peut à présent être parcouru manuellement comme si c'était un périphérique normal de votre ordinateur

```
root@kali:~/Documents# mkdir /mnt/partition2
root@kali:~/Documents# mount -t ntfs -o loop,ro,noexec partition2_28G.img /mnt/partition2/
root@kali:~/Documents# cd /mnt/partition2/
root@kali:/mnt/partition2# ls -la
total 3636173
drwxrwxrwx 1 root root      8192 nov.  7 04:28 .
drwxr-xr-x 3 root root      4096 nov. 16 10:35 ..
-rwxrwxrwx 1 root root 389408 nov. 20 2016 bootmgr
-rwxrwxrwx 1 root root      1 juil. 16 2016 BOOTNXT
lrwxrwxrwx 2 root root      21 nov.  7 04:10 'Documents and Settings' -> /mnt/partition2/
-rwxrwxrwx 1 root root 1692942336 nov. 14 06:54 hiberfil.sys
drwxrwxrwx 1 root root      0 nov.  7 04:21 MSOCache
-rwxrwxrwx 1 root root 2013265920 nov.  7 05:22 pagefile.sys
drwxrwxrwx 1 root root      0 juil. 16 2016 PerfLogs
drwxrwxrwx 1 root root      4096 nov.  7 04:21 ProgramData
drwxrwxrwx 1 root root      4096 nov.  7 04:22 'Program Files'
drwxrwxrwx 1 root root      4096 nov.  7 04:22 'Program Files (x86)'
drwxrwxrwx 1 root root      0 nov.  7 04:10 Recovery
drwxrwxrwx 1 root root      0 nov. 14 05:27 $Recycle.Bin
-rwxrwxrwx 1 root root 16777216 nov.  7 05:22 swapfile.sys
drwxrwxrwx 1 root root      4096 nov.  7 04:28 'System Volume Information'
drwxrwxrwx 1 root root      4096 nov.  7 04:12 Users
drwxrwxrwx 1 root root      28672 nov.  7 05:26 windows
root@kali:/mnt/partition2#
```

# 1

## L'affaire Megacorp Les premières constatations simples

Le répertoire personnel de Mr Durand ne contient pas le fichier *leads.xlsx*

La taille de *C:\$recycle-bin* est de 0 octet, la corbeille est donc vide

Note : utiliser la commande *find* permet de gagner du temps.

```
root@kali:/mnt/partition2/Users/MDurand# ls -la Desktop/
total 9
drwxrwxrwx 1 root root  0 nov.  7 04:12
drwxrwxrwx 1 root root 8192 nov. 14 05:27
-rwxrwxrwx 1 root root 282 nov.  7 04:12 desktop.ini
root@kali:/mnt/partition2/Users/MDurand# ls -la Documents/
total 13
drwxrwxrwx 1 root root 4096 nov. 14 07:04
drwxrwxrwx 1 root root 8192 nov. 14 05:27
-rwxrwxrwx 1 root root 402 nov.  7 04:12 desktop.ini
lrwxrwxrwx 2 root root  35 nov.  7 04:12 'Ma musique' -> /mnt/
lrwxrwxrwx 2 root root  38 nov.  7 04:12 'Mes images' -> /mnt/
lrwxrwxrwx 2 root root  36 nov.  7 04:12 'Mes vidéos' -> /mnt/
root@kali:/mnt/partition2/Users/MDurand# ls -la Downloads/
total 9
drwxrwxrwx 1 root root  0 nov.  7 04:12
drwxrwxrwx 1 root root 8192 nov. 14 05:27
-rwxrwxrwx 1 root root 282 nov.  7 04:12 desktop.ini
root@kali:/mnt/partition2/Users/MDurand# ls -la Pictures/
total 13
drwxrwxrwx 1 root root 4096 nov. 14 07:04
drwxrwxrwx 1 root root 8192 nov. 14 05:27
drwxrwxrwx 1 root root  0 nov.  7 04:13 Camera Roll
-rwxrwxrwx 1 root root 504 nov.  7 04:12 desktop.ini
drwxrwxrwx 1 root root  0 nov.  7 04:13 Saved Pictures
root@kali:/mnt/partition2/Users/MDurand# ls -la Videos/
total 9
drwxrwxrwx 1 root root  0 nov.  7 04:12
drwxrwxrwx 1 root root 8192 nov. 14 05:27
-rwxrwxrwx 1 root root 504 nov.  7 04:12 desktop.ini
root@kali:/mnt/partition2/Users/MDurand#
```



## L'affaire Megacorp

Le fichier leads.xlsx étant absent, c'est un *failed* ?

2 hypothèses :

- Le fichier n'a jamais été sur l'ordinateur portable => Mr Durand est innocent
- Le fichier a été effacé et la corbeille vidée => Mr Durand a supprimé ses traces

Il y a plusieurs façons de restaurer un fichier effacé :

- Explorer la MFT
- Faire une recherche avec la méthode de *file carving*.
- Pour les images uniquement : regarder dans « Thumbs.db » ou « Thumbcache »

Il y a plusieurs façons de trouver des traces d'utilisation de fichiers

- Regarder dans Internet Explorer le fichier « Index.dat » (« Webcache » pour Edge)
- Regarder dans la base de registre pour le MRU (Most Recently Used)
- Faire un *grep* sur le nom de fichier...

1

## L'affaire Megacorp

### Recherche du fichier avec le MFT

Laissons Autopsy faire le boulot. Il trouve 2 fichiers existant et 2 fichiers supprimés :

- 3 des fichiers sont des liens *leads.lnk*
- 1 fichier semble lié à Microsoft Edge

Directory Seek

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

VIEW

File Name Search

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

leads

SEARCH

FILE ANALYSIS

KEYWORD SEARCH

FILE TYPE

IMAGE DETAILS

META DATA

DATA UNIT

HELP

CLOSE

All files with 'leads' in the name

SHOW ALL FILES

Error Parsing File (invalid characters?)  
: V/V 115200: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
✓	r / -	C:/Users/MDurand/AppData/Local/Packages/MicrosoftEdge_8wekyb3d8bbwe/AC/#1001/MicrosoftEdge/Cache/7H8WTJVO/leads[1].xlsx	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	0
	r / r	C:/Users/MDurand/AppData/Roaming/Microsoft/Office/Recent/leads.LNK	2018-11-14 07:03:22 (EST)	2018-11-14 07:03:22 (EST)	2018-11-14 07:03:22 (EST)	2018-11-14 07:03:22 (EST)	295	0	0	113975-128-1
	r / r	C:/Users/MDurand/AppData/Roaming/Microsoft/Windows/Recent/leads.lnk	2018-11-14 07:03:22 (EST)	2018-11-14 07:03:22 (EST)	2018-11-14 07:03:22 (EST)	2018-11-14 07:00:32 (EST)	343	0	0	113878-128-1
✓	- / r	C:/Users/MDurand/AppData/Roaming/Microsoft/Windows/Recent/leads.lnk	2018-11-14 07:00:32 (EST)	2018-11-14 07:00:32 (EST)	2018-11-14 07:00:32 (EST)	2018-11-14 07:00:32 (EST)	430	0	0	114839-128-1

File Browsing Mode



## L'affaire Megacorp

Récupération du fichier effacé avec la méthode de file carving

FTKImager, Foremost, Photorec... ne donnent rien d'intéressant

```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk partition2_28G.img - 30 GB / 28 GiB (R0)
  Partition          Start      End    Size in sectors
  P NTFS              0    0 1 3760 184 8 60416000

28 files saved in /root/Documents/photorec_found/recup_dir directory.
Recovery aborted by the user.
```

```
root@kali:~/Documents/photorec_found/recup_dir.1# ls -lah
total 3,0G
drwxr-xr-x 2 root root 4,0K nov. 16 14:01 .
drwxr-xr-x 3 root root 4,0K nov. 16 11:37 ..
-rw-r--r-- 1 root root 104K mars 20 2010 f0384480.docx
-rw-r--r-- 1 root root 165K mars 20 2010 f0390632.docx
-rw-r--r-- 1 root root 167K mars 20 2010 f0390968.docx
-rw-r--r-- 1 root root 199K mars 20 2010 f0391304.docx
-rw-r--r-- 1 root root 179K mars 20 2010 f0391704.docx
-rw-r--r-- 1 root root 8,4K oct. 5 2006 f0392432.docx
-rw-r--r-- 1 root root 8,6K oct. 5 2006 f0392456_word.zip
-rw-r--r-- 1 root root 8,6K oct. 5 2006 f0392480_word.zip
-rw-r--r-- 1 root root 8,4K oct. 5 2006 f0392504_word.zip
-rw-r--r-- 1 root root 8,3K oct. 5 2006 f0392528_docProps.zip
-rw-r--r-- 1 root root 24K oct. 27 2009 f0392552.docx
-rw-r--r-- 1 root root 146K mars 20 2010 f0470072.docx
-rw-r--r-- 1 root root 83K mars 20 2010 f0470368.docx
-rw-r--r-- 1 root root 118K mars 20 2010 f0470536.docx
-rw-r--r-- 1 root root 128K mars 20 2010 f0472840.docx
-rw-r--r-- 1 root root 118K mars 20 2010 f0536272.docx
-rw-r--r-- 1 root root 170K mars 20 2010 f0536616.docx
-rw-r--r-- 1 root root 172K mars 20 2010 f0541432.docx
-rw-r--r-- 1 root root 3,4M mars 20 2010 f0548336.docx
-rw-r--r-- 1 root root 3,0G nov. 16 14:01 f0602400.docx
```



## L'affaire Megacorp

Case closed?

Nous avons trouvé plusieurs indices indiquant qu'un fichier « leads » a interagi avec le système, donc Mr Durand est coupable non ?

Les preuves ne sont pas convaincantes :

- « Leads » ou « leads.xlsx » pourraient être des noms de fichier contenant autre chose...
- Ces traces pourraient être liées à quelque chose de totalement différent créé ou accédé des semaines avant.
- « leads.lnk » n'est pas « leads.xlsx »

Nous avons besoin de retracer l'historique de ces traces. D'où viennent-elles ? Quelle utilisation de ce fichier a produit ces traces ?





## L'affaire Megacorp Grep

Il y a un lien vers « leads.xlsx » dans un fichier .htm accédé à travers le navigateur Microsoft Edge.

```
root@kali:/mnt/partition2# grep -rn -iI leads > /root/Documents/greps_l
grep: Windows/Logs/CBS/CBS.log: Erreur d'entrée/sortie
grep: Windows/security/logs/scecomp.log: Erreur d'entrée/sortie
grep: Windows/SoftwareDistribution/DeliveryOptimization: Erreur d'entré
grep: Windows/SoftwareDistribution/Download: Erreur d'entrée/sortie
grep: Windows/System32/catroot2: Erreur d'entrée/sortie
grep: Windows/System32/DriverStore: Erreur d'entrée/sortie
grep: Windows/System32/eld65x64.din: Erreur d'entrée/sortie
grep: Windows/System32/eldmsg.dll: Erreur d'entrée/sortie
grep: Windows/System32/ibtproppage.dll: Erreur d'entrée/sortie
grep: Windows/System32/ibtsiva.exe: Erreur d'entrée/sortie
grep: Windows/System32/NicCo4.dll: Erreur d'entrée/sortie
grep: Windows/System32/NicInstD.dll: Erreur d'entrée/sortie
root@kali:/mnt/partition2# grep -rn -iI leads.xlsx > /root/Documents/gr
grep: Windows/Logs/CBS/CBS.log: Erreur d'entrée/sortie
grep: Windows/security/logs/scecomp.log: Erreur d'entrée/sortie
grep: Windows/SoftwareDistribution/DeliveryOptimization: Erreur d'entré
grep: Windows/SoftwareDistribution/Download: Erreur d'entrée/sortie
grep: Windows/System32/catroot2: Erreur d'entrée/sortie
grep: Windows/System32/DriverStore: Erreur d'entrée/sortie
grep: Windows/System32/eld65x64.din: Erreur d'entrée/sortie
grep: Windows/System32/eldmsg.dll: Erreur d'entrée/sortie
grep: Windows/System32/ibtproppage.dll: Erreur d'entrée/sortie
grep: Windows/System32/ibtsiva.exe: Erreur d'entrée/sortie
```

```
dependencies are not supported. Option WISPHidden has a lead WISPHFiles which also has 1 leads.
Users/MDurand/AppData/Roaming/Microsoft/Office/Recent/index.dat:2:leads.LNK=0
Users/MDurand/AppData/Roaming/Microsoft/Office/Recent/index.dat:4:leads.LNK=0
root@kali:~/Documents# tail greps_leads.xlsx.txt
Users/MDurand/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/AC/#!001/MicrosoftEdge/Cache/K
BF1L6EK/R0C60JI4.htm:174:      <li><a href="leads.xlsx">Leads</a></li>
root@kali:~/Documents#
```



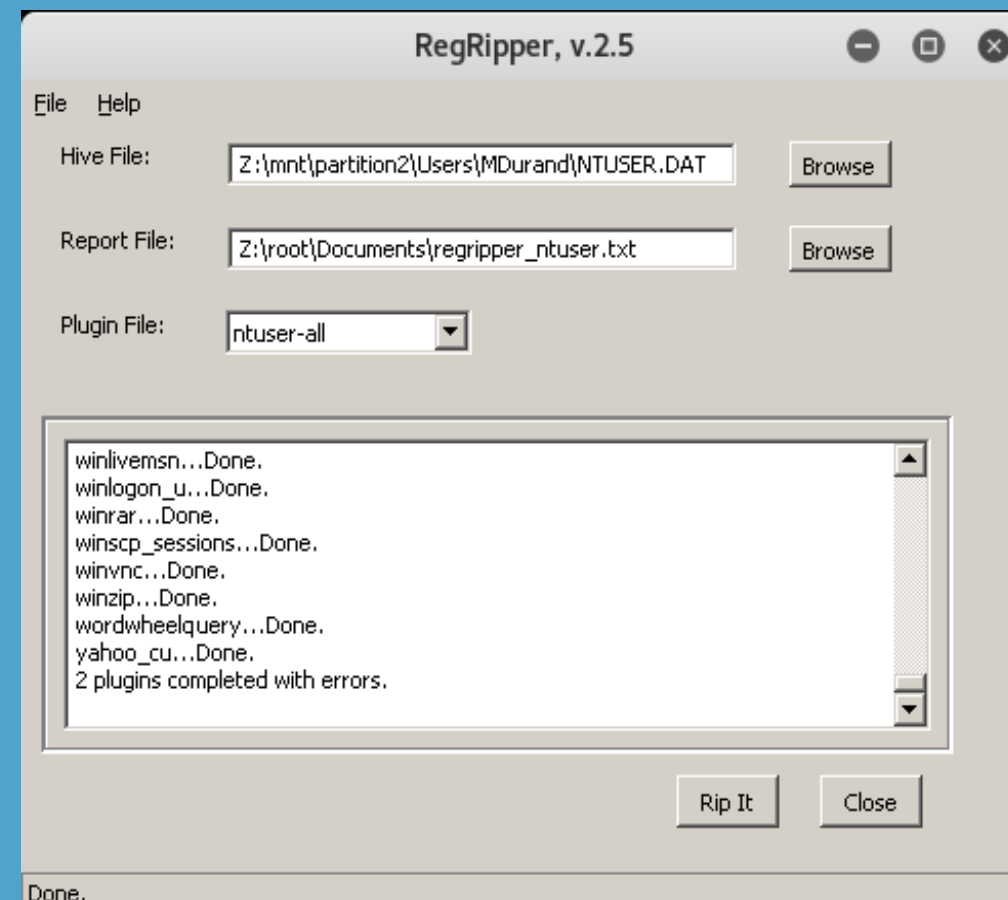
## L'affaire Megacorp

### MRU (Most recently used)

Les listes MRU sont les listes des fichiers utilisés récemment. C'est utilisé par Windows pour suggérer des fichiers à ouvrir.

Les listes MRU sont stockés dans la ruche NTUSER.DAT, il y en a une par utilisateur du système.

Plusieurs outils peuvent être utilisés pour explorer le registre de Windows. RegRipper est l'un des plus connus.





## L'affaire Megacorp

### MRU (Most recently used)

```
-----
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Wed Nov 14 12:03:22 2018 (UTC)
 6 = DURAND_USB (D:)
 3 = Leads.xlsx
 4 = technical_plan.png
 5 = Images
 1 = Internet
 2 = intranet.megacorp.com/
 0 = lemonde.fr/

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.com/
LastWrite Time Wed Nov 14 12:00:04 2018 (UTC)
MRUListEx = 0
 0 = intranet.megacorp.com/

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.fr/
LastWrite Time Wed Nov 14 11:58:09 2018 (UTC)
MRUListEx = 0
 0 = lemonde.fr/

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.png
LastWrite Time Wed Nov 14 12:02:38 2018 (UTC)
MRUListEx = 0
 0 = technical_plan.png

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.xlsx
LastWrite Time Wed Nov 14 12:03:22 2018 (UTC)
MRUListEx = 0
 0 = Leads.xlsx

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
LastWrite Time Wed Nov 14 12:03:22 2018 (UTC)
MRUListEx = 2,1,0
 2 = DURAND_USB (D:)
 1 = Images
 0 = Internet
```

Les preuves trouvées permettent de confirmer qu'un fichier leads.xlsx a été ouvert dans Excel le mercredi 14 novembre 2018 à 12:03:22.

```
-----
officedocs2010 v.2011090
(NTUSER.DAT) Gets user's Office 2010 doc MRU values

MSOffice version 2010 located.
Software\Microsoft\Office\14.0\Word\File MRU not found.

Software\Microsoft\Office\14.0\Excel\File MRU
LastWrite Time Wed Nov 14 12:03:22 2018 (UTC)
  Item 1 -> D:\Leads.xlsx Wed Nov 14 12:03:22 2018

Software\Microsoft\Office\14.0\Access\File MRU not found.

Software\Microsoft\Office\14.0\PowerPoint\File MRU not found.
```



## L'affaire Megacorp

### Le cache de Microsoft Edge

```
C:\Windows\System32>esentutl.exe /mh C:\VM SHARE\WebCacheV01.dat

Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 10.0
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating FILE DUMP mode...
    Database: C:\VM SHARE\WebCacheV01.dat

DATABASE HEADER:
Checksum Information:
Expected Checksum: 0xfe8ffd08
    Actual Checksum: 0xfe8ffd08

Fields:
    File Type: Database
    Checksum: 0xfe8ffd08
    Format ulMagic: 0x89abcdef
    Engine ulMagic: 0x89abcdef
    Format ulVersion: 0x620,20,0 (attached by 0)
    Engine ulVersion: 0x620,30,40 (efvCurrent = 8960)
    Created ulVersion: 0x620,20
    DB Signature: Create time:11/07/2018 10:12:13.824 Rand:200021590 Computer:
    cbDbPage: 32768
    dbtime: 1537 (0x601)
    State: Dirty Shutdown
    Log Required: 18-27 (0x12-0x1b)
    Log Committed: 0-27 (0x0-0x1b)
    Log Recovering: 0 (0x0)
    Log Consistent: 27 (0x1b)
    GenMax Creation: 11/14/2018 12:59:05.460
    Shadowed: Yes
    Last Objid: 28
    Scrub Dbtime: 0 (0x0)
```

Le navigateur Microsoft Edge stocke la plupart de la navigation Internet dans une base de données contenu dans le fichier *WebCacheV01.dat*. Cette base de données contient les cookies, les fichiers en cache, les téléchargements et les sites web visités.

Il y a plusieurs outils pour explorer cela, ESEDatabaseView est l'un d'eux (disponible uniquement sur Windows).

Dans un premier temps, nous devons nous assurer que la base de données n'est pas corrompue par un arrêt brutal de Windows.



## L'affaire Megacorp

### Le cache de Microsoft Edge

Si besoin, l'outil peut la réparer :

```
C:\VM SHARE\WebCache>esentutl.exe /r V01 /d

Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 10.0
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating RECOVERY mode...
  Logfile base name: V01
    Log files: <current directory>
    System files: <current directory>
    Database Directory: <current directory>

Performing soft recovery...
      Restore Status (% complete)

    0    10    20    30    40    50    60    70    80    90   100
  |----|----|----|----|----|----|----|----|----|----|
  .....

Operation completed successfully in 1.187 seconds.
```

```
C:\VM SHARE\WebCache>esentutl.exe /mh WebCacheV01.dat
```

```
Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 10.0
Copyright (C) Microsoft Corporation. All Rights Reserved.
```

```
Initiating FILE DUMP mode...
  Database: WebCacheV01.dat
```

```
DATABASE HEADER:
```

```
Checksum Information:
```

```
Expected Checksum: 0x3c54ce69
Actual Checksum: 0x3c54ce69
```

```
Fields:
```

```
  File Type: Database
  Checksum: 0x3c54ce69
  Format ulMagic: 0x89abcdef
  Engine ulMagic: 0x89abcdef
  Format ulVersion: 0x620,20,0 (attached by 0)
  Engine ulVersion: 0x620,30,40 (efvCurrent = 8960)
  Created ulVersion: 0x620,20
  DB Signature: Create time:11/07/2018 10:12:13.824 Rand:200021590 Computer:
  cbDbPage: 32768
  dbtime: 76104 (0x12948)
  State: Clean Shutdown
  Log Required: 0-0 (0x0-0x0)
  Log Committed: 0-0 (0x0-0x0)
  Log Recovering: 0 (0x0)
  Log Consistent: 0 (0x0)
  GenMax Creation: 00/00/1900 00:00:00.000
  Shadowed: Yes
  Last Objid: 83
  Scrub Dbtime: 0 (0x0)
```

1

## L'affaire Megacorp

### Le cache de Microsoft Edge

IECacheView: C:\VMSHARE\WebCache

File Edit View Options Help

Filename	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hits
R0C6OJI4.htm	text/html	http://intranet.megacorp.com/	14/11/2018 13:00:04	16/11/2018 12:31:03	N/A	N/A	1
megacorp_bann...	image/png	http://intranet.megacorp.com/megacorp_banner.png	14/11/2018 13:00:05	14/11/2018 10:06:51	N/A	N/A	1
technical_plan[1...	image/png	http://intranet.megacorp.com/technical_plan.png	14/11/2018 13:00:58	16/11/2018 12:20:13	N/A	N/A	2

ExpiryTime	ModifiedTime	AccessedTime	PostCheckTime	SyncCount	ExemptionDelta	Url	Filename	FileExtension	RequestHeader
10/12/2018 12:58:09	14/11/2018 12:58:09	14/11/2018 12:58:09	0	06/05/1829 01:50:03	0	Visited: MDurand@http://lemonde.fr/			
10/12/2018 13:00:04	14/11/2018 13:00:04	14/11/2018 13:00:04	0	06/05/1829 01:50:03	0	Visited: MDurand@microsoft-edge:http://intranet.megacorp.com/			
10/12/2018 13:00:32	14/11/2018 13:00:32	14/11/2018 13:00:32	0	06/05/1829 01:50:03	0	06/05/1829 01:50:03			
10/12/2018 12:54:00	14/11/2018 13:01:09	14/11/2018 13:01:09	0	06/05/1829 01:50:03	0	Visited: MDurand@file:///C:/Users/MDurand/Pictures/technical_plan.png			
10/12/2018 12:55:28	14/11/2018 13:02:38	14/11/2018 13:02:38	0	06/05/1829 01:50:03	0	Visited: MDurand@file:///D:/technical_plan.png			

Le fichier .htm était bien celui de l'Intranet accédé avec le compte *MDurand*

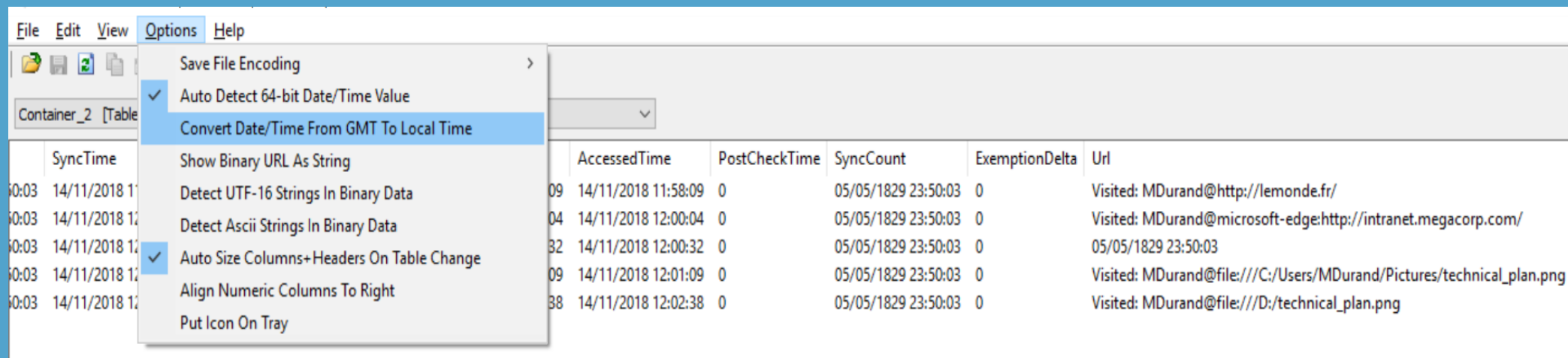




## L'affaire Megacorp

Case closed?

- Mr Durand a été sur l'Intranet le 14/11/2018 à 13:00:04
- Le fichier leads.xlsx a été ouvert dans Excel le 14/11/2018 à 12:03:22
- Le fichier a été ouvert avant d'être téléchargé sur l'intranet ?!? Ah non, c'est juste qu'il faut faire attention car Windows utilise parfois le GMT, l'UTC ou l'heure local... C'était 12:00:04



The screenshot shows the 'Options' menu in Excel. The 'Convert Date/Time From GMT To Local Time' option is selected. The background shows a table with columns: SyncTime, AccessedTime, PostCheckTime, SyncCount, ExemptionDelta, and Url.

SyncTime	AccessedTime	PostCheckTime	SyncCount	ExemptionDelta	Url
14/11/2018 11:58:09	14/11/2018 11:58:09	0	05/05/1829 23:50:03	0	Visited: MDurand@http://lemonde.fr/
14/11/2018 12:00:04	14/11/2018 12:00:04	0	05/05/1829 23:50:03	0	Visited: MDurand@microsoft-edge:http://intranet.megacorp.com/
14/11/2018 12:00:32	14/11/2018 12:00:32	0	05/05/1829 23:50:03	0	05/05/1829 23:50:03
14/11/2018 12:01:09	14/11/2018 12:01:09	0	05/05/1829 23:50:03	0	Visited: MDurand@file:///C:/Users/MDurand/Pictures/technical_plan.png
14/11/2018 12:02:38	14/11/2018 12:02:38	0	05/05/1829 23:50:03	0	Visited: MDurand@file:///D:/technical_plan.png



## L'affaire Megacorp

Case closed?

N'avez-vous pas remarqué un autre élément qui donne envie de creuser ?

?



## L'affaire Megacorp

Un vol peut en cacher un autre

N'avez-vous pas remarqué un autre élément qui donne envie de creuser ?

```
-----
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Wed Nov 14 12:03:22 2018 (UTC)
 6 = DURAND_USB (D:)
 3 = lead.xlsx
 4 = technical_plan.png
 5 = Images
 1 = Internet
 2 = intranet.megacorp.com/
 0 = lemonde.fr/

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.com/
LastWrite Time Wed Nov 14 12:00:04 2018 (UTC)
MRUListEx = 0
 0 = intranet.megacorp.com/

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.fr/
LastWrite Time Wed Nov 14 11:58:09 2018 (UTC)
MRUListEx = 0
 0 = lemonde.fr/

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.png
LastWrite Time Wed Nov 14 12:02:38 2018 (UTC)
MRUListEx = 0
 0 = technical_plan.png
```

IECacheView: C:\VMSHARE\WebCache

Filename	Content Type	URL	Last Accessed
R0C6OJ4.htm	text/html	http://intranet.megacorp.com/	14/11/2018 13:00:04
megacorp_bann...	image/png	http://intranet.megacorp.com/megacorp_banner.png	14/11/2018 13:00:05
technical_plan[1...	image/png	http://intranet.megacorp.com/technical_plan.png	14/11/2018 13:00:58

	AccessedTime	PostCheckTime	SyncCount	ExemptionDelta	Url
9	14/11/2018 12:58:09	0	06/05/1829 01:50:03	0	Visited: MDurand@http://lemonde.fr/
4	14/11/2018 13:00:04	0	06/05/1829 01:50:03	0	Visited: MDurand@microsoft-edge:http://intranet.megacorp.com/
2	14/11/2018 13:00:32	0	06/05/1829 01:50:03	0	06/05/1829 01:50:03
9	14/11/2018 13:01:09	0	06/05/1829 01:50:03	0	Visited: MDurand@file:///C:/Users/MDurand/Pictures/technical_plan.png
8	14/11/2018 13:02:38	0	06/05/1829 01:50:03	0	Visited: MDurand@file:///D:/technical_plan.png

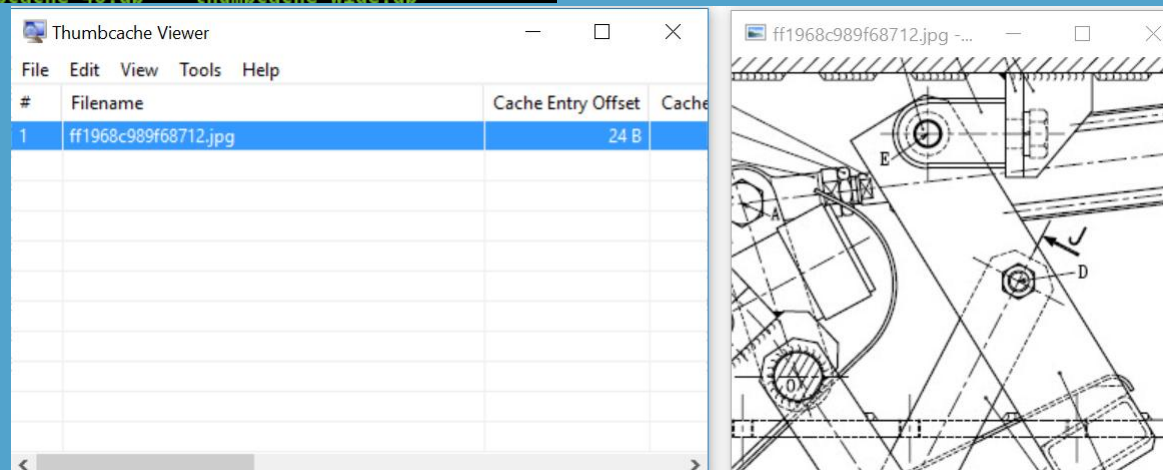
Il semble que Mr Durand s'est intéressé également au fichier *technical\_plan.png*



## L'affaire Megacorp Technical Plan

On peut récupérer une image effacée avec les *thumbnails* de Windows. Ici avec l'outil Thumbcache Viewer :

```
root@kali:/mnt/partition2/Users/MDurand/AppData/Local/Microsoft/Windows/Explorer# ls
ExplorerStartupLog.etl  iconcache_768.db  iconcache_1280.db  iconcache_16.db  iconcache_1920.db  iconcache_2560.db  iconcache_256.db  iconcache_32.db  iconcache_48.db
                        iconcache_96.db  thumbcache_1280.db  thumbcache_16.db  thumbcache_1920.db  thumbcache_2560.db  thumbcache_256.db  thumbcache_32.db  thumbcache_48.db
                        iconcache_custom_stream.db  thumbcache_custom_stream.db  thumbcache_exif.db  thumbcache_idx.db  thumbcache_sr.db  thumbcache_wide_alternate.db  thumbcache_wide.db
```





## L'affaire Megacorp

### Le volume D:

Le volume D: était-il celui qui a permis l'exfiltration de données ?

PostCheckTime	SyncCount	ExemptionDelta	Url
0	06/05/1829 01:50:03	0	Visited: MDurand@http://lemonde.fr/
0	06/05/1829 01:50:03	0	Visited: MDurand@microsoft-edge:http://intranet.megacorp.com/
0	06/05/1829 01:50:03	0	06/05/1829 01:50:03
0	06/05/1829 01:50:03	0	Visited: MDurand@file:///C:/Users/MDurand/Pictures/technical_plan.png
0	06/05/1829 01:50:03	0	Visited: MDurand@file:///D:/technical_plan.png

```
-----
officedocs2010 v.2011090
(NTUSER.DAT) Gets user's Office 2010 doc MRU values

MSOffice version 2010 located.
Software\Microsoft\Office\14.0\Word\File MRU not found.

Software\Microsoft\Office\14.0\Excel\File MRU
LastWrite Time Wed Nov 14 12:03:22 2018 (UTC)
  Item 1 -> D:\Lead.xls Wed Nov 14 12:03:22 2018

Software\Microsoft\Office\14.0\Access\File MRU not found.

Software\Microsoft\Office\14.0\PowerPoint\File MRU not found.
```

```
-----
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Wed Nov 14 12:03:22 2018 (UTC)
  6 = DURAND_USB (D:)
  3 = Lead.xls
  4 = technical_plan.png
  5 = Images
  1 = Internet
  2 = intranet.megacorp.com/
  0 = lemonde.fr/

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.com/
LastWrite Time Wed Nov 14 12:00:04 2018 (UTC)
MRUListEx = 0
  0 = intranet.megacorp.com/

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.fr/
LastWrite Time Wed Nov 14 11:58:09 2018 (UTC)
MRUListEx = 0
  0 = lemonde.fr/

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.png
LastWrite Time Wed Nov 14 12:02:38 2018 (UTC)
MRUListEx = 0
  0 = technical_plan.png

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.xlsx
LastWrite Time Wed Nov 14 12:03:22 2018 (UTC)
MRUListEx = 0
  0 = Lead.xls

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
LastWrite Time Wed Nov 14 12:03:22 2018 (UTC)
MRUListEx = 2,1,0
  2 = DURAND_USB (D:)
  1 = Images
  0 = Internet
```

1

## L'affaire Megacorp

Le volume D:

Les fichiers *.lnk* sont créés quand une application ouvre un fichier. Ils peuvent contenir le *path* du fichier ouvert.

```
ppData/Roaming/Microsoft/Windows/Recent# ls
AutomaticDestinations  http--lemonde.fr-.lnk  microsoft-edgehttp--intranet.megacorp.com-.lnk
CustomDestinations    Images.lnk             technical_plan.lnk
desktop.ini           Internet.lnk
'DURAND_USB (D).lnk'  leads.lnk
root@kali:/mnt/partition2/Users/MDurand/AppData/Roaming/Microsoft/Windows/Recent# cat leads.lnk
L[0][0][0][0]F[0] `00[0][0][0][0]00[0][0]{0[0][0][0]0[0]0[0].0[0]U[0][0]0[0]0[0]D:\t[0][0]^000H0g[0][0]00(0w,00/[0][0]>V
h00`2 .nM[0][0] LEADS~1.XLSF
00nMg`mM0.[0][0]leads.xlsx[0][0][0][0]E[0][0];0[0][0]DURAND_USBD:\leads.xlsx[0][0]:\root@kali:/mnt/partition2/Users/MDurand/A
ppData/Roaming/Microsoft/Windows/Recent#
```

En effet le fichier leads.xlsx a été ouvert depuis la clé USB DURAND\_USB





## L'affaire Megacorp

### Le volume D:

```
-----  
usbdevices v.20120522  
(System) Parses Enum\USB key for devices
```

```
VID_152D&PID_2339  
LastWrite: Wed Nov  7 09:16:24 2018  
SN      : 866BD800EDFF  
LastWrite: Wed Nov  7 09:16:25 2018
```

```
VID_FFFF&PID_5678  
LastWrite: Wed Nov  7 10:25:30 2018  
SN      : 9207125A16884714754  
LastWrite: Wed Nov 14 12:01:54 2018
```

```
-----  
usbstor v.20080418  
(System) Get USBStor key info
```

```
USBStor  
ControlSet001\Enum\USBStor
```

```
CdRom&Ven_hp&Prod_CDDVDW_SN-208DB&Rev_HH01 [Wed Nov  7 09:16:25 2018]  
S/N: 866BD800EDFF&0 [Wed Nov  7 09:16:25 2018]  
FriendlyName : hp CDDVDW SN-208DB USB Device
```

```
Disk&Ven_VendorCo&Prod_ProductCode&Rev_2.00 [Wed Nov  7 10:25:30 2018]  
S/N: 9207125A16884714754&0 [Wed Nov  7 10:25:30 2018]  
FriendlyName : VendorCo ProductCode USB Device
```

```
-----  
DESKTOP-N96E4RN,CdRom&Ven_hp&Prod_CDDVDW_SN-208DB&Rev_HH01,866BD800EDFF&  
SB Device  
DESKTOP-N96E4RN,Disk&Ven_VendorCo&Prod_ProductCode&Rev_2.00,9207125A1688  
ductCode USB Device
```

```
-----  
CdRom&Ven_hp&Prod_CDDVDW_SN-208DB&Rev_HH01,Wed Nov  7 09:16:25 2018,866B  
18,hp CDDVDW SN-208DB USB Device,  
Disk&Ven_VendorCo&Prod_ProductCode&Rev_2.00,Wed Nov  7 10:25:30 2018,920  
25:30 2018,VendorCo ProductCode USB Device,  
-----
```

```
-----  
removdev v.200800611  
(Software) Parses Windows Portable Devices key (Vista)
```

```
RemovDev  
Microsoft\Windows Portable Devices\Devices  
LastWrite Time Wed Nov  7 10:25:31 2018 (UTC)
```

```
Device      : DISK&VEN_VENDORCO&PROD_PRODUCTCODE&REV_2.00  
LastWrite  : Wed Nov  7 10:25:31 2018 (UTC)  
SN          : 9207125A16884714754&0  
Drive      : DURAND_USB
```

```
(System) Get USB device info from the DeviceClasses keys in the System hive
```

```
DevClasses - Disks  
ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
```

```
Wed Nov  7 10:25:30 2018 (UTC)  
Disk&Ven_VendorCo&Prod_ProductCode&Rev_2.00,9207125A16884714754&0
```

```
DevClasses - Volumes  
ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
```

```
-----  
mountdev v.20080324  
(System) Return contents of System hive MountedDevices key
```

```
MountedDevices  
LastWrite time = Wed Nov  7 10:25:30 2018Z
```

```
\DosDevices\C:  
Drive Signature = e7 67 b2 68
```

```
Device: _??_ USBSTOR#Disk&Ven_VendorCo&Prod_ProductCode&Rev_2.00#9207125A16884714754&0#{53  
-94f2-00a0c91efb8b}  
  \DosDevices\D:  
  \??\Volume{069fb4d1-e277-11e8-b4c9-ace2d3991446}
```

```
Device: \??_USBSTOR#CdRom&Ven_hp&Prod_CDDVDW_SN-208DB&Rev_HH01#866BD800EDFF&0#{53f5630d-b  
a0c91efb8b}  
  \??\Volume{f7b403f3-e26c-11e8-b4c8-ace2d3991446}
```



## L'affaire Megacorp

Le volume D:

Nous avons obtenus les informations suivantes au sujet de la clé USB :

Le nom de la clé : DURAND\_USB

Le numéro de série : 9207125A16884714754&0

Le code du vendeur : VendorCo (no name)

Le code du produit : ProductCode (no name)

La lettre du volume où elle était montée : D:

L'horodatage du premier branchement : Wed Nov 7 10:25:30 2018

L'horodatage du dernier branchement : Wed Nov 14 12:01:54 2018

La clé USB n'a pas dû coûter cher car elle n'est pas étiquetée « Designed for Windows »

Le second caractère en partant de la fin est un & => Le numéro de série n'est pas unique et ne peut être utiliser pour identifier de manière unique cette clé.



## L'affaire Megacorp

### Vérifions la clé USB saisi

On la branche sans la monter sur notre machine afin de préserver les données.

2 méthodes permettent d'obtenir des informations intéressantes sur la clé :

- `dmesg`
- `lsusb -D /dev/bus/usb/<bus>/<device>`

Le numéro de série de la clé USB correspond à notre investigation.

```
caron@caron-debian ~/mdurand_usb_acquisition$ sudo lsusb -D /dev/bus/usb/002/012
Device: ID ffff:5678
Device Descriptor:
  bLength                18
  bDescriptorType         1
  bcdUSB                  2.00
  bDeviceClass            0 (Defined at Interface level)
  bDeviceSubClass         0
  bDeviceProtocol         0
  bMaxPacketSize0        64
  idVendor                0xffff
  idProduct              0x5678
  bcdDevice              2.00
  iManufacturer          1 USB
  iProduct               2 Disk 2.0
  iSerial                3 9207125A16884714754
  bNumConfigurations      1
```

```
[141871.158080] ISO 9660 Extensions: Microsoft Joliet Level 3
[141871.158819] ISO 9660 Extensions: RRIP_1991A
[141896.291695] usb 2-2: USB disconnect, device number 9
[143109.609628] usb 2-2: new high-speed USB device number 10 using xhci_hcd
[143109.759727] usb 2-2: New USB device found, idVendor=ffff, idProduct=5678
[143109.759729] usb 2-2: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[143109.759730] usb 2-2: Product: Disk 2.0
[143109.759734] usb 2-2: Manufacturer: USB
[143109.759735] usb 2-2: SerialNumber: 9207125A16884714754
[143109.760270] usb-storage 2-2:1.0: USB Mass Storage device detected
[143109.760567] scsi host4: usb-storage 2-2:1.0
[143110.779962] scsi 4:0:0:0: Direct-Access VendorCo ProductCode 2.00 PQ: 0 ANSI: 4
[143110.780562] sd 4:0:0:0: Attached scsi generic sg2 type 0
[143110.780714] sd 4:0:0:0: [sdb] 15605760 512-byte logical blocks: (7.99 GB/7.44 GiB)
[143110.780845] sd 4:0:0:0: [sdb] Write Protect is off
[143110.780848] sd 4:0:0:0: [sdb] Mode Sense: 03 00 00 00
[143110.780985] sd 4:0:0:0: [sdb] No Caching mode page found
[143110.780989] sd 4:0:0:0: [sdb] Assuming drive cache: write through
[143110.783257] sdb:
[143110.785187] sd 4:0:0:0: [sdb] Attached SCSI removable disk
```



## L'affaire Megacorp

### Vérifions la clé USB saisi

On fait une copie bit à bit avec dd et on utilise le *file carving*... Bingo ? Un fichier *.xlsx* et un *.png*, ça sent bon.

```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk mdurand_usb.img - 7990 MB / 7620 MiB (R0)
  Partition      Start      End      Size in sectors
  P FAT32        0      1 971 105 30 15605760 [DURAND_USB]

2 files saved in /root/Documents/recup_dir directory.
Recovery completed.

You are welcome to donate to support further development and encouragement
http://www.cgsecurity.org/wiki/Donation
```

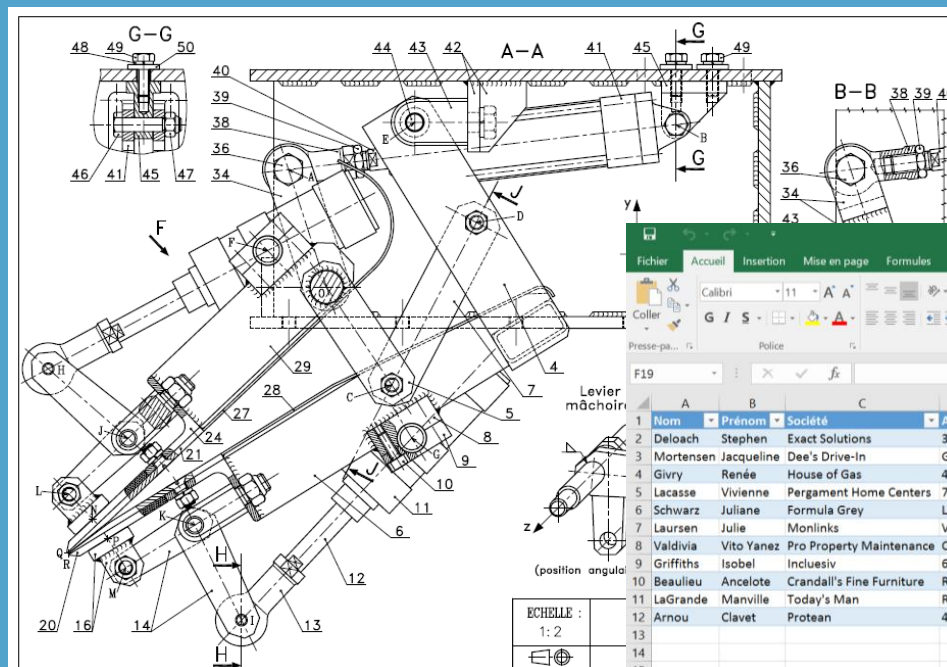
```
root@kali:~/Documents/recup_dir.1# ls -la
total 164
drwxr-xr-x 2 root root  4096 nov. 17 19:59 .
drwxr-xr-x 6 root root  4096 nov. 17 19:59 ..
-rw-r--r-- 1 root root 136136 nov. 17 19:59 f0032800.png
-rw-r--r-- 1 root root  11808 déc. 31 1979 f0033072.xlsx
-rw-r--r-- 1 root root   1778 nov. 17 19:59 report.xml
root@kali:~/Documents/recup_dir.1#
```

1

## L'affaire Megacorp

Vérifions la clé USB saisi

# Bingo !



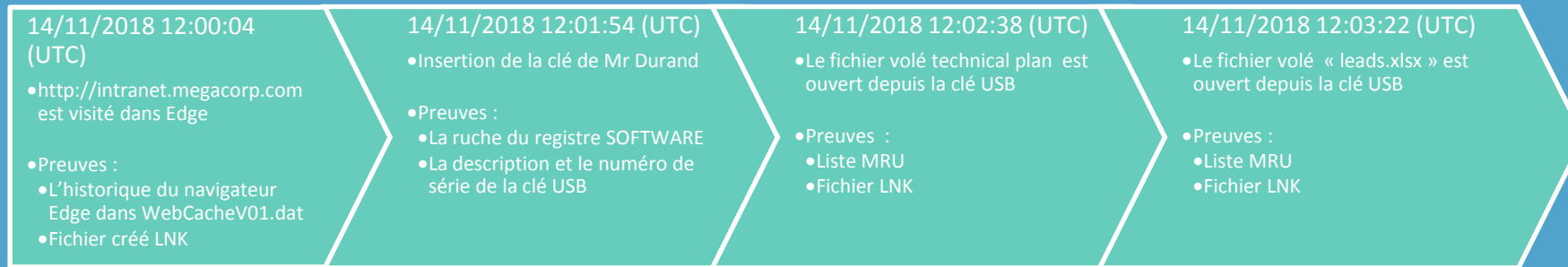
Excel spreadsheet showing a list of companies and their financial data. The spreadsheet is titled 'f0033072.xlsx - Excel'.

A	B	C	D	E	F	G	H
Nom	Prénom	Société	Adresse	Nom du projet	Proposition commerciale	Objectif	Marge de négociation
2	Deloach	Stephen	Exact Solutions	3360 Angie Drive Los Angeles, CA 90017	GeminiActivity	390 000,00 €	360 000,00 € 8,33%
3	Mortensen	Jacqueline	Dee's Drive-In	Gartenhof 102 1277 Arnex-sur-Nyon	PressMarks	778 000,00 €	760 000,00 € 2,37%
4	Givry	Renée	House of Gas	47, rue de la Boétie 86000 POITIERS	Thaddle	1 735 000,00 €	1 500 000,00 € 15,67%
5	Lacasse	Vivienne	Pergament Home Centers	73, rue Cazade 59240 DUNKERQUE	Osleader	235 000,00 €	220 000,00 € 6,82%
6	Schwarz	Juliane	Formula Grey	Leipziger Strasse 19 55246 Wiesbaden-Mainz-Kostheim	Almosiness	745 000,00 €	700 000,00 € 6,43%
7	Laursen	Julie	Monlinks	Viinikantie 61 76130 PIEKSÄMÄKI	Lifehout	172 000,00 €	165 000,00 € 4,24%
8	Valdivia	Vito Yanez	Pro Property Maintenance	Ouid de Arriba, 67 43740 Mora d'Ebre	Spallown	365 000,00 €	355 000,00 € 2,82%
9	Griffiths	Isobel	Inclusiv	60 Harris Street BONNIE DOON VIC 3720	LawnCareRepair	465 000,00 €	430 000,00 € 8,14%
10	Beaulieu	Ancelote	Crandall's Fine Furniture	Raas van Gaverestraat 354 8890 Dadizele	DataFormula	128 000,00 €	120 000,00 € 6,67%
11	LaGrande	Manville	Today's Man	Rue Libert 91 7340 Warquignies	GolfingNorth	378 000,00 €	365 000,00 € 3,56%
12	Arnou	Clavet	Protean	4, rue du Président Roosevelt 67300 SCHILTIGHEIM	PlusApps	1 235 000,00 €	1 115 000,00 € 10,76%

1

## L'affaire Megacorp

### La frise chronologique



- Cela se passe bien durant les vacances de Mr Durand.
- `Technical_plan.png` :
  - Récupéré sur le PC portable de Mr Durand (trouvé dans le *thumbcache*)
  - Récupéré sur la clé USB saisi (avec la méthode du *file carving*)
- `Leads.xlsx` :
  - Récupéré sur la clé USB saisi (avec la méthode du *file carving*)





## L'affaire Megacorp

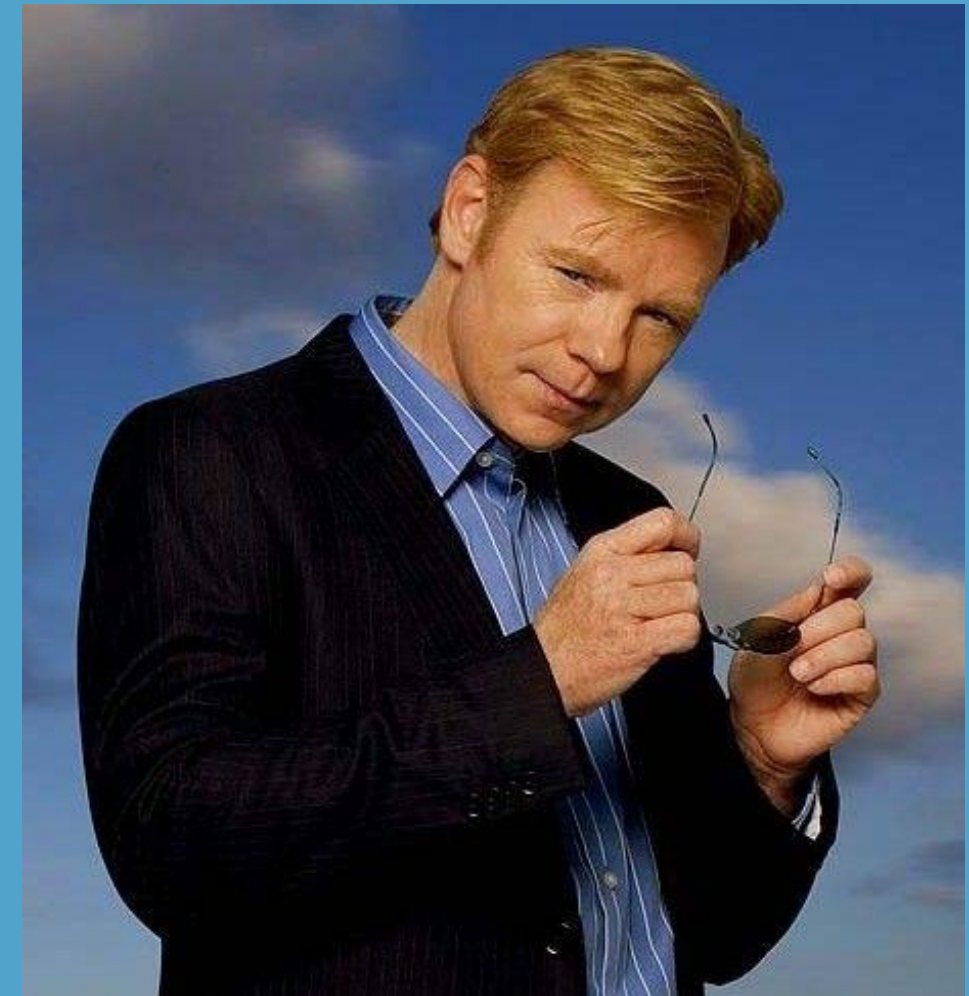
Case is closed!

Bien joué !

Vous avez trouvé suffisamment de preuves pour réaliser une frise chronologique des événements et vous avez même récupéré les fichiers volés. De plus, toutes les précautions nécessaires ont été prise pour que les preuves soient recevables par la justice.

Vous avez rempli avec succès votre mission et Mr Durand va passer en jugement pour ses actes.

Un autre grand jour pour la justice !!





## L'affaire Megacorp OMG!

Euh... vous êtes sur-e-s ?

- Nous ne devons pas être influencé-es par l'opinion de Mme Lecomte sur le fait que Mr Durand était en vacances à ce moment-là et qu'il ne veut pas en dire plus...
- Nous nous sommes focalisés sur *leads.xlsx* mais...





## L'affaire Megacorp

### Les logs Windows

Les logs Windows contiennent de nombreuses informations sur le système, les applications et la sécurité. Ils sont stockés dans des fichiers `.evt` ou `.evtx`

La politique d'audit des authentications était activée sur le PC portable. Récupérons ces authentications avec le script `evtx_dump.py`  
L'évènement 4624 nous indique une authentification locale réussie le 14/11/2018 à 11:57:18 (UTC) par MDurand

```
<EventID Qualifiers="">4624</EventID>
<Version>2</Version>
<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2018-11-14 11:57:18.935987"></TimeCreated>
<EventRecordID>678</EventRecordID>
<Correlation ActivityID="{c86c5833-7683-0002-4758-6cc88376d401}" RelatedActivityID=""></Correlation>
<Execution ProcessID="624" ThreadID="704"></Execution>
<Channel>Security</Channel>
<Computer>DESKTOP-N96E4RN</Computer>
<Security UserID=""></Security>
</System>
<EventData><Data Name="SubjectUserSid">S-1-5-18</Data>
<Data Name="SubjectUserName">DESKTOP-N96E4RN$</Data>
<Data Name="SubjectDomainName">WORKGROUP</Data>
<Data Name="SubjectLogonId">0x000000000000003e7</Data>
<Data Name="TargetUserSid">S-1-5-21-2564730259-2604401790-4054121556-1001</Data>
<Data Name="TargetUserName">MDurand</Data>
<Data Name="TargetDomainName">DESKTOP-N96E4RN</Data>
<Data Name="TargetLogonId">0x000000000000091ecc</Data>
<Data Name="LogonType">2</Data>
<Data Name="LogonProcessName">User32 </Data>
<Data Name="AuthenticationPackageName">Negotiate</Data>
<Data Name="WorkstationName">DESKTOP-N96E4RN</Data>
<Data Name="LogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
<Data Name="TransmittedServices">-</Data>
<Data Name="LmPackageName">-</Data>
<Data Name="KeyLength">0</Data>
<Data Name="ProcessId">0x000000000000003b4</Data>
<Data Name="ProcessName">C:\Windows\System32\svchost.exe</Data>
<Data Name="IpAddress">127.0.0.1</Data>
<Data Name="IpPort">0</Data>
```



## L'affaire Megacorp

### Les logs Windows

13 évènements 4625 d'authentifications ratées précèdent l'authentification réussie. Mr Durand était trop stressé pour bien taper son mot de passe ?

```
<EventID Qualifiers="">4625</EventID>
<TimeCreated SystemTime="2018-11-14 11:54:31.579519"></TimeCreated>
<EventID Qualifiers="">4625</EventID>
<TimeCreated SystemTime="2018-11-14 11:54:34.457140"></TimeCreated>
<EventID Qualifiers="">4625</EventID>
<TimeCreated SystemTime="2018-11-14 11:54:40.994034"></TimeCreated>
<EventID Qualifiers="">4625</EventID>
<TimeCreated SystemTime="2018-11-14 11:54:46.761955"></TimeCreated>
<EventID Qualifiers="">4625</EventID>
<TimeCreated SystemTime="2018-11-14 11:54:52.490179"></TimeCreated>
<EventID Qualifiers="">4625</EventID>
<TimeCreated SystemTime="2018-11-14 11:54:58.418064"></TimeCreated>
<EventID Qualifiers="">4625</EventID>
<TimeCreated SystemTime="2018-11-14 11:55:35.288998"></TimeCreated>
<EventID Qualifiers="">4625</EventID>
<TimeCreated SystemTime="2018-11-14 11:55:40.154783"></TimeCreated>
<EventID Qualifiers="">4625</EventID>
<TimeCreated SystemTime="2018-11-14 11:55:43.904730"></TimeCreated>
<EventID Qualifiers="">4625</EventID>
<TimeCreated SystemTime="2018-11-14 11:56:20.223110"></TimeCreated>
<EventID Qualifiers="">4625</EventID>
<TimeCreated SystemTime="2018-11-14 11:56:28.755869"></TimeCreated>
<EventID Qualifiers="">4625</EventID>
<TimeCreated SystemTime="2018-11-14 11:56:34.398573"></TimeCreated>
<EventID Qualifiers="">4625</EventID>
<TimeCreated SystemTime="2018-11-14 11:57:11.496248"></TimeCreated>
<EventID Qualifiers="">4624</EventID>
```

```
<EventID Qualifiers="">4625</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime="2018-11-14 11:57:11.496248"></TimeCreated>
<EventRecordID>676</EventRecordID>
<Correlation ActivityID="{c86c5833-7683-0002-4758-6cc88376d401}" RelatedActivityID=""></Correlation>
<Execution ProcessID="624" ThreadID="676"></Execution>
<Channel>Security</Channel>
<Computer>DESKTOP-N96E4RN</Computer>
<Security UserID=""></Security>
</System>
<EventData><Data Name="SubjectUserSid">S-1-5-18</Data>
<Data Name="SubjectUserName">DESKTOP-N96E4RN$</Data>
<Data Name="SubjectDomainName">WORKGROUP</Data>
<Data Name="SubjectLogonId">0x000000000000003e7</Data>
<Data Name="TargetUserSid">S-1-0-0</Data>
<Data Name="TargetUserName">MDurand</Data>
<Data Name="TargetDomainName">DESKTOP-N96E4RN</Data>
<Data Name="Status">0xc000006d</Data>
```



## L'affaire Megacorp

### Les traces Wi-Fi

La ruche SOFTWARE de la base de registre Windows trace les points d'accès Wi-Fi auxquels s'est connecté le système.

Juste avant de se connecter à l'Intranet, le PC portable était connecter en Wi-Fi à un SSID « Royal\_Palm »

```
Launching networklist v.20120917
(Software) Collects network info from Vista+ NetworkList key

Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles
"Royal_Palm"
  Key_LastWrite      : Wed Nov 14 11:57:41 2018 UTC
  DateLastConnected: Wed Nov 14 12:57:41 2018
  DateCreated       : Wed Nov 14 12:57:41 2018
  DefaultGatewayMac: 22-17-31-FA-80-0C
  Type              : wireless
```

```
vista_wireless v.20090514
(Software) Get Vista Wireless Info

Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

LastWrite = Wed Nov 14 11:57:41 2018 Z
  "Royal_Palm" ["Royal_Palm"]
-----
```





## L'affaire Megacorp

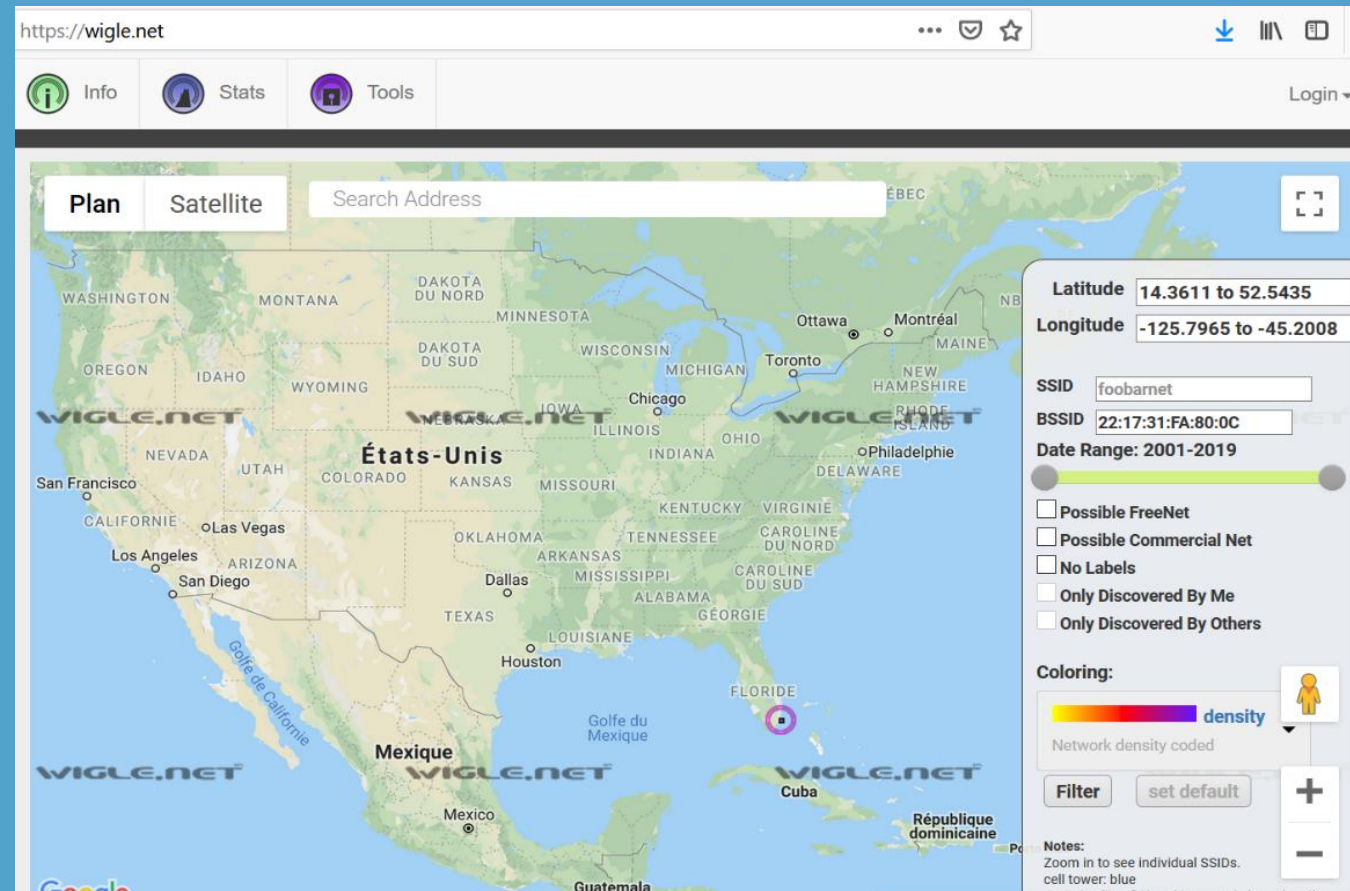
### Around the world

Le BSSID du point d'accès Wi-Fi est  
22:17:31:FA:80:0C

Wigle.net peut être utilisé pour trouver la  
géolocalisation physique d'un point  
d'accès Wi-Fi.

Le PC portable, juste avant le vol des  
documents, était connecté à un point  
d'accès Wi-Fi situé en...

**Floride !**

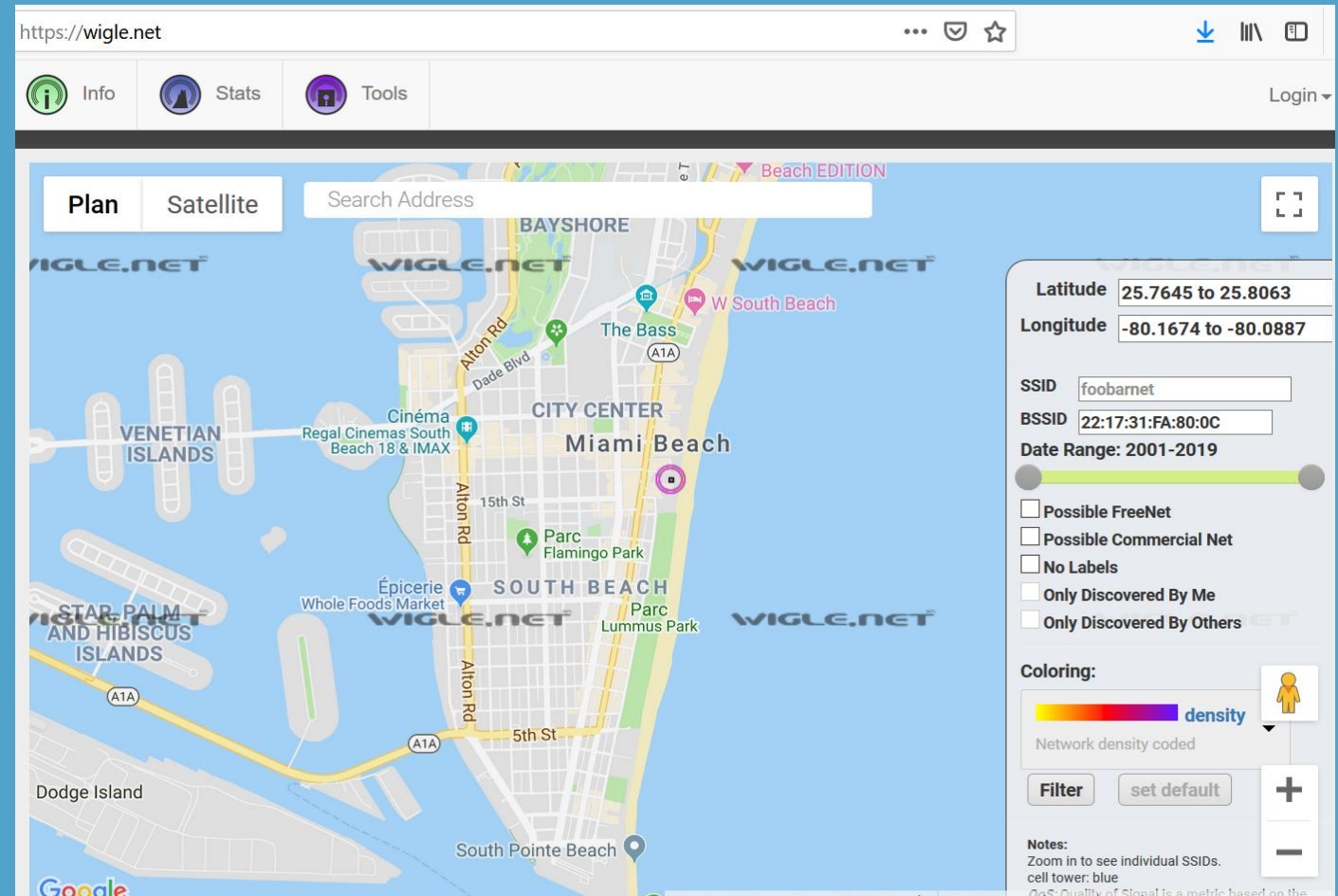




## L'affaire Megacorp

Around the world

Pour être plus précis, à Miami Beach.





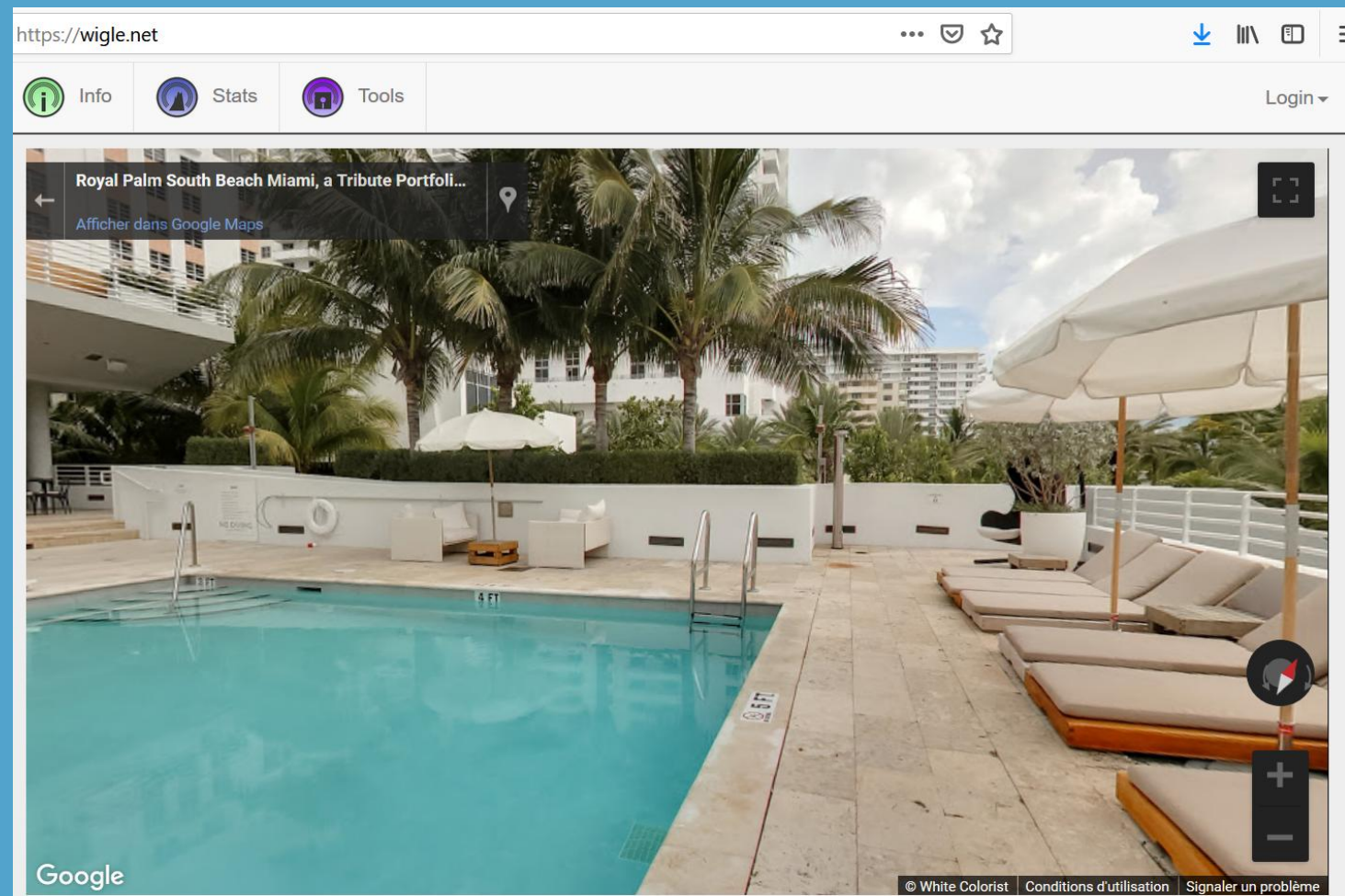


## L'affaire Megacorp

Around the world

Pour être plus précis, au Royal Palm.

Qui était en voyage à Miami récemment ?





## L'affaire Megacorp

Case is really closed!

Mr Dupond a toujours été mécontent de Mme Lecomte : il a travaillé si dur pendant les 10 dernières années et il n'a pas reçu le respect qu'il pense mérité. Il a été très déçu par le nouvel arrivant, Mr Durand, qui ne s'impliquait pas assez selon lui dans l'entreprise.

Quand Mr Dupont a été approché et qu'il s'est vu offrir une large somme d'argent par UltraVenture, il a dû penser que c'était une occasion pour lui de recevoir ce qu'il mérite. Alors il a « emprunté » l'ordinateur portable et la clé USB de Mr Durand en pensant que ça prouverait que le coupable est Mr Durand.



## L'affaire Megacorp

Case is really closed!

Mr Dupond a toujours été mécontent de Mme Lecomte : il a travaillé si dur pendant les 10 dernières années et il n'a pas reçu le respect qu'il pense mérité. Il a été très déçu par le nouvel arrivant, Mr Durand, qui ne s'impliquait pas assez selon lui dans l'entreprise.

Quand Mr Dupont a été approché et qu'il s'est vu offrir une large somme d'argent par UltraVenture, il a dû penser que c'était une occasion pour lui de recevoir ce qu'il mérite. Alors il a « emprunté » l'ordinateur portable et la clé USB de Mr Durand en pensant que ça prouverait que le coupable est Mr Durand.

# Conclusion



# MERCI

[www.squad.fr](http://www.squad.fr)

PUBLIC

