

ANALYSE NUMERIQUE WINDOWS

LE PROF

- Laurent Clévy (@lorenzo2472)
- Informatique Forensique depuis 2013
- Coordination des analyses Forensique et Malware chez Thales depuis 2015
- Giac Certified Forensic Analyst ([GCFA](#)) depuis 2013, [GREM](#) (Malware reversing) depuis 2015
- Auteur de plusieurs articles MISC sur le forensic et l'analyse de malware
- Cours d'analyse forensique à l'AFTI (master 2) entre 2015 et 2019.

ORGANISATION DU COURS

- 9h30-11h30 : cours
- 12h30-15h30 : TDs et évaluation
 - 12h30 : TD1
 - 13h30 : pause de 30mn
 - 14h00 : TD2
 - 15h10 : Evaluation
 - 15h30 : énoncé du projet

AGENDA

- Rappels
- 14/03 : Windows
- 15/03 : Stockage, systèmes de fichiers
- 16/03 : Forensic mémoire
- 17/03 : Android, live

PRINCIPES DE L'ANALYSE FORENSIQUE

INFO(RMATIQUE) (FO)RENSIQUE

- Est une science
 - Reproductible
 - Méthodique
 - Argumenté
- Un art
 - Il n'y a pas de recette miracle
 - Discipline naissante (15 à 20 ans)
 - Repose beaucoup sur le savoir faire et la bonne utilisations des outils

OBJECTIFS DE L'INFORENSIQUE

Reconstituer une scène de crime numérique

- **Préserver** les données

On travaille toujours sur des copies

- Permettre une **contre-expertise**

Tracer qui a eu accès aux données et sur quelle période

Expliquer la démarche d'analyse, le contexte initial, les outils utilisés

- **Chronologie** / timeline

Recueillir de métadonnées datées

- **Traces** et Interprétation de celles-ci

2 choses différentes ! Les traces ne mentent pas. Une interprétation peut être fausse, et c'est là que l'on attend votre expertise !

SOURCES D'INFORMATION

Réseau

- Sur le serveur Web
- Routeur, serveur DHCP, serveur DNS, pare-feu, proxy

Endpoint

- **Disque** : secteurs, partitions, système de fichiers (fichiers, répertoires, métadonnées)
- **Système** : journaux, configuration (registre Windows), comptes, groupes/accès
- **Système** : preuves d'exécution Windows (prefetch, Ink, jumplist...)
- **Application** : navigation internet, journaux. Stockage en ligne, messagerie instantanée, Réseau sociaux, comptes en lignes / Webmail
- **Source de sécurité** : antivirus/EDR, proxy, pare-feu local
- **Réseau** : cache ARP, DNS
- **Mémoire** : processus, connexions réseau, fichiers ouverts...

WINDOWS : PREUVES D'EXÉCUTION

Prefetch (optimisation du chargement)

Lnk (raccourcis)

Jumplist

SRUM (system performance)

Amcache

Shimcache (compatibilité)

UserAssist

RecentApps

Win10 BAM/DAM (activity moderator)

Win10 timeline

PREFETCH

Rôle: performance du chargement des applications

Localisation: `C:\Windows\Prefetch`

Nom de fichier: appname-hash.pf

Dates du fichier Prefetch:

- Birth/Création : **première exécution** de l'application
- Modification : **dernière exécution** de l'application
- (à 10 secondes près)

Configuration: `KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters`

Prefetch Deep Dive (13Cubed) : https://www.youtube.com/watch?v=f4RAtR_3zcs

Hash algorithm (Hexacorn) : <http://www.hexacorn.com/blog/2012/06/13/prefetch-hash-calculator-a-hash-lookup-table-xpvistaw7w2k3w2k8/>

Nom	Date de création	Modifié le	Type	Taille
ReadyBoot	30/08/2020 16:32	30/08/2020 16:33	Dossier de fichiers	
7ZFM.EXE-44040917.pf	09/09/2020 21:39	09/01/2023 18:34	Fichier PF	22 Ko
7ZG.EXE-88D7305A.pf	20/05/2022 18:49	29/09/2022 19:29	Fichier PF	105 Ko
7ZG.EXE-D9AA3A0B.pf	11/09/2020 22:18	02/03/2023 22:15	Fichier PF	79 Ko
ACROBAT.EXE-4C6D315E.pf	30/05/2022 17:53	16/10/2022 19:40	Fichier PF	33 Ko
ACROBAT.EXE-4E1700B7.pf	29/11/2021 22:15	06/03/2023 16:47	Fichier PF	65 Ko
ACRORD32.EXE-41B0A0C8.pf	05/09/2020 11:55	26/11/2021 23:09	Fichier PF	25 Ko
ADOBE DESKTOP SERVICE.EXE-8163FB66.pf	25/10/2020 22:44	28/02/2023 21:12	Fichier PF	85 Ko
ADOBEARM.EXE-813E932C.pf	12/12/2022 22:55	26/02/2023 18:18	Fichier PF	88 Ko
ADOBENOTIFICATIONHELPER.EXE-462EE9B7.pf	06/03/2023 20:59	06/03/2023 20:59	Fichier PF	10 Ko
ADOBEUPDATER.EXE-0E2638A0.pf	28/02/2023 22:34	28/02/2023 22:34	Fichier PF	17 Ko
AGSSERVICE.EXE-52BA2B96.pf	06/03/2023 18:12	06/03/2023 18:13	Fichier PF	6 Ko
APDPPOXY.EXE-171AE38A.pf	30/08/2020 17:19	27/01/2023 09:46	Fichier PF	11 Ko
APPLICATIONFRAMEHOST.EXE-4CE44C83.pf	05/11/2022 12:00	17/02/2023 23:07	Fichier PF	18 Ko
AUDIODG.EXE-9848A323.pf	06/03/2023 17:44	06/03/2023 21:14	Fichier PF	7 Ko
AVBUGREPORT.EXE-F9E2C280.pf	06/03/2023 19:44	06/03/2023 19:44	Fichier PF	7 Ko

PREFETCH (PARSING)

Eric Zimmerman PECmd

<https://ericzimmerman.github.io/#!index.md>

```
Description:
  PECmd version 1.5.0.0

  Author: Eric Zimmerman (saericzimmerman@gmail.com)
  https://github.com/EricZimmerman/PECmd

  Examples: PECmd.exe -f "C:\Temp\CALC.EXE-3FBEF7FD.pf"
            PECmd.exe -f "C:\Temp\CALC.EXE-3FBEF7FD.pf" --json "D:\jsonOutput" --jsonpretty
            PECmd.exe -d "C:\Temp" -k "system32, fonts"
            PECmd.exe -d "C:\Temp" --csv "c:\temp" --csvf foo.csv --json c:\temp\json
            PECmd.exe -d "C:\Windows\Prefetch"
```

[illegible]

Commande applicable sur un fichier ou un répertoire.

Sorties en CSV ou JSON

PREFETCH (EXEMPLE) 7ZIP

Command line: -f c:\Windows\Prefetch\7ZG.EXE-88D7305A.pf

Warning: Administrator privileges not found!

Keywords: temp, tmp

Processing c:\Windows\Prefetch\7ZG.EXE-88D7305A.pf

Created on: 2022-05-20 16:49:24

Modified on: 2022-09-29 17:29:36

Last accessed on: 2023-03-06 20:55:04

Dates du fichier Prefetch

Executable name: 7ZG.EXE

Hash: 88D7305A

File size (bytes): 739 304

Version: Windows 10 or Windows 11

Run count: 43

Last run: 2022-09-29 17:29:25

Other run times: 2022-09-29 17:26:46, 2022-09-16 10:02:24, 2022-09-12 17:18:00, 2022-09-09 17:09:39, 2022-09-05 07:12:26, 2022-09-05 07:03:52, 2022-07-28 06:25:01

Heures et dates d'exécution

Volume information:

Création des volumes

#0: Name: \VOLUME{01d471d99550ead2-2897dc34} Serial: 2897DC34 Created: 2018-11-01 11:54:02 Directories: 0 File references: 0

#1: Name: \VOLUME{01d472fe782f4777-2078664c} Serial: 2078664C Created: 2018-11-02 22:50:36 Directories: 11 File references: 47

Fichiers manipulés

Directories referenced: 11

00: \VOLUME{01d472fe782f4777-2078664c}\PROGRAM FILES

01: \VOLUME{01d472fe782f4777-2078664c}\PROGRAM FILES\7-ZIP

02: \VOLUME{01d472fe782f4777-2078664c}\PROGRAM FILES\7-ZIP\LANG

03: \VOLUME{01d472fe782f4777-2078664c}\PROGRAM FILES\AVG

04: \VOLUME{01d472fe782f4777-2078664c}\PROGRAM FILES\AVG\ANTIVIRUS

05: \VOLUME{01d472fe782f4777-2078664c}\WINDOWS

06: \VOLUME{01d472fe782f4777-2078664c}\WINDOWS\FONTS

07: \VOLUME{01d472fe782f4777-2078664c}\WINDOWS\GLOBALIZATION

08: \VOLUME{01d472fe782f4777-2078664c}\WINDOWS\GLOBALIZATION\SORTING

09: \VOLUME{01d472fe782f4777-2078664c}\WINDOWS\SYSTEM32

10: \VOLUME{01d472fe782f4777-2078664c}\WINDOWS\WINSXS\AMD64_MICROSOFT.WINDOWS.COMMON-CONTROLS_6595B64144CCF1DF_6.0.19041.1110_NONE_60B5254171F9507E

43: \VOLUME{01d471d99550ead2-2897dc34}\CANON_HACK\FIRMWARE\V101-SL1-100D-X7-WIN\UPDATE-PROCEDURE-PDF\100D_SL1_X7-FIRMWAREUPDATE-EN.PDF

44: \VOLUME{01d471d99550ead2-2897dc34}\CANON_HACK\FIRMWARE\V101-SL1-100D-X7-WIN\UPDATE-PROCEDURE-PDF\100D_SL1_X7-FIRMWAREUPDATE-FR.PDF

45: \VOLUME{01d471d99550ead2-2897dc34}\CANON_HACK\FIRMWARE\V101-SL1-100D-X7-WIN\UPDATE-PROCEDURE-PDF\100D_SL1_X7-FIRMWAREUPDATE-JP.PDF

46: \VOLUME{01d471d99550ead2-2897dc34}\CANON_HACK\FIRMWARE\V101-SL1-100D-X7-WIN\UPDATE-PROCEDURE-PDF\100D_SL1_X7-FIRMWAREUPDATE-SP.PDF

47: \VOLUME{01d471d99550ead2-2897dc34}\CANON_HACK\FIRMWARE\V101-SL1-100D-X7-WIN\UPDATE-PROCEDURE-PDF\100D_SL1_X7-FIRMWAREUPDATE-ZH.PDF

48: \VOLUME{01d471d99550ead2-2897dc34}\CANON_HACK\FIRMWARE\V101-SL1-100D-X7-WIN\CCF16101.FIR

29: \VOLUME{01d472fe782f4777-2078664c}\WINDOWS\SYSTEM32\UXTHEME.DLL

30: \VOLUME{01d472fe782f4777-2078664c}\PROGRAM FILES\7-ZIP\LANG\FR.TXT

31: \VOLUME{01d472fe782f4777-2078664c}\PROGRAM FILES\7-ZIP\7Z.DLL

32: \VOLUME{01d472fe782f4777-2078664c}\WINDOWS\SYSTEM32\MSCTF.DLL

DLL utilisées

Files referenced: 889

LNK, RACCOURCIS

Lien vers une application cible ou document ouvert récemment

Les fichiers .lnk sont visibles dans la MFT!

Exemples de localisation:

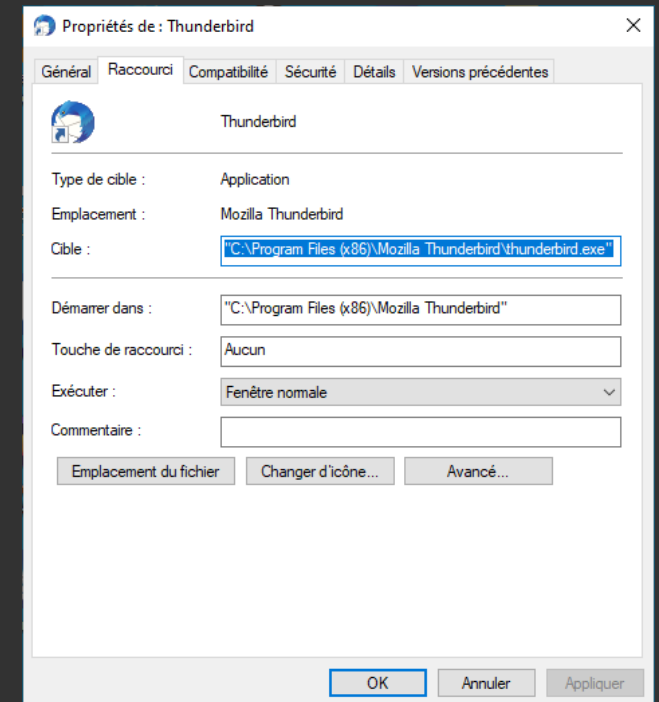
`c:\users\[username]\Desktop`

`c:\users\[username]\AppData\Roaming\Microsoft\Windows\Recent`

Nom de fichier: appname.lnk ou filename.lnk

LNK and Jump lists

<https://www.youtube.com/watch?v=wu4-nREmzGM>



LNK, ANALYSE

Eric Zimmerman LECmd

<https://github.com/EricZimmerman/LECmd>

```
Description:
  LECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

Examples: LECmd.exe -f "C:\Temp\foobar.lnk"
          LECmd.exe -f "C:\Temp\somelink.lnk" --json "D:\jsonOutput" --pretty
          LECmd.exe -d "C:\Temp" --csv "c:\temp" --html c:\temp --xml c:\temp\xml -q
          LECmd.exe -f "C:\Temp\some other link.lnk" --nid --neb
          LECmd.exe -d "C:\Temp" --all
```

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texte Décodé
00000000	4C	00	00	00	01	14	02	00	00	00	00	00	C0	00	00	00	L.....À...
00000010	00	00	00	46	9B	00	00	00	20	00	00	00	7F	45	D9	5A	...F>... ..EÜZ
00000020	C7	72	D4	01	7F	45	D9	5A	C7	72	D4	01	BC	31	8A	A1	ÇrÔ..EÜZÇrÔ.41Š;
00000030	4C	70	D4	01	D0	5D	03	00	00	00	00	00	01	00	00	00	LpÔ.Ə].....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	A3	01	14	00É...
00000050	1F	50	E0	4F	D0	20	EA	3A	69	10	A2	D8	08	00	2B	30	.PàOB è:i.cø...+0
00000060	30	9D	19	00	2F	43	3A	5C	00	00	00	00	00	00	00	00	0.../C:\.....
00000070	00	00	00	00	00	00	00	00	00	00	00	98	00	31	00	00~.1..
00000080	00	00	00	62	4D	03	82	11	00	50	52	4F	47	52	41	7E	...bM,...PROGRA~
00000090	32	00	00	80	00	09	00	04	00	EF	BE	3D	4B	D1	6D	62	2..€.....i%Kmb
000000A0	4D	03	82	2E	00	00	00	C5	04	00	00	00	00	01	00	00	M,...À.....
000000B0	00	00	00	00	00	00	00	56	00	00	00	00	00	13	88	0EV.....
000000C0	01	50	00	72	00	6F	00	67	00	72	00	61	00	6D	00	20	.P.r.o.g.r.a.m.
000000D0	00	46	00	69	00	6C	00	65	00	73	00	20	00	28	00	78	.F.i.l.e.s. .(.x

LNK, EXEMPLE

```
Command line: -f c:\users\laurent\Desktop\Thunderbird.lnk
```

```
Warning: Administrator privileges not found!
```

```
Processing c:\users\laurent\Desktop\Thunderbird.lnk
```

```
Source file: c:\users\laurent\Desktop\Thunderbird.lnk
```

```
Source created: 2018-11-02 21:21:52 Cr  ation du lnk : premi  re ex  cution de Thunderbird
```

```
Source modified: 2018-11-02 21:21:52
```

```
Source accessed: 2023-03-07 09:07:22 Modification du lnk : premi  re ex  cution de Thunderbird
```

```
--- Header ---
```

```
Target created: 2018-11-02 16:16:04 Date d'installation de Thunderbird (hors MAJ)
```

```
Target modified: 2018-10-30 12:32:33 Date de compilation de Thunderbird
```

```
Target accessed: 2018-11-02 16:16:04
```

```
File size: 220 624 Filesize de Thunderbird
```

```
Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasWorkingDir, IsUnicode
```

```
File attributes: FileAttributeArchive
```

```
Icon index: 0
```

```
Show window: SwNormal (Activates and displays the window. The window is restored to its original size and position if the window was maximized.)
```

```
Relative Path: ..\..\..\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe
```

```
Working Directory: C:\Program Files (x86)\Mozilla Thunderbird Filepath de Thunderbird
```

```
--- Link information ---
```

```
Flags: VolumeIdAndLocalBasePath
```

```
>> Volume information
```

```
Drive type: Fixed storage media (Hard drive)
```

```
Serial number: 2078664C
```

```
Label: (No label) Num  ro de s  rie du volume
```

```
Local path: C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe
```

LNK, EXEMPLE (2)

```
Tracker database block
Machine ID: desktop-5b94hc1
MAC Address: 18:31:bf:0a:49:ac
MAC Vendor: ASUS
Creation: 2018-11-02 22:59:15
```

Information sur la machine,
l'adresse MAC

```
-Drive letter ==> C:

-Directory ==> (None)
Short name: PROGRA~2
Modified: 2018-11-02 16:16:06
Extension block count: 1

----- Block 0 (Beef0004) -----
Long name:
Localized name: @shell32.dll,-21817
Created: 2017-09-29 13:46:34
Last access: 2018-11-02 16:16:06
MFT entry/sequence #: 1221/1 (0x4C5/0x1)

-Directory ==> Mozilla Thunderbird
Short name: MOZILL~2
Modified: 2018-11-02 16:16:06
Extension block count: 1

----- Block 0 (Beef0004) -----
Long name: Mozilla Thunderbird
Created: 2018-11-02 16:16:06
Last access: 2018-11-02 16:16:06
MFT entry/sequence #: 91941/1 (0x16725/0x1)

-File ==> thunderbird.exe
Short name: THUNDE~1.EXE
Modified: 2018-10-30 12:32:34
Extension block count: 1

----- Block 0 (Beef0004) -----
Long name: thunderbird.exe
Created: 2018-11-02 16:16:06
Last access: 2018-11-02 16:16:06
MFT entry/sequence #: 92034/1 (0x16782/0x1)
```

Lien vers les métadonnées NTFS (MFT) du
répertoire parent

Lien vers les métadonnées NTFS (MFT) de
la cible

JUMPLIST

Liens vers documents ouverts

2 types :

- AutomaticDestinations (OLE2 CFB streams)
- CustomDestination (sequence of LNK)

- Un fichier par application (AppID)

Localisation:

- C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
- C:\users\[username]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

Analyse avec: <https://github.com/EricZimmerman/JLECmd>

Nom	filenames	Modifié le	Type	Taille
5f7b5f1e01b83767.automaticDestinations-ms		07/03/2023 11:22	Fichier AUTOMATI...	2 452 Ko
f01b4d95cf55d32a.automaticDestinations-ms		07/03/2023 10:13	Fichier AUTOMATI...	1 049 Ko
e4ea035065b5789a.automaticDestinations-ms		06/03/2023 21:46	Fichier AUTOMATI...	575 Ko
9fda41b86ddcf1db.automaticDestinations-ms		06/03/2023 19:01	Fichier AUTOMATI...	624 Ko
f065ac336abcaa3e.automaticDestinations-ms		06/03/2023 16:47	Fichier AUTOMATI...	75 Ko
d00655d2aa12ff6d.automaticDestinations-ms		06/03/2023 16:46	Fichier AUTOMATI...	46 Ko
6824f4a902c78fbd.automaticDestinations-ms		06/03/2023 12:22	Fichier AUTOMATI...	401 Ko
d97efdf3888fe7eb.automaticDestinations-ms		06/03/2023 12:14	Fichier AUTOMATI...	4 Ko
e70d383b15687e37.automaticDestinations-ms		06/03/2023 11:50	Fichier AUTOMATI...	1 032 Ko
fb3b0dbfee58fac8.automaticDestinations-ms		06/03/2023 11:47	Fichier AUTOMATI...	78 Ko
dd7c3b1adb1c168b.automaticDestinations-ms		06/03/2023 11:25	Fichier AUTOMATI...	43 Ko

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texte Décodé
00000000	D0	CF	11	E0	A1	B1	1A	E1	00	00	00	00	00	00	00	00	Đ ĩ . à ; ± . á
00000010	00	00	00	00	00	00	00	00	3E	00	03	00	FE	FF	09	00 > . . . p ý . .
00000020	06	00	00	00	00	00	00	00	00	00	00	00	27	00	00	00 '
00000030	01	00	00	00	00	00	00	00	10	00	00	02	00	00	00	00
00000040	CB	00	00	00	FE	FF	FF	FF	00	00	00	00	00	00	00	00	Ě . . . p ý ý ý

JUMPLIST, ANALYSE

```
Command line: -f c:\users\laurent\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5bb830f67194431a.automaticDestinations-ms
```

```
Warning: Administrator privileges not found!
```

```
Processing c:\users\laurent\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5bb830f67194431a.automaticDestinations-ms
```

```
Source file: c:\users\laurent\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5bb830f67194431a.automaticDestinations-ms
```

```
--- AppId information ---
```

```
AppID: 5bb830f67194431a
```

```
Description: 7-Zip 18.05 (x64)
```

Correspondance entre AppID et application

```
--- DestList information ---
```

```
Expected DestList entries: 39
```

```
Actual DestList entries: 39
```

```
DestList version: 4
```

Nombre de « Destination »

```
Entry #: 32
```

```
MRU: 7
```

MRU = Most Recently Used

```
Path: I:\ctf\2021_google\raiders_of_corruption_misc~\chall.tar
```

```
Pinned: False
```

```
Created on: 2021-07-15 21:13:28
```

```
Last modified: 2021-07-17 11:21:54
```

```
Hostname: desktop-5b94hcl
```

```
Mac Address: 18:31:bf:0a:49:ac
```

```
Interaction count: 1
```

```
--- Lnk information ---
```

```
Absolute path: My Computer\I:\ctf\2021_google\raiders_of_corruption_misc~\chall.tar
```

JUMPLIST, ANALYSE D'UN RÉPERTOIRE

JLECmd.exe -d c:\users\laurent\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations --csv . -q
-d pour un répertoire
--csv pour le repertoire de sortie du fichier csv
-q pour "quiet"

```
----- Processed c:\users\laurent\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\fe043abf98ef3782.automaticDestinations-ms in 0,00096010 seconds -----  
----- Processed c:\users\laurent\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\fe57f5df17b45fe.automaticDestinations-ms in 0,01286540 seconds -----  
  
Processed 119 out of 119 files in 5,6790 seconds  
  
AutomaticDestinations CSV output will be saved to .\20230307103257_AutomaticDestinations.csv
```

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
1	SourceFile	SourceCreated	SourceModified	SourceAccessed	ApplId	ApplIdDescription	DestListVersion	LastUsedEntryNumber	MRU	EntryNumber	CreationTime	LastModified	Hostname	MacAddress	Path
1620	c:\users\laurent\	02/11/2018 16:14	06/03/2023 11:22	07/03/2023 10:33	6824f4a902c78fbd	Firefox 64.0	4	307	84 E2		12/09/2022 10:01	12/09/2022 21:19	desktop-5b94hcl	18:31:bf:0a:49:ac	C:\Users\laurent\Downloads\COMPTEDDEPOT
1621	c:\users\laurent\	02/11/2018 16:14	06/03/2023 11:22	07/03/2023 10:33	6824f4a902c78fbd	Firefox 64.0	4	307	85 E1		12/09/2022 10:01	12/09/2022 21:19	desktop-5b94hcl	18:31:bf:0a:49:ac	C:\Users\laurent\Downloads\COMPTEDDEPOT
1622	c:\users\laurent\	02/11/2018 16:14	06/03/2023 11:22	07/03/2023 10:33	6824f4a902c78fbd	Firefox 64.0	4	307	86 E0		12/09/2022 10:01	12/09/2022 21:19	desktop-5b94hcl	18:31:bf:0a:49:ac	C:\Users\laurent\Downloads\COMPTEDDEPOT
1623	c:\users\laurent\	02/11/2018 16:14	06/03/2023 11:22	07/03/2023 10:33	6824f4a902c78fbd	Firefox 64.0	4	307	87 DF		12/09/2022 10:01	12/09/2022 21:18	desktop-5b94hcl	18:31:bf:0a:49:ac	C:\Users\laurent\Downloads\COMPTEDDEPOT
1624	c:\users\laurent\	02/11/2018 16:14	06/03/2023 11:22	07/03/2023 10:33	6824f4a902c78fbd	Firefox 64.0	4	307	88 DE		12/09/2022 10:01	12/09/2022 21:17	desktop-5b94hcl	18:31:bf:0a:49:ac	C:\Users\laurent\Downloads\COMPTEDDEPOT
1625	c:\users\laurent\	02/11/2018 16:14	06/03/2023 11:22	07/03/2023 10:33	6824f4a902c78fbd	Firefox 64.0	4	307	89 DD		12/09/2022 10:01	12/09/2022 21:17	desktop-5b94hcl	18:31:bf:0a:49:ac	C:\Users\laurent\Downloads\COMPTEDDEPOT

JUMPLIST, CUSTOM DESTINATIONS

```
JLECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/JLECmd

Command line: -f c:\users\laurent\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1ced32d74a95c7bc.customDestinations-ms

Warning: Administrator privileges not found!

Processing c:\users\laurent\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1ced32d74a95c7bc.customDestinations-ms

Source file: c:\users\laurent\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1ced32d74a95c7bc.customDestinations-ms

--- AppId information ---
AppID: 1ced32d74a95c7bc, Description: Microsoft Visual Studio Code
--- DestList information ---
  Entries: 1

    Entry #: 0, lnk count: 1 Rank: 2,8026E-45

--- Lnk #0 information ---
Lnk target created: 2022-11-16 20:33:38
Lnk target modified: 2022-11-09 03:56:40
Lnk target accessed: 2023-02-08 22:40:01

Absolute path: Shared Documents Folder (Users Files)\AppData\Local\Programs\Microsoft VS Code\Code.exe
```

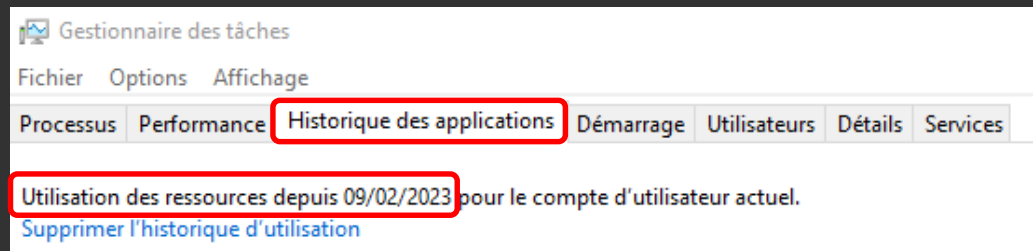
Informations sur Visual Studio Code (dates installation, compilation, dernier usage)

SRUM : SYSTEM RESOURCE USAGE MONITOR

Historique des applications et ressources utilisées.

Situé dans: `C:\Windows\System32\SRU\SRUDB.dat`

Fichier au format ESE/Bluejet



```
Répertoire de c:\windows\system32\sru
11/03/2023 11:43 <DIR> .
11/03/2023 11:43 <DIR> ..
11/03/2023 11:43      8 192 SRU.chk
11/03/2023 11:43     65 536 SRU.log
11/03/2023 11:41     65 536 SRU0EB1A.log
11/03/2023 11:41     65 536 SRU0EB1B.log
11/03/2023 11:41     65 536 SRU0EB1C.log
11/03/2023 11:43     65 536 SRU0EB1C.log
11/03/2023 11:45    82 411 520 SRUDB.dat
11/03/2023 11:43     16 384 SRUDB.jfm
30/08/2020 15:32     65 536 SRUres000001.jrs
30/08/2020 15:32     65 536 SRUres000002.jrs
11/03/2023 11:40     65 536 SRUtmp.log
10 fichier(s)      82 894 848 octets
2 Rép(s)    225 486 196 736 octets libres
```

SRUM : EXTRACTION

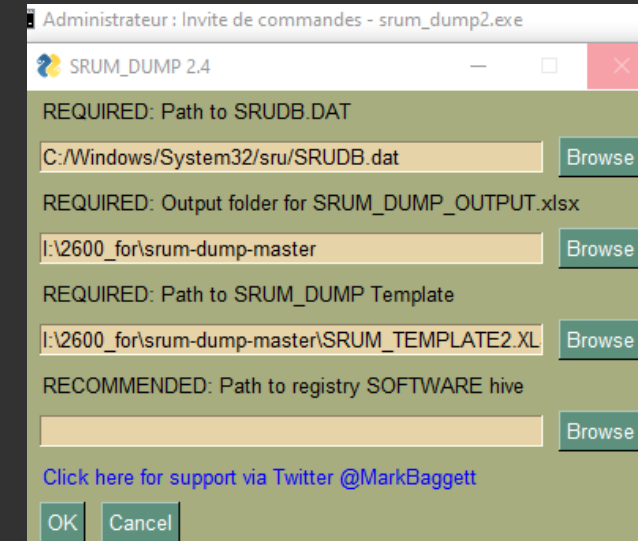
Analyse facile avec:

<https://github.com/MarkBaggett/srum-dump>

(À lancer en admin)

Un script python utilisant esentutl.exe pour extraire la base,
et permettant de combiner les informations de la ruche
SOFTWARE

Le résultat est une feuille Excel



SRUM : RÉSULTATS

En exercice...

Un exemple ci-dessous tout de même

ruDbCheckpoint	App Timeline Provider	Energy Usage	Energy Usage LT	Windows Push Notifications	Network Data Usage	Application Resource Usage	Network Connectivity Usage	vfuprov
----------------	-----------------------	--------------	-----------------	----------------------------	--------------------	----------------------------	----------------------------	---------

B	C	D	E	H	I
SRUM ENTRY CREATION	Application	User SID	Interface	Bytes Sent	Bytes Received
2023-01-10 18:27:00	\device\harddiskvolume4\program files\mozilla firefox\firefox.exe	S-1-5-21-2510752544-4166367489-199343150-1001 (laurent)	IF_TYPE_ETHERNET_CSMACD	149795	2581999
2023-01-10 18:27:00			IF_TYPE_ETHERNET_CSMACD	784943	10402999
2023-01-10 18:27:00	\device\harddiskvolume4\program files\adobe\adobe lightroom classic\lightroom.exe	S-1-5-21-2510752544-4166367489-199343150-1001 (laurent)	IF_TYPE_ETHERNET_CSMACD	12286	36821
2023-01-10 18:27:00	\device\harddiskvolume4\windows\syswow64\vmnat.exe	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_CSMACD	750	1038
2023-01-10 18:27:00	\device\harddiskvolume4\program files (x86)\adobe\adobe sync\coresync\coresync.exe	S-1-5-21-2510752544-4166367489-199343150-1001 (laurent)	IF_TYPE_ETHERNET_CSMACD	34876	55051
2023-01-10 18:27:00	\device\harddiskvolume4\program files (x86)\dropbox\client\dropbox.exe	S-1-5-21-2510752544-4166367489-199343150-1001 (laurent)	IF_TYPE_ETHERNET_CSMACD	27318	31578
2023-01-10 18:27:00	\device\harddiskvolume4\users\laurent\appdata\local\discord\app-1.0.9008\discord.exe	S-1-5-21-2510752544-4166367489-199343150-1001 (laurent)	IF_TYPE_ETHERNET_CSMACD	21514	48571
2023-01-10 18:27:00	Microsoft.Windows.Search_1.14.7.19041_neutral_neutral_cw5n1h2txyewy	S-1-5-21-2510752544-4166367489-199343150-1001 (laurent)	IF_TYPE_ETHERNET_CSMACD	27967	78842

WINDOWS : BACK IN TIME / DELETED FILES

Recycle Bin (Corbeille)

Shadow copy (sauvegardes système)

Thumbnail (miniatures)

RECYCLE BIN (CORBEILLE)

Système	Système de fichiers par défaut	Localisation de la corbeille
Win 95/98/ME	FAT32	C:\Recycled\INFO2
Win NT/2000/XP	NTFS	C:\Recycler\INFO2
Depuis Vista	NTFS	C:\\$Recycle.Bin\

Situé dans : c:\\$Recycle.Bin\[SID]



Préfixe \$I = métadonnées

Préfixe \$R = données

Recycle Bin Forensics (13 cubed)

<https://www.youtube.com/watch?v=Gkir-wGqG2c>

RECYCLE BIN (STRUCTURE)

Nom	Emplacement d'origine	Date de suppression	Taille	Type d'élément	Modifié le
 trains_25_et_27dec.pdf	C:\Users\laurent\Desktop\pdf	07/03/2023 13:44	115 Ko	Document Adobe Acrobat	06/11/2018 21:49
 FastRawViewer Manual	C:\Users\laurent\Desktop\pdf	07/03/2023 13:44	2 Ko	Raccourci	01/05/2019 15:07

Date de **suppression** = date de modification des fichiers \$I

Date de **modification** = modification des fichiers \$D

```
Répertoire de c:\$Recycle.Bin\S-1-5-21-2510752544-4166367489-199343150-1001
07/03/2023 13:44 <DIR> .
07/03/2023 13:44 <DIR> ..
28/10/2022 15:46 00 $I3D0PVM
07/03/2023 13:44 132 $IC8BA3T.pdf
07/03/2023 13:44 136 $IDSVH44.lnk
30/05/2021 22:08 106 $I00RPYA.7z
28/10/2022 15:47 90 $IRRLUQI
06/11/2018 21:49 116 773 $RC8BA3T.pdf
01/05/2019 14:07 1 067 $RDSVH44.lnk
02/11/2018 17:06 129 desktop.ini
8 fichier(s) 118 523 octets
2 Rép(s) 230 804 840 448 octets libres
```

```
$IC8BA3T.pdf
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Texte Décodé
00000000 02 00 00 00 00 00 00 00 25 C8 01 00 00 00 00 00 .....%E.....
00000010 50 C5 35 82 F2 50 D9 01 34 00 00 00 43 00 3A 00 PÅs,ôPÜ.4...C.:.
00000020 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 6C 00 \.U.s.e.r.s.\.l.
00000030 61 00 75 00 72 00 65 00 6E 00 74 00 5C 00 44 00 a.u.r.e.n.t.\.D.
00000040 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 70 00 e.s.k.t.o.p.\.p.
00000050 64 00 66 00 5C 00 74 00 72 00 61 00 69 00 6E 00 d.f.\.t.r.a.i.n.
00000060 73 00 5F 00 32 00 35 00 5F 00 65 00 74 00 5F 00 s..2.5...e.t..
00000070 32 00 37 00 64 00 65 00 63 00 2E 00 70 00 64 00 2.7.d.e.c...p.d.
00000080 66 00 00 00 f...
```

RECYCLE BIN (ANALYSE)

<https://github.com/EricZimmerman/RBCmd>

```
Command line: -d c:\$Recycle.Bin\S-1-5-21-2510752544-4166367489-199343150-1001
Warning: Administrator privileges not found!
```

```
Looking for files in c:\$Recycle.Bin\S-1-5-21-2510752544-4166367489-199343150-1001
```

```
Found 5 files. Processing...
```

```
Source file: c:\$Recycle.Bin\S-1-5-21-2510752544-4166367489-199343150-1001\IC8BA3T.pdf
```

```
Version: 2 (Windows 10/11)
```

```
File size: 116 773 (114KB)
```

```
File name: C:\Users\laurent\Desktop\pdf\trains_25_et_27dec.pdf
```

```
Deleted on: 2023-03-07 13:44:08
```

```
Source file: c:\$Recycle.Bin\S-1-5-21-2510752544-4166367489-199343150-1001\IDSVH44.lnk
```

```
Version: 2 (Windows 10/11)
```

```
File size: 1 067 (1KB)
```

```
File name: C:\Users\laurent\Desktop\pdf\FastRawViewer Manual.lnk
```

```
Deleted on: 2023-03-07 13:44:19
```

SHADOW COPIES

Sauvegardes automatiques des fichiers critiques du système,
comme le registre

VSS = Volume Shadow Service

- Une fois par semaine pour les desktops
- Une fois par jour pour les serveurs

Existe depuis Vista

> **Vssadmin** list shadows

```
Administrateur : Invite de commandes
C:\WINDOWS\system32>vssadmin list shadows
vssadmin 1.1 - Outil ligne de commande d'administration du service de cliché instantané de volume
(C) Copyright 2001-2013 Microsoft Corp.

Contenu du jeu de clichés instantanés n° : {5d06d4dc-3b57-45af-8cc6-1efef1602b84}
  Contenait 1 clichés instantanés à la date de création : 23/02/2023 21:17:32
    ID du cliché instantané : {e3f63594-9731-44fd-a7c2-618c92eeed95}
    Volume original : (C:)\\?\Volume{41e9c01d-9d10-4990-a134-964aab82c20c}\
    Volume de cliché instantané : \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
    Ordinateur d'origine : DESKTOP-5B94HCL
    Ordinateur de service : DESKTOP-5B94HCL
    Fournisseur : 'Microsoft Software Shadow Copy provider 1.0'
    Type : ClientAccessibleWriters
    Attributs : Persistent, Accessible par client, Pas de libération automatique, Différentielle,

Contenu du jeu de clichés instantanés n° : {25800c2a-8154-4070-bb04-5a400716d183}
  Contenait 1 clichés instantanés à la date de création : 06/03/2023 13:43:55
    ID du cliché instantané : {f29765d4-1ee6-432e-a31a-6533e1c7de31}
    Volume original : (C:)\\?\Volume{41e9c01d-9d10-4990-a134-964aab82c20c}\
    Volume de cliché instantané : \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4
    Ordinateur d'origine : DESKTOP-5B94HCL
    Ordinateur de service : DESKTOP-5B94HCL
    Fournisseur : 'Microsoft Software Shadow Copy provider 1.0'
    Type : ClientAccessibleWriters
    Attributs : Persistent, Accessible par client, Pas de libération automatique, Différentielle,
```

SHADOW COPY (ACCÈS LIVE)

Avec <https://github.com/EricZimmerman/VSCMount>

En temps qu'admin

On retourne dans le passé !

```
Le numéro de série du volume est 7647-5582
Répertoire de I:\2600_for\VSCMount\vss_mp_C\vss003-20230223T201732.4448390
14/05/2021  22:11    <DIR>        avast! sandbox
29/12/2021  15:55    <DIR>        bin
17/12/2020  22:41    <DIR>        cygwin64
03/04/2020  21:35    <DIR>        Go
02/11/2018  20:40    <DIR>        Intel
30/12/2018  19:27    <DIR>        MinGW
13/04/2020  16:21    <DIR>        mozilla-build
07/05/2020  21:59    <DIR>        mozilla-central
07/12/2019  10:14    <DIR>        PerfLogs
14/02/2023  20:25    <DIR>        Program Files
22/02/2023  20:58    <DIR>        Program Files (x86)
09/05/2022  21:10    <DIR>        Python27
09/05/2022  21:10    <DIR>        Python27amd64
08/12/2018  13:24    <DIR>        Strawberry
13/11/2022  18:07    <DIR>        Users
14/02/2023  23:04    <DIR>        Windows
            0 fichier(s)                0 octets
            16 Rép(s)  233 500 205 056 octets libres
```

Ces données
datent du 23/02,
nous sommes le
7/03 !

```
Administrateur : Invite de commandes

I:\2600_for\VSCMount>VSCMount.exe --dl c --mp vss_mp
VSCMount version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/VSCMount

Command line: --dl c --mp vss_mp

Creating directory vss_mp_C
Mounting VSCs to vss_mp_C

VSCs found on volume C: 2. Mounting...
VSS 3 (Id {e3f63594-9731-44fd-a7c2-6f8c92eed95}, Created on: 2023-02-23 20:17:32.4448390 UTC) mounted OK!
VSS 4 (Id {f29765d4-1ee6-432e-a31a-6533e1c7de31}, Created on: 2023-03-06 12:43:55.0790390 UTC) mounted OK!

Mounting complete. Navigate VSCs via symbolic links in vss_mp_C

To remove VSC access, delete individual VSC directories or the main mountpoint directory
```

SHADOW COPY (ACCÈS OFFLINE)

Using SANS SIFT VM, for example

1. Ewfmount, to mount the EWF image
 2. Vshadowmount, to mount shadow copy volumes
- <https://github.com/libyal/libewf/tree/main/ewftools> (Joachim Metz)
 - See <https://www.youtube.com/watch?v=qYTVRjb7Krl> (13cubed)
 - SANS SIFT : <https://www.sans.org/tools/sift-workstation/>

MINIATURES, THUMBS.DB (XP)

Fichier cache situé dans chaque répertoire contenant des images

Au format OLE Compound File (comme .doc)

Aussi parfois sous Win7/8/8.1

Vinetto pour analyser ce format (Linux)

<http://vinetto.sourceforge.net/>

MiTEC WFA (Windows)

<http://www.mitec.cz/wfa.html>

MINIATURES, THUMBCACHE (VISTA)

Dans

`\Users\%username%\AppData\Local\Microsoft\Windows\Explorer`

Thumbcache viewer (Windows)

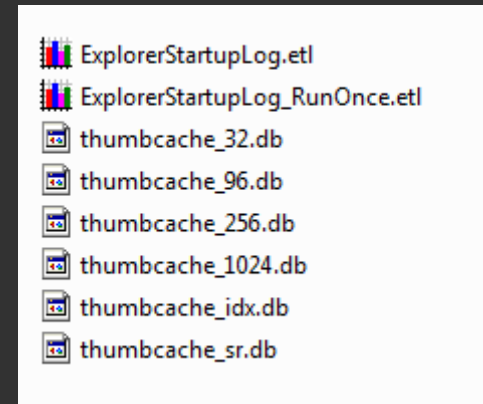
<https://code.google.com/p/thumbcache-viewer/>

Windows thumbcache DB library:

<https://github.com/libyal/libwtcdb/wiki>

<https://github.com/libyal/libwtcdb/>

Par Joachim Metz



LE REGISTRE

- Base de données organisées en arbres et clé/valeurs, en plusieurs ruches/hives
- Registres système
 - %SystemRoot%\System32\Config
 - HKEY_LOCAL_MACHINE (HKLM)
 - System
 - Software
 - SAM
 - Security
 - HKEY_USERS\DEFAULT
 - Default
 - HKEY_CURRENT_CONFIG (HKCC), points to
HKLM\SYSTEM\CurrentControlSet\CurrentControlSet\HardwareProfiles\Current
- Registre Utilisateur, HKEY_CURRENT_USER (HKCU)
 - %UserProfile%\NTUSER.DAT
 - C:\Users\laurent\NTUSER.DAT
 - %UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat

LE REGISTRE (SYSTÈME)

(extrait)

```
Répertoire de c:\Windows\System32\config
07/12/2019 10:14 <DIR> Journal
07/12/2019 10:14 <DIR> RegBack
14/02/2023 23:06      32 768 SAM
07/12/2019 10:03      32 768 SAM.LOG1
07/12/2019 10:03      28 672 SAM.LOG2
07/12/2019 16:40      65 536 SAM{53b39e57-18c4-11ea-a811-000d3aa4692b}.TM.blf
07/12/2019 16:40     524 288 SAM{53b39e57-18c4-11ea-a811-000d3aa4692b}.TMContainer000000000000000001.regtrans-ms
07/12/2019 16:40     524 288 SAM{53b39e57-18c4-11ea-a811-000d3aa4692b}.TMContainer000000000000000002.regtrans-ms
14/02/2023 23:06      65 536 SECURITY
07/12/2019 10:03          0 SECURITY.LOG1
07/12/2019 10:03      16 384 SECURITY.LOG2
07/12/2019 16:40      65 536 SECURITY{53b39e4b-18c4-11ea-a811-000d3aa4692b}.TM.blf
07/12/2019 16:40     524 288 SECURITY{53b39e4b-18c4-11ea-a811-000d3aa4692b}.TMContainer000000000000000001.regtrans-ms
07/12/2019 16:40     524 288 SECURITY{53b39e4b-18c4-11ea-a811-000d3aa4692b}.TMContainer000000000000000002.regtrans-ms
14/02/2023 23:06     196 345 856 SOFTWARE
07/12/2019 10:03      25 165 824 SOFTWARE.LOG1
07/12/2019 10:03      31 981 568 SOFTWARE.LOG2
07/12/2019 16:40      65 536 SOFTWARE{53b39e2f-18c4-11ea-a811-000d3aa4692b}.TM.blf
07/12/2019 16:40     524 288 SOFTWARE{53b39e2f-18c4-11ea-a811-000d3aa4692b}.TMContainer000000000000000001.regtrans-ms
07/12/2019 16:40     524 288 SOFTWARE{53b39e2f-18c4-11ea-a811-000d3aa4692b}.TMContainer000000000000000002.regtrans-ms
14/02/2023 23:06      26 476 544 SYSTEM
07/12/2019 10:03          5 832 704 SYSTEM.LOG1
07/12/2019 10:03          6 573 056 SYSTEM.LOG2
07/12/2019 10:14 <DIR> systemprofile
07/12/2019 16:40      65 536 SYSTEM{53b39e3e-18c4-11ea-a811-000d3aa4692b}.TM.blf
07/12/2019 16:40     524 288 SYSTEM{53b39e3e-18c4-11ea-a811-000d3aa4692b}.TMContainer000000000000000001.regtrans-ms
07/12/2019 16:40     524 288 SYSTEM{53b39e3e-18c4-11ea-a811-000d3aa4692b}.TMContainer000000000000000002.regtrans-ms
17/09/2021 22:35 <DIR> TxR
```

LE REGISTRE

Pour extraire la ruche/hive **system**, il est préférable d'extraire les fichiers *.log? (les transactions logs):
system, system.**log1**, system.**log2**

- <https://www.mandiant.com/resources/blog/digging-up-the-past-windows-registry-forensics-revisited> (2019, FireEye)
- <https://github.com/msuhanov/regf/blob/master/Windows%20registry%20file%20format%20specification.md> (2015-2018, Maxim Suhanov)
- [https://github.com/libyal/libregf/blob/main/documentation/Windows%20NT%20Registry%20File%20\(REGF\)%20format.asciidoc](https://github.com/libyal/libregf/blob/main/documentation/Windows%20NT%20Registry%20File%20(REGF)%20format.asciidoc) (2009-2021, Joachim Metz)

LE REGISTRE : POUR LE FORENSIC

Le registre se trouve aussi via les shadow copy et en RAM.

On peut faire aussi du forensic sur la base de données elle-même, sur les clés effacées ou sur les dates (last write timestamp)

Voir : <https://www.inversecos.com/2022/04/malicious-registry-timestamp.html>

LE REGISTRE : DEVICES USB

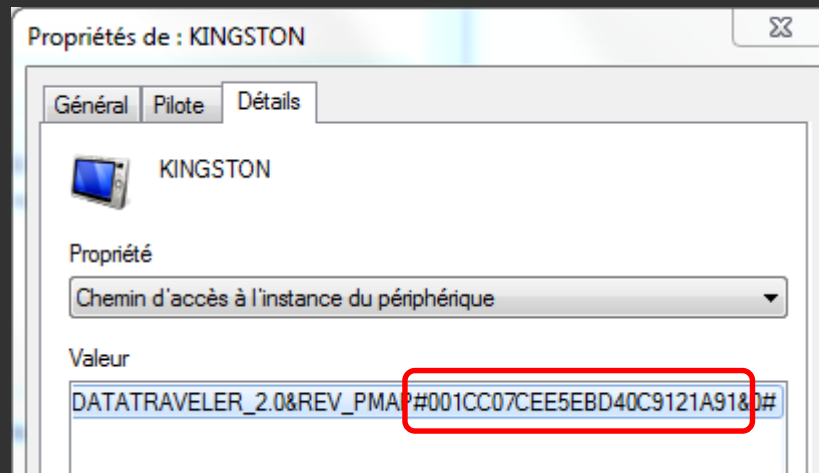
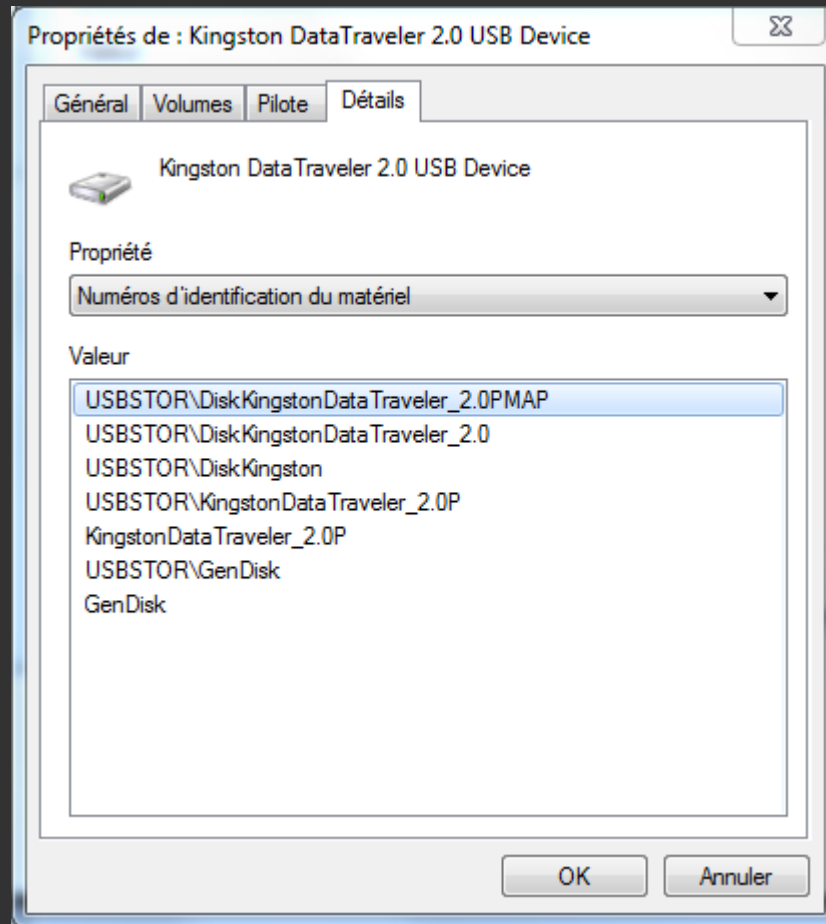
Retrouver les artefacts relatifs à l'utilisation d'un stockage USB

- Première et dernière utilisation d'un périphérique donné (en utilisant le S/N and Volume ID)
- Quel utilisateur est concerné ?

Windows stocke ces informations dans la **base de registres** et le journal **setupapi.dev.log**

https://www.researchgate.net/publication/318514858_USB_Storage_Device_Forensics_for_Windows_10

LE REGISTRE : PROPRIÉTÉS USB



S/N

CLÉS DE REGISTRE USBSTOR ET WINDOWS PORTABLE DEVICES

Éditeur du Registre

Fichier Edition Affichage Favoris ?

USB
USBPRINT
USBSTOR

Class=Disk, Vendor=Kingston, Product=DataTraveler 2.0

Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
Capabilities	REG_DWORD	0x00000010 (16)
Class	REG_SZ	DiskDrive
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{f0dc0163-982c-5adc-88d8-76e8702d2402}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Lecteur de disque
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0025
FriendlyName	REG_SZ	Kingston DataTraveler 2.0 USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskKingstonDataTraveler_2.0\PMAP USBSTOR\DiskKingstonDataTraveler_2.0 USBSTOR\DiskKingston USBSTOR\Kin
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Lecteurs de disque standard)
Service	REG_SZ	disk

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Kingston&Prod_DataTraveler_2.0&Rev_PMAP\001CC07CEE5EBD40C9121A91&0

Éditeur du Registre

Fichier Edition Affichage Favoris ?

USB#VID_22B8&PID_2E82#ZX183282ST

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_&PROD_&REV_1.00#001CC0830384F060E0C602EC&0#

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_&PROD_&REV_1.00#001CC0EC32C7AD406711B864&0#

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_&PROD_&REV_1.00#001CC0EC32FEAD40670FB889&0#

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_&PROD_&REV_1.00#001CC0EC347CAD40671CB893&0#

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_&PROD_USB_DISK_2.0&REV_PMAP#0791175A0111&0#

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_CANON&PROD_MP620_SERIES&REV_0108#8&FB066B7&0&229B83&0#

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_GT-15700&PROD_-_CARD#57006044A285&0#

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_HTC&PROD_ANDROID_PHONE&REV_0100#HT05LPL03797&0#

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_JETFLASH&PROD_TRANSCEND_8GB&REV_8.07#4EWSLSMC&0#

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_KINGSTON&PROD_DATATRAVELER_109&REV_PMAP#001D7D06ED29BBA1B000006A&0#

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_KINGSTON&PROD_DATATRAVELER_2.0&REV_PMAP#001CC07CEE5EBD40C9121A91&0#

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_KINGSTON&PROD_DATATRAVELER_2.0&REV_PMAP#001D0F0CAAB55B88050105F0&0#

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_KINGSTON&PROD_DATATRAVELER_G2&REV_1.00#000FEAFD3EAEF9A0A7630BB1&0#

WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_KINGSTON&PROD_DATATRAVELER_G3&REV_1.00#001372A609DDAAC0C51A003C&0#

Ordinateur\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Portable Devices\Devices\WPDBUSENUMROOT#UMB#2&37C186B&0&STORAGE#VOLUME#_??_USBSTOR#DISK&VEN_KINGSTON&PROD_DATATRAVELER_2.0&REV_PMAP#001CC07CEE5EBD40C9121A91&0

MÉTHODE (WIN7-10)

SYSTEM\CurrentControlSet\Enum\USBSTOR:
vendeur, produit, S/N.

SYSTEM\MountedDevices:
lettre du lecteur ou Volume ID (en utilisant le S/N)

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2:
liste tous les Device GUID utilisé par l'utilisateur. Toutes les ruches (hive) de chaque utilisateurs doivent être testées

SYSTEM\CurrentControlSet\Enum\USB:
dernière connexion

Setupapi.dev.log:
première connexion

EXERCICE

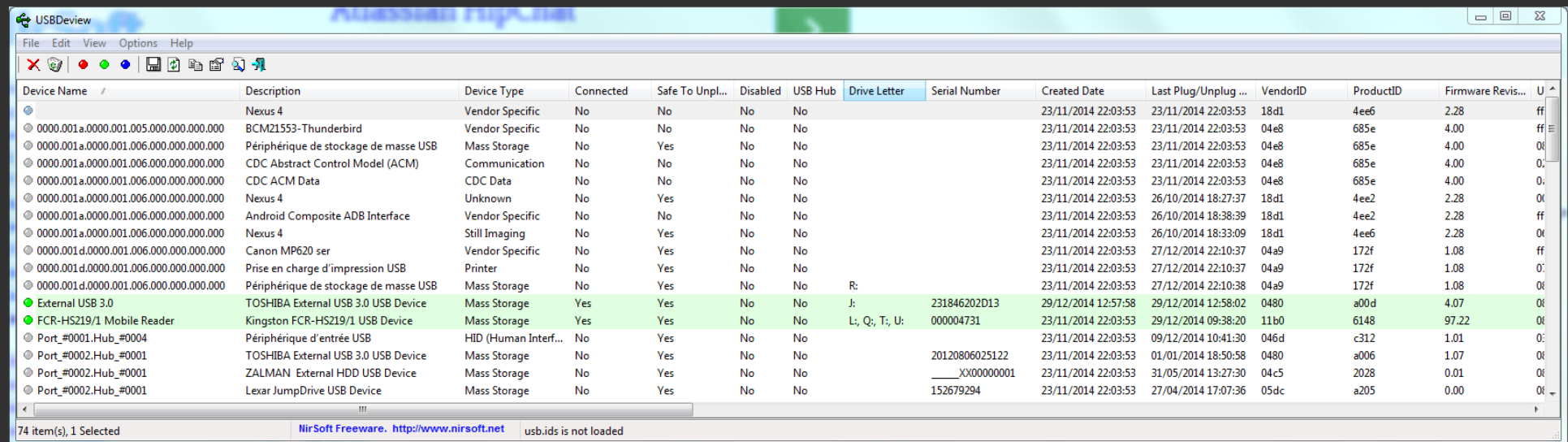
Cet après-midi avec RegRipper

USB, LIVE FORENSIC

USBDeview de NirSoft

Freeware

Pas d'installation nécessaire



The screenshot shows the USBDeview application window. The title bar reads 'USBDeview'. The menu bar includes 'File', 'Edit', 'View', 'Options', and 'Help'. Below the menu bar is a toolbar with various icons. The main area is a table listing USB devices. The table has columns: Device Name, Description, Device Type, Connected, Safe To Unpl..., Disabled, USB Hub, Drive Letter, Serial Number, Created Date, Last Plug/Unplug..., VendorID, ProductID, Firmware Revis..., and a final column with a small icon. The table contains 74 items, with the first item selected. The status bar at the bottom indicates '74 item(s), 1 Selected' and provides a link to 'NirSoft Freeware, http://www.nirsoft.net'.

Device Name	Description	Device Type	Connected	Safe To Unpl...	Disabled	USB Hub	Drive Letter	Serial Number	Created Date	Last Plug/Unplug ...	VendorID	ProductID	Firmware Revis...	
Nexus 4		Vendor Specific	No	No	No	No			23/11/2014 22:03:53	23/11/2014 22:03:53	18d1	4ee6	2.28	ff
0000.001a.0000.001.005.000.000.000.000	BCM21553-Thunderbird	Vendor Specific	No	No	No	No			23/11/2014 22:03:53	23/11/2014 22:03:53	04e8	685e	4.00	ff
0000.001a.0000.001.006.000.000.000.000	Périphérique de stockage de masse USB	Mass Storage	No	Yes	No	No			23/11/2014 22:03:53	23/11/2014 22:03:53	04e8	685e	4.00	00
0000.001a.0000.001.006.000.000.000.000	CDC Abstract Control Model (ACM)	Communication	No	No	No	No			23/11/2014 22:03:53	23/11/2014 22:03:53	04e8	685e	4.00	00
0000.001a.0000.001.006.000.000.000.000	CDC ACM Data	CDC Data	No	No	No	No			23/11/2014 22:03:53	23/11/2014 22:03:53	04e8	685e	4.00	00
0000.001a.0000.001.006.000.000.000.000	Nexus 4	Unknown	No	Yes	No	No			23/11/2014 22:03:53	26/10/2014 18:27:37	18d1	4ee2	2.28	00
0000.001a.0000.001.006.000.000.000.000	Android Composite ADB Interface	Vendor Specific	No	No	No	No			23/11/2014 22:03:53	26/10/2014 18:38:39	18d1	4ee2	2.28	ff
0000.001a.0000.001.006.000.000.000.000	Nexus 4	Still Imaging	No	Yes	No	No			23/11/2014 22:03:53	26/10/2014 18:33:09	18d1	4ee6	2.28	00
0000.001d.0000.001.006.000.000.000.000	Canon MP620 ser	Vendor Specific	No	Yes	No	No			23/11/2014 22:03:53	27/12/2014 22:10:37	04a9	172f	1.08	ff
0000.001d.0000.001.006.000.000.000.000	Prise en charge d'impression USB	Printer	No	Yes	No	No			23/11/2014 22:03:53	27/12/2014 22:10:37	04a9	172f	1.08	00
0000.001d.0000.001.006.000.000.000.000	Périphérique de stockage de masse USB	Mass Storage	No	Yes	No	No	R:		23/11/2014 22:03:53	27/12/2014 22:10:38	04a9	172f	1.08	00
External USB 3.0	TOSHIBA External USB 3.0 USB Device	Mass Storage	Yes	Yes	No	No	J:	231846202D13	29/12/2014 12:57:58	29/12/2014 12:58:02	0480	a00d	4.07	00
FCR-HS219/1 Mobile Reader	Kingston FCR-HS219/1 USB Device	Mass Storage	Yes	Yes	No	No	L; Q; T; U:	000004731	23/11/2014 22:03:53	29/12/2014 09:38:20	11b0	6148	97.22	00
Port_#0001.Hub_#0004	Périphérique d'entrée USB	HID (Human Interf...	No	Yes	No	No			23/11/2014 22:03:53	09/12/2014 10:41:30	046d	c312	1.01	00
Port_#0002.Hub_#0001	TOSHIBA External USB 3.0 USB Device	Mass Storage	No	Yes	No	No		20120806025122	23/11/2014 22:03:53	01/01/2014 18:50:58	0480	a006	1.07	00
Port_#0002.Hub_#0001	ZALMAN External HDD USB Device	Mass Storage	No	Yes	No	No		XX00000001	23/11/2014 22:03:53	31/05/2014 13:27:30	04c5	2028	0.01	00
Port_#0002.Hub_#0001	Lexar JumpDrive USB Device	Mass Storage	No	Yes	No	No		152679294	23/11/2014 22:03:53	27/04/2014 17:07:36	05dc	a205	0.00	00

READYBOOST

Test de performance pour les périphériques externes, dont les résultats sont écrits dans la base de registre

SOFTWARE\Microsoft\Windows NT\CurrentVersion\Emdmngmt

« External Memory Device Management »

```
Disk&Ven_Kingston&Prod_DataTraveler_2.0&Rev_PMAP  
  LastWrite: Mon Apr 21 09:06:14 2014 Z  
  SN: 001D0F0CAAB55B88050105F0&0  
  Vol Name: KINGSTON  
  VSN: 0  
  LastTestedTime: Mon Apr 21 09:06:14 2014 Z
```

```
Disk&Ven_Kingston&Prod_DataTraveler_2.0&Rev_PMAP  
  LastWrite: Sat May 31 12:30:19 2014 Z  
  SN: 001D0F0CAAB55B88050105F0&0  
  Vol Name: MYLINUXLIVE  
  VSN: 8E12-F953
```

Voir <http://windowsir.blogspot.fr/2013/04/plugin-emdmngmt.html>

PREUVES D'EXÉCUTION DANS LE REGISTRE

Userassist

RunMRU

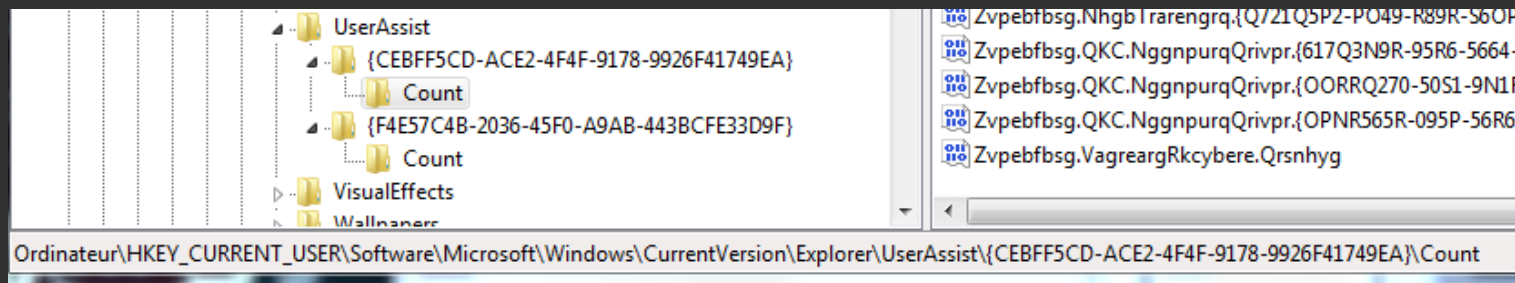
REGISTRE: USERASSIST

Exécutables fréquemment lancés par l'utilisateur via le Windows Shell
Indique le dernier lancement, la date et l'heure, le filepath et combien d'exécutions

Dans NTUSER.DAT:

- `Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist`

Les noms sont encodés en ROT13



Voir <http://windowsir.blogspot.fr/2007/09/more-on-userassist-keys.html>

USERASSIST

```
rip -r Users\laurent\NTUSER.DAT -p userassist
```

```
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Fri Dec 28 18:35:39 2012 (UTC)

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Wed Dec 24 13:31:02 2014 Z
  C:\MinGW\msys\1.0\msys.bat (6)
Wed Dec 24 13:25:58 2014 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Notepad++\notepad++.exe (10)  FOLDERID_ProgramFilesX86
Wed Dec 24 13:12:15 2014 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (9)  FOLDERID_System
Wed Dec 24 13:11:55 2014 Z
  Microsoft.AutoGenerated.{36DE05A7-E039-A6D1-4355-B3C0AF61F524} (4)
Wed Dec 24 10:37:39 2014 Z
  K:\afti_forensic\tools\Imager_Lite_3.1.1\FTK Imager.exe (1)
Wed Dec 24 10:34:52 2014 Z
  {F38BF404-1D43-42F2-9305-67DE0B28FC23}\explorer.exe (14)  FOLDERID_Windows
Wed Dec 24 10:19:42 2014 Z
  8216C80C92C4E828 (10)  Semble être WindowAppID Thunderbird
```

<http://msdn.microsoft.com/en-us/library/windows/desktop/dd378457%28v=vs.85%29.aspx>

RUNMRU (À PARTIR DE 2000/XP)

- Programmes lancés via le menu « démarrer »
- Software\Microsoft\Windows\CurrentVersion\Explorer\Run MRU
 - MRU=Most Recent Used

Bonus: List of Windows MRU location:

http://forensicswiki.org/wiki/List_of_Windows_MRU_Locations

DOCUMENTS RECENTS

RecentDocs

OpenRunSaveMRU / LastVisitedMRU

RECENTDOCS

Fichiers récemment utilisés

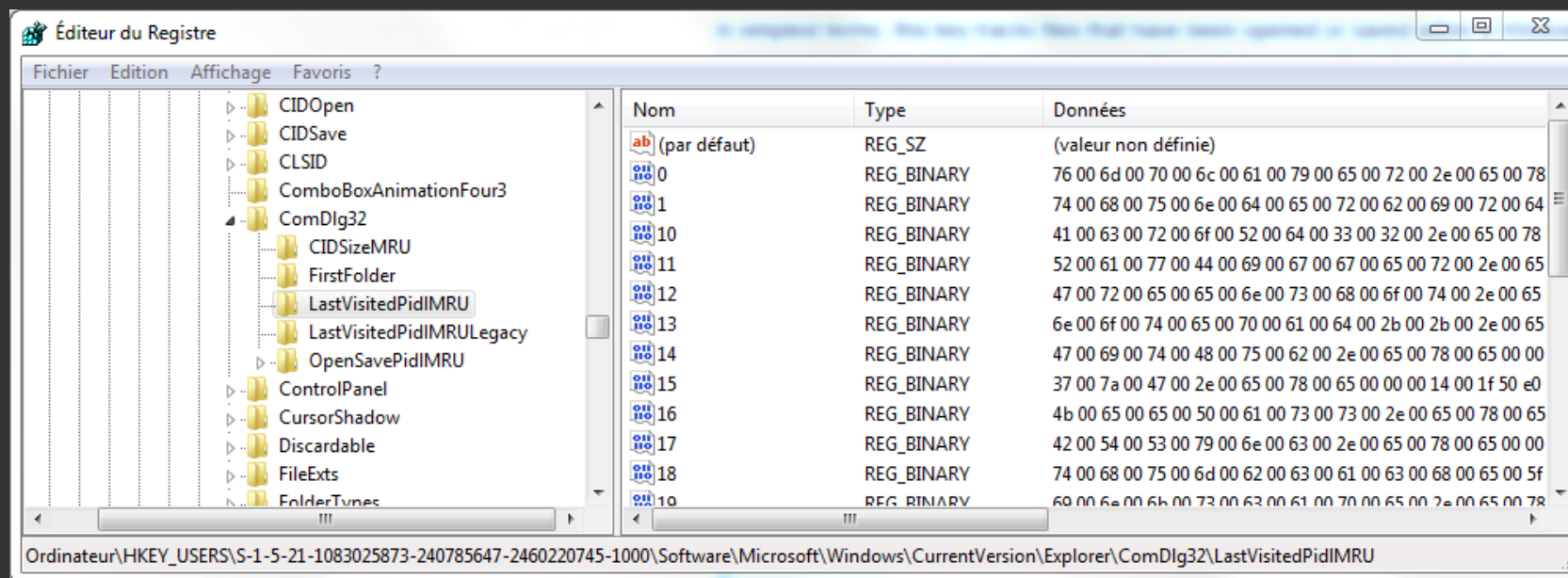
```
>rip.exe -r i:\dump_c_files\Users\laurent\NTUSER.DAT -p recentdocs
Launching recentdocs v.20100405
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key
```

```
RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Wed Dec 24 13:25:58 2014 (UTC)
56 = forensic
8 = for508_notes.txt
3 = afti_forensic
38 = notes.txt
86 = dump_c
50 = win.E01
97 = Imager_Lite_3.1.1.zip
48 = 3_windows.ppt
110 = usbdevview-x64.zip
149 = pdfid_v0_2_1.zip
140 = usp64.v.0.30.win
96 = usp_readme.htm
```

Voir <http://www.4n6k.com/2014/02/forensics-quickie-pinpointing-recent.html>

OPENRUNSAVEMRU ET LASTVISITEDMRU

Liste des fichiers récemment ouverts ou sauvegardés avec la fenêtre de dialogue Windows

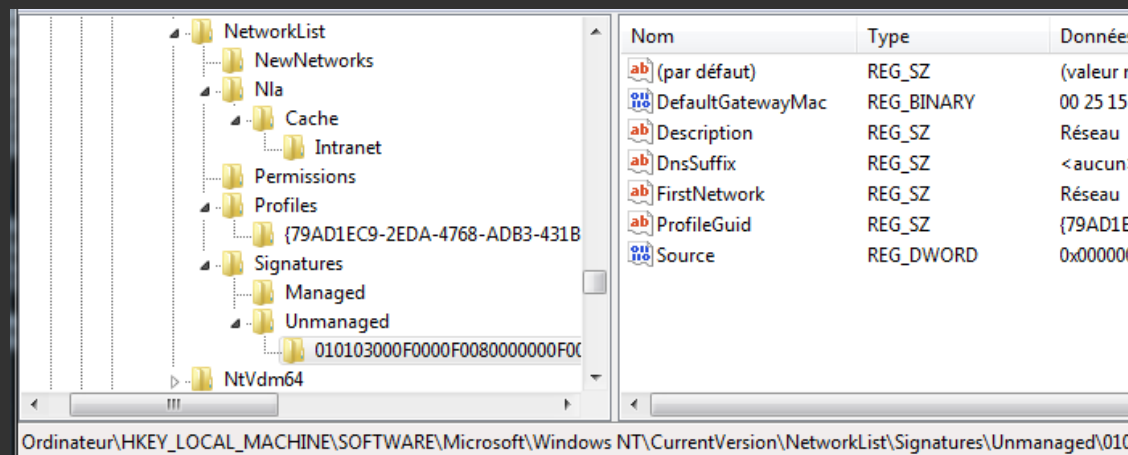


<https://www.sans.org/blog/opensavemru-and-lastvisitedmru/>

ENVIRONNEMENT

NetworkList

NETWORKLIST (DEPUIS VISTA)



```
>rip.exe -r i:\dump_c_files\software -p networklist
Launching networklist v.20141204
Launching networklist v.20141204
(Software) Collects network info from Vista+ NetworkList key
```

```
Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles
```

```
R\@seau
```

```
Key LastWrite      : Wed Dec 24 10:16:08 2014 UTC
DateLastConnected: Wed Dec 24 11:16:08 2014
DateCreated       : Fri Dec 28 19:36:39 2012
DefaultGatewayMac : 00-25-15-xx-xx-xx
Type              : wired
Category         : Private
```

Voir aussi le plugin SSID

See <http://forensicartifacts.com/2011/06/networklist-vistawindows-7/>

NETWORKLIST (VISTA)

Registry Explorer v1.0.0.4

File Tools Options Bookmarks (23/0) View Help

Registry hives (2) Available bookmarks (50/0)

Key name	# values	# subkeys	Last write timestamp
[-]			
ICM	0	2	2009-07-14 04:53:25
Image File Execution Options	0	2	2009-07-14 04:53:26
IniFileMapping	0	5	2009-07-14 04:53:25
InstalledFeatures	0	1	2009-07-14 04:53:25
KnownFunctionTableDlls	1	0	2015-09-09 15:14:44
KnownManagedDebuggingDlls	1	0	2015-09-09 15:14:44
LanguagePack	1	2	2009-07-14 04:53:25
MCI Extensions	50	0	2009-07-14 05:09:22
MCI32	5	0	2009-07-14 04:53:25
MiniDumpAuxiliaryDlls	1	0	2015-09-09 15:14:44
MsiCorruptedFileRecovery	0	1	2009-07-14 04:53:25
Multimedia	0	1	2009-07-14 04:53:25
NetworkCards	0	1	2015-09-09 14:16:57
NetworkList	2	5	2015-09-09 14:17:01
NtVdm64	0	8	2009-07-14 04:53:25
NvCache	0	0	2009-07-14 05:09:34
OpenGLDrivers	0	0	2009-07-14 04:53:25
PeerDist	0	6	2009-07-14 11:22:23
PeerNet	0	2	2009-07-14 04:53:25
Perfib	5	3	2015-09-10 08:58:55
PerHwIdStorage	1	131	2009-07-14 04:53:25
Ports	11	0	2009-07-14 05:09:04

[-] Microsoft\Windows NT\CurrentVersion\NetworkList

Selected hive: software Last write: 2015-09-09 14:17:01 2 of 2 values shown (100,00 %) Load complete

Values Known networks

Drag a column header here to group by that column

Network N...	Name Type	First Connect LOCAL	Last Connected LOCAL	Managed	DNS Suffix	Gateway Mac Address	Profile GUID
[-]							
Réseau 3	Wired	2015-09-10 10:31:26	2015-09-10 10:52:22	<input type="checkbox"/>	home	6C-2E-85-D1-0E-12	{9C21AFC9-AA62-4B8C-A91A-065A40D2FB7A}
Réseau 2	Wired	2015-09-09 23:10:16	2015-09-10 10:23:39	<input type="checkbox"/>	localdomain	00-50-56-FE-F4-1B	{D7A41D39-FFF1-4B44-8D8B-06358AE35B53}
Réseau	Wired	2015-09-09 16:17:01	2015-09-09 16:20:50	<input type="checkbox"/>	localdomain	00-50-56-EB-BD-14	{FE5703AE-AD63-4BF7-894E-86F13D5AC1E7}

Total rows: 3 Export ?

Type viewer Slack viewer Binary viewer

Value name (default) Value: (default) Collapse all hives

Hidden keys: 0 30

NETWORKLIST (EXERCICE)

Avec RegRipper

Utilisation de RawCopy pour copier un fichier protégé par le système

PERSISTENCE

Run keys (registry)

Scheduled Tasks

Services

WMI

...

PERSISTANCE: AUTO RUNS

Liste des logiciels lancés au démarrage de Windows ou de la session

- HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

Outils Autoruns (Live):

<http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx>

Volatility plug-in (Thomas Chopita)

<https://github.com/tomchop/volatility-autoruns>

```
$ python vol.py --plugins=/c/Users/lclevy/Documents/volatility-autoruns-master -f memdump.mem --profile=WinXPSP3x86 autoruns >autoruns.txt
```


PERSISTENCE : SCHEDULED TASKS

In filesystem:

- %SystemRoot%\System32\Tasks
- %SystemRoot%\Tasks

In Registry:

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\Taskcache\Tasks
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\Taskcache\Tree

<https://nasbench.medium.com/a-deep-dive-into-windows-scheduled-tasks-and-the-processes-running-them-218d1eed4cce>

JOURNAUX

Etvx

Journaux des AV et EDR

JOURNAUX DES ÉVÉNEMENTS

```
Répertoire de c:\Windows\System32\winevt\Logs
05/11/2022 13:49 <DIR> .
05/11/2022 13:49 <DIR> ..
08/03/2023 21:25 18 944 000 Application.evtx
30/08/2020 15:33 69 632 HardwareEvents.evtx
30/08/2020 15:33 69 632 Internet Explorer.evtx
30/08/2020 15:33 69 632 Key Management Service.evtx
08/03/2023 19:12 1 052 672 Microsoft-Client-Licensing-Platform%4Admin.evtx
13/11/2022 18:07 69 632 Microsoft-Windows-AAD%4Operational.evtx
08/03/2023 19:10 1 052 672 Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx
30/08/2020 15:50 69 632 Microsoft-Windows-Application-Experience%4Program-Compatibility-Troubleshooter.evtx
30/08/2020 15:50 69 632 Microsoft-Windows-Application-Experience%4Program-Inventory.evtx
08/03/2023 19:12 1 052 672 Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx
30/08/2020 15:50 69 632 Microsoft-Windows-Application-Experience%4Steps-Recorder.evtx
08/03/2023 19:12 1 052 672 Microsoft-Windows-AppModel-Runtime%4Admin.evtx
```

La taille maximale par défaut est de 20Mb, soit quelques jours à quelques semaines selon l'activité...

Il faut envoyer les journaux critiques dans un SIEM !

JOURNAUX EVTX, LES PLUS INTÉRESSANTS

`Application.evtx`

`Microsoft-Windows-Bits-Client%4Operational.evtx`

`Microsoft-Windows-Kernel-EventTracing%4Admin.evtx`

`Microsoft-Windows-PowerShell%4Admin.evtx`, `Microsoft-Windows-PowerShell%4Operational.evtx`

`Microsoft-Windows-RemoteAssistance%4Admin.evtx`, `Microsoft-Windows-RemoteAssistance%4Operational.evtx`

`Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx`, `Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx`

`Microsoft-Windows-SmbClient%4Audit.evtx`, `Microsoft-Windows-SmbClient%4Connectivity.evtx`, `Microsoft-Windows-SMBClient%4Operational.evtx`,

`Microsoft-Windows-SmbClient%4Security.evtx`,

`Microsoft-Windows-SMBServer%4Audit.evtx`, `Microsoft-Windows-SMBServer%4Connectivity.evtx`, `Microsoft-Windows-SMBServer%4Operational.evtx`,

`Microsoft-Windows-SMBServer%4Security.evtx`

`Microsoft-Windows-TaskScheduler%4Maintenance.evtx`

`Microsoft-Windows-TerminalServices-LocalSessionManager%4Admin.evtx`, `Microsoft-Windows-TerminalServices-`

`LocalSessionManager%4Operational.evtx`

`Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.evtx`, `Microsoft-Windows-TerminalServices-`

`RemoteConnectionManager%4Operational.evtx`

`Microsoft-Windows-WebAuthN%4Operational.evtx`

`Microsoft-Windows-Windows Defender%4Operational.evtx`, `Microsoft-Windows-Windows Defender%4WHC.evtx`

`Microsoft-Windows-Windows Firewall With Advanced Security%4ConnectionSecurity.evtx`, `Microsoft-Windows-Windows Firewall With Advanced`

`Security%4Firewall.evtx`, `Microsoft-Windows-Windows Firewall With Advanced Security%4FirewallDiagnostics.evtx`

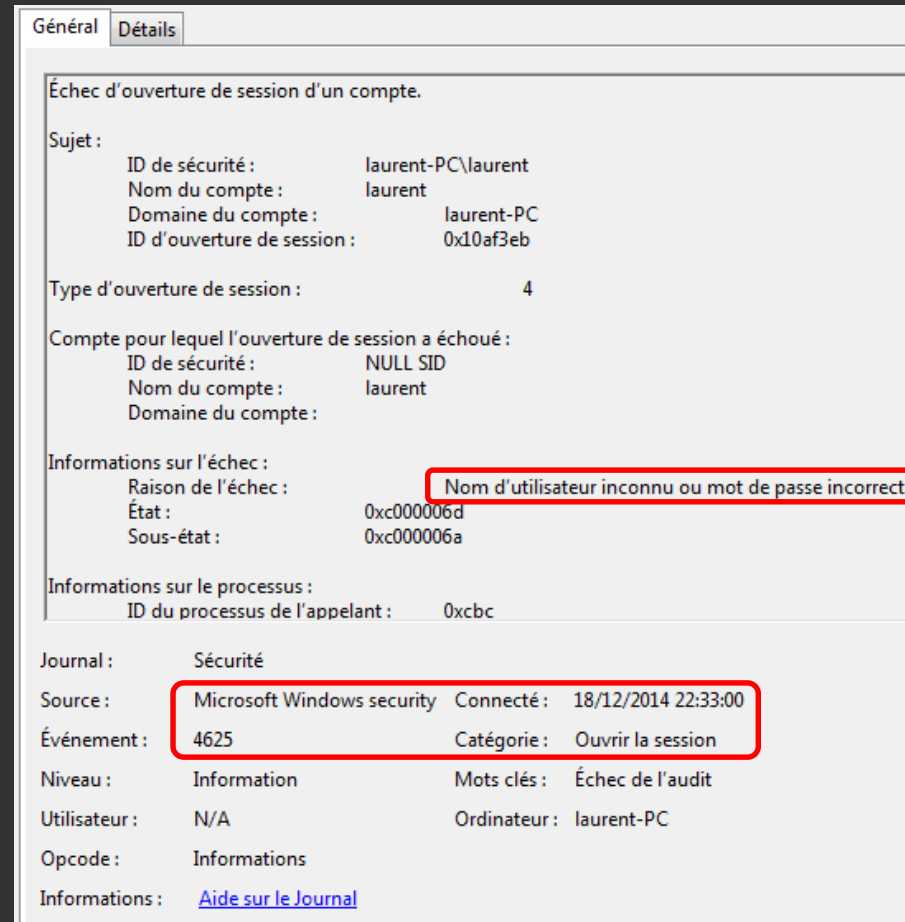
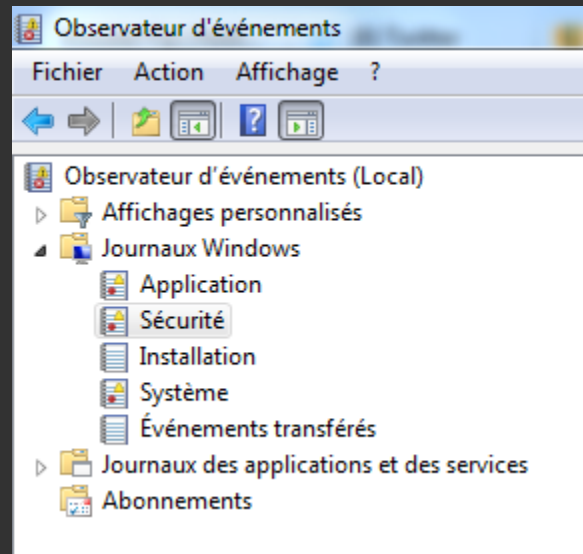
`Microsoft-Windows-Winlogon%4Operational.evtx`

`Microsoft-Windows-WMI-Activity%4Operational.evtx`

`Security.evtx`

`System.evtx`

JOURNAL DES ÉVÉNEMENTS SÉCURITÉ



JOURNAUX DES ÉVÉNEMENTS

Type d'événement	Event ID sous XP/2000	Event ID à partir de Vista (+4096)
User logon/logoff events	Successful logon 528, 540; failed logon 529-537, 539; logoff 538, 551, etc	Successful logon 4624, 4636; failed logon 4625-4633, 4635; logoff 4634, 4647, etc
User account changes	Created 624; enabled 626; changed 642; disabled 629; deleted 630	Created 4720; enabled 4722; changed 4738; disabled 4725; deleted 4726
Password changes	To self: 628; to others: 627	To self: 4724; to others: 4723
Service started or stopped	7035, 7036, etc.	11131, 11132, etc.
Object access denied (if auditing enabled)	560, 567, etc	4656, 4663, etc

La plupart des événements ne sont stockés que sur le Domain Controller.

Source: <http://zeltser.com/log-management/security-incident-log-review-checklist.html>

WINDOWS 10

Voir slides de Brent Muir:

<http://fr.slideshare.net/bsmuir/windows-10-forensics-os-evidentiary-artefacts>

- Windows Store,
- Cortana (contacts, location, online search)
- Applications Metro UI
 - Installées dans « \Program Files\WindowsApp »
 - Données dans %userprofile%\AppData\Local\Package\...
 - Base de données SQL ou .EDB
- Edge Browser (historique et cookies dans WebCache*.edb).
 - La session active est stockée
- Unified Communication (Skype, LinkedIn, Twitter, Windows Live),
- OneDrive,
- Maps (Long/Lat searched)

LIVRES DE RÉFÉRENCES

- Windows Forensic analysis, 3rd edition (Win7), Harlan Carvey <http://www.amazon.fr/Windows-Forensic-Analysis-Toolkit-Third/dp/BooE282JXM/>
- Windows Forensic analysis, 4th edition (Win8.1), Harlan Carvey <http://www.amazon.fr/Windows-Forensic-Analysis-Toolkit-Techniques-ebook/dp/BooJ997LYQ/>
- The Art of Memory Forensic <http://www.amazon.fr/The-Art-Memory-Forensics-Detecting-ebook/dp/BooJUUZSQC/>