

Panorama des outils d'investigations pour les recherches de trace sur internet

Détail des nouveautés IE10 et IE11

23 septembre 2014

Jean-Philippe NOAT - URIEL EXPERT
Instructeur Encase
EnCE 15-0914-6379





Panorama des outils d'investigations
pour les recherches de trace sur internet

Liste des outils analysés

- Encase 7.10
- Net Analysis 2.0
- IEF 6.4.2
- Belkasoft Evidence Center Ultimate 6.3
- Et demain ?
- Application pratique : IE 10 et IE 11





Encase 7

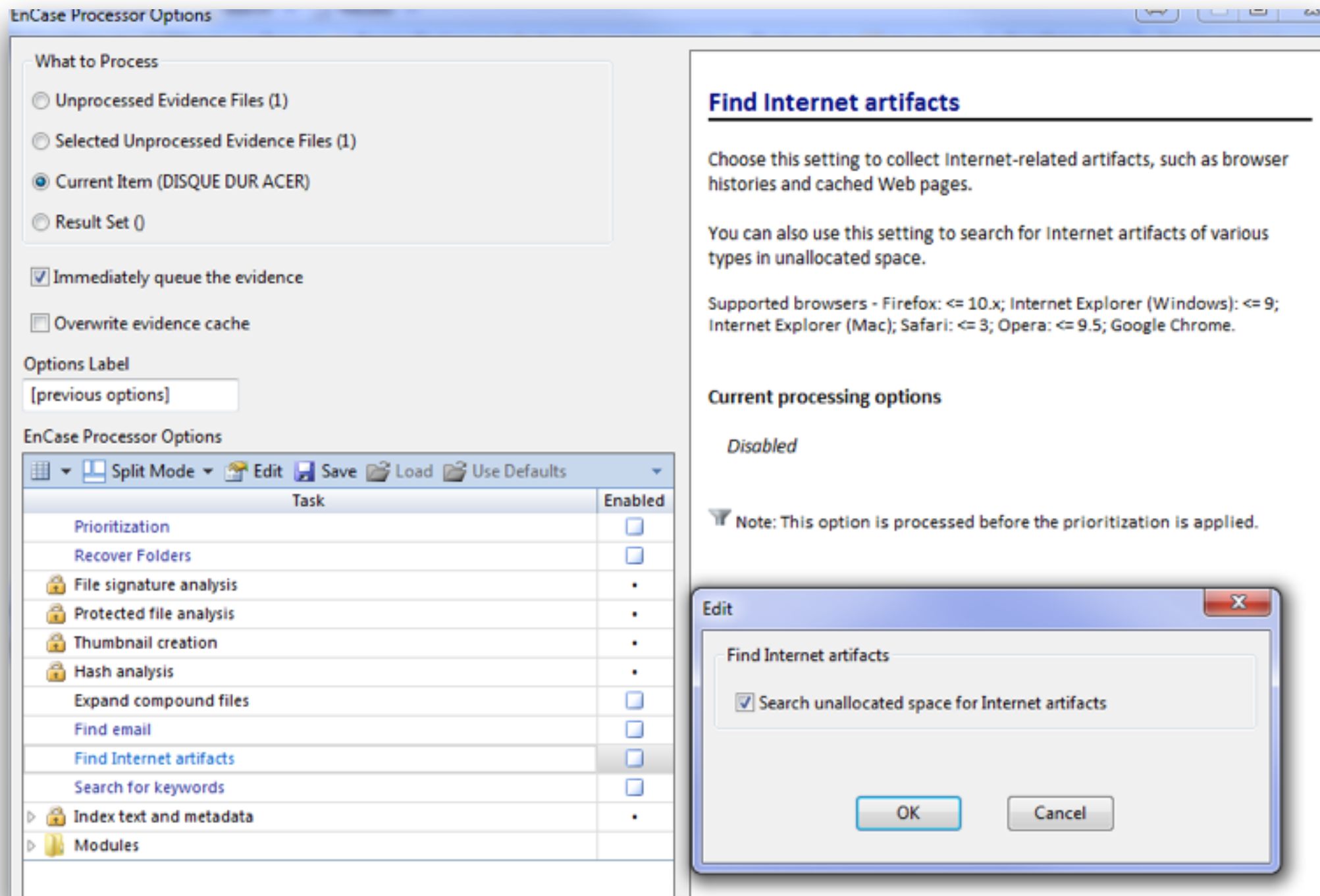


Encase 7.10

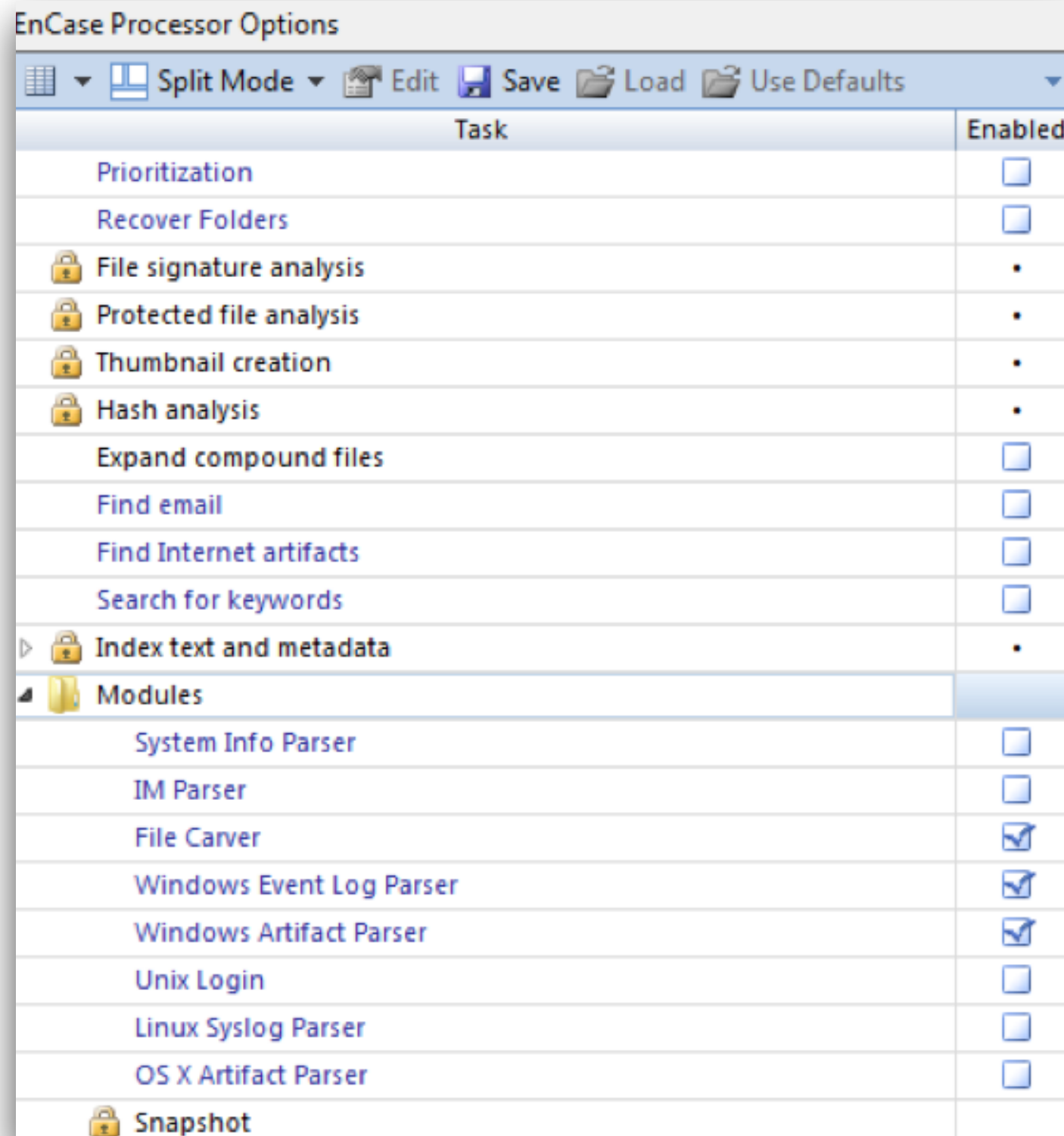
- Outil d'investigation numérique global
- Fait au départ pour traiter un dossier de A à Z.
- Possibilité d'extension via Enscript
- Traces internet recherchées via l'Evidence Processor
- Relativement pauvre en recherches spécialisées (Ex traces gmail)
- La référence mondiale
- Investigation en réseau native (Entreprise)



Encase : recherche de trace via l'evidence processor



Encase : les options de l'evidence processor



Avantages d'Encase

- Gestion des signets (raw text et transcript)
- Recherche brute et indexée
- Rapport rapide et propre
- Création de filtres intelligents
- Gestion des fichiers connus (bases de hash)
- Combinaison de recherches précédentes.





Net Analysis

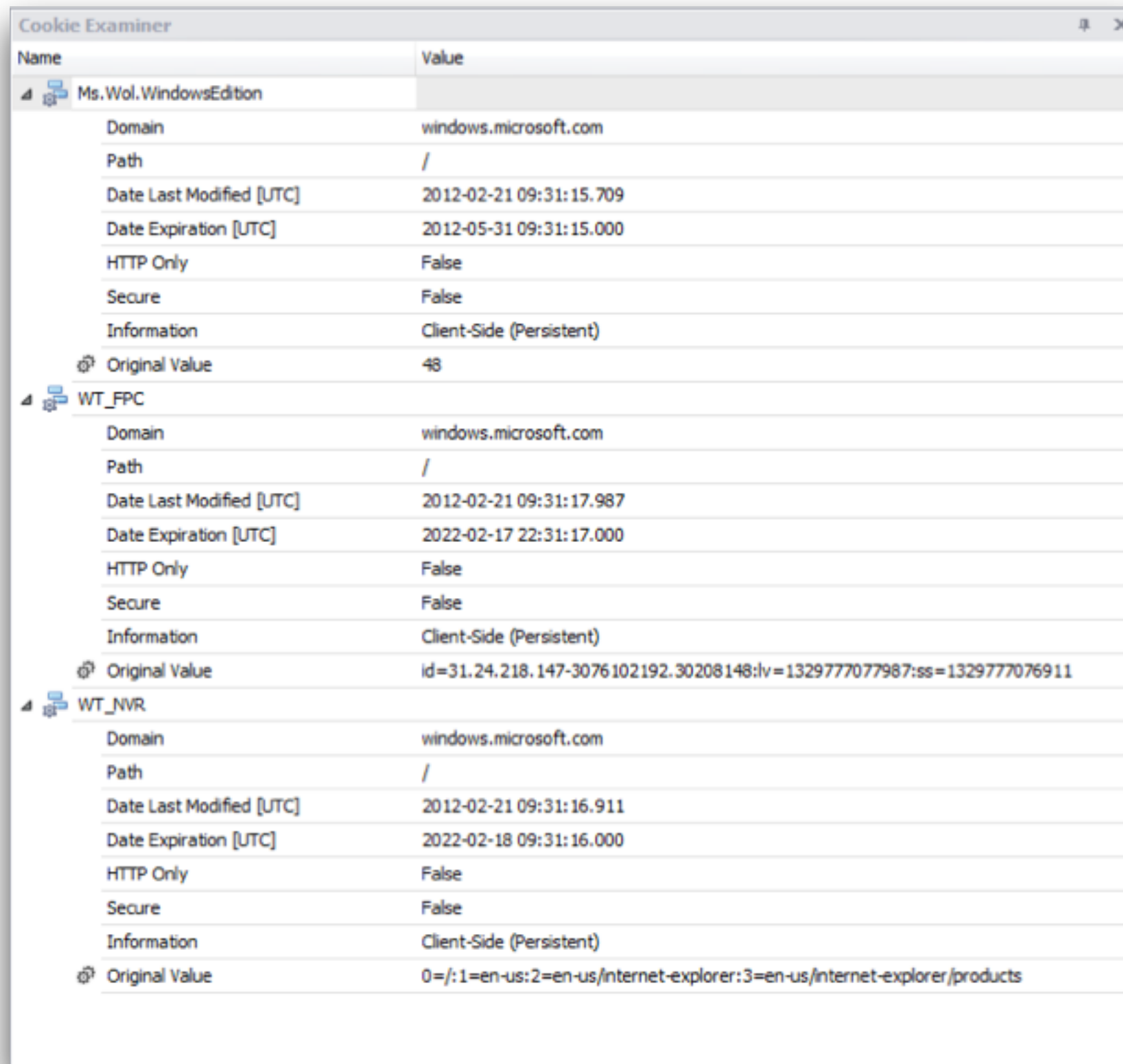


Netanalysis

- Produit ancien dont les mises à jour tardent à arriver.
 - Apple Safari v3 - 7
 - Comodo Dragon v4 - 33
 - Comodo Ice Dragon v13 - 26
 - CoolNovo v1 - 2
 - Flock v0 - 3
 - Google Chrome v0 - 37
 - Microsoft Internet Explorer v3
 - Microsoft Internet Explorer v4
 - Microsoft Internet Explorer v5 – 9
 - Microsoft Internet Explorer v10 - 11
 - Microsoft Internet Explorer XBOX
 - Mozilla Firefox v1 - 32
 - Netscape v6 - 9
 - Opera Blink v15 - 24
 - Opera Presto v3 - 12
 - Pale Moon v3 - 24



Visualisation des cookies

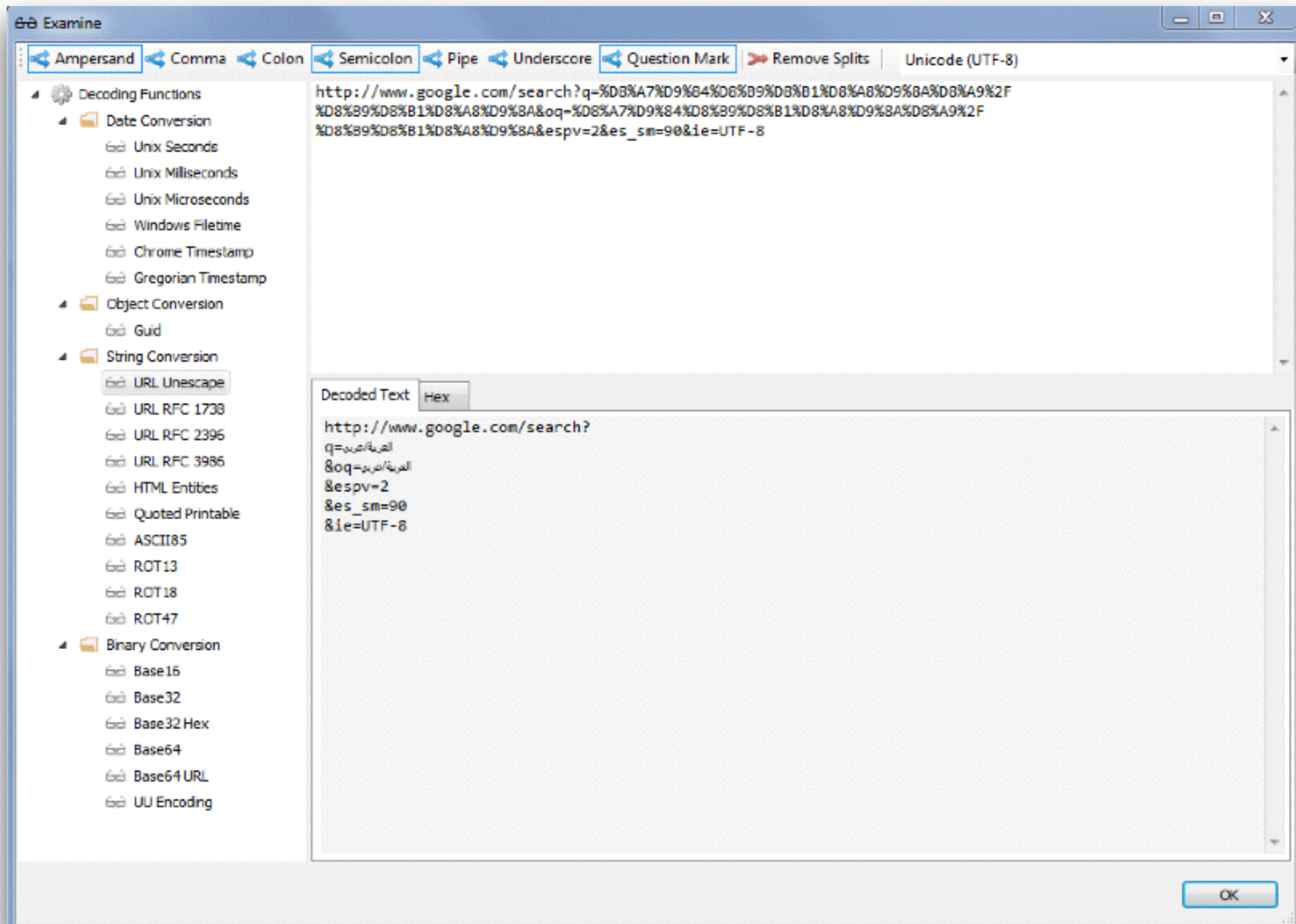


The screenshot shows the 'Cookie Examiner' application window. It displays a list of cookies with their details. The cookies are grouped by domain, and each group is expanded to show its properties. The cookies are:

- Ms.Wol.WindowsEdition**: Domain: windows.microsoft.com, Path: /, Date Last Modified [UTC]: 2012-02-21 09:31:15.709, Date Expiration [UTC]: 2012-05-31 09:31:15.000, HTTP Only: False, Secure: False, Information: Client-Side (Persistent), Original Value: 48.
- WT_FPC**: Domain: windows.microsoft.com, Path: /, Date Last Modified [UTC]: 2012-02-21 09:31:17.987, Date Expiration [UTC]: 2022-02-17 22:31:17.000, HTTP Only: False, Secure: False, Information: Client-Side (Persistent), Original Value: id=31.24.218.147-3076102192.30208148;lv=1329777077987:ss=1329777076911.
- WT_NVR**: Domain: windows.microsoft.com, Path: /, Date Last Modified [UTC]: 2012-02-21 09:31:16.911, Date Expiration [UTC]: 2022-02-18 09:31:16.000, HTTP Only: False, Secure: False, Information: Client-Side (Persistent), Original Value: 0=/:1=en-us:2=en-us/internet-explorer:3=en-us/internet-explorer/products.

Name	Value
Ms.Wol.WindowsEdition	
Domain	windows.microsoft.com
Path	/
Date Last Modified [UTC]	2012-02-21 09:31:15.709
Date Expiration [UTC]	2012-05-31 09:31:15.000
HTTP Only	False
Secure	False
Information	Client-Side (Persistent)
Original Value	48
WT_FPC	
Domain	windows.microsoft.com
Path	/
Date Last Modified [UTC]	2012-02-21 09:31:17.987
Date Expiration [UTC]	2022-02-17 22:31:17.000
HTTP Only	False
Secure	False
Information	Client-Side (Persistent)
Original Value	id=31.24.218.147-3076102192.30208148;lv=1329777077987:ss=1329777076911
WT_NVR	
Domain	windows.microsoft.com
Path	/
Date Last Modified [UTC]	2012-02-21 09:31:16.911
Date Expiration [UTC]	2022-02-18 09:31:16.000
HTTP Only	False
Secure	False
Information	Client-Side (Persistent)
Original Value	0=/:1=en-us:2=en-us/internet-explorer:3=en-us/internet-explorer/products

Analyse d'URL



Recherche par mots clés

NetAnalysis® v2.0 - Forensic Internet History Analysis - [Richardson]

File View Tools Search Index Filter Reports Column Window Help

(UTC) Dublin, Edinburgh, Lisbon, London

Entry Type	Scheme	Tag	Date Visited [UTC]	Date Visited [Local]	Visits	URL
History	http		2014-05-15 11:33:56.470	2014-05-15 12:33:56.470	1	http://www.bing.com/videos/search?q=cannabis+cultivation&qpv=cannabis+cultivation&FORM=VDRE
History	http		2014-05-15 11:33:46.979	2014-05-15 12:33:46.979	1	http://www.bing.com/search?q=cannabis+cultivation&pc=MOZI&form=MOZSBR
Form History			2014-05-15 11:33:46.881	2014-05-15 12:33:46.881	1	searchbar-history : cannabis cultivation
Cache	http		2014-05-15 11:33:40.000	2014-05-15 12:33:40.000	1	http://api.bing.com/osjson.aspx?query=cannabis+cultivation&form=OSDJAS&language=en-GB
Cache	http		2014-05-15 11:33:57.000	2014-05-15 12:33:57.000	1	http://www.bing.com/videos/asyncv2?q=cannabis+cultivation&async=content&first=1&count=35&dgst=
Cache	http		2014-05-14 14:56:13.000	2014-05-14 15:56:13.000	1	http://ts2.mm.bing.net/th?q=Cannabis+Drug&w=50&h=50&c=1&pid=1.7&mkt=en-GB&adit=moderate&t
Cache	http		2014-05-15 11:33:46.000	2014-05-15 12:33:46.000	1	http://www.bing.com/search?q=cannabis+cultivation&pc=MOZI&form=MOZSBR

Record 0 of 7

Keyword Manager

- Keyword List
 - Child Protection
 - Drugs
 - Cutting Agents
 - Drugs A-Z
 - Hazardous Substances
 - Firearms
 - Fraud

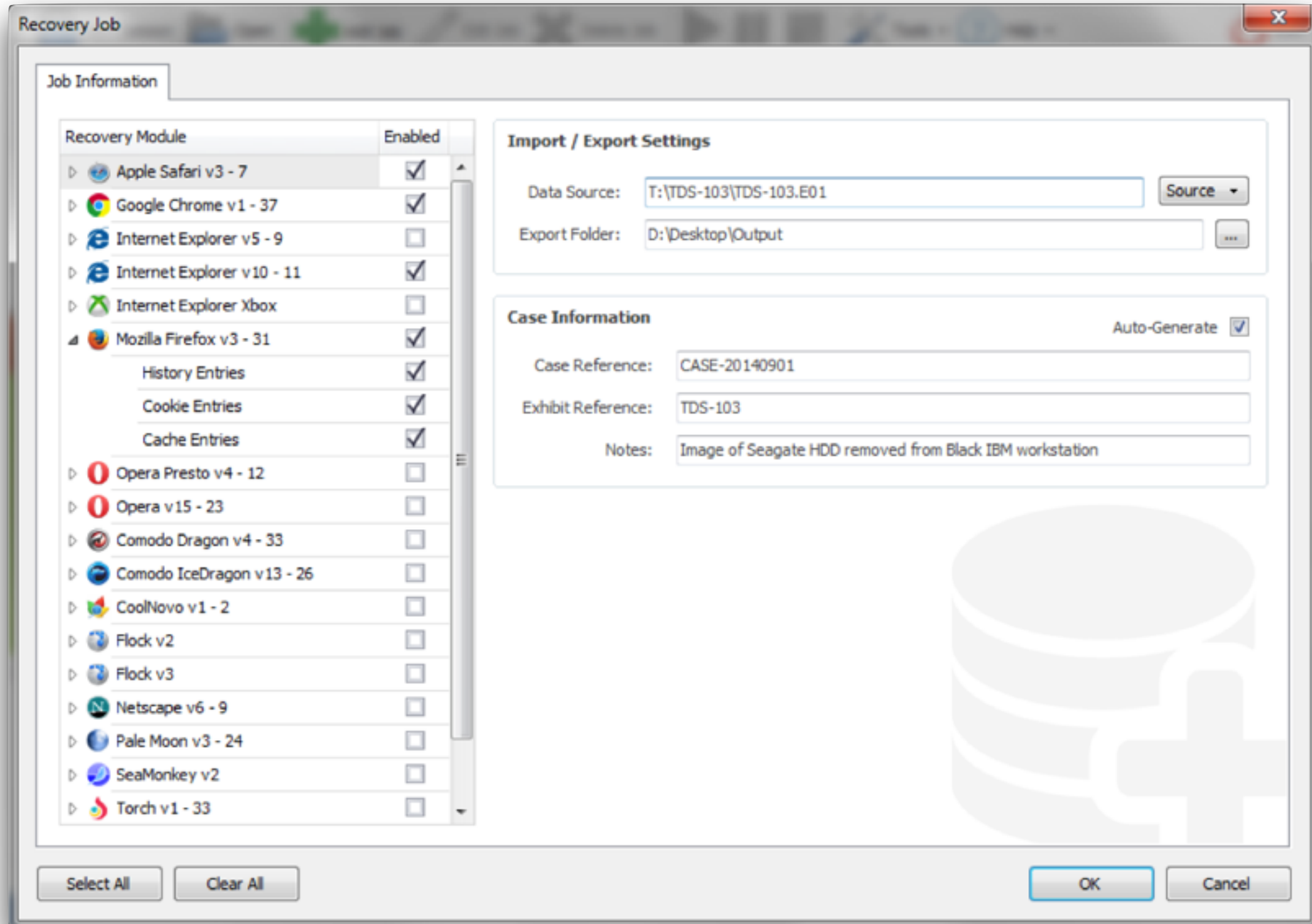
Search Results

Keyword Hits

- acid (6)
- amphetamine (2)
- base (1941)
- blast (4)
- bonsai (3)
- bounce (2)
- brown (3)
- brownies (1)
- bubble (23)
- cannabis (7)
- chang (92)
- charge (6)
- cocaine (2)
- codeine (1)

www.digital-detective.net D:\TDS\Jan Richardson\... \Cache_CACHE_MAP_ FO: 139188

Données effacées





Belkasoft



Belkasoft Evidence Center Ultimate



Instant Messenger Analysis



Browser Analysis



E-mail Analysis



Case Management



Deleted Information Retrieval



Document Analysis



Mobile Backup Analysis



Live RAM Dump Analysis



Network Traffic Analysis



Mounting Images



Picture Analysis



Video Analysis



Encryption Detection



System Files



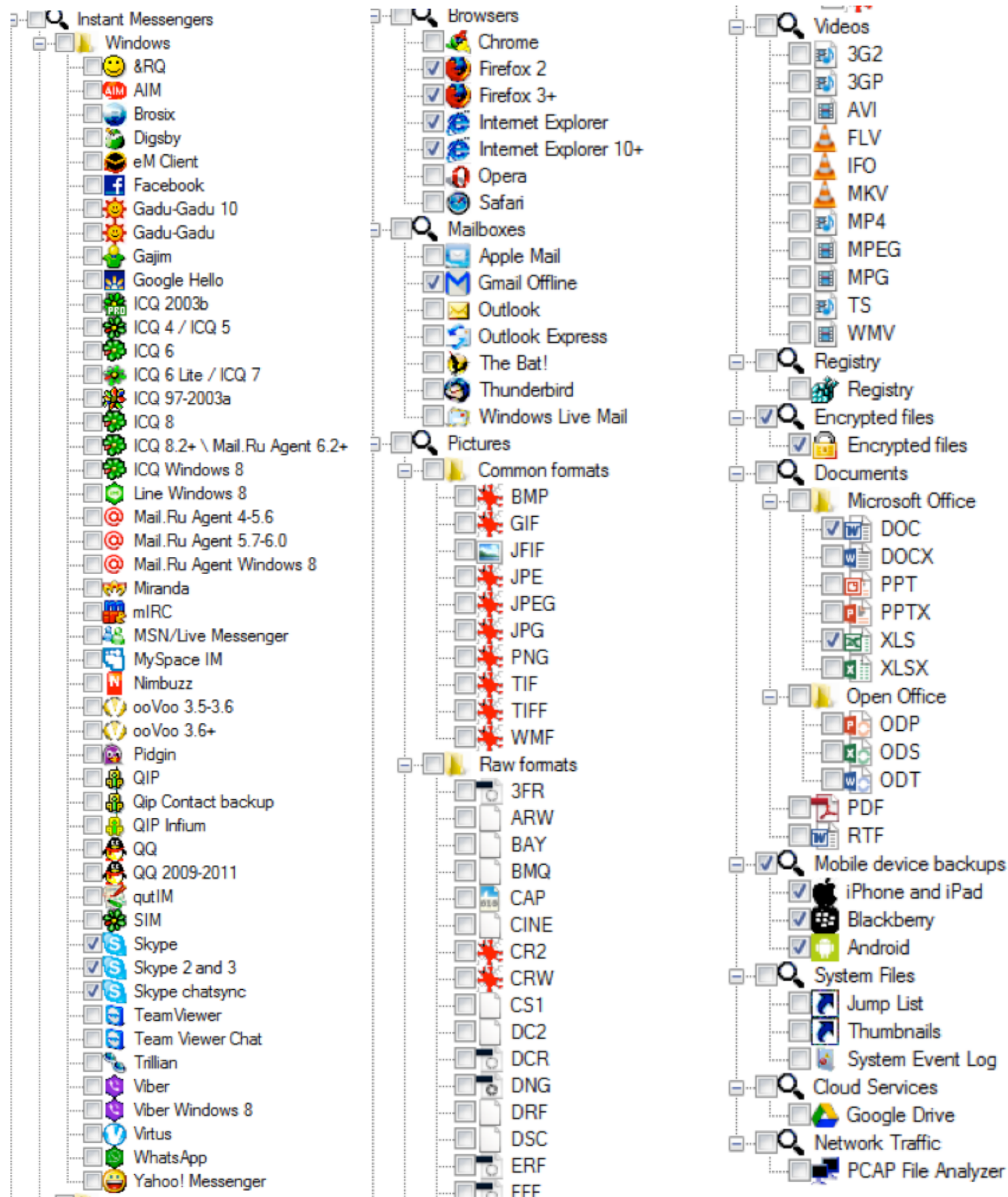
Registry Analysis



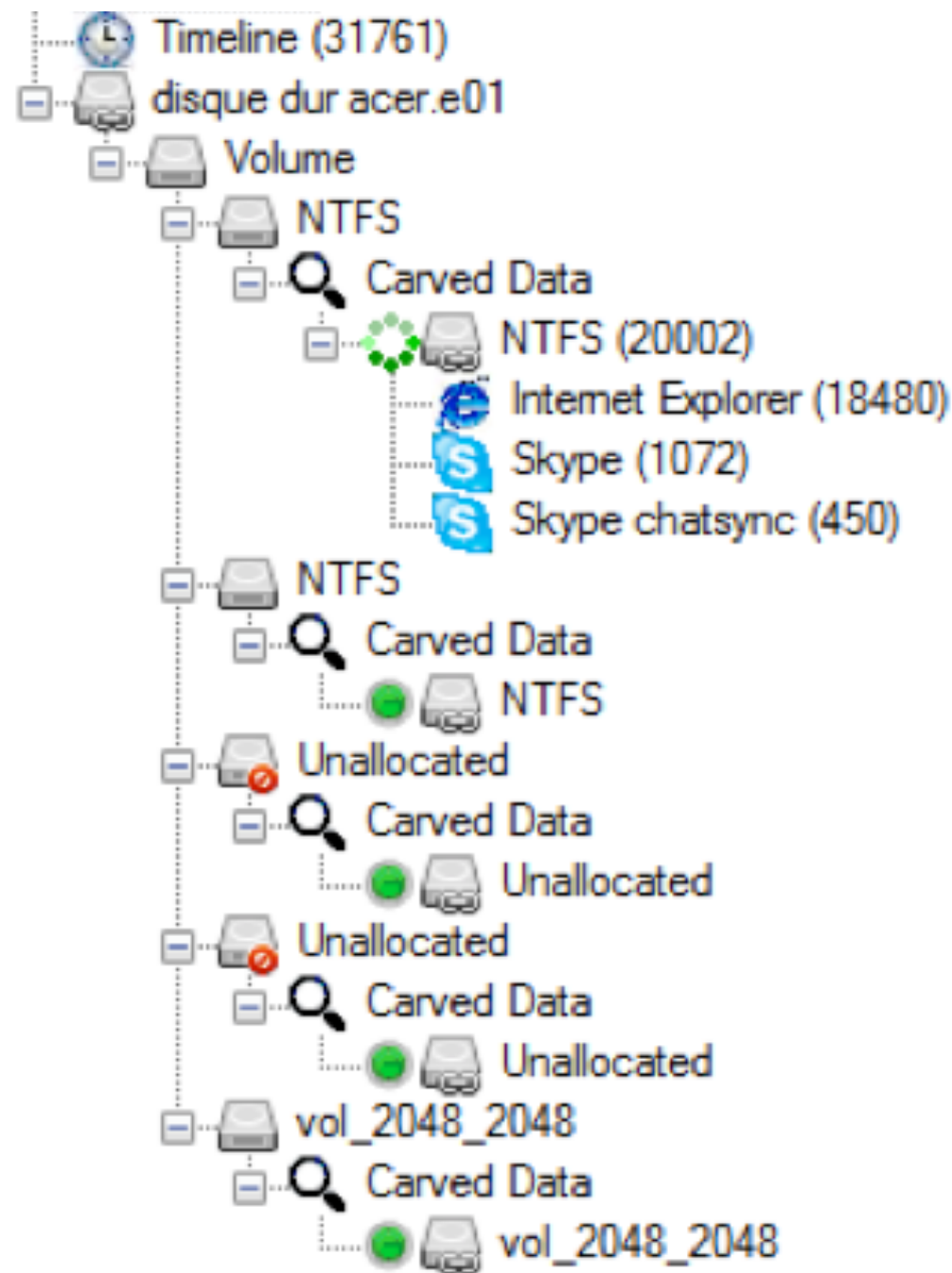
Forgery Analysis



Belkasoft



Belkasoft : Présentation des résultats



Belkasoft

Data List	Graphical Timeline	SQLite Viewer			
Type	URL	Last Modified	Last Accessed	Offset	Length
JRL	:Host: www.google.fr	2012.07.22 08:3...	2012.07.22 10:3...	156037120	256
JRL	:Host: www.google.it	2012.07.22 08:3...	2012.07.22 10:3...	156037376	256
JRL	http://www.web-provence.com/autour/...	2012.07.22 08:3...	2012.07.22 10:3...	156037632	256
JRL	:Host: www.web-provence.com	2012.07.22 08:3...	2012.07.22 10:3...	156037888	256
JRL	http://www.web-provence.com/autour/...	2012.07.22 08:3...	2012.07.22 10:3...	156038144	256
JRL	http://www.homelidays.com/FR-Locatio...	2012.07.22 18:1...	2012.07.22 20:1...	156038400	256
JRL	http://www.google.fr/url?sa=t&rct=j&q=&...	2012.07.22 08:3...	2012.07.22 10:3...	156038656	512
JRL	http://www.tendemerveilles.com/images...	2012.07.22 10:3...	2012.07.22 12:3...	156039168	256
JRL	:Host: www.tendemerveilles.com	2012.07.22 08:3...	2012.07.22 10:3...	156039424	256
JRL	http://www.meteo.it/	2012.07.22 18:1...	2012.07.22 20:1...	156039680	256
JRL	:Host: www.homelidays.com	2012.07.22 08:3...	2012.07.22 10:3...	156039936	256
JRL	http://alicegate.homenet.telecomitalia.it/...	2012.07.22 10:0...	2012.07.22 12:0...	156040192	256
JRL	:Host: alicegate.homenet.telecomitalia.it	2012.07.22 10:0...	2012.07.22 12:0...	156040448	256
JRL	http://alicegate.homenet.telecomitalia.it/i...	2012.07.22 10:0...	2012.07.22 12:0...	156040704	256
JRL	http://archiveofourown.org/	2012.07.22 10:0...	2012.07.22 12:0...	156040960	256

Gestion du Timeline
Visualisateur SQLite



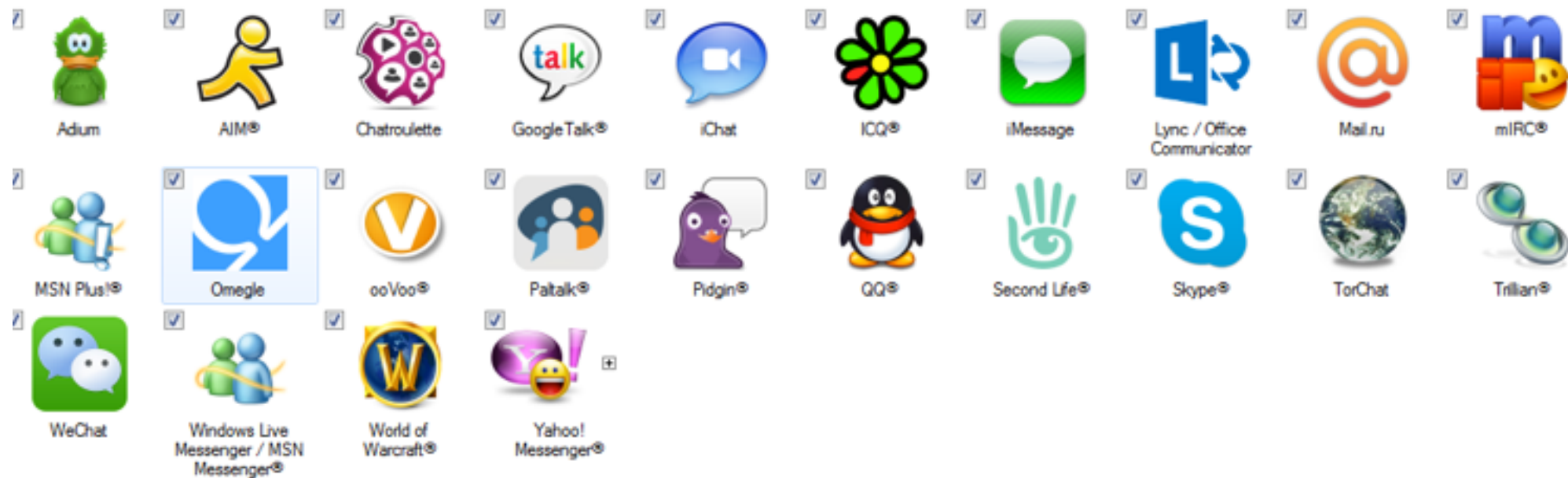


I.E.F.



Internet Evidence Finder

Chat (24 of 24 items)



Cloud (7 of 7 items)



Documents (4 of 4 items)



E-mail (9 of 9 items)



Internet Evidence Finder

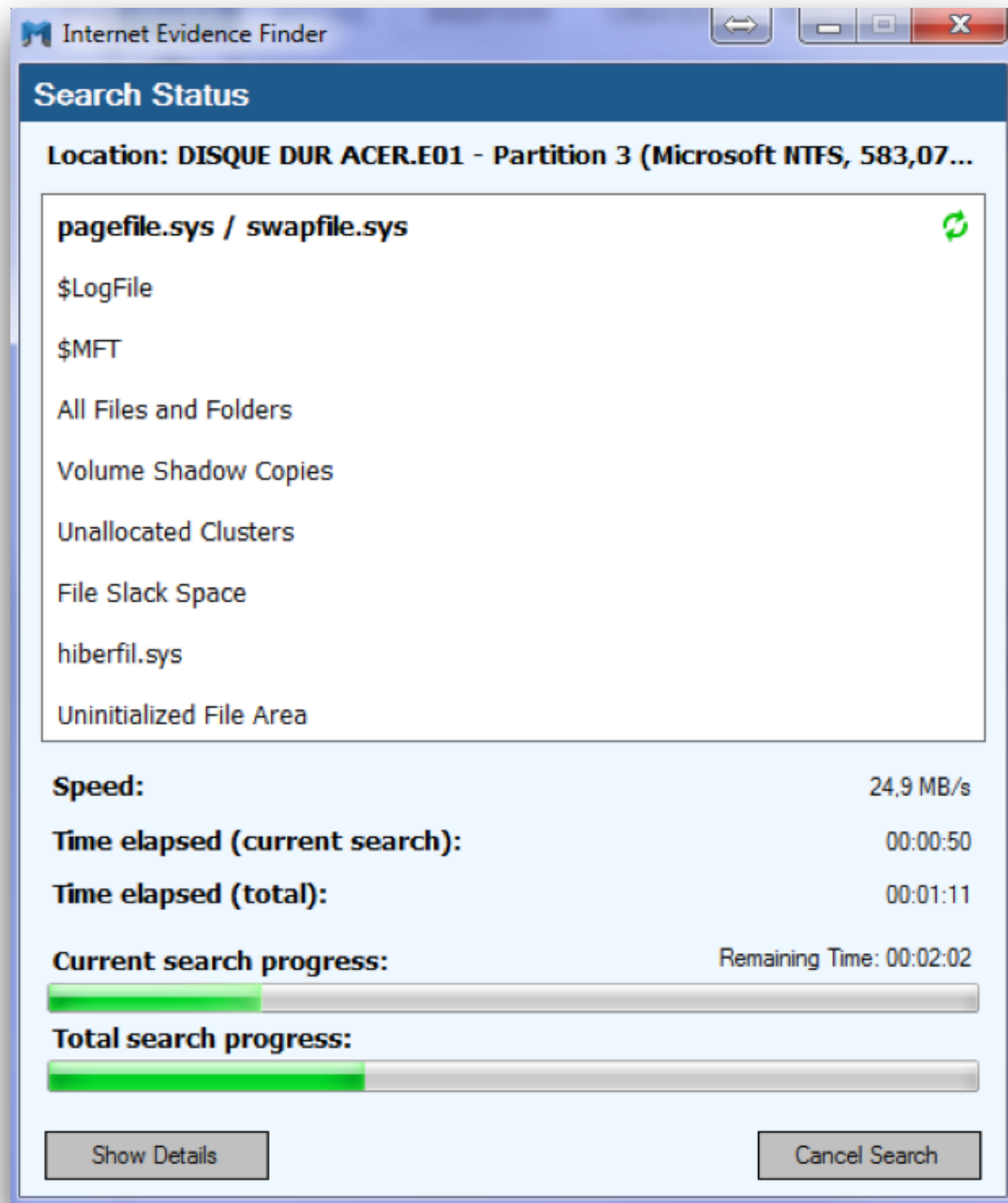


Internet Evidence Finder

Web Related (15 of 15 items)



IEF : exploitation des résultats



IEF exploitation des résultats

IEF Refined Results

 Classifieds URLs	119
 Cloud Services URLs	65
 Dating Sites URLs	72
 Facebook URLs	16175
 Google Analytics First Visit Cookies	2071
 Google Analytics Referral Cookies	1907
 Google Analytics Session Cookies	1243
 Google Analytics URLs	634
 Google Maps Queries	156
 Google Translate	36
 Malware/Phishing URLs	181
 Parsed Search Queries	18749
 Pomography URLs	7682
 Rebuilt Webpages	948
 Social Media URLs	3911
 Torrent URLs	2
 Web Chat URLs	162

Chat

 QQ	1
 Skype Accounts	9
 Skype Calls	972
 Skype Calls Carved	1227
 Skype Chat Messages	3590
 Skype Chatsync Messages	1084
 Skype Chatsync Messages Carved	131
 Skype Contacts	60
 Skype Group Chat	7
 Skype IP Addresses	450
 Skype SMS	1
 Skype Voicemails	1



IEF : exploitation des résultats

Documents

 Excel Documents	35
 PowerPoint Documents	4
 Word Documents	50

Email

 Gmail Fragments	4250
 Gmail Webmail	101613
 MBOX Emails	3
 Offline Gmail	3
 Outlook Webmail Inbox	1
 Outlook Webmail Inbox Fragments	1

 Carved Video	1712
 Facebook Pictures	2125
 Pictures	223176
 Videos	1497
 Web Video Fragments	1356

Mobile Backups

 iOS iMessage/SMS/MMS Backup	1
--	---

Peer to Peer

 Ares Search Keywords	3
---	---

Social Networking

 Facebook Chat	4
 Facebook Pages	13061
 Facebook Status Updates/Wall Po...	816
 Instagram Posts	87
 Twitter	12078

 Browser Activity	40352
 Chrome Archived Web History	4666
 Chrome Cache Records	1282
 Chrome Cookies	1166
 Chrome Current Session	6
 Chrome Current Tabs	3
 Chrome Downloads	2
 Chrome FavIcons	539
 Chrome Keyword Search Terms	4
 Chrome Last Session	1
 Chrome Last Tabs	8
 Chrome Logins	4
 Chrome Top Sites	25
 Chrome Web History	591
 Chrome Web Visits	815
 Chrome/360 Safe Browser Carved ...	69
 Chrome/360 Safe Browser/Opera ...	12714
 Firefox Bookmarks	27
 Firefox Cache Records	6612



IEF Exploitation des résultats

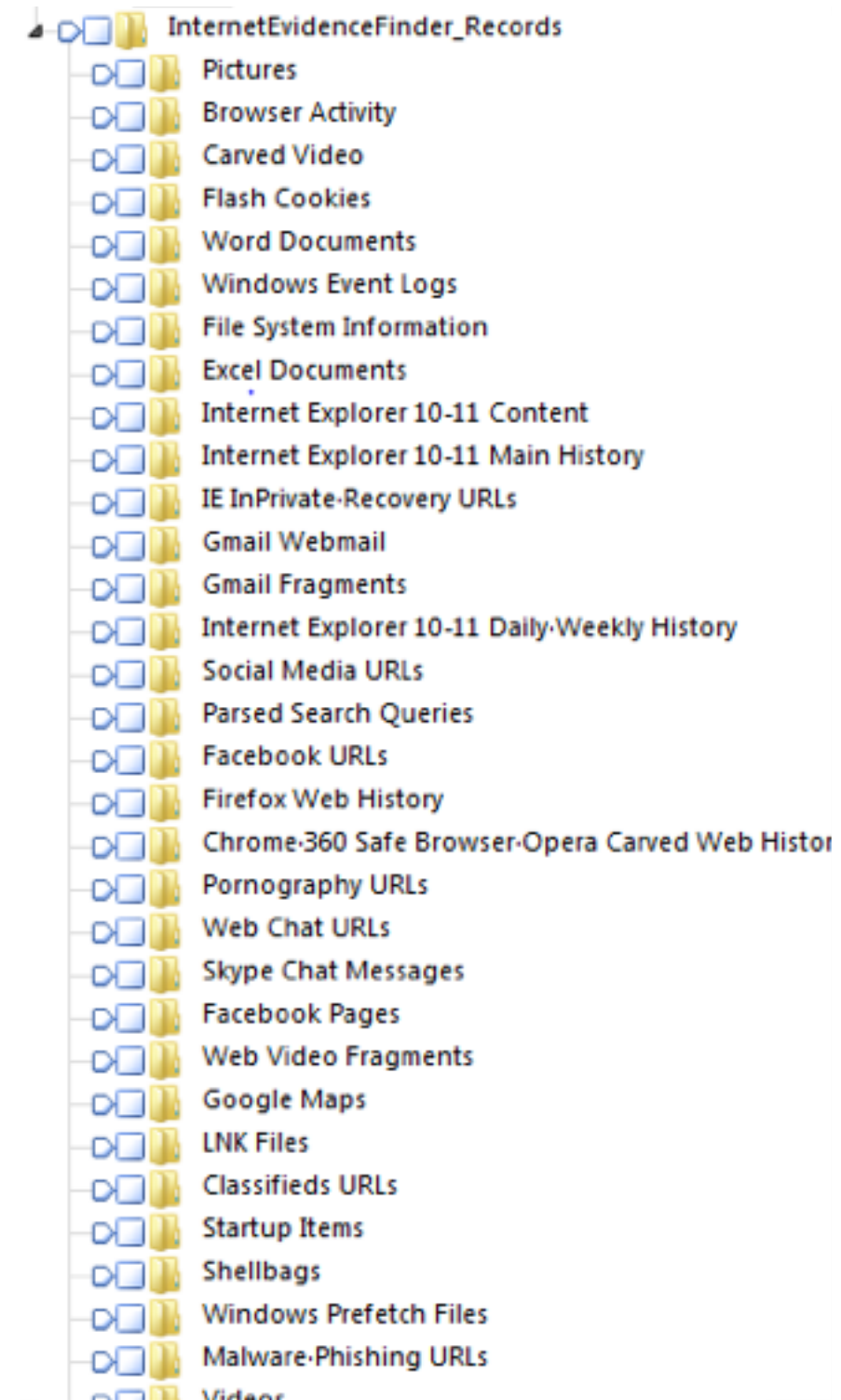
 IE InPrivate/Recovery URLs	21037
 Internet Explorer 10-11 Content	134905
 Internet Explorer 10-11 Cookies	1178
 Internet Explorer 10-11 Daily/Week...	11357
 Internet Explorer 10-11 Dependenc...	1022
 Internet Explorer 10-11 Downloads	10
 Internet Explorer 10-11 Main History	82480
 Internet Explorer Cache Records	14785
 Internet Explorer Cache Records C...	14868
 Internet Explorer Cookie Records	117
 Internet Explorer Cookies	27725
 Internet Explorer Daily History	354
 Internet Explorer Leak Records	50
 Internet Explorer Main History	416
 Internet Explorer PrivacIE Records	222
 Internet Explorer Redirect Records	1221
 Internet Explorer Weekly History	418

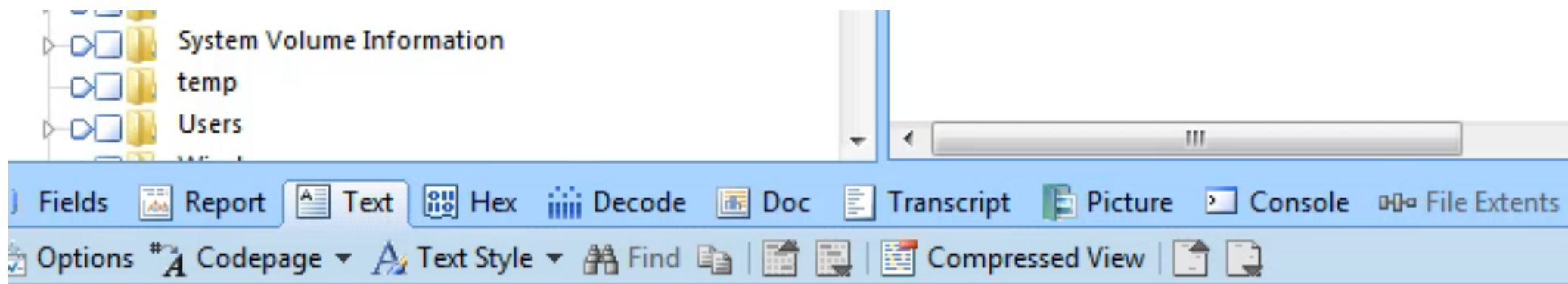
 File System Information	1
 Jump List Dest List Entries	2302
 Jump List Shortcut Entries	2098
 LNK Files	336
 Operating System Information	2
 Shellbags	387
 Startup Items	66
 Timezone Information	2
 USB Devices	44
 User Accounts	14
 Windows Event Logs	235040
 Windows Prefetch Files	181



Encase + IEF la solution ?

- Avantages multiples de la solution
- Intégration en tant que fichier logique
- Possibilité de filtres élaborés (Encase)
- Indexation
- 2 modes de recherche (raw, index)
- Bénéficie de l'indexation
- Permet de se focaliser si besoin
- Intégration comme signets
- Intégration dans le rapport





Détail des nouveautés
IE10 et IE11

Internet Explorer 10 et 11 Windows 7/8

History Files

- %USERPROFILE%\AppData\Local\Microsoft\Windows**Webcache**\WebCacheV*.dat

Cache

- %USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
- %USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5

Cookies

- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies\Low

Bookmarks

- %USERPROFILE%\Favorites

Download History

- %USERPROFILE%\AppData\Local\Microsoft\Windows**Webcache**\WebCacheV*.dat



Internet Explorer 10/11 Windows 8.1

History Files

- %USERPROFILE%\AppData\Local\Microsoft\Windows\Webcache\WebCacheV*.dat

Cache

- %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache\IE
- %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache\Low\IE

Cookies

- %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCookies
- %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCookies\Low

Bookmarks

- %USERPROFILE%\Favorites

Download History

- %USERPROFILE%\AppData\Local\Microsoft\Windows\Webcache\WebCacheV*.dat



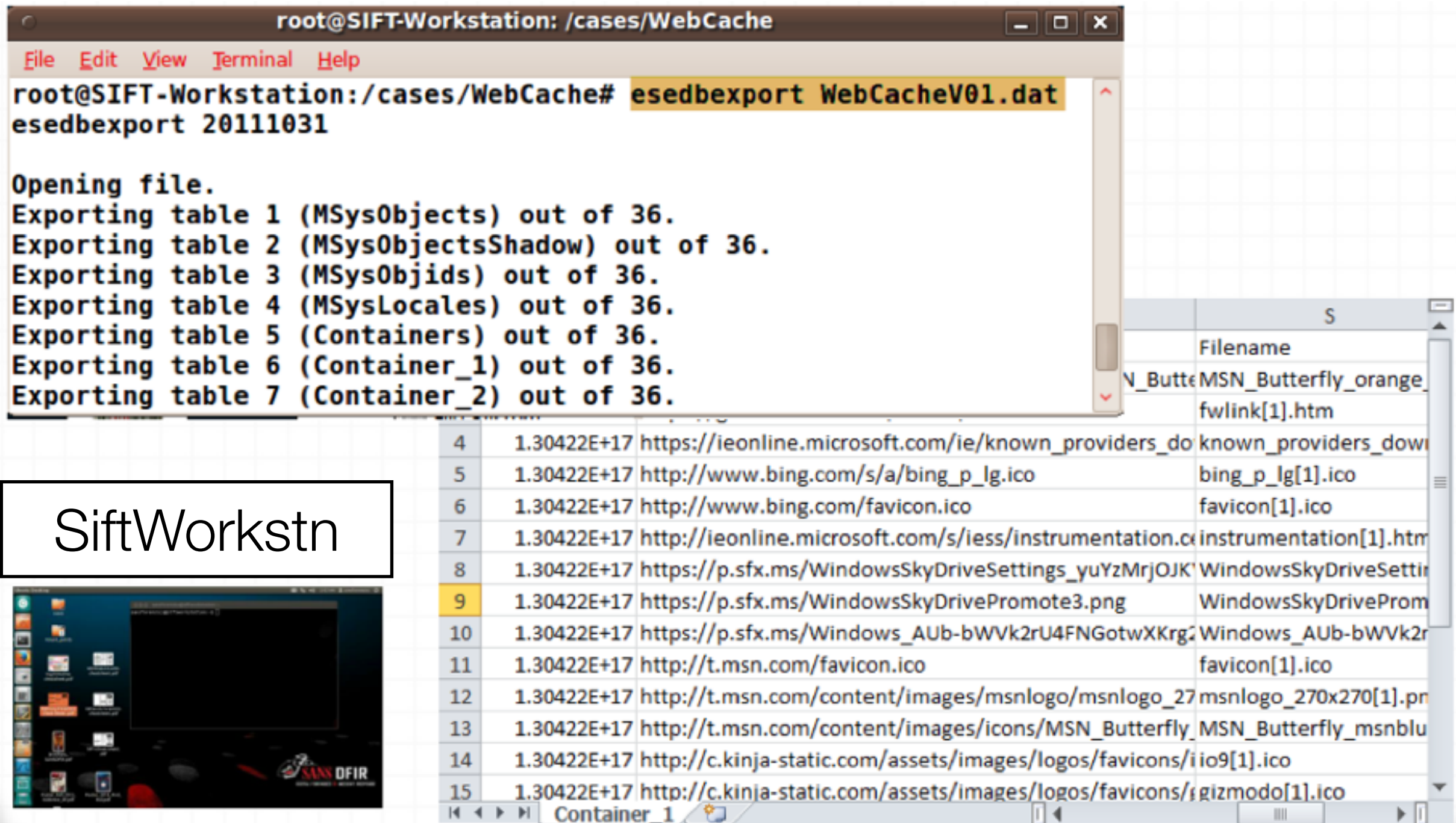
Format de base de données JETBLUE

- Extensible Storage Engine (ESE) 1Mb à 1To
- Possibilité d'effectuer des récupérations importantes (journaux transactions)
- Internet Explorer est le dernier d'un certain nombre d'autres logiciels
- Exchange.edb
- Active Directory
- Windows Search
- Applications Windows Store



Libesedb (Joachim Metz)

- <https://code.google.com/p/libesedb/>



The terminal window shows the following output:

```
root@SIFT-Workstation: /cases/WebCache
File Edit View Terminal Help
root@SIFT-Workstation:/cases/WebCache# esedbexport WebCacheV01.dat
esedbexport 20111031

Opening file.
Exporting table 1 (MSysObjects) out of 36.
Exporting table 2 (MSysObjectsShadow) out of 36.
Exporting table 3 (MSysObjids) out of 36.
Exporting table 4 (MSysLocales) out of 36.
Exporting table 5 (Containers) out of 36.
Exporting table 6 (Container_1) out of 36.
Exporting table 7 (Container_2) out of 36.
```

The list of exported files is as follows:

	S
	Filename
	N_ButteMSN_Butterfly_orange_fwlink[1].htm
4	1.30422E+17 https://ieonline.microsoft.com/ie/known_providers_down known_providers_down
5	1.30422E+17 http://www.bing.com/s/a/bing_p_lg.ico bing_p_lg[1].ico
6	1.30422E+17 http://www.bing.com/favicon.ico favicon[1].ico
7	1.30422E+17 http://ieonline.microsoft.com/s/iess/instrumentation.c instrumentation[1].htm
8	1.30422E+17 https://p.sfx.ms/WindowsSkyDriveSettings_yuYzMrjOJK WindowsSkyDriveSettin
9	1.30422E+17 https://p.sfx.ms/WindowsSkyDrivePromote3.png WindowsSkyDriveProm
10	1.30422E+17 https://p.sfx.ms/Windows_AUb-bWVvk2rU4FNGotwXKrg2 Windows_AUb-bWVvk2r
11	1.30422E+17 http://t.msn.com/favicon.ico favicon[1].ico
12	1.30422E+17 http://t.msn.com/content/images/msnlogo/msnlogo_27 msnlogo_270x270[1].pr
13	1.30422E+17 http://t.msn.com/content/images/icons/MSN_Butterfly_MSN_Butterfly_msnblu
14	1.30422E+17 http://c.kinja-static.com/assets/images/logos/favicons/iio9[1].ico
15	1.30422E+17 http://c.kinja-static.com/assets/images/logos/favicons/gizmodo[1].ico

The terminal window also shows a list of containers:

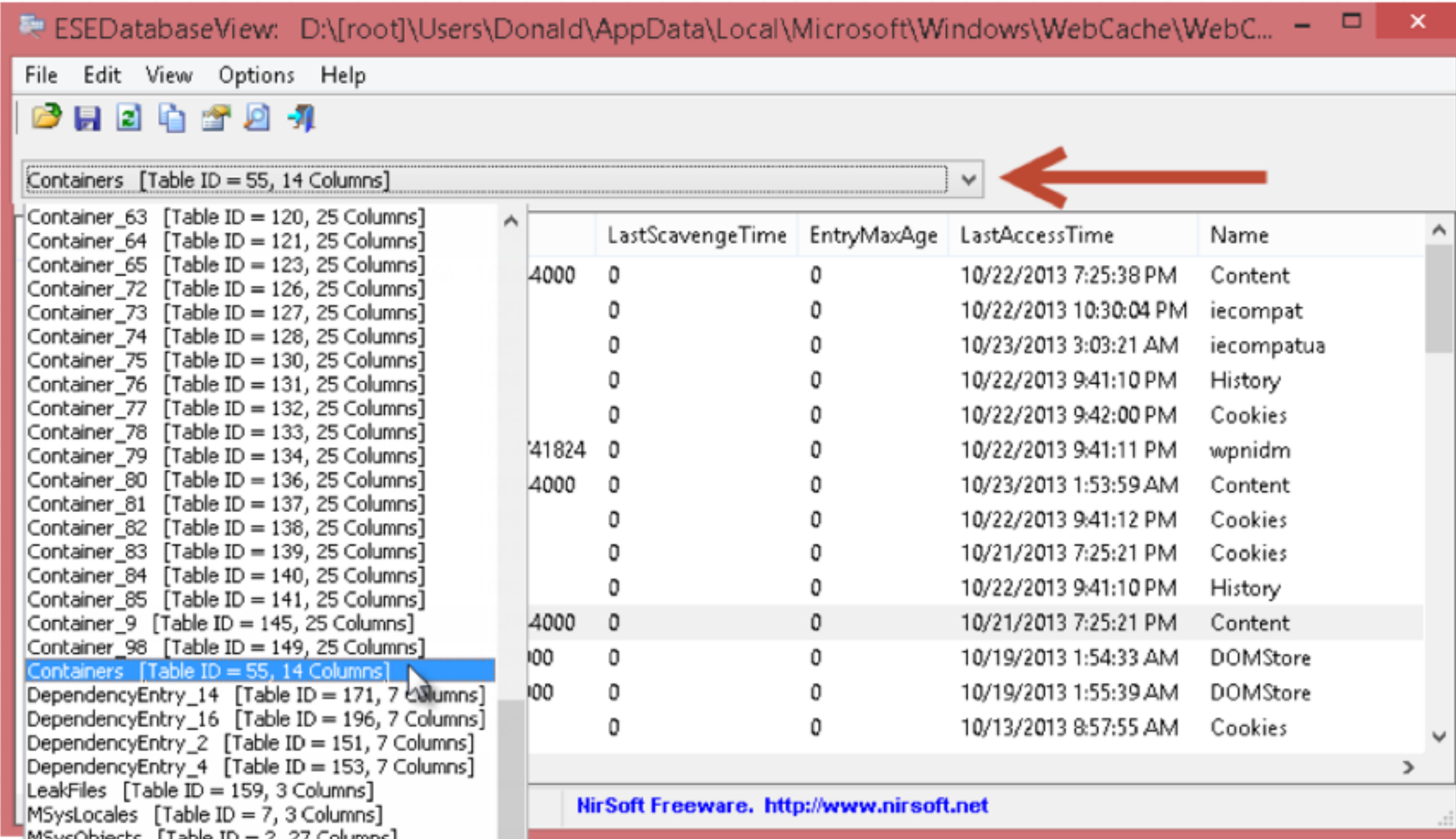
	S
4	1.30422E+17 https://ieonline.microsoft.com/ie/known_providers_down known_providers_down
5	1.30422E+17 http://www.bing.com/s/a/bing_p_lg.ico bing_p_lg[1].ico
6	1.30422E+17 http://www.bing.com/favicon.ico favicon[1].ico
7	1.30422E+17 http://ieonline.microsoft.com/s/iess/instrumentation.c instrumentation[1].htm
8	1.30422E+17 https://p.sfx.ms/WindowsSkyDriveSettings_yuYzMrjOJK WindowsSkyDriveSettin
9	1.30422E+17 https://p.sfx.ms/WindowsSkyDrivePromote3.png WindowsSkyDriveProm
10	1.30422E+17 https://p.sfx.ms/Windows_AUb-bWVvk2rU4FNGotwXKrg2 Windows_AUb-bWVvk2r
11	1.30422E+17 http://t.msn.com/favicon.ico favicon[1].ico
12	1.30422E+17 http://t.msn.com/content/images/msnlogo/msnlogo_27 msnlogo_270x270[1].pr
13	1.30422E+17 http://t.msn.com/content/images/icons/MSN_Butterfly_MSN_Butterfly_msnblu
14	1.30422E+17 http://c.kinja-static.com/assets/images/logos/favicons/iio9[1].ico
15	1.30422E+17 http://c.kinja-static.com/assets/images/logos/favicons/gizmodo[1].ico

SiftWorkstn



Nirsoft : ESEDatabase View

- http://www.nirsoft.net/utils/ease_database_view.html



The screenshot shows the ESEDatabaseView application window. The title bar reads "ESEDatabaseView: D:\[root]\Users\Donald\AppData\Local\Microsoft\Windows\WebCache\WebC...". The menu bar includes File, Edit, View, Options, and Help. Below the menu is a toolbar with icons for file operations. A dropdown menu is open, showing "Containers [Table ID = 55, 14 Columns]". A red arrow points to this dropdown. The main area displays a list of containers on the left and a detailed view of the selected container on the right. The detailed view shows columns: LastScavengeTime, EntryMaxAge, LastAccessTime, and Name. The list of containers includes Container_63 through Container_98, DependencyEntry_14, DependencyEntry_16, DependencyEntry_2, DependencyEntry_4, LeakFiles, MSysLocales, MSysObjects, and MSysObjectsShadow. The detailed view shows data for the selected container, including LastScavengeTime, EntryMaxAge, LastAccessTime, and Name.

Container	Table ID	Columns	LastScavengeTime	EntryMaxAge	LastAccessTime	Name
Container_63	120	25				
Container_64	121	25				
Container_65	123	25				
Container_72	126	25				
Container_73	127	25				
Container_74	128	25				
Container_75	130	25				
Container_76	131	25				
Container_77	132	25				
Container_78	133	25				
Container_79	134	25				
Container_80	136	25				
Container_81	137	25				
Container_82	138	25				
Container_83	139	25				
Container_84	140	25				
Container_85	141	25				
Container_9	145	25				
Container_98	149	25				
Containers	55	14				
DependencyEntry_14	171	7				
DependencyEntry_16	196	7				
DependencyEntry_2	151	7				
DependencyEntry_4	153	7				
LeakFiles	159	3				
MSysLocales	7	3				
MSysObjects	2	27				
MSysObjectsShadow	3	27				

NirSoft Freeware. <http://www.nirsoft.net>

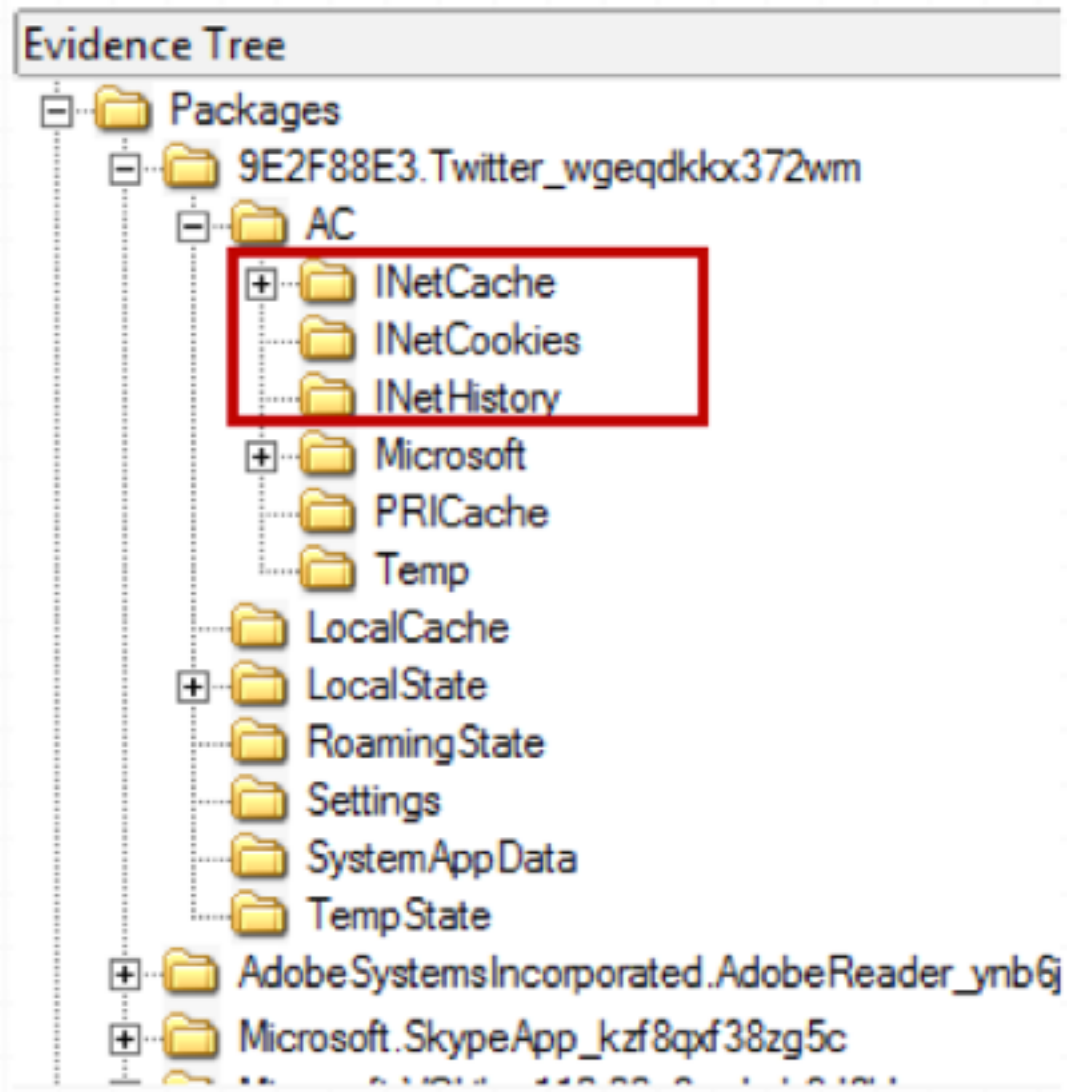
Définition des dates pour les fichiers dans le cache

- Date de création : 1ère fois que le contenu est visualisé, en UTC
- Date de dernier accès : dernière fois que l'utilisateur a vu le fichier (attention aux interprétations sur Windows 7/8)... Un antivirus peut aussi modifier cette information.
- Date de dernière modification : correspond à la dernière fois où le contenu a été modifié sur le serveur web.
- Date d'expiration : Utilisé par le système de cache pour mettre en évidence et vérifier les vieilles versions des pages.

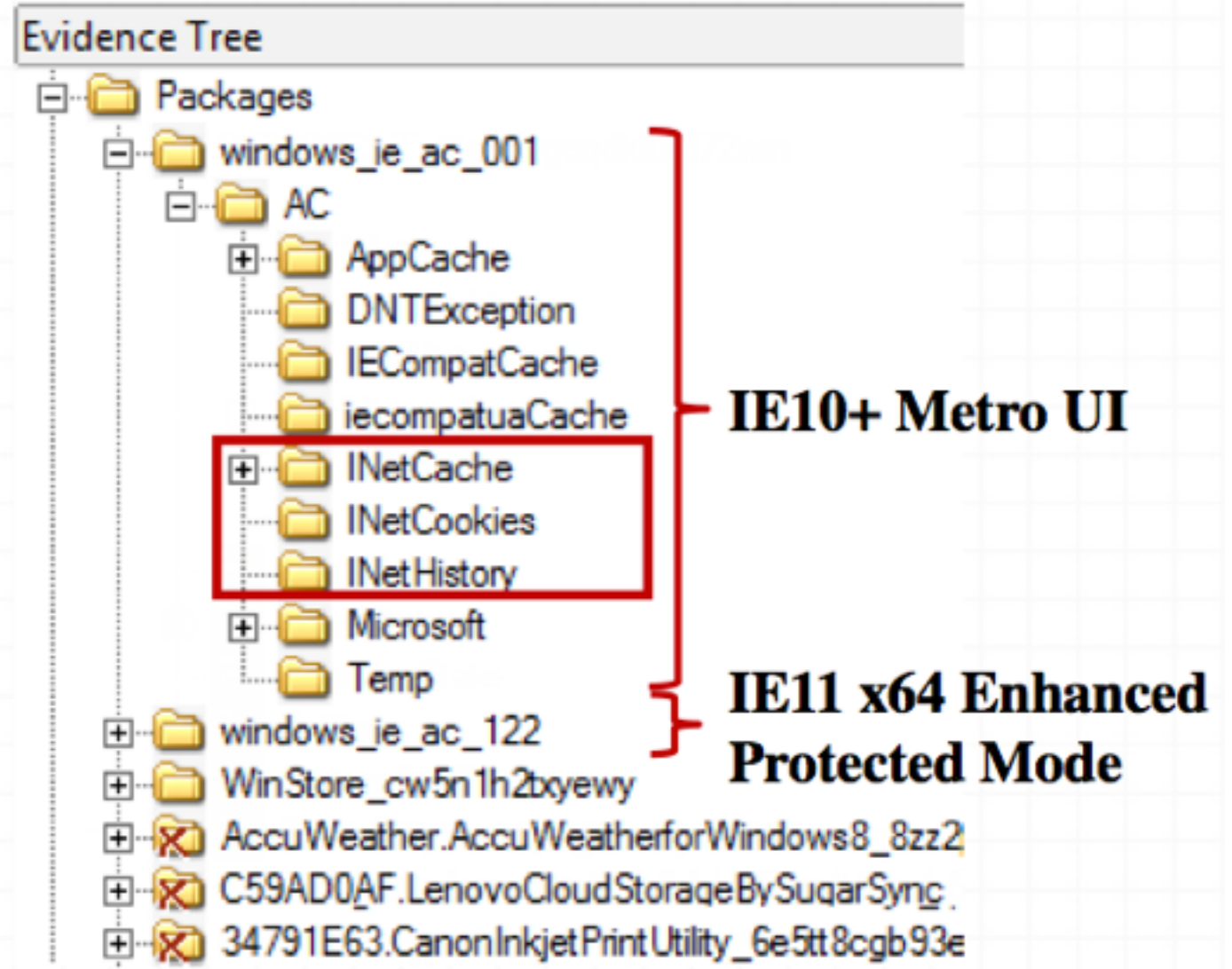


Gestion des applications tierces

Twitter App



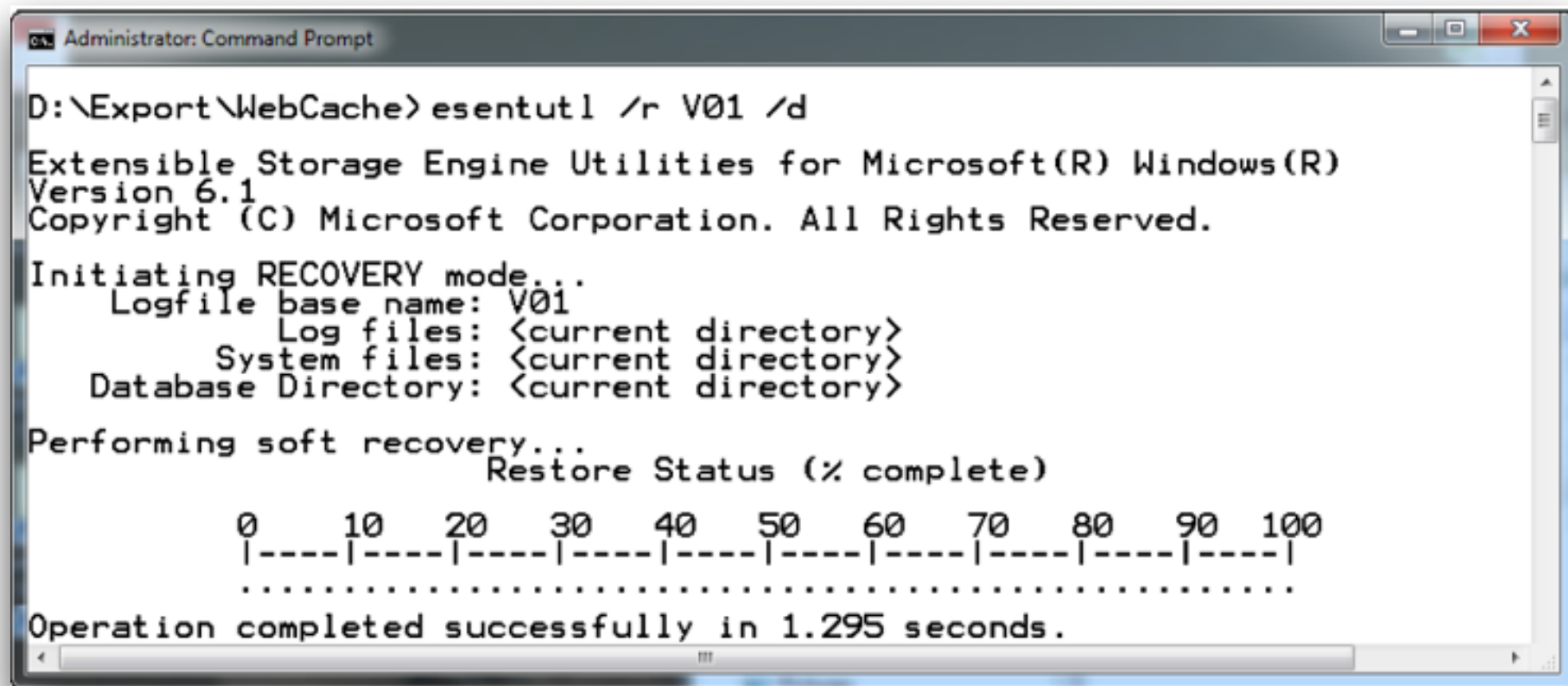
IE App Containers



%UserProfile%\Appdata\local\Packages

Utilitaires ESE sous Windows

- Utilitaire esentutl :
- Lecture entête : esentutl /mh WebCacheV01.dat
- Réparation de base de données : esentutl /r V01/d



```
Administrator: Command Prompt

D:\Export\WebCache>esentutl /r V01 /d

Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 6.1
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 1.295 seconds.
```



Merci de votre attention

Jean-Philippe NOAT - URIEL EXPERT
Instructeur Encase
EnCE 15-0914-6379

E-mail

jpnoat@uriel.mc

Website

www.uriel.mc

