



INDEX.DAT **ASEGURANDO NUESTRA PRIVACIDAD**

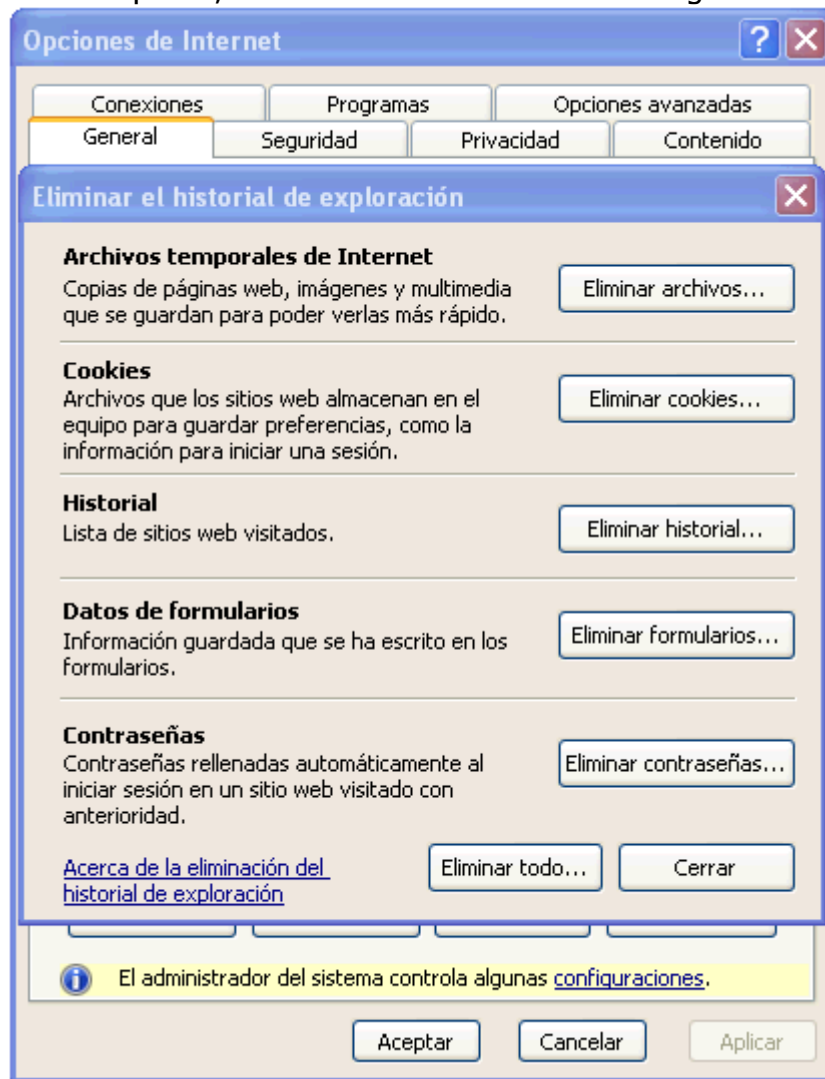
[Paper publicado en <http://www.mipistus.blogspot.com>]

Jorge Alejandro Mieres
jamieres@gmail.com

©2007 Jorge Alejandro Mieres



Como ya muchos saben, la manera más rápida y sencilla de borrar la información que se almacena en la computadora con relación a nuestra navegación (caché, cookies, historial, etc.) al utilizar Internet Explorer, es hacerlo desde el mismo navegador:



Herramientas→Opciones de Internet→Eliminar Archivos.

Ahora bien, existe un archivo llamado **Index.dat** que es propio del sistema y permanece oculto en el mismo, éste archivo contiene un índice de referencia que guarda las direcciones de todas las páginas web que visitamos.

Eliminando los archivos de la forma convencional antes mencionada, la información contenida en el **Index.dat** no se borra, por ende, quien pueda localizar y leer este archivo podrá ver absolutamente todos los sitios que hayamos visitado, sin importar que hayamos, previamente, eliminado el historial del IE y demás información. Si bien no se trata de un archivo crítico, toma relativa importancia al ser propenso a comprometer uno de los principios básicos de la Seguridad Informática, nuestra **privacidad**.

Y es aquí cuando surge la siguiente pregunta: **¿es paranoico pensar que este archivo puede comprometer nuestra privacidad?** Yo creo que sí, que no constituye una amenaza grave, pero también creo que evidentemente no deja de ser una amenaza y por tal motivo debemos conocerla y tenerla en cuenta sin darle un nivel de importancia más allá del que realmente se merece y sin hacer del tema una cuestión extremadamente paranoica.

De todas maneras es importante tenerlo en cuenta a la hora de querer eliminar las huellas que dejamos al manipular un sistema, además es un archivo a examinar a la hora de realizar un análisis sobre un sistema comprometido.

Veamos ahora algunas herramientas de las cuales disponemos para poder manipular este archivo y eliminar completamente su contenido.

En primer lugar debemos saber que este archivo puede estar alojado en diferentes sectores de nuestro sistema dependiendo del sistema operativo que usemos, por ejemplo:

Windows 9x > Windows ME

```
\Windows\Cookies
\Windows\History\history.ie5
\Windows\History\History.ie5\sub-folders
\Windows\Temporary Internet Files
\Windows\Temporary Internet Files\Content.IE5\
\Windows\Temporary Internet Files\Content.IE5\sub-folders
```

Windows NT > Windows Server 2003

```
\Documents and settings\<username>\cookies
\Documents and settings\<username>\Local Settings\History
\Documents and settings\<username>\Local Settings\Temporary Internet Files
\Documents and settings\<username>\Local Settings\Temporary Internet Files\Content.IE5
\Documents and settings\<username>\Local Settings\Temporary Internet Files\Content.IE5\sub-folders
\Documents and settings\All Users\cookies
\Documents and settings\All Users\Local Settings\History
\Documents and settings\All Users\Local Settings\Temporary Internet Files
\Documents and settings\All Users\Local Settings\Temporary Internet Files\Content.IE5
\Documents and settings\All Users\Local Settings\Temporary Internet Files\Content.IE5\sub-folders
\Documents and settings\Default User\cookies
\Documents and settings\Default User\Local Settings\History
\Documents and settings\Default User\Local Settings\Temporary Internet Files
\Documents and settings\Default User\Local Settings\Temporary Internet Files\Content.IE5
\Documents and settings\Default User\Local Settings\Temporary Internet Files\Content.IE5\sub-folders
```

También en

```
\windows\system32\config\systemprofile\cookies
\windows\system32\config\systemprofile\local settings\history
\windows\system32\config\systemprofile\local settings\history\sub-folders
\windows\system32\config\systemprofile\local settings\temporary internet files\content.ie5
```

Como ya se mencionó anteriormente, el Index.dat se encuentra oculto y con privilegios de ser un archivo necesario para el sistema, por tal motivo no podremos eliminarlo de la manera en que estamos acostumbrados a hacerlo con cualquier otro archivo.

Existen varios programas, tanto en línea de comando como para entorno gráfico, que nos permiten manipular, ver y borrar el contenido de estos archivos. Veamos algunos métodos y usos.

Find

Para poder visualizarlo podemos recurrir al DOS, bajo línea de comandos escribimos en C:\Documents and Settings\[Usuario]\Configuración local\Historial\History.IE5 (ruta donde se aloja el archivo) el siguiente comando:

```
find /i "http://" index.dat | sort > C:\cont-index-dat.txt
```

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Mi Pistus\Configuración local\Historial\History.IE5>find /i "http://" index.dat | sort > C:\cont-index-dat.txt_
```

Con el comando **find** le pedimos que busque dentro del archivo Index.dat cadenas de texto, en este caso los caracteres "**http://**", el parámetro **/i** omite mayúsculas y minúsculas al buscar; y con el comando **sort** le decimos que ordene lo encontrado en forma alfabética y que lo guarde como **cont-index-dat.txt** en la raíz del disco **C**.

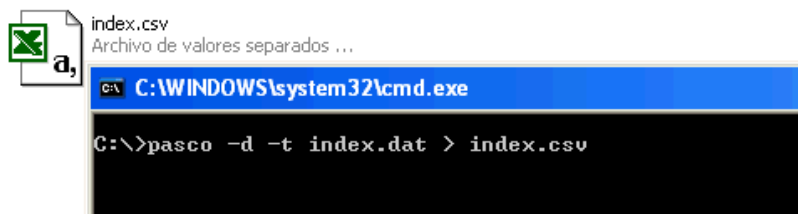
De esta manera obtendremos un archivo .txt llamado cont-index-dat.txt con el contenido de todas las páginas web visitadas.

Pasco

Una segunda opción para visualizar su contenido, podría ser utilizando una herramienta llamada **pasco** de la firma Foundstone. **Pasco**, que significa "navegar" en latín, es una herramienta gratuita que se utiliza en análisis forense y nos permite generar un archivo .CSV que podremos visualizar, por ejemplo, en una planilla de cálculo de Excel.

Para ejecutarlo debemos escribir en el prompt de DOS un simple comando:

```
C:\>pasco -d -t index.dat > index.csv
```



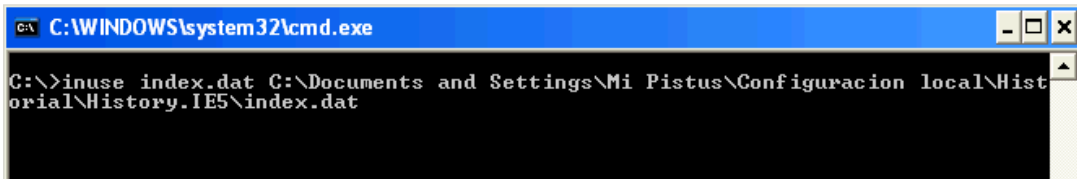
De esta manera podremos generar un archivo con extensión .csv que podremos exportar a una planilla de cálculo .

InUse

Si lo que queremos hacer es directamente borrar el archivo Index.dat, podemos utilizar una herramienta de Microsoft llamada **InUse**, ésta herramienta nos permite cambiar archivos que no se pueden manipular mientras son usados por el sistema, es rápida, pesa 40 Kb y se utiliza bajo línea de comando. Su sintaxis es sencilla. C:\>inuse [origen] [destino]

Veamos un ejemplo. En primer lugar tenemos que crear, mediante el block de notas, un archivo llamado Index.dat y guardarlo, por ejemplo, en la misma carpeta donde esta el InUse.exe (lo mas práctico es guardar ambos en la raíz del C). Una vez que tengamos el archivo, bajo DOS escribimos los siguiente:

C:\INUSE> inuse index.dat C:\Documents and Settings\Mi Pistus\Configuración local\Historial\History.IE5

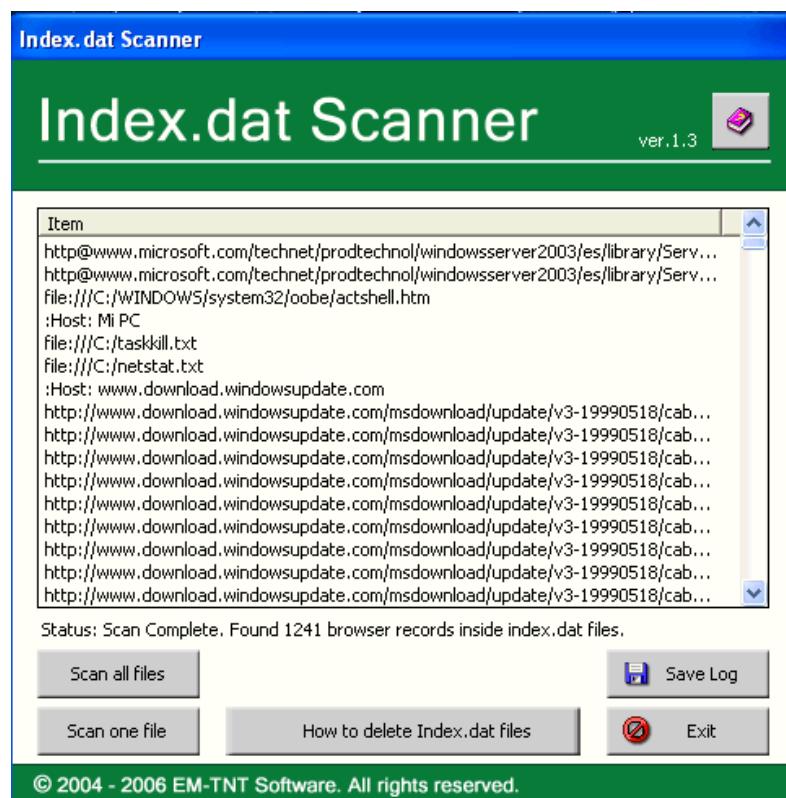


Luego de reiniciar la computadora, Internet Explorer creará un nuevo archivo vacío llamado Index.dat, con lo cual nos aseguramos de haber borrado todo el rastro que haya guardado en su índice de referencia.

Si no se sienten cómodos utilizando herramientas bajo línea de comandos, existen muchas otras que nos permiten manipular el Index.dat bajo un entorno gráfico. Veamos algunas de ellas.

Index.dat Scanner

Si bien todas las herramientas mostradas son sencillas de utilizar, ésta tiene la particularidad de que no necesita instalación, es decir, con solo hacer doble click sobre el ejecutable es suficiente para que nos muestre todo el contenido del Index.dat, brindándonos la opción de guardar el resultado en un log con extensión .txt o escanear un archivo Index.dat en particular, por ejemplo, alguno que hayamos extraído de otra/s computadoras.



Si nuestro objetivo es visualizar el contenido del archivo, ésta es una herramienta ideal ya que solo pesa 87 Kb, con lo cual podremos transportarla en un disquete. Aquí tienen una captura del log generado con este programa.

```

index.txt - Bloc de notas
Archivo Edición Formato Ver Ayuda

=====
Index.dat Scanner Results. by EM-TNT Software, soft.EM-TNT.com
Scanned all index.dat files.
=====

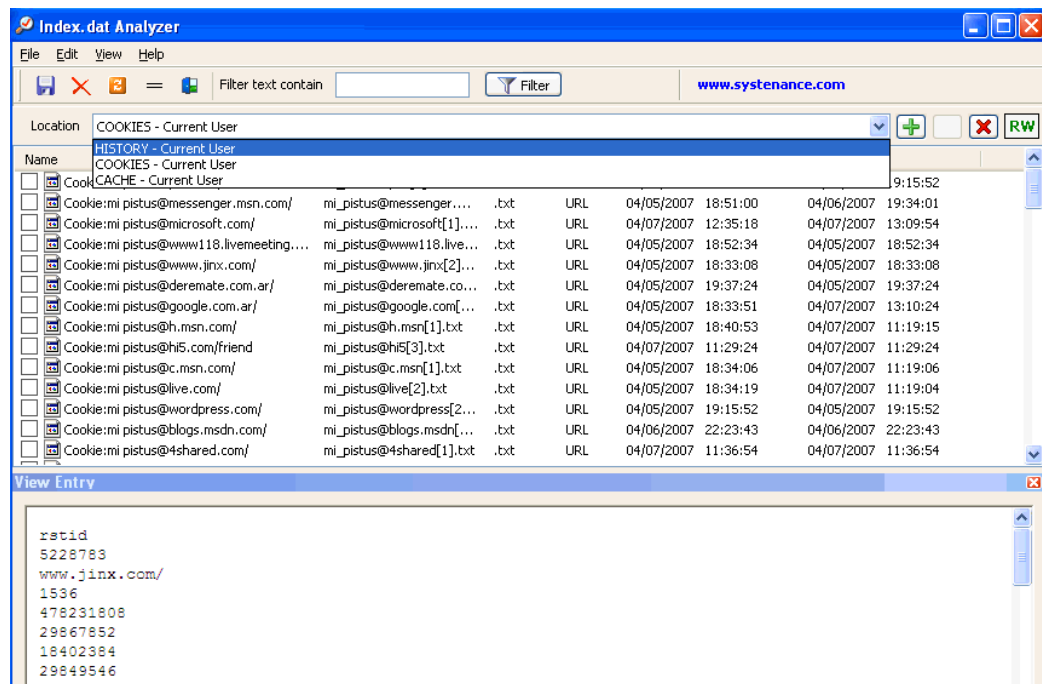
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/mnpFrames
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/mnpFrames
file:///C:/WINDOWS/system32/oobe/actshell.htm
:Host: Mi PC
file:///C:/taskkill.txt
file:///C:/netstat.txt
:Host: www.download.windowsupdate.com
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb8858
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb8883
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb8874
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb8917
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb8858
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb8733
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb9278
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb9246
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb9277
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb9181
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb9264
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb9280
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb9259
http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb9318

```

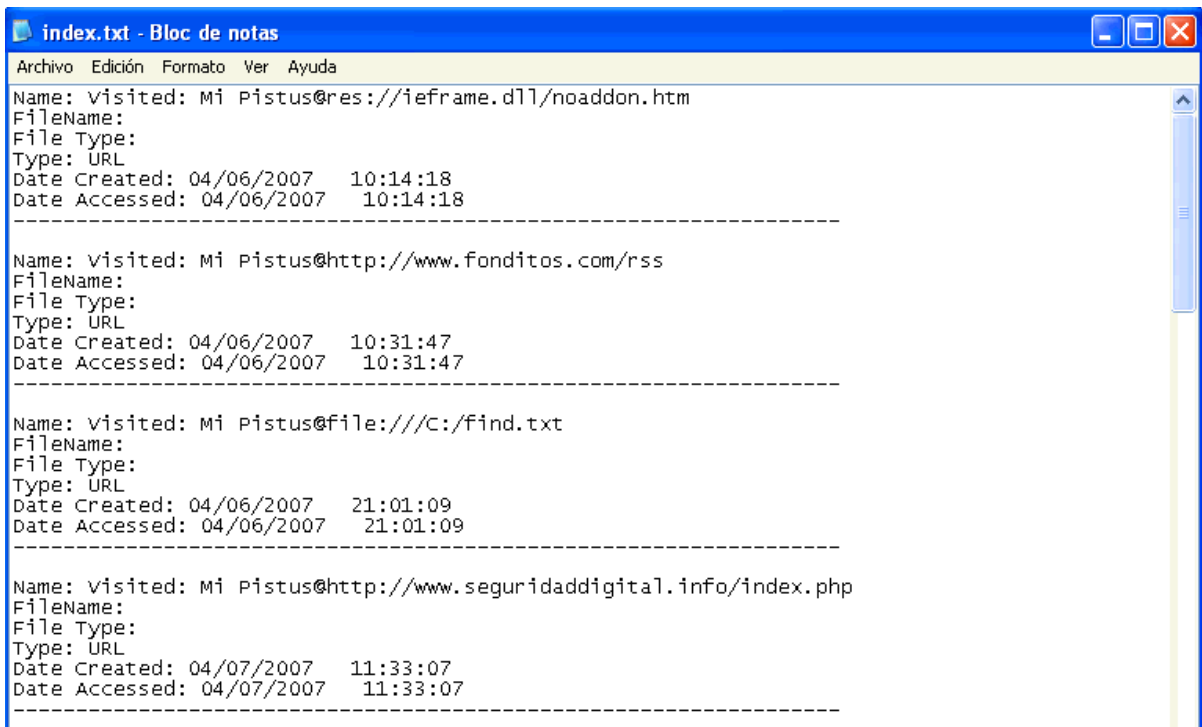
Index.dat Analyzer

Index.dat Analyzer no solo nos permite visualizar el contenido del archivo sino que también nos permite eliminar aquellas entradas que no son de nuestro interés.

Una buena característica de este programa es que nos deja interactuar entre el contenido del caché, las cookies y el historial, pudiendo seleccionar de cada una de ellas las entradas que queremos eliminar. Al igual que el anterior, es muy sencilla de utilizar y a diferencia requiere ser instalado en el disco rígido.



Para poder guardar su contenido, tendremos que seleccionar todos los items, o seleccionar aquellos que luego queremos analizar, y elegir la opción **File→Save Selected Items**, de esta forma obtendremos un archivo .txt con las entradas que hayamos seleccionado.

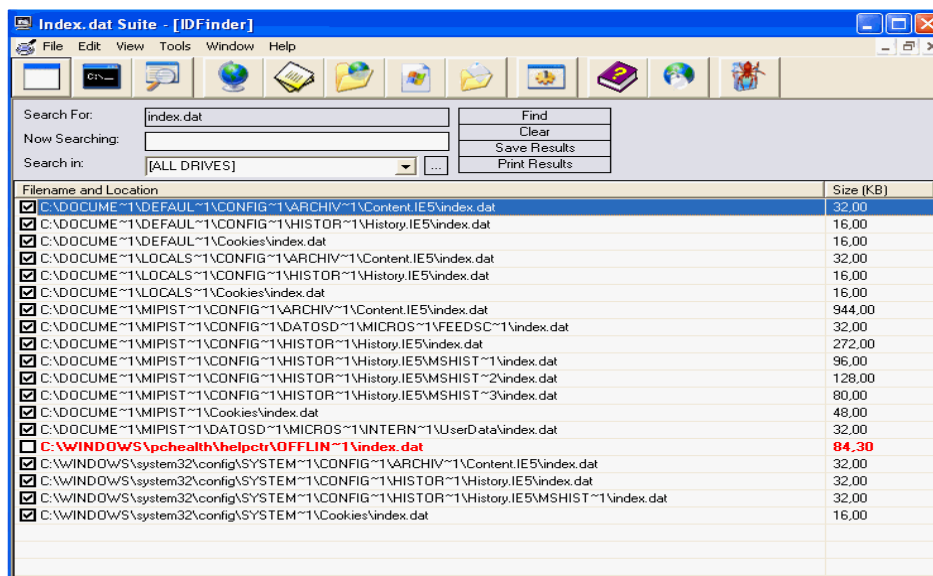


Index.dat Suite

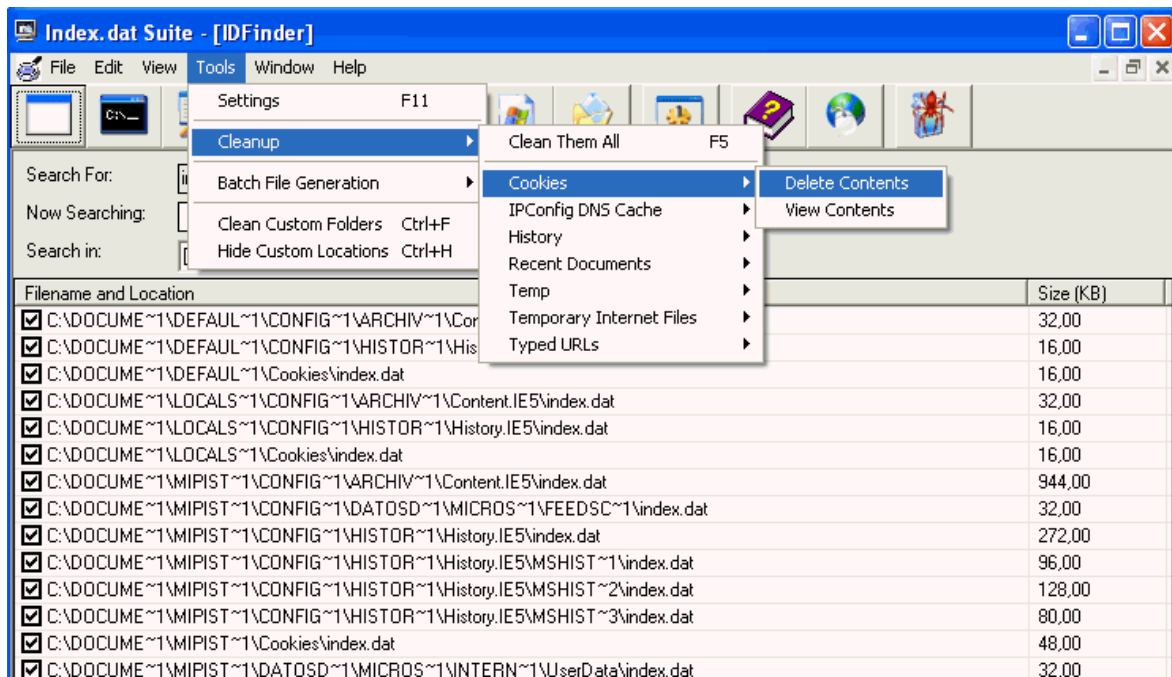
Por ultimo, veamos ésta herramienta que nos sirve para eliminar no solo el index.dat sino que también cualquier otra información que se haya almacenado después de nuestra actividad en una computadora. Posee muchas mas herramientas que las dos mencionadas anteriormente y requiere instalación.

Entre sus funciones se encuentran:

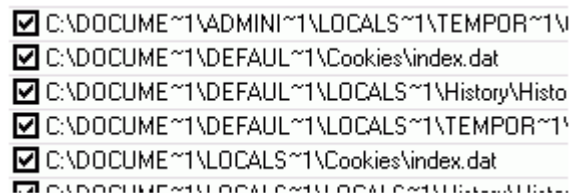
- Ver, borrar y hacer copias de seguridad de los archivos Index.dat
- Ver y borrar archivos temporales de Internet
- Ver y borrar cookies, historial, archivos temporales y documentos recientes
- Borrar URL's que no nos interese
- Borrar el contenido de la carpeta Prefetch, entre otras.



Para eliminar nuestras huellas, primero debemos asegurarnos de escanear todos los discos (Search in: ALL DRIVERS), luego seleccionar la opción "Find". Por último, Seleccionar del menú Tools la opción Cleanup→Cookies (History, Temp., etc)→Delete Contents.



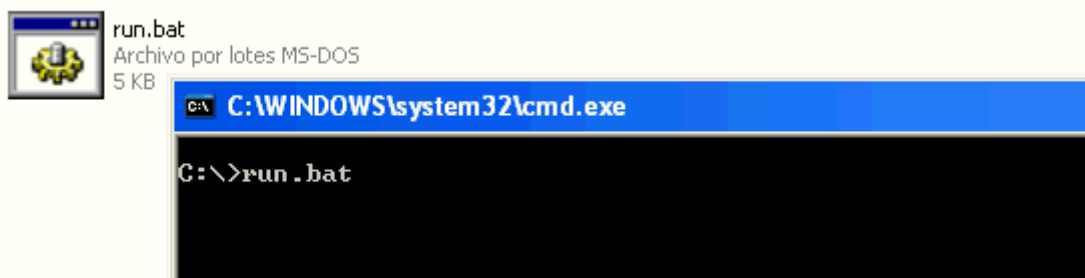
Y por ultimo, para eliminar el Index.dat debemos, previo escaneo, seleccionar los archivos index.dat que queremos eliminar, tal como lo muestra la captura.



Una vez hecho esto, tendremos que generar un archivo .bat, para lo cual haremos clic sobre el botón con el dibujo de una consola DOS.



Esto generará el archivo run.bat en la raíz del C que nos permitirá eliminar el Index.dat. Bajo línea de comando tipear simplemente **run.bat** y el índice de referencia del Index.dat se eliminará por completo.



InUse

<http://download.microsoft.com/download/win2000platform/inuse/1.0/NT5/EN-US/inuse.exe>

Pasco

<http://www.foundstone.com/resources/termsofuse.htm?file=pasco.zip>

Index.dat Scanner

<http://soft.em-tnt.com/files/IdatScan.exe>

Index.dat Analyzer

<http://www.systemance.com/download/indexdat-setup.exe>

Index.dat Suite

<http://support.it-mate.co.uk/?mode=Products&act=DL&p=index.datsuite&g=idsuite.exe>



ESTE "PAPER" SE PUBLICA BAJO UNA LICENCIA CREATIVE COMMONS BY-NC-SA 2.5 AR.

Por lo tanto, usted es libre de: 1) copiar, distribuir, exhibir, y ejecutar la obra. 2) Hacer obras derivadas. Bajo las siguientes condiciones: 1) Debe dar atribución mencionando el nombre del autor. 2) Usted no puede usar esta obra con fines comerciales. 3) Si usted altera, transforma, o crea sobre estos textos, sólo podrá distribuir la obra derivada resultante bajo una licencia idéntica a ésta.

Ante cualquier reutilización o distribución, usted debe dejar claro a los otros los términos de la licencia de esta obra. Cualquiera de estas condiciones puede dispensarse si usted obtiene permiso del titular de los derechos de autor. Nada en esta licencia menoscaba o restringe los derechos morales del autor.