Centro Federal de Educação Tecnológica do Rio Grande do Norte
Unidade de Ensino Descentralizada de Currais Novos
Departamento Acadêmico em Gestão Tecnológica

Perícia Forense em Web Browsers

Ricardo Kléber Martins Galvão
rk@cefetrn.br
http://www.ricardokleber.com.br

GTS
Grupo de Trabalho em Segurança

Salvador/BA, 01/06/2008

Análise Forense

> “A aplicação de princípios das ciências físicas ao direito na busca da verdade em questões cíveis, criminais e de comportamento social para que não se cometam injustiças contra qualquer membro da sociedade”

(Manual de Patologia Forense do Colégio de Patologistas Americanos, 1990).

– Levantar evidências que contam a história do fato:

  - Quando?
  - Como?
  - Porque?
  - Onde?

– **Normas e Procedimentos**

Computação Forense

- Supre as necessidades das instituições legais para manipulação de evidências eletrônicas;
- Estuda a aquisição, preservação, recuperação e análise de dados em formato eletrônico;
- Produz informações diretas e não interpretativas.

Computação Forense

Principais Fases

- Identificação
- Preservação
- Análise
- Apresentação

Foco desta apresentação:

Análise de Evidências em Web Browsers

Computação Forense em Web Browsers
Contextualização

- Importância das Evidências Eletrônicas
- Evidências Convencionais → Métodos Convencionais
- Evidências Eletrônicas → Novos Métodos/Ferramentas
- Por exemplo (e neste caso específico):
  - *Históricos de navegadores web;*
  - *E-mails recebidos/enviados via Webmail;*
  - *Consultas a sites de busca...*

- *Nem sempre as evidências estão nos arquivos (presentes na mídia periciada ou recuperados pós-deleção)*
- *Os web browsers podem ser fundamentais em uma investigação*

Computação Forense em Web Browsers
Onde buscar evidências?

- **Lado do Cliente**
  - *Web Browsers*
- **Lado do Servidor**
  - *Web Servers*
  - *Servidores de Aplicação*
  - *Servidores de Banco de Dados*
- **Ou ainda...**
  - *Tráfego de Rede*
  - *Características de Sistemas Operacionais Utilizados*

Computação Forense em Web Browsers
Quais os objetivos deste tipo de análise?

- Pornografia Infantil / Pedofilia
- Fraudes Eletrônicas
- Roubo de Identidade
- Espionagem Industrial
- Incidentes de Segurança “convencionais”
  - Vírus / Worms / Phishing
  - Hacking (casual ou direcionado)
  - ...

Um dos primeiros objetivos da análise é identificar se o(s) usuário(s) do equipamento/mídia periciado(a) é vítima ou está envolvido no incidente

Computação Forense em Web Browsers

Browsers Utilizados (opções):

- Internet Explorer
- Firefox / Mozilla / Netscape
- Outros:
  - *Konqueror*
  - *Opera*
  - *Safari*
  - *Galeon*
  - *Lynx / Links*
  - ...

Em <u>alguns casos</u> pode-se não dispôr de uma ferramenta adequada ao web browser utilizado/analisado

Computação Forense em Web Browsers

Internet Explorer (Windows)

- Registros de Evidências
  - **Web Browser History:** URLs de sites visitados
  - **Cookies:** Cookies que o usuário aceitou enquanto navegava
  - **Temporary Internet Files (cache):** Cópias de arquivos que foram usados para construir as páginas web
  - **Informações de Preenchimento de Formulários:** Se o recurso AutoComplete estiver habilitado
  - **Favorite Folder:** URLs de sites que o usuário marcou como favoritos
    - `C:\Documents and Settings\usuário\Favorites\`
      - Arquivos com extensão `.url`

Computação Forense em Web Browsers

Internet Explorer (Windows)

- Encontrando Informações:
  - Armazena informações de acesso de cada usuário em seu profile Windows:
    - Informações de Cache

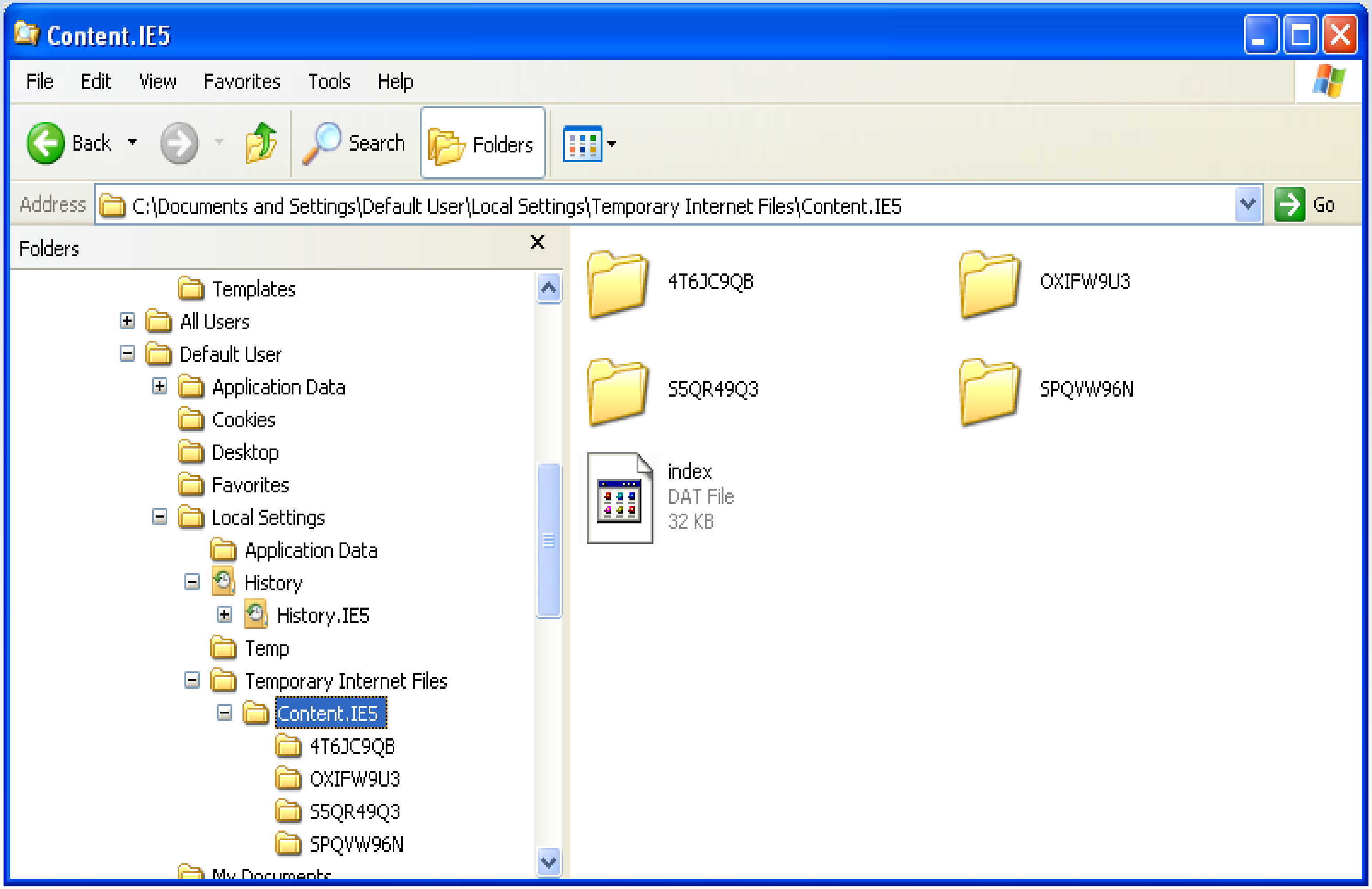
      C:\Documents and Settings\usuário\Local Settings\Temporary Internet Files\Content.IE5\
    - Histórico
      - C:\Documents and Settings\usuário\Local Settings\History\
    - Cookies
      - C:\Documents and Settings\usuário\Cookies\
    - Arquivos Temporários
      - C:\Documents and Settings\usuário\Local Settings\Temp\

Arquivo com Informações: *index.dat*

Computação Forense em Web Browsers

Internet Explorer (Windows)

- **Informações de Cache**



Content.IE5

File Edit View Favorites Tools Help

Back Search Folders

Address C:\Documents and Settings\Default User\Local Settings\Temporary Internet Files\Content.IE5

Go

Folders

- Templates
- All Users
- Default User
  - Application Data
  - Cookies
  - Desktop
  - Favorites
  - Local Settings
    - Application Data
    - History
      - History.IE5
    - Temp
    - Temporary Internet Files
      - Content.IE5
        - 4T6JC9QB
        - OXIFW9U3
        - S5QR49Q3
        - SPQVW96N
- My Documents

4T6JC9QB

OXIFW9U3

S5QR49Q3

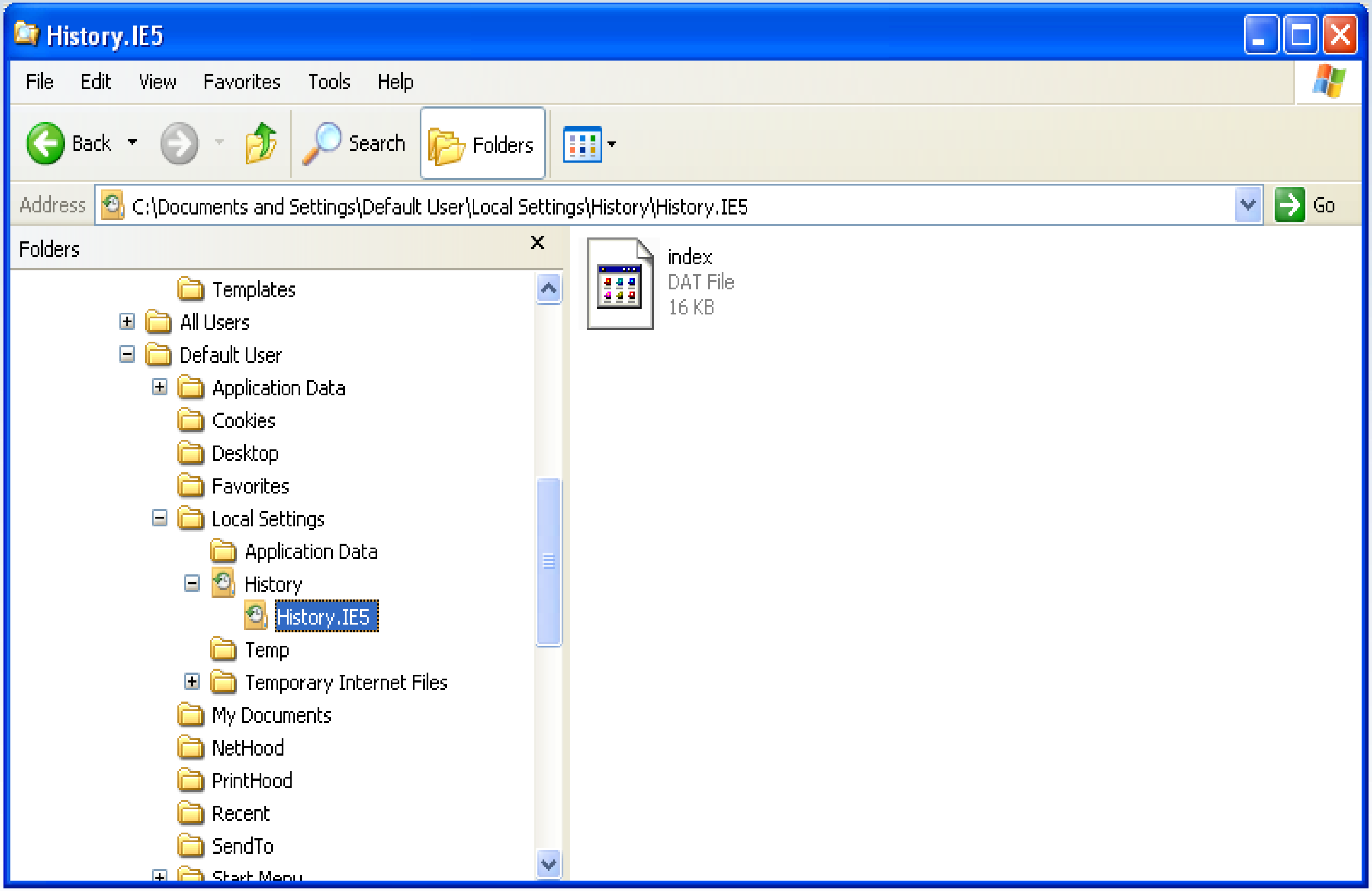
SPQVW96N

index
DAT File
32 KB

Computação Forense em Web Browsers

Internet Explorer (Windows)

- **Histórico**



History.IE5

Address: C:\Documents and Settings\Default User\Local Settings\History\History.IE5

index
DAT File
16 KB

Computação Forense em Web Browsers

Internet Explorer (Windows)

- Informações de Cache:
  - Recomenda-se o uso de ferramentas para explorar o arquivo index.dat com informações de cache (o arquivo tem formato específico) para a coleta de informações como:
    - URLs visitadas;
    - Nomes de arquivos armazenados localmente;
      - Permite visualizar a página acessada pelo usuário (que pode ser diferente da página atualmente exibida na URL)
    - Cabeçalhos (headers) HTTP
    - Timestamps de arquivos (último acesso, última modificação,...)

Computação Forense em Web Browsers

Internet Explorer (Windows)

- Cookies:
  - O acesso a páginas web é feito de modo stateless (nenhuma informação sobre conexões e estado de sessões é armazenada);
  - Cookies são usados para armazenar informações de quem acessa essas páginas (para aplicações que exigem informações persistentes)
  - Existem dois tipos de cookies: **session** e **persistent**
    - ***session cookies*** são armazenados na memória
    - ***persistent cookies*** são armazenados em disco

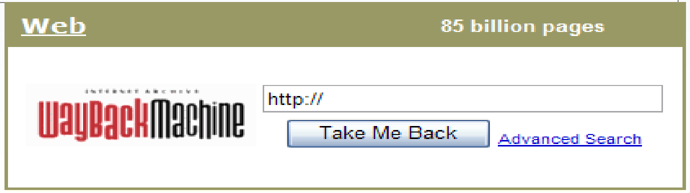
Cada persistent cookie é armazenado como um pequeno arquivo texto contendo nomes e valores, tempo em que o cookie foi baixado, tempo até que o cookie expire, informações de status ***(histórico dos cookies e não das URLs)***

Computação Forense em Web Browsers

Internet Explorer (Windows)

- Favorites:
  - URLs de páginas visitadas e assinaladas como favoritas pelo usuário (geralmente por interesse em retornar à página);
  - A perícia nestes sites deve ser realizada copiando a pasta para uma estação pericial e acessando as URLs para identicar seus conteúdos (sujeito à alteração de conteúdo);
  - É importante comparar a informação de data de modificação (Date Modified) com a data em que o link foi inserido na pasta;
  - O nome do link (caso o usuário não o tenha alterado ao inserir na pasta) é o título da mesma;

*Dica: Usar sites como o WayBackMachine (***www.archive.org***) para visualizar o conteúdo da página em uma data no passado*



Computação Forense em Web Browsers

Internet Explorer (Windows)

- Histórico (History Files):
  - Lista de sites recentemente visitados (mesmo que não tenham sido marcados como favoritos);
  - Esta lista é utilizada pelo recurso *AutoComplete* para sugerir URLs durante a digitação no browser;
- Registro do Windows:
  - Quando o usuário digita informações (nomes, endereços e senhas) em campos de formulário, o IE oferece a opção para relembrar estas informações...
  - ... Estas informações são armazenadas encriptadas no registro do Windows.

Computação Forense em Web Browsers

Firefox

- Histórico (History Files):
  - C:\Documents and Settings\usuário\Application Data\Mozilla\Firefox\Profiles\**<profilename>**\history.dat
- Cookies:
  - C:\Documents and Settings\usuário\Application Data\Mozilla\Firefox\Profiles\**<profilename>**\cookies.txt

O arquivo de cookies está em formato legível, enquanto o de histórico necessita de um “parser” para identificar informações

- Caching:
  - C:\Documents and Settings\usuário\Local Settings\Temp

Computação Forense em Web Browsers
Ferramentas

- Vantagens no uso de ferramentas específicas:
  - Identificação automática da **localização de arquivos**;
  - Resolução de problemas como nomes diferentes de arquivos (em função, por exemplo, de idioma ou versão do S.O.);
  - Parser automático de arquivos codificados;
  - Uso em vários tipos de browsers;
  - Apresentação mais “agradável”;
  - Relatórios mais detalhados;
  - Exportação para formatos manipuláveis.

Computação Forense em Web Browsers

Ferramentas

- Pasco
- Galleta
- Web Historian
- NetAnalysis
- Cache View
- IE History Viewer
- IE HistoryView
- IE CookiesView
- IE CacheView
- Mozilla HistoryView
- Mozilla CacheView
- Mozilla CookiesView

- wbf (Web Browser Forensics)
- Cache Monitor
- IE Cache Auditor
- Internet Cache Explorer
- STG Cache Audit
- Web Cache Illuminator
- Index.dat Analyzer (anti-forense)
- IE History Manager (anti-forense)

- Forensic Tool Kit
- EnCase
- Autopsy / Sleuthkit

Computação Forense em Web Browsers
Ferramenta :: Pasco

- Autor: Keith Jones
- Do latim “busca” (browse em inglês)
- Foco principal: Análise de arquivos de Cache
- Versões para Windows (Cygwin), MacOs X, Linux e BSDs
- Interface em linha de comando
- Reconstrói as estruturas internas do arquivo Index.dat do IE.
  - Recebe um arquivo Index.dat, reconstrói os registros, e retorna a informação em um arquivo formato texto.
  - Formato bastante prático em caso de necessidade de exportação de dados para uma planilha (como o Microsoft Excel).

Computação Forense em Web Browsers
Ferramenta :: Pasco

- Uso: pasco [opções] <nome_do_arquivo>

```
-d Undelete Activity Records

-t Field Delimiter (TAB by default)
```

- Exemplo de Uso:

```
% ./pasco index.dat > index.txt
```

  - Arquivo `index.txt` gerado com delimitador default TAB padronizado para abertura em planilha (MS Excel p.ex.)

```
http://www.foundstone.com/us/resources/proddesc/pasco.htm
```

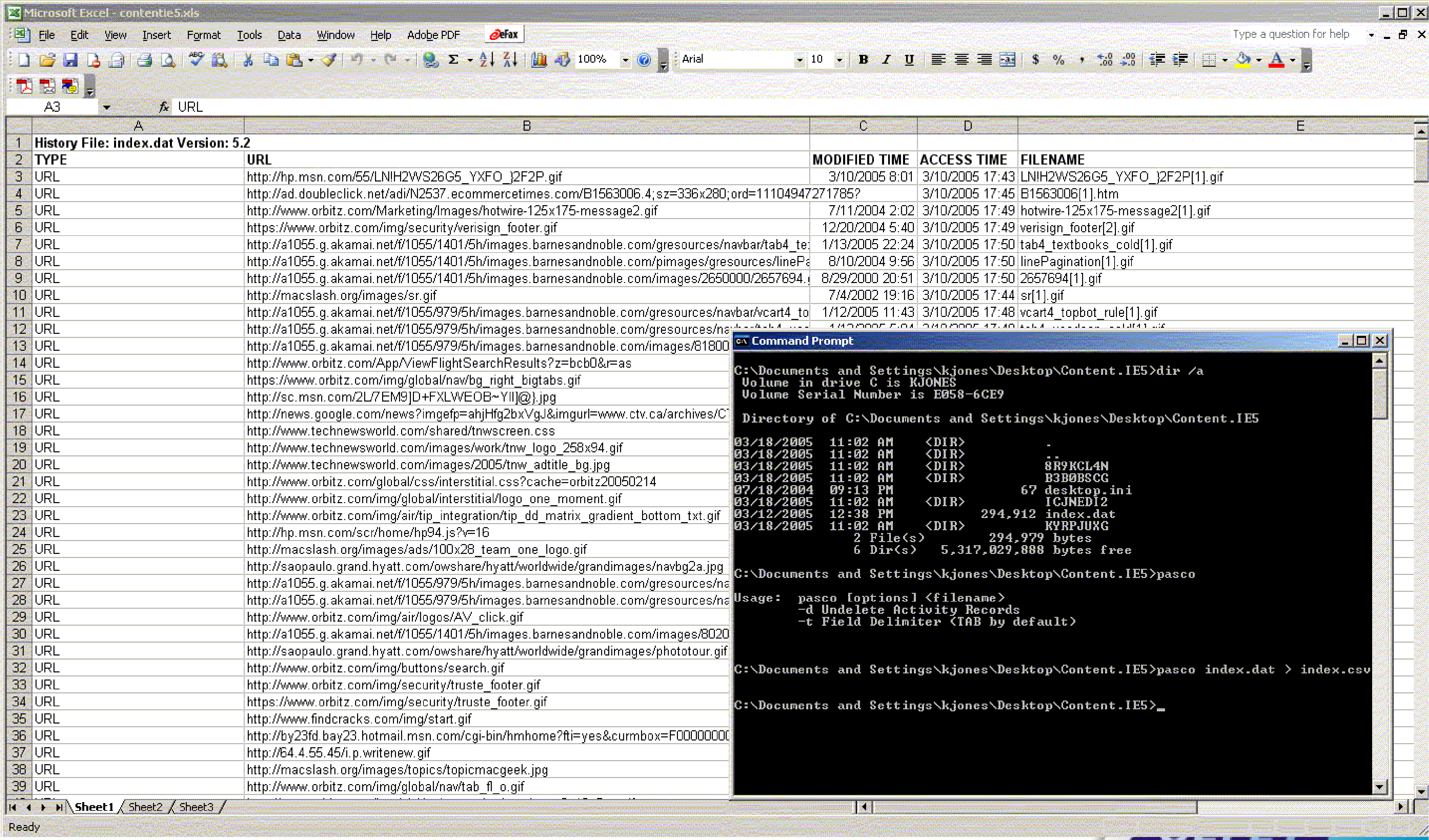
Computação Forense em Web Browsers

Ferramenta :: Pasco

- Campos exibidos (retirados do Index.dat):
  - The record type – Define se a atividade é uma URL, ou uma URL que foi procurada e direcionada para outro site.
  - URL – O site atual que foi visitado pelo usuário.
  - Modified Time – A última alteração sofrida pelo site.
  - Access Time – O momento que o usuário acessou o site.
  - Filename – O nome local do arquivo que contém uma cópia da URL listada.
  - Directory – Diretório local onde se pode achar o “Nome do Arquivo” acima.
  - HTTP Headers – Os cabeçalhos HTTP que o usuário recebeu quando acessou a URL.

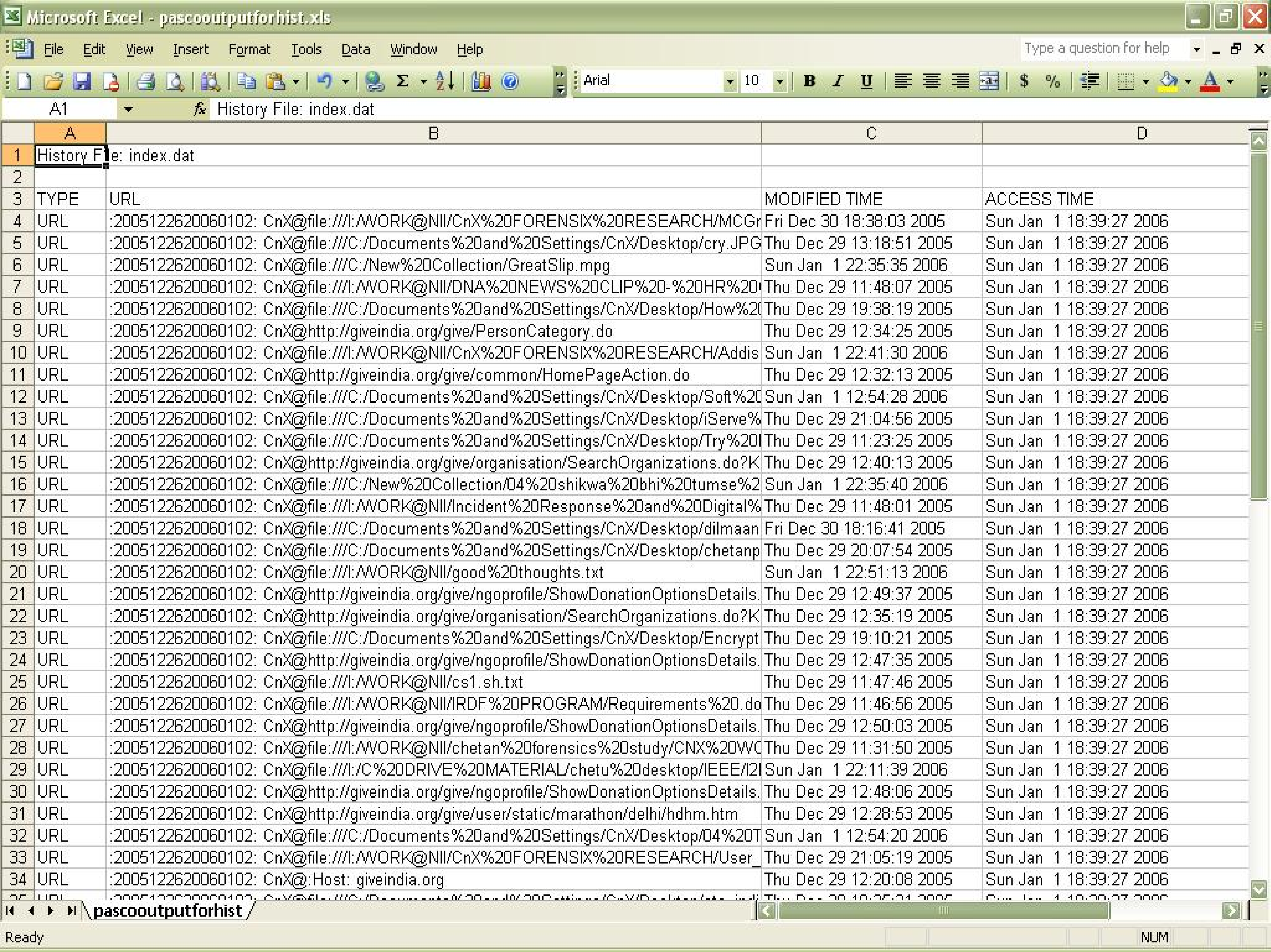
Computação Forense em Web Browsers

Ferramenta :: Pasco


Microsoft Excel - contentie5.xls
File Edit View Insert Format Tools Data Window Help Adobe PDF
eFax
Type a question for help
100%
Arial
10
A3
URL
Sheet1 Sheet2 Sheet3
Ready
Command Prompt

	A	B	C	D	E
1	**History File: index.dat Version: 5.2**				
2	**TYPE**	**URL**	**MODIFIED TIME**	**ACCESS TIME**	**FILENAME**
3	URL	http://hp.msn.com/55/LN!H2WS26G5_YXFO_}2F2P.gif	3/10/2005 8:01	3/10/2005 17:43	LN!H2WS26G5_YXFO_}2F2P[1].gif
4	URL	http://ad.doubleclick.net/adi/N2537.ecommercetimes.com/B1563006.4;sz=336x280;ord=11104947271785?		3/10/2005 17:45	B1563006[1].htm
5	URL	http://www.orbitz.com/Marketing/Images/hotwire-125x175-message2.gif	7/11/2004 2:02	3/10/2005 17:49	hotwire-125x175-message2[1].gif
6	URL	https://www.orbitz.com/img/security/verisign_footer.gif	12/20/2004 5:40	3/10/2005 17:49	verisign_footer[2].gif
7	URL	http://a1055.g.akamai.net/f/1055/1401/5h/images.barnesandnoble.com/gresources/navbar/tab4_te	1/13/2005 22:24	3/10/2005 17:50	tab4_textbooks_cold[1].gif
8	URL	http://a1055.g.akamai.net/f/1055/1401/5h/images.barnesandnoble.com/pimages/gresources/linePa	8/10/2004 9:56	3/10/2005 17:50	linePagination[1].gif
9	URL	http://a1055.g.akamai.net/f/1055/1401/5h/images.barnesandnoble.com/images/2650000/2657694.	8/29/2000 20:51	3/10/2005 17:50	2657694[1].gif
10	URL	http://macslash.org/images/sr.gif	7/4/2002 19:16	3/10/2005 17:44	sr[1].gif
11	URL	http://a1055.g.akamai.net/f/1055/979/5h/images.barnesandnoble.com/gresources/navbar/vcart4_to	1/12/2005 11:43	3/10/2005 17:48	vcart4_topbot_rule[1].gif
12	URL	http://a1055.g.akamai.net/f/1055/979/5h/images.barnesandnoble.com/gresources/na			
13	URL	http://a1055.g.akamai.net/f/1055/979/5h/images.barnesandnoble.com/images/81800			
14	URL	http://www.orbitz.com/App/ViewFlightSearchResults?z=bcb0&r=as			
15	URL	https://www.orbitz.com/img/global/nav/bg_right_bigtabs.gif			
16	URL	http://sc.msn.com/2L/7EM9]D+FXLWEOB~YII]@}.jpg			
17	URL	http://news.google.com/news?imgefp=ahjHfg2bxVgJ&imgurl=www.ctv.ca/archives/C			
18	URL	http://www.technewsworld.com/shared/tnwscreen.css			
19	URL	http://www.technewsworld.com/images/work/tnw_logo_258x94.gif			
20	URL	http://www.technewsworld.com/images/2005/tnw_adtitle_bg.jpg			
21	URL	http://www.orbitz.com/global/css/interstitial.css?cache=orbitz20050214			
22	URL	http://www.orbitz.com/img/global/interstitial/logo_one_moment.gif			
23	URL	http://www.orbitz.com/img/air/tip_integration/tip_dd_matrix_gradient_bottom_txt.gif			
24	URL	http://hp.msn.com/scr/home/hp94.js?v=16			
25	URL	http://macslash.org/images/ads/100x28_team_one_logo.gif			
26	URL	http://saopaulo.grand.hyatt.com/owshare/hyatt/worldwide/grandimages/navbg2a.jpg			
27	URL	http://a1055.g.akamai.net/f/1055/979/5h/images.barnesandnoble.com/gresources/na			
28	URL	http://a1055.g.akamai.net/f/1055/979/5h/images.barnesandnoble.com/gresources/na			
29	URL	http://www.orbitz.com/img/air/logos/AV_click.gif			
30	URL	http://a1055.g.akamai.net/f/1055/1401/5h/images.barnesandnoble.com/images/8020			
31	URL	http://saopaulo.grand.hyatt.com/owshare/hyatt/worldwide/grandimages/phototour.gif			
32	URL	http://www.orbitz.com/img/buttons/search.gif			
33	URL	http://www.orbitz.com/img/security/truste_footer.gif			
34	URL	https://www.orbitz.com/img/security/truste_footer.gif			
35	URL	http://www.findcracks.com/img/start.gif			
36	URL	http://by23fd.bay23.hotmail.msn.com/cgi-bin/hmhome?fti=yes&curmbox=F0000000			
37	URL	http://64.4.55.45/i.p.writenew.gif			
38	URL	http://macslash.org/images/topics/topicmacgeek.jpg			
39	URL	http://www.orbitz.com/img/global/nav/tab_fl_o.gif			

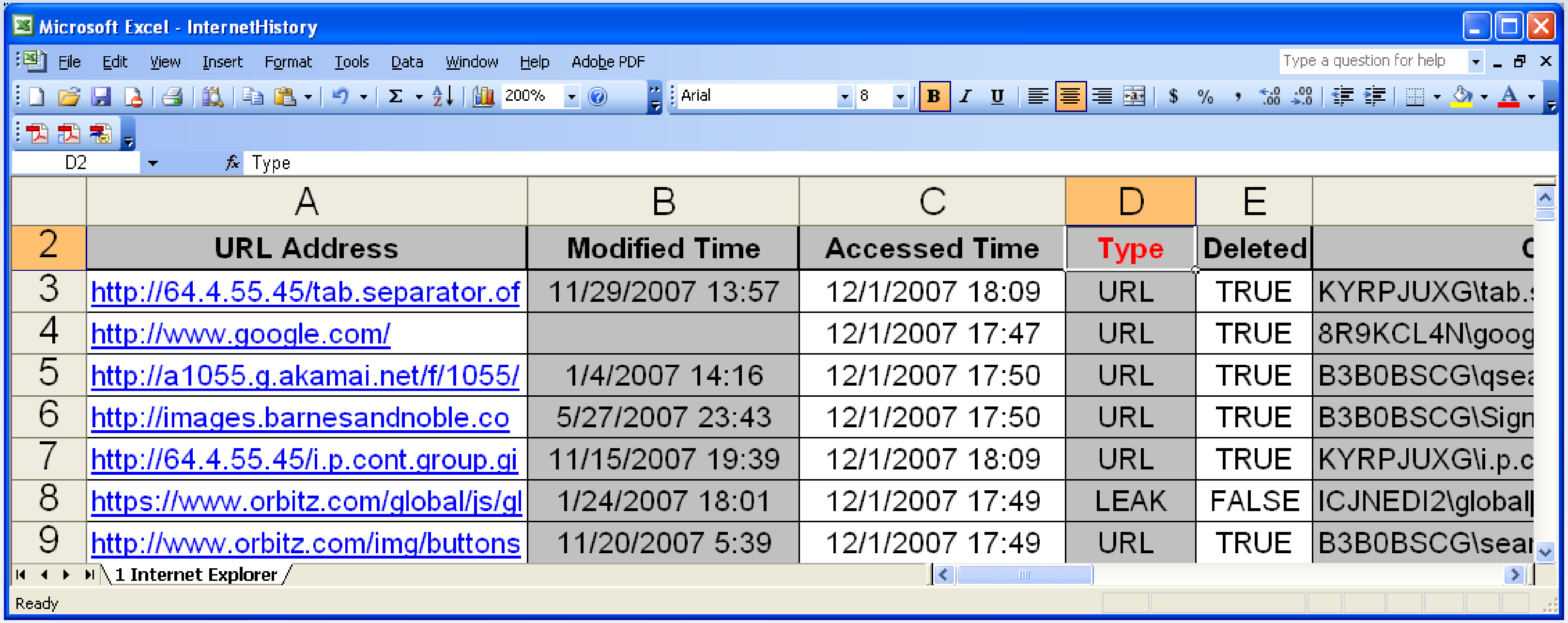
```
C:\Documents and Settings\kjones\Desktop\Content.IE5>dir /a
 Volume in drive C is KJONES
 Volume Serial Number is E058-6CE9

 Directory of C:\Documents and Settings\kjones\Desktop\Content.IE5

03/18/2005  11:02 AM    <DIR>          .
03/18/2005  11:02 AM    <DIR>          ..
03/18/2005  11:02 AM    <DIR>          8R9KCL4N
03/18/2005  11:02 AM    <DIR>          B3B0BSCG
07/18/2004  09:13 PM                67 desktop.ini
03/18/2005  11:02 AM    <DIR>          ICJNEDI2
03/12/2005  12:38 PM           294,912 index.dat
03/18/2005  11:02 AM    <DIR>          KYRPJUXG
               2 File(s)        294,979 bytes
               6 Dir(s)   5,317,029,888 bytes free

C:\Documents and Settings\kjones\Desktop\Content.IE5>pasco

Usage:   pasco [options] <filename>
         -d Undelete Activity Records
         -t Field Delimiter (TAB by default)


C:\Documents and Settings\kjones\Desktop\Content.IE5>pasco index.dat > index.csv


C:\Documents and Settings\kjones\Desktop\Content.IE5>_
```


Microsoft Excel - pascooutputforhist.xls
File Edit View Insert Format Tools Data Window Help
Type a question for help
Arial
10
A1
History File: index.dat
pascooutputforhist
Ready
NUM

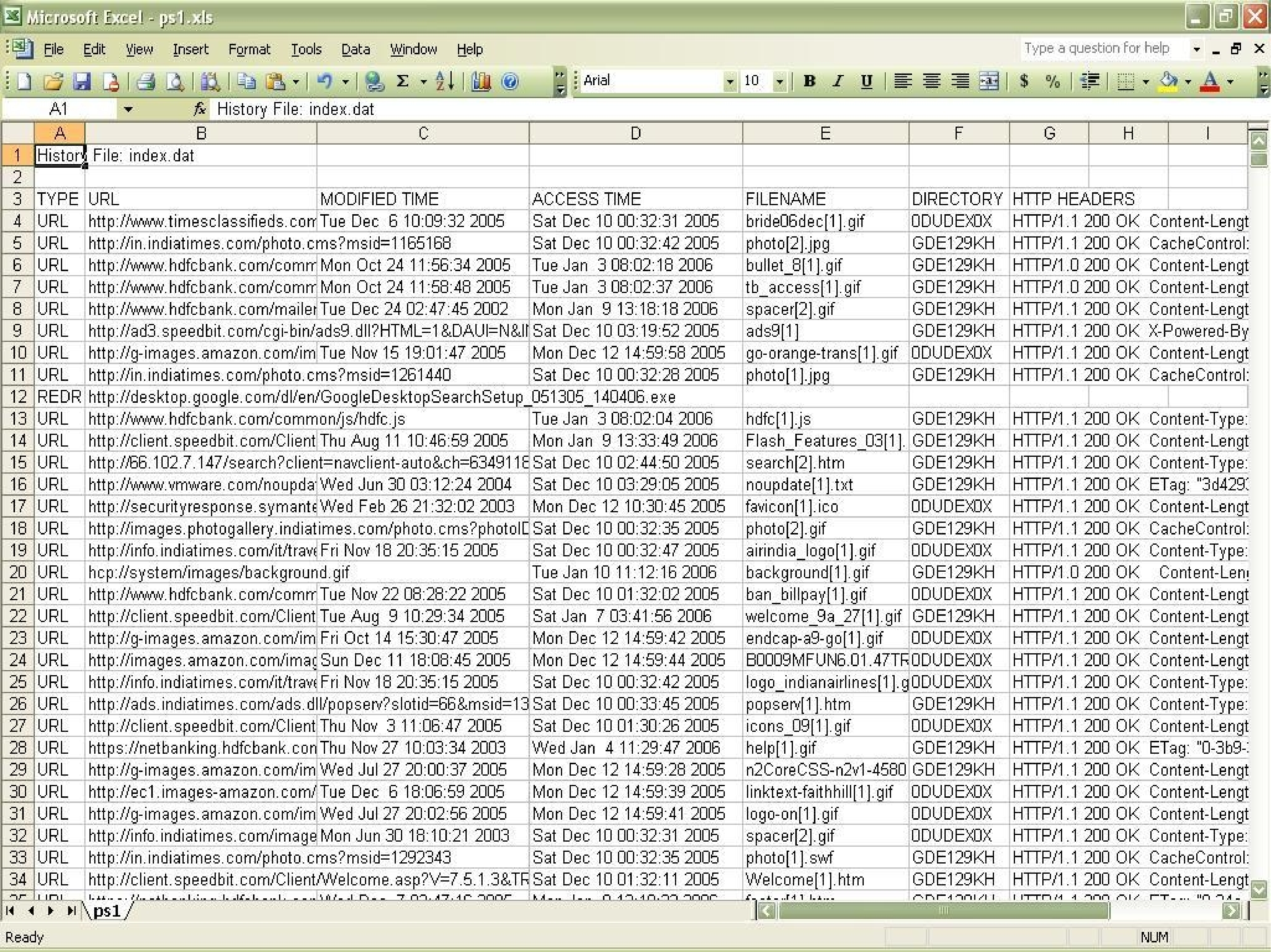
	A	B	C	D
1	History File: index.dat			
2				
3	TYPE	URL	MODIFIED TIME	ACCESS TIME
4	URL	:2005122620060102: CnX@file:///I:/WORK@NII/CnX%20FORENSIX%20RESEARCH/MCGr	Fri Dec 30 18:38:03 2005	Sun Jan 1 18:39:27 2006
5	URL	:2005122620060102: CnX@file:///C:/Documents%20and%20Settings/CnX/Desktop/cry.JPG	Thu Dec 29 13:18:51 2005	Sun Jan 1 18:39:27 2006
6	URL	:2005122620060102: CnX@file:///C:/New%20Collection/GreatSlip.mpg	Sun Jan 1 22:35:35 2006	Sun Jan 1 18:39:27 2006
7	URL	:2005122620060102: CnX@file:///I:/WORK@NII/DNA%20NEWS%20CLIP%20-%20HR%20	Thu Dec 29 11:48:07 2005	Sun Jan 1 18:39:27 2006
8	URL	:2005122620060102: CnX@file:///C:/Documents%20and%20Settings/CnX/Desktop/How%20	Thu Dec 29 19:38:19 2005	Sun Jan 1 18:39:27 2006
9	URL	:2005122620060102: CnX@http://giveindia.org/give/PersonCategory.do	Thu Dec 29 12:34:25 2005	Sun Jan 1 18:39:27 2006
10	URL	:2005122620060102: CnX@file:///I:/WORK@NII/CnX%20FORENSIX%20RESEARCH/Addis	Sun Jan 1 22:41:30 2006	Sun Jan 1 18:39:27 2006
11	URL	:2005122620060102: CnX@http://giveindia.org/give/common/HomePageAction.do	Thu Dec 29 12:32:13 2005	Sun Jan 1 18:39:27 2006
12	URL	:2005122620060102: CnX@file:///C:/Documents%20and%20Settings/CnX/Desktop/Soft%20	Sun Jan 1 12:54:28 2006	Sun Jan 1 18:39:27 2006
13	URL	:2005122620060102: CnX@file:///C:/Documents%20and%20Settings/CnX/Desktop/iServe%	Thu Dec 29 21:04:56 2005	Sun Jan 1 18:39:27 2006
14	URL	:2005122620060102: CnX@file:///C:/Documents%20and%20Settings/CnX/Desktop/Try%20	Thu Dec 29 11:23:25 2005	Sun Jan 1 18:39:27 2006
15	URL	:2005122620060102: CnX@http://giveindia.org/give/organisation/SearchOrganizations.do?K	Thu Dec 29 12:40:13 2005	Sun Jan 1 18:39:27 2006
16	URL	:2005122620060102: CnX@file:///C:/New%20Collection/04%20shikwa%20bhi%20tumse%2	Sun Jan 1 22:35:40 2006	Sun Jan 1 18:39:27 2006
17	URL	:2005122620060102: CnX@file:///I:/WORK@NII/Incident%20Response%20and%20Digital%	Thu Dec 29 11:48:01 2005	Sun Jan 1 18:39:27 2006
18	URL	:2005122620060102: CnX@file:///C:/Documents%20and%20Settings/CnX/Desktop/dilmaan	Fri Dec 30 18:16:41 2005	Sun Jan 1 18:39:27 2006
19	URL	:2005122620060102: CnX@file:///C:/Documents%20and%20Settings/CnX/Desktop/chetanp	Thu Dec 29 20:07:54 2005	Sun Jan 1 18:39:27 2006
20	URL	:2005122620060102: CnX@file:///I:/WORK@NII/good%20thoughts.txt	Sun Jan 1 22:51:13 2006	Sun Jan 1 18:39:27 2006
21	URL	:2005122620060102: CnX@http://giveindia.org/give/ngoprofile/ShowDonationOptionsDetails.	Thu Dec 29 12:49:37 2005	Sun Jan 1 18:39:27 2006
22	URL	:2005122620060102: CnX@http://giveindia.org/give/organisation/SearchOrganizations.do?K	Thu Dec 29 12:35:19 2005	Sun Jan 1 18:39:27 2006
23	URL	:2005122620060102: CnX@file:///C:/Documents%20and%20Settings/CnX/Desktop/Encrypt	Thu Dec 29 19:10:21 2005	Sun Jan 1 18:39:27 2006
24	URL	:2005122620060102: CnX@http://giveindia.org/give/ngoprofile/ShowDonationOptionsDetails.	Thu Dec 29 12:47:35 2005	Sun Jan 1 18:39:27 2006
25	URL	:2005122620060102: CnX@file:///I:/WORK@NII/cs1.sh.txt	Thu Dec 29 11:47:46 2005	Sun Jan 1 18:39:27 2006
26	URL	:2005122620060102: CnX@file:///I:/WORK@NII/IRDF%20PROGRAM/Requirements%20.do	Thu Dec 29 11:46:56 2005	Sun Jan 1 18:39:27 2006
27	URL	:2005122620060102: CnX@http://giveindia.org/give/ngoprofile/ShowDonationOptionsDetails.	Thu Dec 29 12:50:03 2005	Sun Jan 1 18:39:27 2006
28	URL	:2005122620060102: CnX@file:///I:/WORK@NII/chetan%20forensics%20study/CNX%20W	Thu Dec 29 11:31:50 2005	Sun Jan 1 18:39:27 2006
29	URL	:2005122620060102: CnX@file:///I:/C%20DRIVE%20MATERIAL/chetu%20desktop/IEEE/I2	Sun Jan 1 22:11:39 2006	Sun Jan 1 18:39:27 2006
30	URL	:2005122620060102: CnX@http://giveindia.org/give/ngoprofile/ShowDonationOptionsDetails.	Thu Dec 29 12:48:06 2005	Sun Jan 1 18:39:27 2006
31	URL	:2005122620060102: CnX@http://giveindia.org/give/user/static/marathon/delhi/hdhm.htm	Thu Dec 29 12:28:53 2005	Sun Jan 1 18:39:27 2006
32	URL	:2005122620060102: CnX@file:///C:/Documents%20and%20Settings/CnX/Desktop/04%20T	Sun Jan 1 12:54:20 2006	Sun Jan 1 18:39:27 2006
33	URL	:2005122620060102: CnX@file:///I:/WORK@NII/CnX%20FORENSIX%20RESEARCH/User_	Thu Dec 29 21:05:19 2005	Sun Jan 1 18:39:27 2006
34	URL	:2005122620060102: CnX@:Host: giveindia.org	Thu Dec 29 12:20:08 2005	Sun Jan 1 18:39:27 2006

Computação Forense em Web Browsers

Ferramenta :: Pasco



	A	B	C	D	E	
2	URL Address	Modified Time	Accessed Time	Type	Deleted	C
3	http://64.4.55.45/tab.separator.of	11/29/2007 13:57	12/1/2007 18:09	URL	TRUE	KYRPJUXG\tab.s
4	http://www.google.com/		12/1/2007 17:47	URL	TRUE	8R9KCL4N\goog
5	http://a1055.g.akamai.net/f/1055/	1/4/2007 14:16	12/1/2007 17:50	URL	TRUE	B3B0BSCG\qsea
6	http://images.barnesandnoble.co	5/27/2007 23:43	12/1/2007 17:50	URL	TRUE	B3B0BSCG\Sign
7	http://64.4.55.45/i.p.cont.group.gi	11/15/2007 19:39	12/1/2007 18:09	URL	TRUE	KYRPJUXG\i.p.c
8	https://www.orbitz.com/global/js/gl	1/24/2007 18:01	12/1/2007 17:49	LEAK	FALSE	ICJNEDI2\global
9	http://www.orbitz.com/img/buttons	11/20/2007 5:39	12/1/2007 17:49	URL	TRUE	B3B0BSCG\sear



A1 History File: index.dat

	A	B	C	D	E	F	G	H	I
1	History File: index.dat								
2									
3	TYPE	URL	MODIFIED TIME	ACCESS TIME	FILENAME	DIRECTORY	HTTP HEADERS		
4	URL	http://www.timesclassifieds.con	Tue Dec 6 10:09:32 2005	Sat Dec 10 00:32:31 2005	bride06dec[1].gif	0DUDEX0X	HTTP/1.1 200 OK Content-Lengt		
5	URL	http://in.indiatimes.com/photo.cms?msid=1165168		Sat Dec 10 00:32:42 2005	photo[2].jpg	GDE129KH	HTTP/1.1 200 OK CacheControl:		
6	URL	http://www.hdfcbank.com/comm	Mon Oct 24 11:56:34 2005	Tue Jan 3 08:02:18 2006	bullet_8[1].gif	GDE129KH	HTTP/1.0 200 OK Content-Lengt		
7	URL	http://www.hdfcbank.com/comm	Mon Oct 24 11:58:48 2005	Tue Jan 3 08:02:37 2006	tb_access[1].gif	GDE129KH	HTTP/1.0 200 OK Content-Lengt		
8	URL	http://www.hdfcbank.com/mailer	Tue Dec 24 02:47:45 2002	Mon Jan 9 13:18:18 2006	spacer[2].gif	GDE129KH	HTTP/1.1 200 OK Content-Lengt		
9	URL	http://ad3.speedbit.com/cgi-bin/ads9.dll?HTML=1&DAUI=N&II		Sat Dec 10 03:19:52 2005	ads9[1]	GDE129KH	HTTP/1.1 200 OK X-Powered-By		
10	URL	http://g-images.amazon.com/im	Tue Nov 15 19:01:47 2005	Mon Dec 12 14:59:58 2005	go-orange-trans[1].gif	0DUDEX0X	HTTP/1.1 200 OK Content-Lengt		
11	URL	http://in.indiatimes.com/photo.cms?msid=1261440		Sat Dec 10 00:32:28 2005	photo[1].jpg	GDE129KH	HTTP/1.1 200 OK CacheControl:		
12	REDR	http://desktop.google.com/dl/en/GoogleDesktopSearchSetup_051305_140406.exe							
13	URL	http://www.hdfcbank.com/common/js/hdfc.js		Tue Jan 3 08:02:04 2006	hdfc[1].js	GDE129KH	HTTP/1.1 200 OK Content-Type:		
14	URL	http://client.speedbit.com/Client	Thu Aug 11 10:46:59 2005	Mon Jan 9 13:33:49 2006	Flash_Features_03[1].	GDE129KH	HTTP/1.1 200 OK Content-Lengt		
15	URL	http://66.102.7.147/search?client=navclient-auto&ch=6349118		Sat Dec 10 02:44:50 2005	search[2].htm	GDE129KH	HTTP/1.1 200 OK Content-Type:		
16	URL	http://www.vmware.com/noupda	Wed Jun 30 03:12:24 2004	Sat Dec 10 03:29:05 2005	noupdate[1].txt	GDE129KH	HTTP/1.1 200 OK ETag: "3d429:		
17	URL	http://securityresponse.symante	Wed Feb 26 21:32:02 2003	Mon Dec 12 10:30:45 2005	favicon[1].ico	0DUDEX0X	HTTP/1.1 200 OK Content-Lengt		
18	URL	http://images.photogallery.indiatimes.com/photo.cms?photoID		Sat Dec 10 00:32:35 2005	photo[2].gif	GDE129KH	HTTP/1.1 200 OK CacheControl:		
19	URL	http://info.indiatimes.com/it/trav	Fri Nov 18 20:35:15 2005	Sat Dec 10 00:32:47 2005	airindia_logo[1].gif	0DUDEX0X	HTTP/1.1 200 OK Content-Type:		
20	URL	hcp://system/images/background.gif		Tue Jan 10 11:12:16 2006	background[1].gif	GDE129KH	HTTP/1.0 200 OK Content-Len		
21	URL	http://www.hdfcbank.com/comm	Tue Nov 22 08:28:22 2005	Sat Dec 10 01:32:02 2005	ban_billpay[1].gif	0DUDEX0X	HTTP/1.1 200 OK Content-Lengt		
22	URL	http://client.speedbit.com/Client	Tue Aug 9 10:29:34 2005	Sat Jan 7 03:41:56 2006	welcome_9a_27[1].gif	GDE129KH	HTTP/1.1 200 OK Content-Lengt		
23	URL	http://g-images.amazon.com/im	Fri Oct 14 15:30:47 2005	Mon Dec 12 14:59:42 2005	endcap-a9-go[1].gif	0DUDEX0X	HTTP/1.1 200 OK Content-Lengt		
24	URL	http://images.amazon.com/imag	Sun Dec 11 18:08:45 2005	Mon Dec 12 14:59:44 2005	B0009MFUN6.01.47TR	0DUDEX0X	HTTP/1.1 200 OK Content-Lengt		
25	URL	http://info.indiatimes.com/it/trav	Fri Nov 18 20:35:15 2005	Sat Dec 10 00:32:42 2005	logo_indianairlines[1].g	0DUDEX0X	HTTP/1.1 200 OK Content-Type:		
26	URL	http://ads.indiatimes.com/ads.dll/popserv?slotid=66&msid=13		Sat Dec 10 00:33:45 2005	popserv[1].htm	GDE129KH	HTTP/1.1 200 OK Content-Type:		
27	URL	http://client.speedbit.com/Client	Thu Nov 3 11:06:47 2005	Sat Dec 10 01:30:26 2005	icons_09[1].gif	0DUDEX0X	HTTP/1.1 200 OK Content-Lengt		
28	URL	https://netbanking.hdfcbank.con	Thu Nov 27 10:03:34 2003	Wed Jan 4 11:29:47 2006	help[1].gif	GDE129KH	HTTP/1.1 200 OK ETag: "0-3b9-:		
29	URL	http://g-images.amazon.com/im	Wed Jul 27 20:00:37 2005	Mon Dec 12 14:59:28 2005	n2CoreCSS-n2v1-4580	GDE129KH	HTTP/1.1 200 OK Content-Lengt		
30	URL	http://ec1.images-amazon.com/	Tue Dec 6 18:06:59 2005	Mon Dec 12 14:59:39 2005	linktext-faithhill[1].gif	0DUDEX0X	HTTP/1.1 200 OK Content-Lengt		
31	URL	http://g-images.amazon.com/im	Wed Jul 27 20:02:56 2005	Mon Dec 12 14:59:41 2005	logo-on[1].gif	0DUDEX0X	HTTP/1.1 200 OK Content-Lengt		
32	URL	http://info.indiatimes.com/image	Mon Jun 30 18:10:21 2003	Sat Dec 10 00:32:31 2005	spacer[2].gif	0DUDEX0X	HTTP/1.1 200 OK Content-Type:		
33	URL	http://in.indiatimes.com/photo.cms?msid=1292343		Sat Dec 10 00:32:35 2005	photo[1].swf	GDE129KH	HTTP/1.1 200 OK CacheControl:		
34	URL	http://client.speedbit.com/Client/Welcome.asp?V=7.5.1.3&TR		Sat Dec 10 01:32:11 2005	Welcome[1].htm	GDE129KH	HTTP/1.1 200 OK Content-Lengt		

Computação Forense em Web Browsers
Ferramenta :: Galleta

- Autor: Keith Jones
- Do espanhol “cookie”
- Foco principal: Análise de arquivos de Cookie
- Versões para Windows (Cygwin), MacOs X, Linux e BSDs
- Interface em linha de comando
  - Recebe um arquivo de Cookie, reconstrói os registros, e retorna a informação em um arquivo formato texto.
  - Formato bastante prático em caso de necessidade de exportação de dados para uma planilha (como o Microsoft Excel).

Computação Forense em Web Browsers

Ferramenta :: Galleta

- Uso: `galleta [opções] <nome_do_arquivo>`

  `-t Campo delimitador (TAB por default)`

- Exemplo de Uso:

  ```
  % ./galleta arquivoexemplo.txt > cookies.txt
  ```

  - Arquivo `cookies.txt` gerado com delimitador default TAB padronizado para abertura em planilha (MS Excel p.ex.)

http://www.foundstone.com/us/resources/proddesc/galleta.htm

Computação Forense em Web Browsers
Ferramenta :: Web Historian

- Autor: Red Cliff's (Mandiant)
- Foco principal: Histórico de URLs visitadas
- S.O.: MS Windows

Free Software

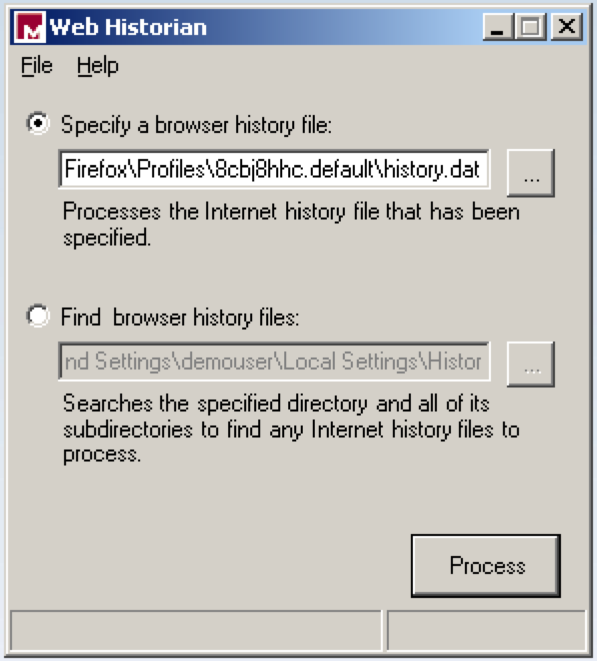
```
http://www.mandiant.com/webhistorian.htm
```

- **Busca e identifica arquivos importantes dos seguintes navegadores:**
  - Internet Explorer
  - Mozilla / Firefox / Netscape
  - Safari (Apple OS X)
  - Opera

– **Produz resultados nos formatos:**
  - Excel Nativo
  - HTML
  - Arquivo Texto

Computação Forense em Web Browsers

Ferramenta :: Web Historian



● Specify a browser history file:

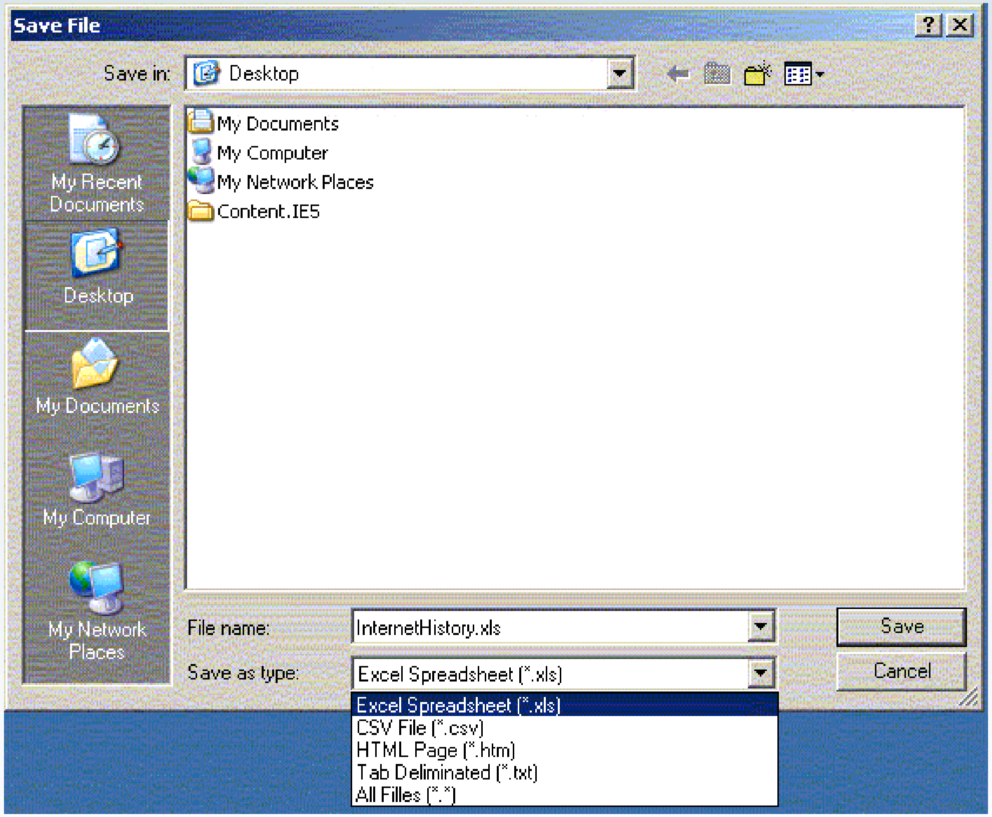
Firefox\Profiles\8cbj8hhc.default\history.dat

Processes the Internet history file that has been specified.

○ Find browser history files:

nd Settings\demouser\Local Settings\Histor

Searches the specified directory and all of its subdirectories to find any Internet history files to process.



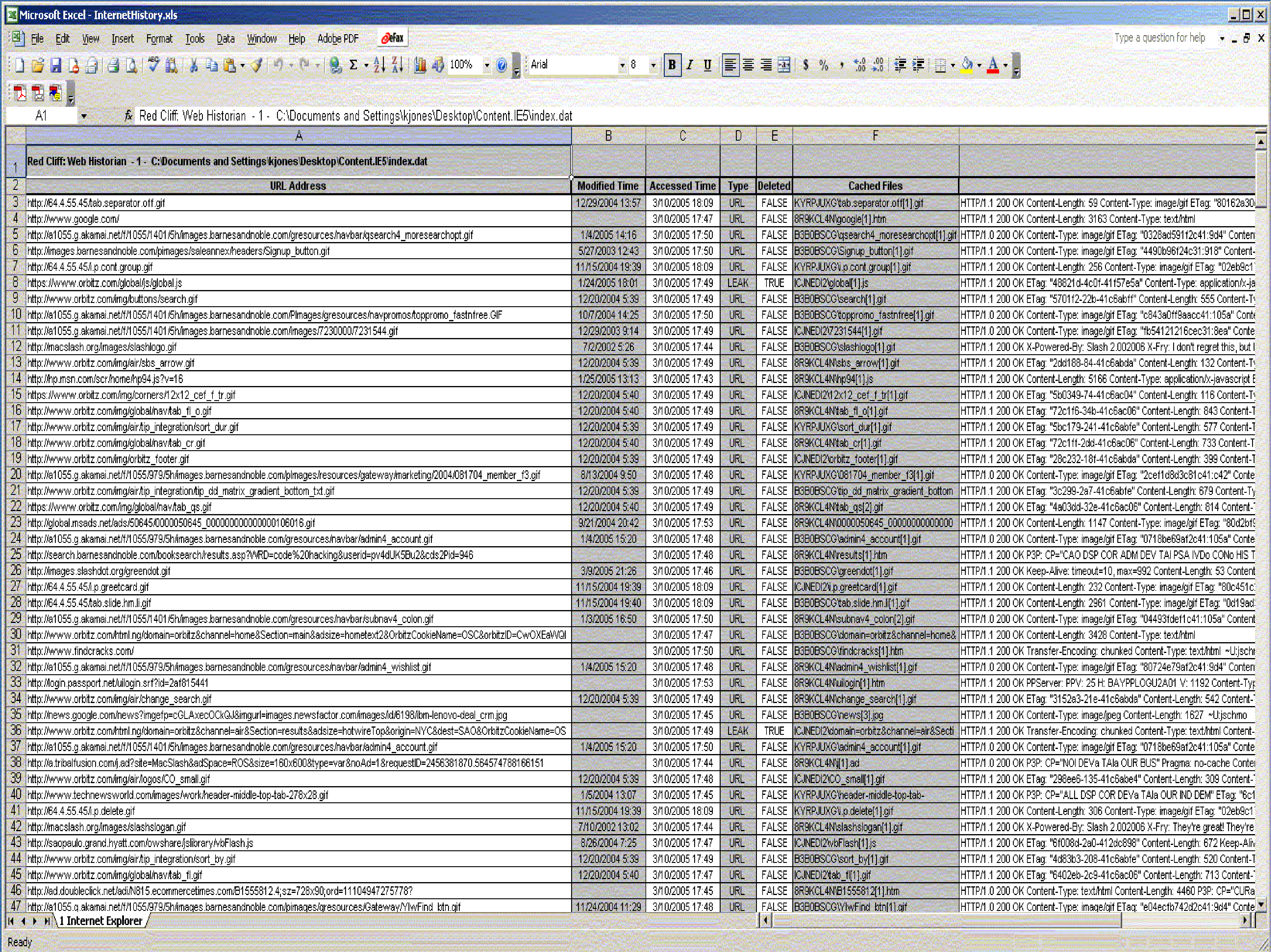
Save in: Desktop

My Documents
My Computer
My Network Places
Content.IE5

File name: InternetHistory.xls

Save as type: Excel Spreadsheet (*.xls)

Excel Spreadsheet (*.xls)
CSV File (*.csv)
HTML Page (*.htm)
Tab Deliminated (*.txt)
All Files (*.*)

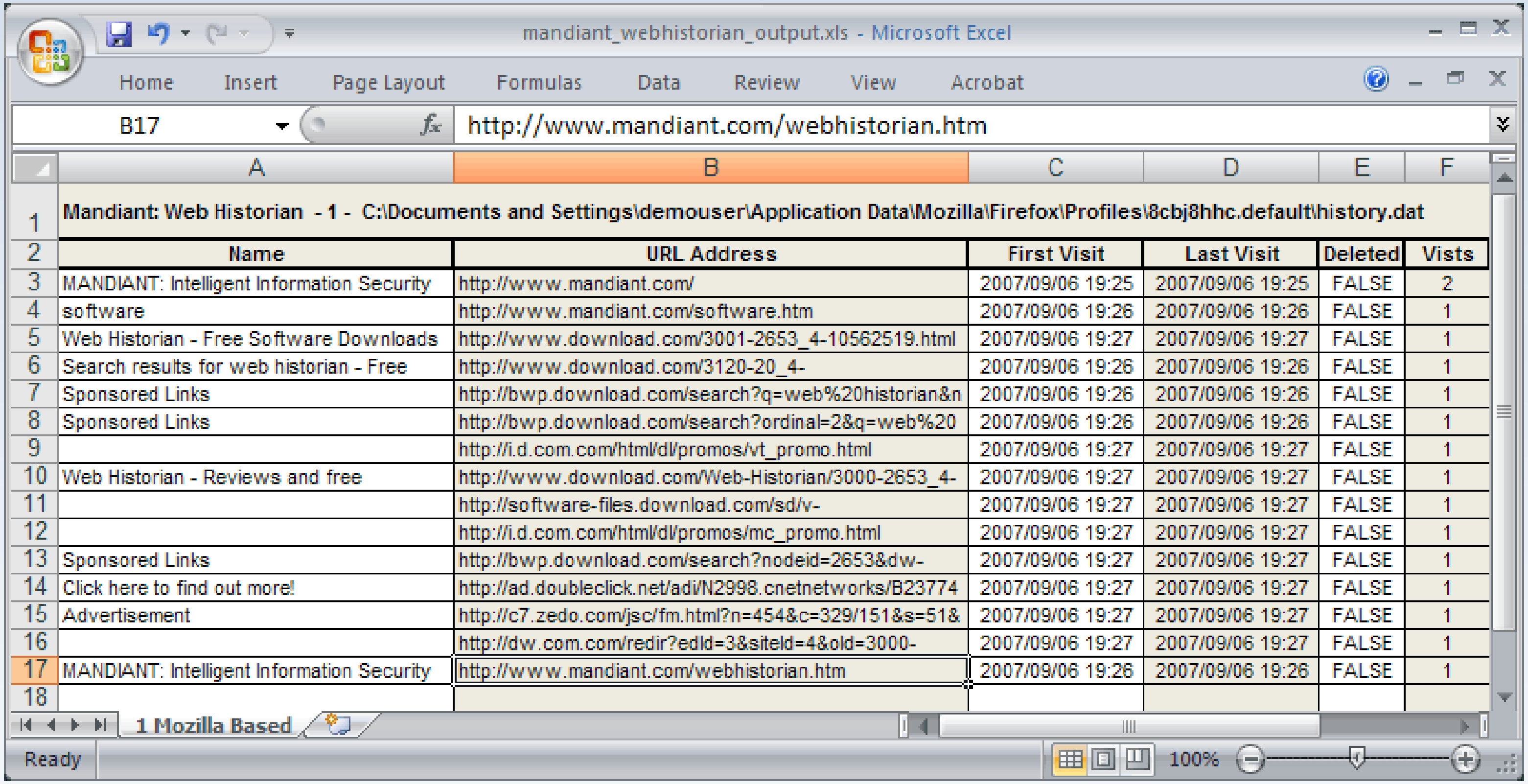


A1 *fx* Red Cliff: Web Historian - 1 - C:\Documents and Settings\kjones\Desktop\Content.IE5\index.dat

	A	B	C	D	E	F	
1	Red Cliff: Web Historian - 1 - C:\Documents and Settings\kjones\Desktop\Content.IE5\index.dat						
2	URL Address	Modified Time	Accessed Time	Type	Deleted	Cached Files	
3	http://64.4.55.45/tab.separator.off.gif	12/29/2004 13:57	3/10/2005 18:09	URL	FALSE	KYRPJUXG\tab.separator.off[1].gif	HTTP/1.1 200 OK Content-Length: 59 Content-Type: image/gif ETag: "80162a30
4	http://www.google.com/		3/10/2005 17:47	URL	FALSE	8R9KCL4N\google[1].htm	HTTP/1.1 200 OK Content-Length: 3163 Content-Type: text/html
5	http://a1055.g.akamai.net/f/1055/1401/5h/images.barnesandnoble.com/gresources/navbar/qsearch4_moresearchopt.gif	1/4/2005 14:16	3/10/2005 17:50	URL	FALSE	B3B0BSCG\qsearch4_moresearchopt[1].gif	HTTP/1.0 200 OK Content-Type: image/gif ETag: "0328ad591f2c41:9d4" Conten
6	http://images.barnesandnoble.com/pimages/saleannex/headers/Signup_button.gif	5/27/2003 12:43	3/10/2005 17:50	URL	FALSE	B3B0BSCG\Signup_button[1].gif	HTTP/1.1 200 OK Content-Type: image/gif ETag: "4490b96f24c31:918" Content-
7	http://64.4.55.45/i.p.cont.group.gif	11/15/2004 19:39	3/10/2005 18:09	URL	FALSE	KYRPJUXG\i.p.cont.group[1].gif	HTTP/1.1 200 OK Content-Length: 256 Content-Type: image/gif ETag: "02eb9c1
8	https://www.orbitz.com/global/js/global.js	1/24/2005 18:01	3/10/2005 17:49	LEAK	TRUE	ICJNEDI2\global[1].js	HTTP/1.1 200 OK ETag: "48821d-4c0f-41f57e5a" Content-Type: application/x-ja
9	http://www.orbitz.com/img/buttons/search.gif	12/20/2004 5:39	3/10/2005 17:49	URL	FALSE	B3B0BSCG\search[1].gif	HTTP/1.1 200 OK ETag: "5701f2-22b-41c6abff" Content-Length: 555 Content-Ty
10	http://a1055.g.akamai.net/f/1055/1401/5h/images.barnesandnoble.com/PImages/gresources/navpromos/toppromo_fastnfree.GIF	10/7/2004 14:25	3/10/2005 17:50	URL	FALSE	B3B0BSCG\toppromo_fastnfree[1].gif	HTTP/1.0 200 OK Content-Type: image/gif ETag: "c843a0ff9aacc41:105a" Conte
11	http://a1055.g.akamai.net/f/1055/1401/5h/images.barnesandnoble.com/images/7230000/7231544.gif	12/29/2003 9:14	3/10/2005 17:49	URL	FALSE	ICJNEDI2\7231544[1].gif	HTTP/1.0 200 OK Content-Type: image/gif ETag: "fb54121216cec31:8ea" Conte
12	http://macslash.org/images/slashlogo.gif	7/2/2002 5:26	3/10/2005 17:44	URL	FALSE	B3B0BSCG\slashlogo[1].gif	HTTP/1.1 200 OK X-Powered-By: Slash 2.002006 X-Fry: I don't regret this, but I
13	http://www.orbitz.com/img/air/sbs_arrow.gif	12/20/2004 5:39	3/10/2005 17:49	URL	FALSE	8R9KCL4N\sbs_arrow[1].gif	HTTP/1.1 200 OK ETag: "2dd188-84-41c6abda" Content-Length: 132 Content-Ty
14	http://hp.msn.com/scr/home/hp94.js?v=16	1/25/2005 13:13	3/10/2005 17:43	URL	FALSE	8R9KCL4N\hp94[1].js	HTTP/1.1 200 OK Content-Length: 5166 Content-Type: application/x-javascript E
15	https://www.orbitz.com/img/corners/12x12_cef_f_tr.gif	12/20/2004 5:40	3/10/2005 17:49	URL	FALSE	ICJNEDI2\12x12_cef_f_tr[1].gif	HTTP/1.1 200 OK ETag: "5b0349-74-41c6ac04" Content-Length: 116 Content-Ty
16	http://www.orbitz.com/img/global/nav/tab_fl_o.gif	12/20/2004 5:40	3/10/2005 17:49	URL	FALSE	8R9KCL4N\tab_fl_o[1].gif	HTTP/1.1 200 OK ETag: "72c1f6-34b-41c6ac06" Content-Length: 843 Content-T
17	http://www.orbitz.com/img/air/tip_integration/sort_dur.gif	12/20/2004 5:39	3/10/2005 17:49	URL	FALSE	KYRPJUXG\sort_dur[1].gif	HTTP/1.1 200 OK ETag: "5bc179-241-41c6abfe" Content-Length: 577 Content-T
18	http://www.orbitz.com/img/global/nav/tab_cr.gif	12/20/2004 5:40	3/10/2005 17:49	URL	FALSE	8R9KCL4N\tab_cr[1].gif	HTTP/1.1 200 OK ETag: "72c1ff-2dd-41c6ac06" Content-Length: 733 Content-T
19	http://www.orbitz.com/img/orbitz_footer.gif	12/20/2004 5:39	3/10/2005 17:49	URL	FALSE	ICJNEDI2\orbitz_footer[1].gif	HTTP/1.1 200 OK ETag: "28c232-18f-41c6abda" Content-Length: 399 Content-T
20	http://a1055.g.akamai.net/f/1055/979/5h/images.barnesandnoble.com/pImages/resources/gateway/marketing/2004/081704_member_f3.gif	8/13/2004 9:50	3/10/2005 17:48	URL	FALSE	KYRPJUXG\081704_member_f3[1].gif	HTTP/1.0 200 OK Content-Type: image/gif ETag: "2cef1d8d3c81c41:c42" Conte
21	http://www.orbitz.com/img/air/tip_integration/tip_dd_matrix_gradient_bottom_txt.gif	12/20/2004 5:39	3/10/2005 17:49	URL	FALSE	B3B0BSCG\tip_dd_matrix_gradient_bottom	HTTP/1.1 200 OK ETag: "3c299-2a7-41c6abfe" Content-Length: 679 Content-Ty
22	https://www.orbitz.com/img/global/nav/tab_qs.gif	12/20/2004 5:40	3/10/2005 17:49	URL	FALSE	8R9KCL4N\tab_qs[2].gif	HTTP/1.1 200 OK ETag: "4a03dd-32e-41c6ac06" Content-Length: 814 Content-T
23	http://global.msads.net/ads/50645/0000050645_000000000000000106016.gif	9/21/2004 20:42	3/10/2005 17:53	URL	FALSE	8R9KCL4N\0000050645_0000000000000	HTTP/1.1 200 OK Content-Length: 1147 Content-Type: image/gif ETag: "80d2bf9
24	http://a1055.g.akamai.net/f/1055/979/5h/images.barnesandnoble.com/gresources/navbar/admin4_account.gif	1/4/2005 15:20	3/10/2005 17:48	URL	FALSE	B3B0BSCG\admin4_account[1].gif	HTTP/1.0 200 OK Content-Type: image/gif ETag: "0718be69af2c41:105a" Conte
25	http://search.barnesandnoble.com/booksearch/results.asp?WRD=code%20hacking&userid=pv4dUK5Bu2&cds2Pid=946		3/10/2005 17:48	URL	FALSE	8R9KCL4N\results[1].htm	HTTP/1.1 200 OK P3P: CP="CAO DSP COR ADM DEV TAI PSA IVDo CONo HIS T
26	http://images.slashdot.org/greendot.gif	3/9/2005 21:26	3/10/2005 17:46	URL	FALSE	B3B0BSCG\greendot[1].gif	HTTP/1.1 200 OK Keep-Alive: timeout=10, max=992 Content-Length: 53 Content
27	http://64.4.55.45/i.p.greetcard.gif	11/15/2004 19:39	3/10/2005 18:09	URL	FALSE	ICJNEDI2\i.p.greetcard[1].gif	HTTP/1.1 200 OK Content-Length: 232 Content-Type: image/gif ETag: "80c451c
28	http://64.4.55.45/tab.slide.hm.li.gif	11/15/2004 19:40	3/10/2005 18:09	URL	FALSE	B3B0BSCG\tab.slide.hm.li[1].gif	HTTP/1.1 200 OK Content-Length: 2961 Content-Type: image/gif ETag: "0d19ad
29	http://a1055.g.akamai.net/f/1055/1401/5h/images.barnesandnoble.com/gresources/navbar/subnav4_colon.gif	1/3/2005 16:50	3/10/2005 17:50	URL	FALSE	8R9KCL4N\subnav4_colon[2].gif	HTTP/1.0 200 OK Content-Type: image/gif ETag: "04493fdef1c41:105a" Content
30	http://www.orbitz.com/html.ng/domain=orbitz&channel=home&Section=main&adsize=hometext2&OrbitzCookieName=OSC&orbitzID=CwOXEaWQI		3/10/2005 17:47	URL	FALSE	B3B0BSCG\domain=orbitz&channel=home&	HTTP/1.1 200 OK Content-Length: 3428 Content-Type: text/html
31	http://www.findcracks.com/		3/10/2005 17:50	URL	FALSE	B3B0BSCG\findcracks[1].htm	HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: text/html ~U:jschn
32	http://a1055.g.akamai.net/f/1055/979/5h/images.barnesandnoble.com/gresources/navbar/admin4_wishlist.gif	1/4/2005 15:20	3/10/2005 17:48	URL	FALSE	8R9KCL4N\admin4_wishlist[1].gif	HTTP/1.0 200 OK Content-Type: image/gif ETag: "80724e79af2c41:9d4" Conten
33	http://login.passport.net/uilogin.srf?id=2af815441		3/10/2005 17:53	URL	FALSE	8R9KCL4N\uilogin[1].htm	HTTP/1.1 200 OK PPServer: PPV: 25 H: BAYPPLOGU2A01 V: 1192 Content-Typ
34	http://www.orbitz.com/img/air/change_search.gif	12/20/2004 5:39	3/10/2005 17:49	URL	FALSE	8R9KCL4N\change_search[1].gif	HTTP/1.1 200 OK ETag: "3152a3-21e-41c6abda" Content-Length: 542 Content-T
35	http://news.google.com/news?imgefp=cGLAxecOCkQJ&imgurl=images.newsfactor.com/images/id/6198/ibm-lenovo-deal_crm.jpg		3/10/2005 17:45	URL	FALSE	B3B0BSCG\news[3].jpg	HTTP/1.1 200 OK Content-Type: image/jpeg Content-Length: 1627 ~U:jschmo
36	http://www.orbitz.com/html.ng/domain=orbitz&channel=air&Section=results&adsize=hotwireTop&origin=NYC&dest=SAO&OrbitzCookieName=OS		3/10/2005 17:49	LEAK	TRUE	ICJNEDI2\domain=orbitz&channel=air&Secti	HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: text/html Content-
37	http://a1055.g.akamai.net/f/1055/1401/5h/images.barnesandnoble.com/gresources/navbar/admin4_account.gif	1/4/2005 15:20	3/10/2005 17:50	URL	FALSE	KYRPJUXG\admin4_account[1].gif	HTTP/1.0 200 OK Content-Type: image/gif ETag: "0718be69af2c41:105a" Conte
38	http://a.tribalfusion.com/j.ad?site=MacSlash&adSpace=ROS&size=160x600&type=var&noAd=1&requestID=2456381870.564574788166151		3/10/2005 17:44	URL	FALSE	8R9KCL4N\j[1].ad	HTTP/1.0 200 OK P3P: CP="NOI DEVa TAIa OUR BUS" Pragma: no-cache Conte
39	http://www.orbitz.com/img/air/logos/CO_small.gif	12/20/2004 5:39	3/10/2005 17:48	URL	FALSE	ICJNEDI2\CO_small[1].gif	HTTP/1.1 200 OK ETag: "298ee6-135-41c6abe4" Content-Length: 309 Content-T
40	http://www.technewsworld.com/images/work/header-middle-top-tab-278x28.gif	1/5/2004 13:07	3/10/2005 17:45	URL	FALSE	KYRPJUXG\header-middle-top-tab-	HTTP/1.1 200 OK P3P: CP="ALL DSP COR DEVa TAIa OUR IND DEM" ETag: "6c1
41	http://64.4.55.45/i.p.delete.gif	11/15/2004 19:39	3/10/2005 18:09	URL	FALSE	KYRPJUXG\i.p.delete[1].gif	HTTP/1.1 200 OK Content-Length: 306 Content-Type: image/gif ETag: "02eb9c1
42	http://macslash.org/images/slashslogan.gif	7/10/2002 13:02	3/10/2005 17:44	URL	FALSE	8R9KCL4N\slashslogan[1].gif	HTTP/1.1 200 OK X-Powered-By: Slash 2.002006 X-Fry: They're great! They're
43	http://saopaulo.grand.hyatt.com/owshare/jslibrary/vbFlash.js	8/26/2004 7:25	3/10/2005 17:47	URL	FALSE	ICJNEDI2\vbFlash[1].js	HTTP/1.1 200 OK ETag: "6f008d-2a0-412dc898" Content-Length: 672 Keep-Aliv
44	http://www.orbitz.com/img/air/tip_integration/sort_by.gif	12/20/2004 5:39	3/10/2005 17:49	URL	FALSE	B3B0BSCG\sort_by[1].gif	HTTP/1.1 200 OK ETag: "4d83b3-208-41c6abfe" Content-Length: 520 Content-T
45	http://www.orbitz.com/img/global/nav/tab_fl.gif	12/20/2004 5:40	3/10/2005 17:47	URL	FALSE	ICJNEDI2\tab_fl[1].gif	HTTP/1.1 200 OK ETag: "6402eb-2c9-41c6ac06" Content-Length: 713 Content-T
46	http://ad.doubleclick.net/adi/N815.ecommercetimes.com/B1555812.4;sz=728x90;ord=11104947275778?		3/10/2005 17:45	URL	FALSE	8R9KCL4N\B1555812[1].htm	HTTP/1.0 200 OK Content-Type: text/html Content-Length: 4460 P3P: CP="CURa
47	http://a1055.g.akamai.net/f/1055/979/5h/images.barnesandnoble.com/pimages/gresources/Gateway/YlwFind_btn.gif	11/24/2004 11:29	3/10/2005 17:48	URL	FALSE	B3B0BSCG\YlwFind_btn[1].gif	HTTP/1.0 200 OK Content-Type: image/gif ETag: "e04ecfb742d2c41:9d4" Conte

Computação Forense em Web Browsers

Ferramenta :: Web Historian

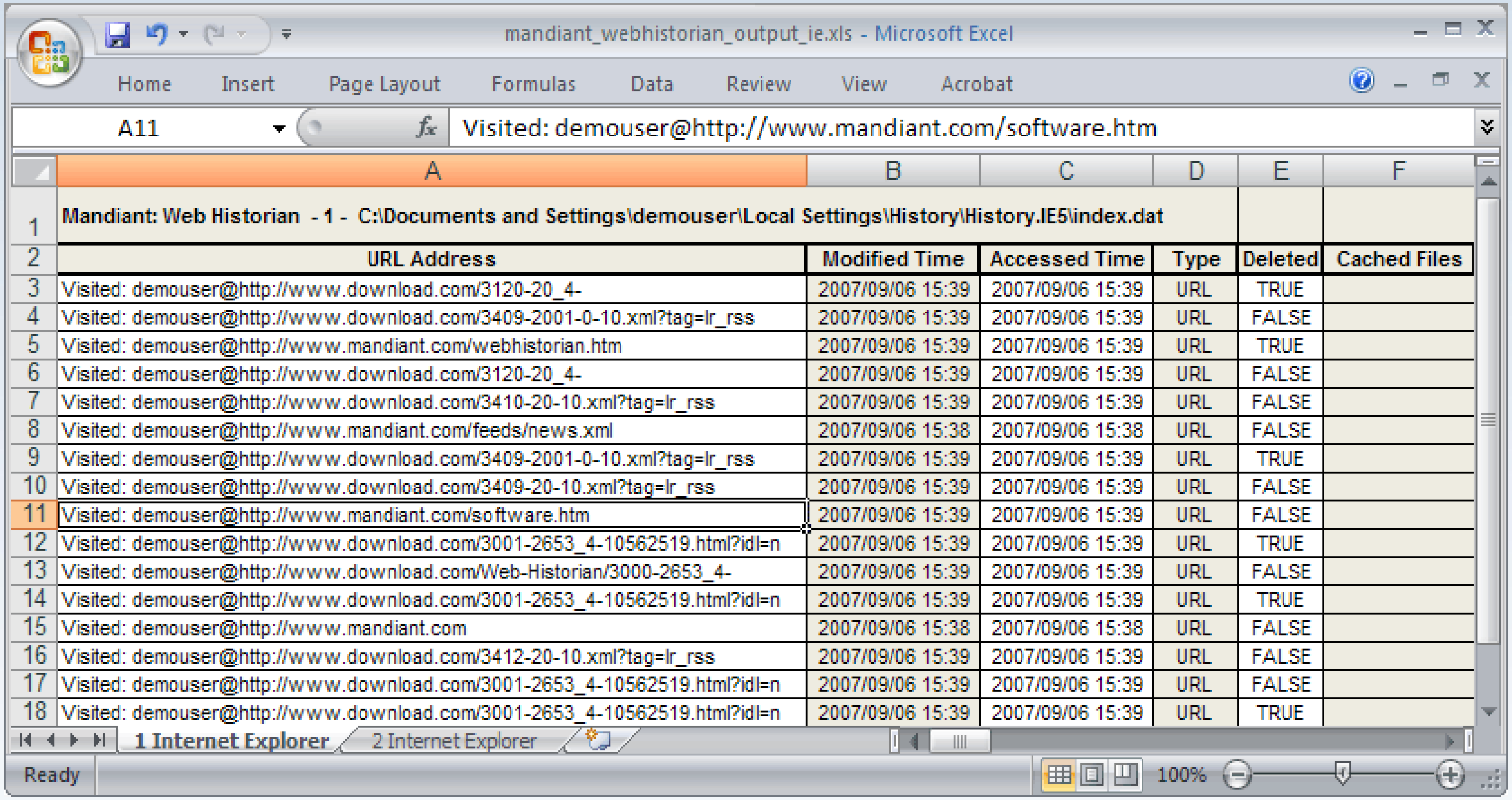


B17 http://www.mandiant.com/webhistorian.htm

	A	B	C	D	E	F
1	Mandiant: Web Historian - 1 - C:\Documents and Settings\demouser\Application Data\Mozilla\Firefox\Profiles\8cbj8hhc.default\history.dat					
2	Name	URL Address	First Visit	Last Visit	Deleted	Vists
3	MANDIANT: Intelligent Information Security	http://www.mandiant.com/	2007/09/06 19:25	2007/09/06 19:25	FALSE	2
4	software	http://www.mandiant.com/software.htm	2007/09/06 19:26	2007/09/06 19:26	FALSE	1
5	Web Historian - Free Software Downloads	http://www.download.com/3001-2653_4-10562519.html	2007/09/06 19:27	2007/09/06 19:27	FALSE	1
6	Search results for web historian - Free	http://www.download.com/3120-20_4-	2007/09/06 19:26	2007/09/06 19:26	FALSE	1
7	Sponsored Links	http://bwp.download.com/search?q=web%20historian&n	2007/09/06 19:26	2007/09/06 19:26	FALSE	1
8	Sponsored Links	http://bwp.download.com/search?ordinal=2&q=web%20	2007/09/06 19:26	2007/09/06 19:26	FALSE	1
9		http://i.d.com.com/html/dl/promos/vt_promo.html	2007/09/06 19:27	2007/09/06 19:27	FALSE	1
10	Web Historian - Reviews and free	http://www.download.com/Web-Historian/3000-2653_4-	2007/09/06 19:27	2007/09/06 19:27	FALSE	1
11		http://software-files.download.com/sd/v-	2007/09/06 19:27	2007/09/06 19:27	FALSE	1
12		http://i.d.com.com/html/dl/promos/mc_promo.html	2007/09/06 19:27	2007/09/06 19:27	FALSE	1
13	Sponsored Links	http://bwp.download.com/search?nodeid=2653&dw-	2007/09/06 19:27	2007/09/06 19:27	FALSE	1
14	Click here to find out more!	http://ad.doubleclick.net/adi/N2998.cnetnetworks/B23774	2007/09/06 19:27	2007/09/06 19:27	FALSE	1
15	Advertisement	http://c7.zedo.com/jsc/fm.html?n=454&c=329/151&s=51&	2007/09/06 19:27	2007/09/06 19:27	FALSE	1
16		http://dw.com.com/redir?edId=3&siteId=4&oId=3000-	2007/09/06 19:27	2007/09/06 19:27	FALSE	1
17	MANDIANT: Intelligent Information Security	http://www.mandiant.com/webhistorian.htm	2007/09/06 19:26	2007/09/06 19:26	FALSE	1
18						

Computação Forense em Web Browsers

Ferramenta :: Web Historian



Visited: demouser@http://www.mandiant.com/software.htm

Mandiant: Web Historian - 1 - C:\Documents and Settings\demouser\Local Settings\History\History.IE5\index.dat

URL Address	Modified Time	Accessed Time	Type	Deleted	Cached Files
Visited: demouser@http://www.download.com/3120-20_4-	2007/09/06 15:39	2007/09/06 15:39	URL	TRUE	
Visited: demouser@http://www.download.com/3409-2001-0-10.xml?tag=lr_rss	2007/09/06 15:39	2007/09/06 15:39	URL	FALSE	
Visited: demouser@http://www.mandiant.com/webhistorian.htm	2007/09/06 15:39	2007/09/06 15:39	URL	TRUE	
Visited: demouser@http://www.download.com/3120-20_4-	2007/09/06 15:39	2007/09/06 15:39	URL	FALSE	
Visited: demouser@http://www.download.com/3410-20-10.xml?tag=lr_rss	2007/09/06 15:39	2007/09/06 15:39	URL	FALSE	
Visited: demouser@http://www.mandiant.com/feeds/news.xml	2007/09/06 15:38	2007/09/06 15:38	URL	FALSE	
Visited: demouser@http://www.download.com/3409-2001-0-10.xml?tag=lr_rss	2007/09/06 15:39	2007/09/06 15:39	URL	TRUE	
Visited: demouser@http://www.download.com/3409-20-10.xml?tag=lr_rss	2007/09/06 15:39	2007/09/06 15:39	URL	FALSE	
Visited: demouser@http://www.mandiant.com/software.htm	2007/09/06 15:39	2007/09/06 15:39	URL	FALSE	
Visited: demouser@http://www.download.com/3001-2653_4-10562519.html?idl=n	2007/09/06 15:39	2007/09/06 15:39	URL	TRUE	
Visited: demouser@http://www.download.com/Web-Historian/3000-2653_4-	2007/09/06 15:39	2007/09/06 15:39	URL	FALSE	
Visited: demouser@http://www.download.com/3001-2653_4-10562519.html?idl=n	2007/09/06 15:39	2007/09/06 15:39	URL	TRUE	
Visited: demouser@http://www.mandiant.com	2007/09/06 15:38	2007/09/06 15:38	URL	FALSE	
Visited: demouser@http://www.download.com/3412-20-10.xml?tag=lr_rss	2007/09/06 15:39	2007/09/06 15:39	URL	FALSE	
Visited: demouser@http://www.download.com/3001-2653_4-10562519.html?idl=n	2007/09/06 15:39	2007/09/06 15:39	URL	FALSE	
Visited: demouser@http://www.download.com/3001-2653_4-10562519.html?idl=n	2007/09/06 15:39	2007/09/06 15:39	URL	TRUE	

Computação Forense em Web Browsers

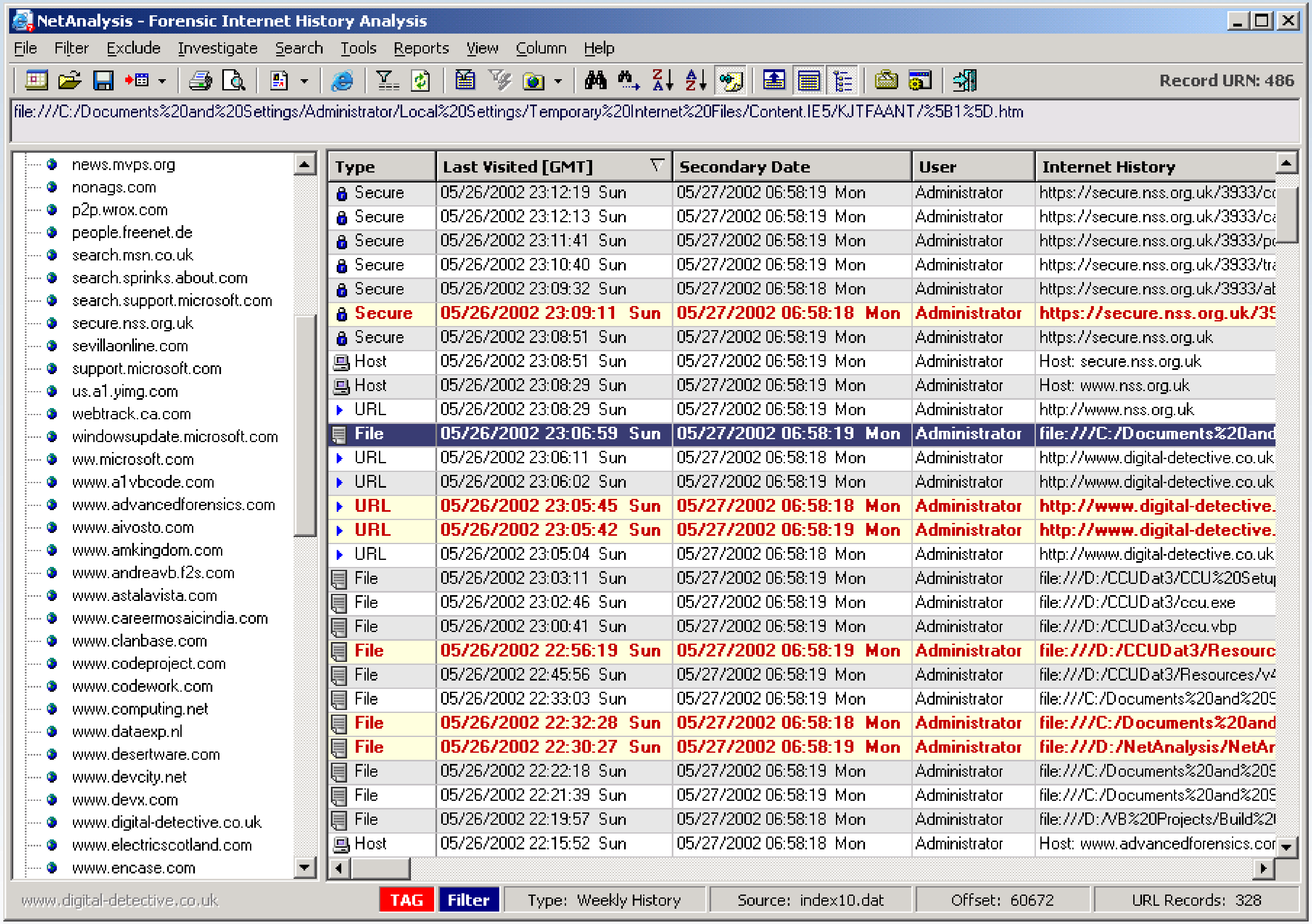
Ferramenta :: Net Analysis

- **Paraben** (www.paraben-forensics.com)
- **Funcionalidades:**
  - Análise de Histórico (Internet History)
  - Análise de Cache (Viewing Cache Data)
  - “Auto Investigação” (Auto Investigate Feature)
    - Filtros configuráveis para busca por:
      - Sites de pedofilia
      - usuários, senhas e padrões específicos
  - Busca de históricos deletados em:
    - Espaços não alocados
    - Arquivos swap
    - Arquivos binários
  - Armazena buscas em bancos SQL

~ $ 250

Computação Forense em Web Browsers

Ferramenta :: Net Analysis



NetAnalysis - Forensic Internet History Analysis
File Filter Exclude Investigate Search Tools Reports View Column Help
Record URN: 486

file:///C:/Documents%20and%20Settings/Administrator/Local%20Settings/Temporary%20Internet%20Files/Content.IE5/KJTFAANT/%5B1%5D.htm

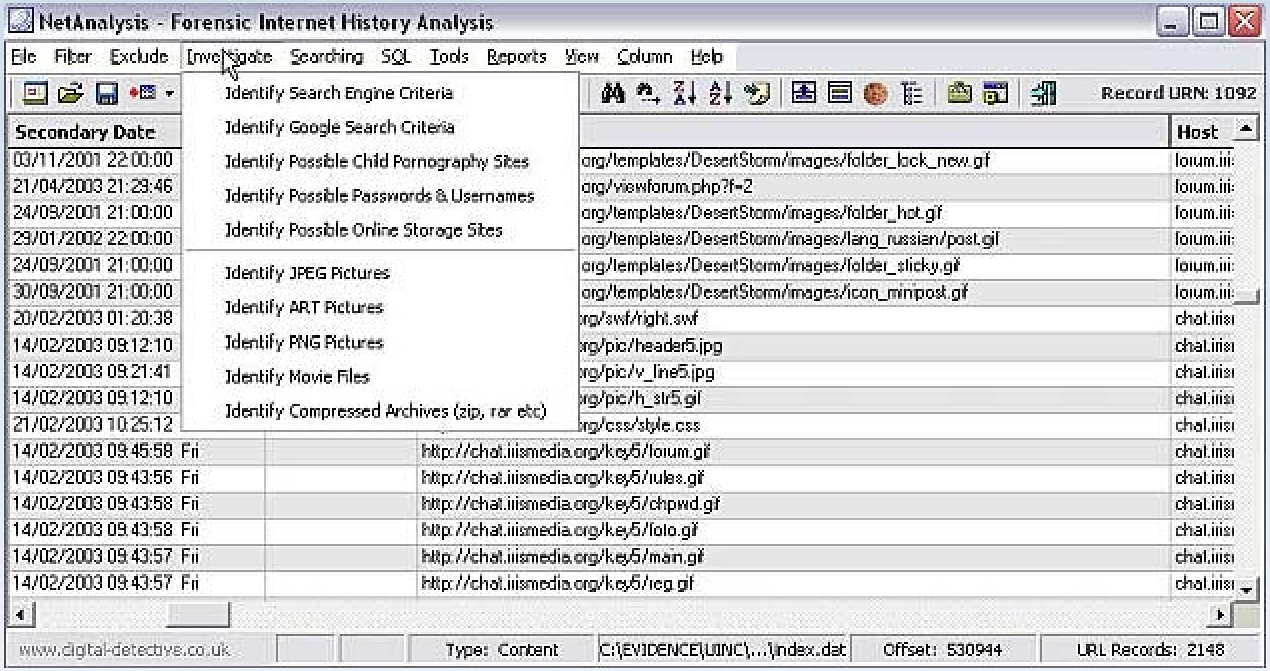
- news.mvps.org
- nonags.com
- p2p.wrox.com
- people.freenet.de
- search.msn.co.uk
- search.sprinks.about.com
- search.support.microsoft.com
- secure.nss.org.uk
- sevillaonline.com
- support.microsoft.com
- us.a1.yimg.com
- webtrack.ca.com
- windowsupdate.microsoft.com
- ww.microsoft.com
- www.a1vbcode.com
- www.advancedforensics.com
- www.aivosto.com
- www.amkingdom.com
- www.andreavb.f2s.com
- www.astalavista.com
- www.careermosaicindia.com
- www.clanbase.com
- www.codeproject.com
- www.codework.com
- www.computing.net
- www.dataexp.nl
- www.desertware.com
- www.devcity.net
- www.devx.com
- www.digital-detective.co.uk
- www.electricscotland.com
- www.encase.com

Type	Last Visited [GMT]	Secondary Date	User	Internet History
Secure	05/26/2002 23:12:19 Sun	05/27/2002 06:58:19 Mon	Administrator	https://secure.nss.org.uk/3933/cc
Secure	05/26/2002 23:12:13 Sun	05/27/2002 06:58:19 Mon	Administrator	https://secure.nss.org.uk/3933/ca
Secure	05/26/2002 23:11:41 Sun	05/27/2002 06:58:19 Mon	Administrator	https://secure.nss.org.uk/3933/pa
Secure	05/26/2002 23:10:40 Sun	05/27/2002 06:58:19 Mon	Administrator	https://secure.nss.org.uk/3933/tra
Secure	05/26/2002 23:09:32 Sun	05/27/2002 06:58:18 Mon	Administrator	https://secure.nss.org.uk/3933/ab
Secure	**05/26/2002 23:09:11 Sun**	**05/27/2002 06:58:18 Mon**	**Administrator**	**https://secure.nss.org.uk/39**
Secure	05/26/2002 23:08:51 Sun	05/27/2002 06:58:19 Mon	Administrator	https://secure.nss.org.uk
Host	05/26/2002 23:08:51 Sun	05/27/2002 06:58:19 Mon	Administrator	Host: secure.nss.org.uk
Host	05/26/2002 23:08:29 Sun	05/27/2002 06:58:19 Mon	Administrator	Host: www.nss.org.uk
URL	05/26/2002 23:08:29 Sun	05/27/2002 06:58:19 Mon	Administrator	http://www.nss.org.uk
File	05/26/2002 23:06:59 Sun	05/27/2002 06:58:19 Mon	Administrator	file:///C:/Documents%20and
URL	05/26/2002 23:06:11 Sun	05/27/2002 06:58:18 Mon	Administrator	http://www.digital-detective.co.uk
URL	05/26/2002 23:06:02 Sun	05/27/2002 06:58:19 Mon	Administrator	http://www.digital-detective.co.uk
URL	**05/26/2002 23:05:45 Sun**	**05/27/2002 06:58:18 Mon**	**Administrator**	**http://www.digital-detective.**
URL	**05/26/2002 23:05:42 Sun**	**05/27/2002 06:58:19 Mon**	**Administrator**	**http://www.digital-detective.**
URL	05/26/2002 23:05:04 Sun	05/27/2002 06:58:18 Mon	Administrator	http://www.digital-detective.co.uk
File	05/26/2002 23:03:11 Sun	05/27/2002 06:58:19 Mon	Administrator	file:///D:/CCUDat3/CCU%20Setu
File	05/26/2002 23:02:46 Sun	05/27/2002 06:58:19 Mon	Administrator	file:///D:/CCUDat3/ccu.exe
File	05/26/2002 23:00:41 Sun	05/27/2002 06:58:19 Mon	Administrator	file:///D:/CCUDat3/ccu.vbp
File	**05/26/2002 22:56:19 Sun**	**05/27/2002 06:58:19 Mon**	**Administrator**	**file:///D:/CCUDat3/Resourc**
File	05/26/2002 22:45:56 Sun	05/27/2002 06:58:19 Mon	Administrator	file:///D:/CCUDat3/Resources/v4
File	05/26/2002 22:33:03 Sun	05/27/2002 06:58:19 Mon	Administrator	file:///C:/Documents%20and%20S
File	**05/26/2002 22:32:28 Sun**	**05/27/2002 06:58:18 Mon**	**Administrator**	**file:///C:/Documents%20and**
File	**05/26/2002 22:30:27 Sun**	**05/27/2002 06:58:19 Mon**	**Administrator**	**file:///D:/NetAnalysis/NetAr**
File	05/26/2002 22:22:18 Sun	05/27/2002 06:58:19 Mon	Administrator	file:///C:/Documents%20and%20S
File	05/26/2002 22:21:39 Sun	05/27/2002 06:58:19 Mon	Administrator	file:///C:/Documents%20and%20S
File	05/26/2002 22:19:57 Sun	05/27/2002 06:58:18 Mon	Administrator	file:///D:/VB%20Projects/Build%2
Host	05/26/2002 22:15:52 Sun	05/27/2002 06:58:18 Mon	Administrator	Host: www.advancedforensics.cor

Type: Weekly History | Source: index10.dat | Offset: 60672 | URL Records: 328

Computação Forense em Web Browsers

Ferramenta :: Net Analysis


NetAnalysis - Forensic Internet History Analysis
File Filter Exclude Investigate Searching SQL Tools Reports View Column Help
Identify Search Engine Criteria
Identify Google Search Criteria
Identify Possible Child Pornography Sites
Identify Possible Passwords & Usernames
Identify Possible Online Storage Sites
Identify JPEG Pictures
Identify ART Pictures
Identify PNG Pictures
Identify Movie Files
Identify Compressed Archives (zip, rar etc)
Record URN: 1092

Secondary Date			Host
03/11/2001 22:00:00		org/templates/DesertStorm/images/folder_lock_new.gif	forum.iii:
21/04/2003 21:29:46		org/viewforum.php?f=2	forum.iii:
24/09/2001 21:00:00		org/templates/DesertStorm/images/folder_hot.gif	forum.iii:
29/01/2002 22:00:00		org/templates/DesertStorm/images/lang_russian/post.gif	forum.iii:
24/09/2001 21:00:00		org/templates/DesertStorm/images/folder_sticky.gif	forum.iii:
30/09/2001 21:00:00		org/templates/DesertStorm/images/icon_minipost.gif	forum.iii:
20/02/2003 01:20:38		rg/swf/right.swf	chat.iiis
14/02/2003 09:12:10		rg/pic/header5.jpg	chat.iiis
14/02/2003 09:21:41		rg/pic/v_line5.jpg	chat.iiis
14/02/2003 09:12:10		rg/pic/h_str5.gif	chat.iiis
21/02/2003 10:25:12		rg/css/style.css	chat.iiis
14/02/2003 09:45:58	Fri	http://chat.iiismedia.org/key5/forum.gif	chat.iiis
14/02/2003 09:43:56	Fri	http://chat.iiismedia.org/key5/rules.gif	chat.iiis
14/02/2003 09:43:58	Fri	http://chat.iiismedia.org/key5/chpwd.gif	chat.iiis
14/02/2003 09:43:58	Fri	http://chat.iiismedia.org/key5/foto.gif	chat.iiis
14/02/2003 09:43:57	Fri	http://chat.iiismedia.org/key5/main.gif	chat.iiis
14/02/2003 09:43:57	Fri	http://chat.iiismedia.org/key5/reg.gif	chat.iiis

www.digital-detective.co.uk | Type: Content | C:\EVIDENCE\UINC\...\index.dat | Offset: 530944 | URL Records: 2148

Computação Forense em Web Browsers
Ferramenta :: Cache View

- Autor: Tim Johnson
- Foco principal: Cache (IE, Netscape, Firefox e Opera)
- S.O.: MS Windows

Free Software

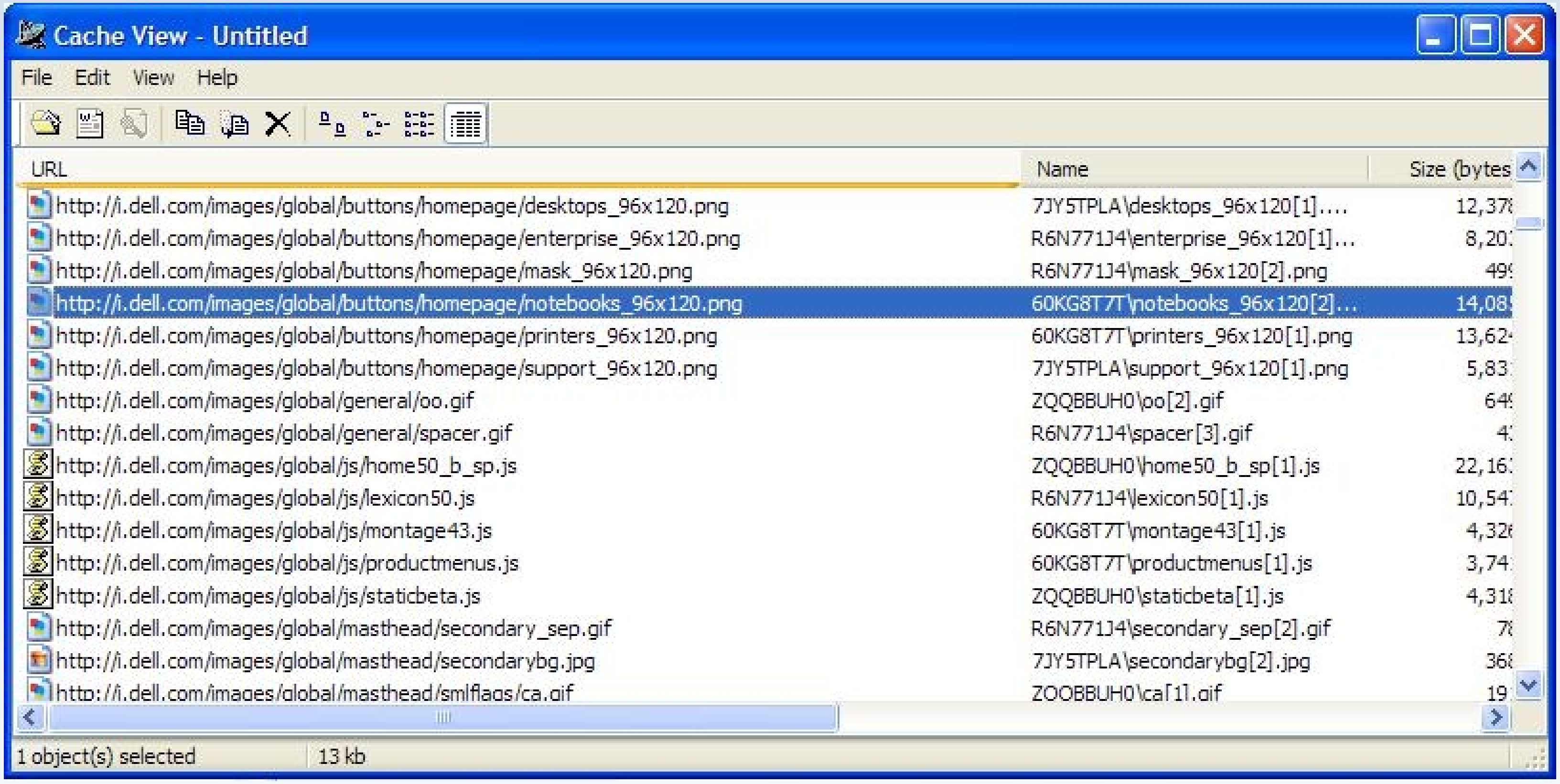
```
http://www.progsoc.uts.edu.au/~timj/cv/
```

- Extrai informações dos arquivos de Cache:
  - URL, nome do arquivo em cache, tamanho (em bytes), MIME Type, data da última modificação, data do download, data de expiração e cabeçalho HTTP

Computação Forense em Web Browsers

Ferramenta :: Cache View

- Versão não-registrada



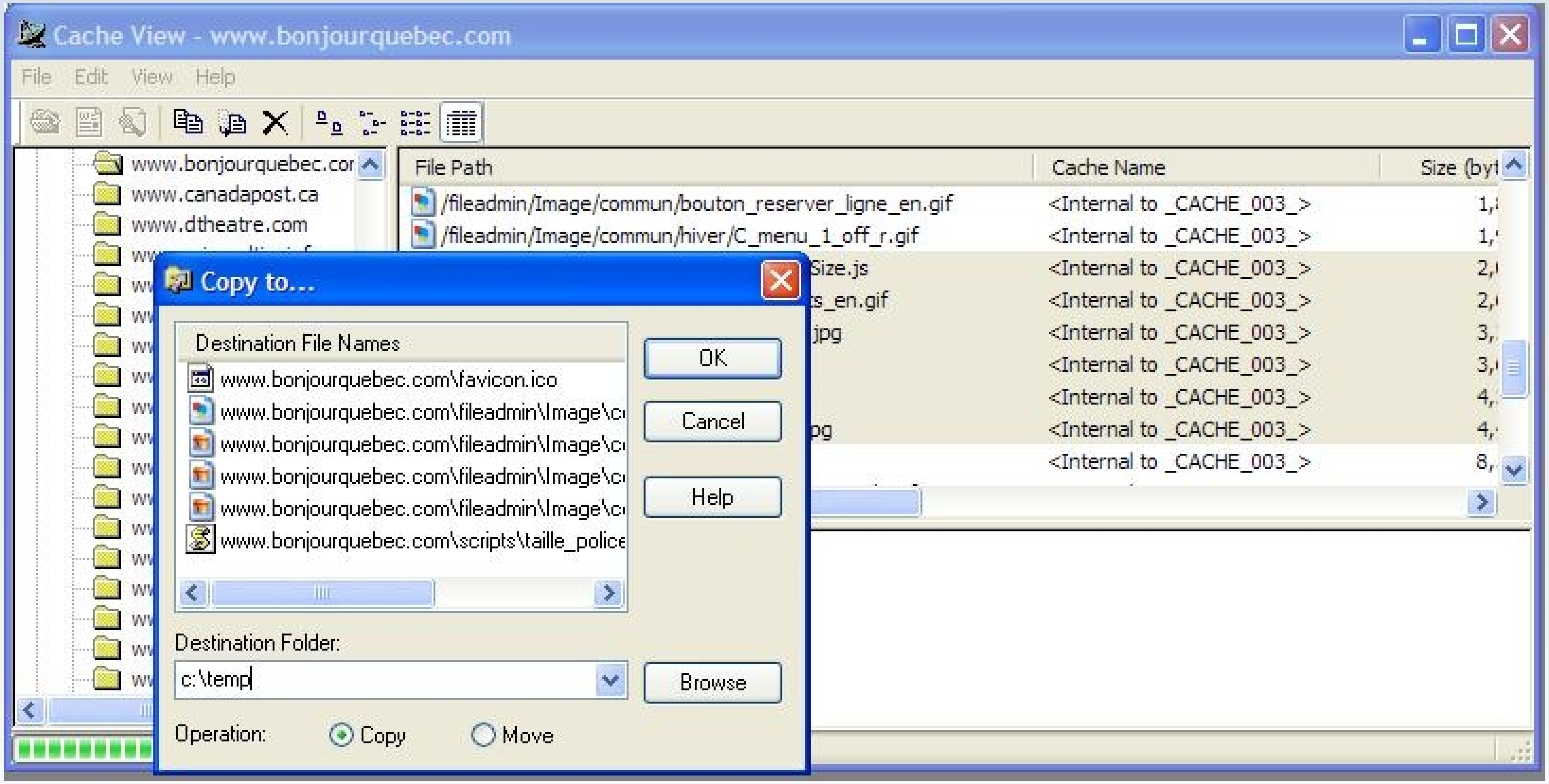
URL	Name	Size (bytes
http://i.dell.com/images/global/buttons/homepage/desktops_96x120.png	7JY5TPLA\desktops_96x120[1]....	12,37
http://i.dell.com/images/global/buttons/homepage/enterprise_96x120.png	R6N771J4\enterprise_96x120[1]...	8,20
http://i.dell.com/images/global/buttons/homepage/mask_96x120.png	R6N771J4\mask_96x120[2].png	49
http://i.dell.com/images/global/buttons/homepage/notebooks_96x120.png	60KG8T7T\notebooks_96x120[2]...	14,08
http://i.dell.com/images/global/buttons/homepage/printers_96x120.png	60KG8T7T\printers_96x120[1].png	13,62
http://i.dell.com/images/global/buttons/homepage/support_96x120.png	7JY5TPLA\support_96x120[1].png	5,83
http://i.dell.com/images/global/general/oo.gif	ZQQBBUH0\oo[2].gif	64
http://i.dell.com/images/global/general/spacer.gif	R6N771J4\spacer[3].gif	4
http://i.dell.com/images/global/js/home50_b_sp.js	ZQQBBUH0\home50_b_sp[1].js	22,16
http://i.dell.com/images/global/js/lexicon50.js	R6N771J4\lexicon50[1].js	10,54
http://i.dell.com/images/global/js/montage43.js	60KG8T7T\montage43[1].js	4,32
http://i.dell.com/images/global/js/productmenus.js	60KG8T7T\productmenus[1].js	3,74
http://i.dell.com/images/global/js/staticbeta.js	ZQQBBUH0\staticbeta[1].js	4,31
http://i.dell.com/images/global/masthead/secondary_sep.gif	R6N771J4\secondary_sep[2].gif	7
http://i.dell.com/images/global/masthead/secondarybg.jpg	7JY5TPLA\secondarybg[2].jpg	36
http://i.dell.com/images/global/masthead/smlflags/ca.gif	ZQQBBUH0\ca[1].gif	19

1 object(s) selected   13 kb

Computação Forense em Web Browsers

Ferramenta :: Cache View

- Versão não-registrada



Cache View - www.bonjourquebec.com

www.bonjourquebec.cor
www.canadapost.ca
www.dtheatre.com

File Path	Cache Name	Size (byt
/fileadmin/Image/commun/bouton_reserver_ligne_en.gif	<Internal to _CACHE_003_>	1,
/fileadmin/Image/commun/hiver/C_menu_1_off_r.gif	<Internal to _CACHE_003_>	1,
Size.js	<Internal to _CACHE_003_>	2,
s_en.gif	<Internal to _CACHE_003_>	2,
jpg	<Internal to _CACHE_003_>	3,
	<Internal to _CACHE_003_>	3,
	<Internal to _CACHE_003_>	4,
pg	<Internal to _CACHE_003_>	4,
	<Internal to _CACHE_003_>	8,

Copy to...

Destination File Names

www.bonjourquebec.com\favicon.ico
www.bonjourquebec.com\fileadmin\Image\c
www.bonjourquebec.com\fileadmin\Image\c
www.bonjourquebec.com\fileadmin\Image\c
www.bonjourquebec.com\fileadmin\Image\c
www.bonjourquebec.com\scripts\taille_police

Destination Folder: c:\temp

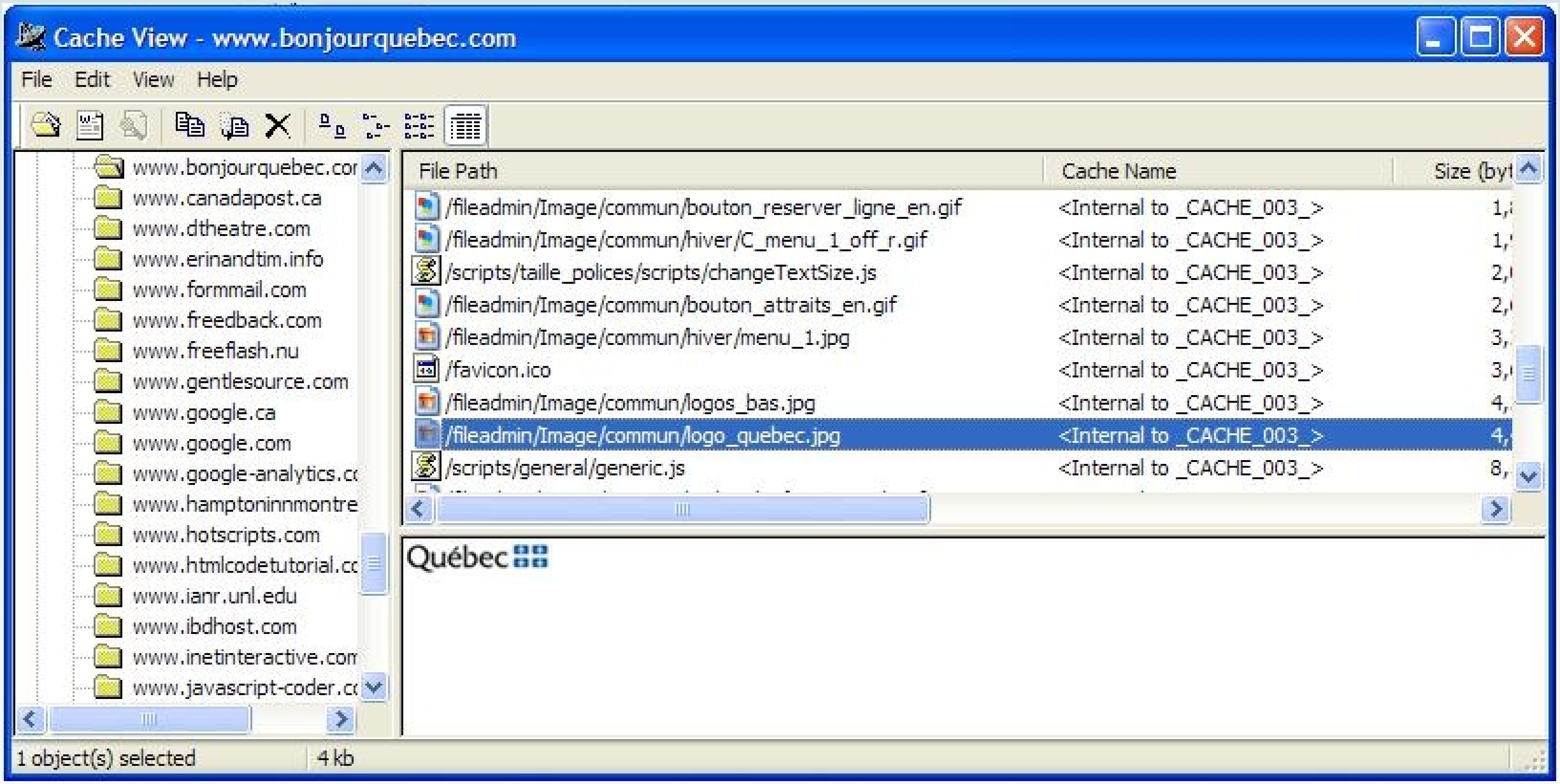
Operation: ● Copy ○ Move

Computação Forense em Web Browsers

Ferramenta :: Cache View

~ $ 25

- Versão registrada



Cache View - www.bonjourquebec.com

www.bonjourquebec.cor
www.canadapost.ca
www.dtheatre.com
www.erinandtim.info
www.formmail.com
www.freedback.com
www.freeflash.nu
www.gentlesource.com
www.google.ca
www.google.com
www.google-analytics.cc
www.hamptoninnmontre
www.hotscripts.com
www.htmlcodetutorial.cc
www.ianr.unl.edu
www.ibdhost.com
www.inetinteractive.com
www.javascript-coder.cc

File Path	Cache Name	Size (byt
/fileadmin/Image/commun/bouton_reserver_ligne_en.gif	<Internal to _CACHE_003_>	1,
/fileadmin/Image/commun/hiver/C_menu_1_off_r.gif	<Internal to _CACHE_003_>	1,
/scripts/taille_polices/scripts/changeTextSize.js	<Internal to _CACHE_003_>	2,
/fileadmin/Image/commun/bouton_attraits_en.gif	<Internal to _CACHE_003_>	2,
/fileadmin/Image/commun/hiver/menu_1.jpg	<Internal to _CACHE_003_>	3,
/favicon.ico	<Internal to _CACHE_003_>	3,
/fileadmin/Image/commun/logos_bas.jpg	<Internal to _CACHE_003_>	4,
/fileadmin/Image/commun/logo_quebec.jpg	<Internal to _CACHE_003_>	4,
/scripts/general/generic.js	<Internal to _CACHE_003_>	8,

Québec

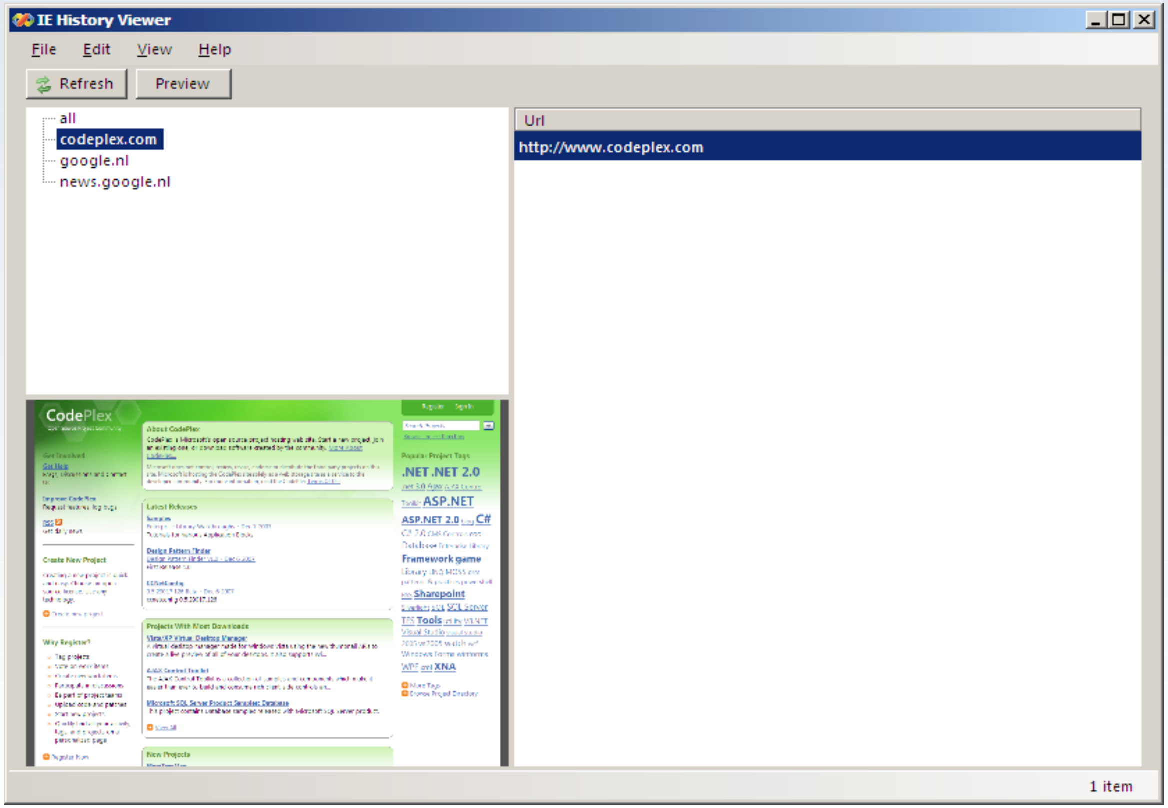
1 object(s) selected 4 kb

Computação Forense em Web Browsers

Ferramenta :: IE History Viewer

- Autor: Jonas Butt
- S.O.: MS Windows

http://www.codeplex.com/IEHistoryViewer



- all
- codeplex.com
- google.nl
- news.google.nl

Url

http://www.codeplex.com

1 item

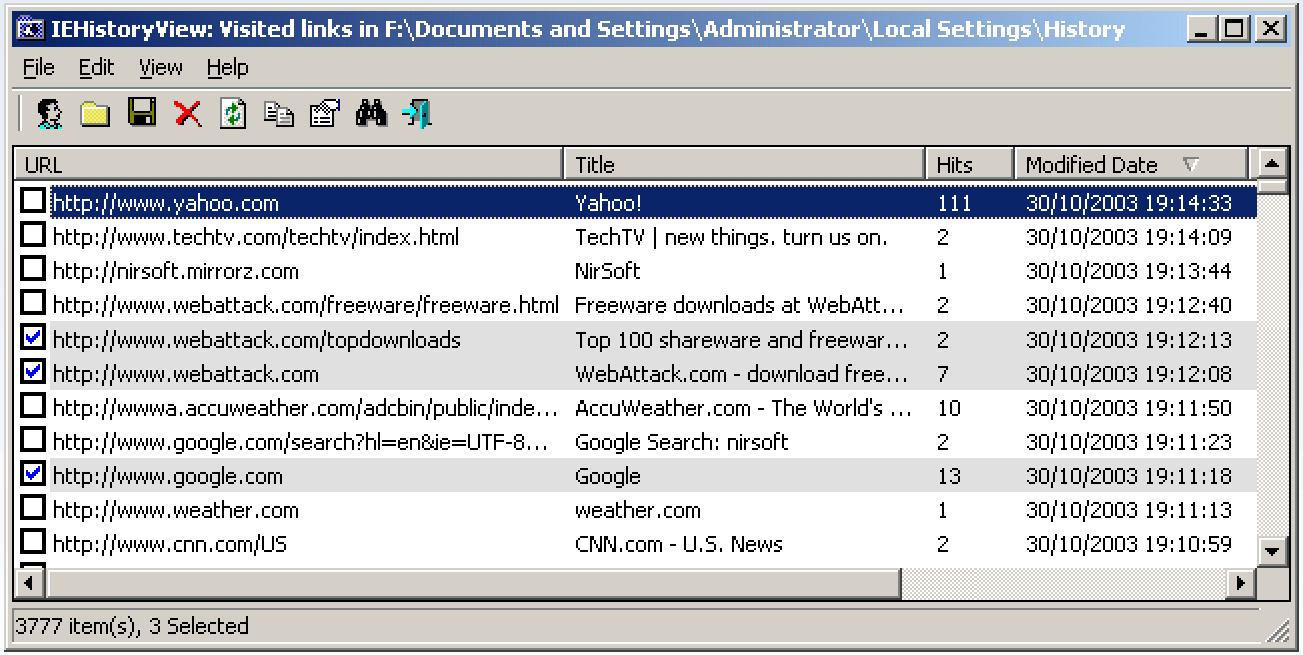
Computação Forense em Web Browsers

Ferramenta :: IE HistoryView

- Autor: Nirsoft
- S.O.: MS Windows

Free Software

http://www.nirsoft.net/utils/iehv.html



IEHistoryView: Visited links in F:\Documents and Settings\Administrator\Local Settings\History

	URL	Title	Hits	Modified Date
☐	http://www.yahoo.com	Yahoo!	111	30/10/2003 19:14:33
☐	http://www.techtv.com/techtv/index.html	TechTV | new things. turn us on.	2	30/10/2003 19:14:09
☐	http://nirsoft.mirrorz.com	NirSoft	1	30/10/2003 19:13:44
☐	http://www.webattack.com/freeware/freeware.html	Freeware downloads at WebAtt...	2	30/10/2003 19:12:40
☑	http://www.webattack.com/topdownloads	Top 100 shareware and freewar...	2	30/10/2003 19:12:13
☑	http://www.webattack.com	WebAttack.com - download free...	7	30/10/2003 19:12:08
☐	http://wwwa.accuweather.com/adcbin/public/inde...	AccuWeather.com - The World's ...	10	30/10/2003 19:11:50
☐	http://www.google.com/search?hl=en&ie=UTF-8...	Google Search: nirsoft	2	30/10/2003 19:11:23
☑	http://www.google.com	Google	13	30/10/2003 19:11:18
☐	http://www.weather.com	weather.com	1	30/10/2003 19:11:13
☐	http://www.cnn.com/US	CNN.com - U.S. News	2	30/10/2003 19:10:59

3777 item(s), 3 Selected

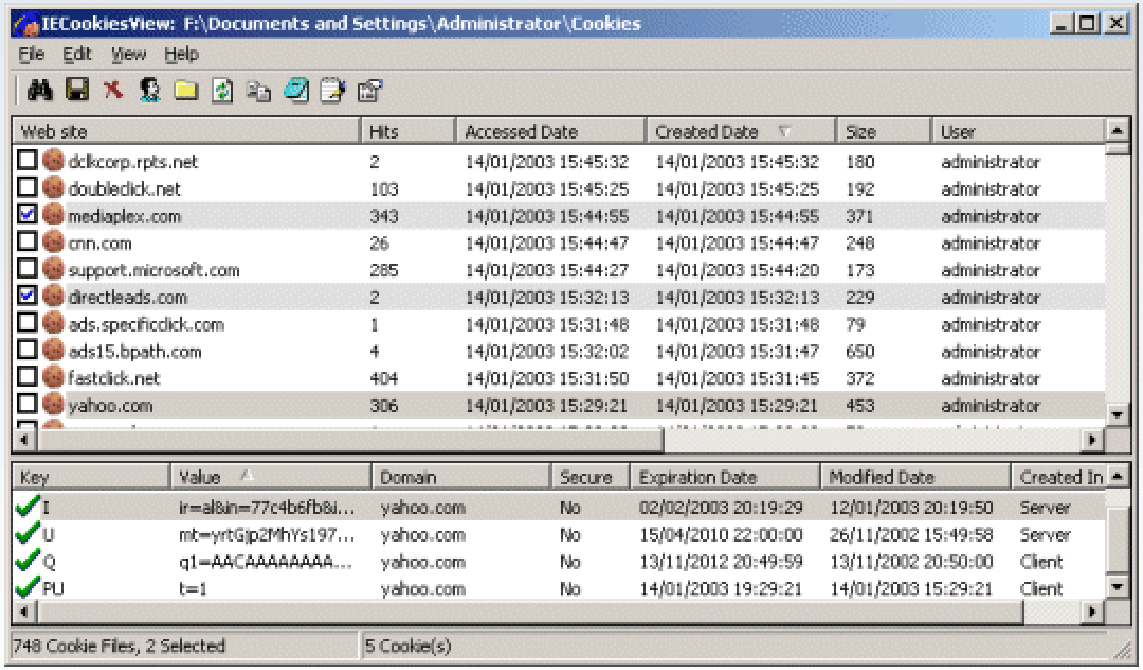
Computação Forense em Web Browsers

Ferramenta :: IE CookiesView

- Autor: Nirsoft
- S.O.: MS Windows

Free Software

http://www.nirsoft.net/utils/iecookies.html



IECookiesView: F:\Documents and Settings\Administrator\Cookies
File
Edit
View
Help

	Web site	Hits	Accessed Date	Created Date	Size	User
□	dclkcorp.rpts.net	2	14/01/2003 15:45:32	14/01/2003 15:45:32	180	administrator
□	doubleclick.net	103	14/01/2003 15:45:25	14/01/2003 15:45:25	192	administrator
☑	mediaplex.com	343	14/01/2003 15:44:55	14/01/2003 15:44:55	371	administrator
□	cnn.com	26	14/01/2003 15:44:47	14/01/2003 15:44:47	248	administrator
□	support.microsoft.com	285	14/01/2003 15:44:27	14/01/2003 15:44:20	173	administrator
☑	directleads.com	2	14/01/2003 15:32:13	14/01/2003 15:32:13	229	administrator
□	ads.specificclick.com	1	14/01/2003 15:31:48	14/01/2003 15:31:48	79	administrator
□	ads15.bpath.com	4	14/01/2003 15:32:02	14/01/2003 15:31:47	650	administrator
□	fastclick.net	404	14/01/2003 15:31:50	14/01/2003 15:31:45	372	administrator
□	yahoo.com	306	14/01/2003 15:29:21	14/01/2003 15:29:21	453	administrator

Key	Value	Domain	Secure	Expiration Date	Modified Date	Created In
✓ I	ir=al&in=77c4b6fb8i...	yahoo.com	No	02/02/2003 20:19:29	12/01/2003 20:19:50	Server
✓ U	mt=yrtGjp2MhYs197...	yahoo.com	No	15/04/2010 22:00:00	26/11/2002 15:49:58	Server
✓ Q	q1=AACAAAAAAAA...	yahoo.com	No	13/11/2012 20:49:59	13/11/2002 20:50:00	Client
✓ PU	t=1	yahoo.com	No	14/01/2003 19:29:21	14/01/2003 15:29:21	Client

748 Cookie Files, 2 Selected | 5 Cookie(s)

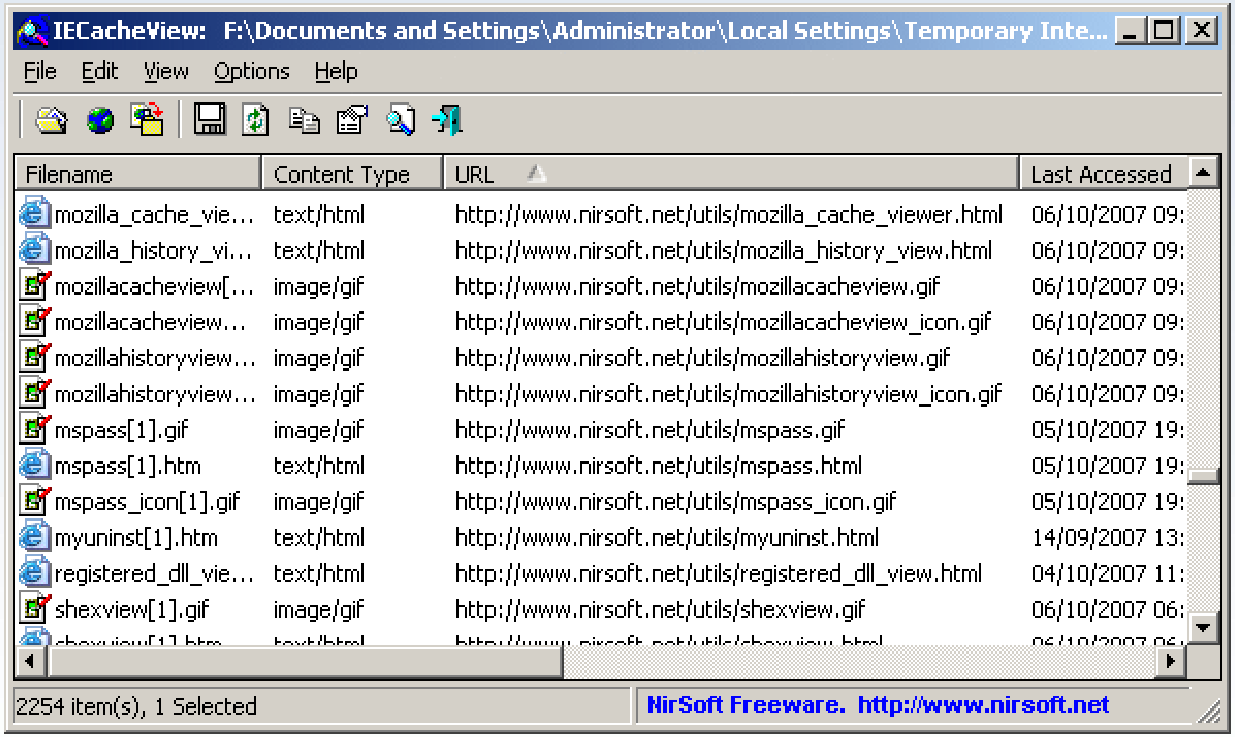
Computação Forense em Web Browsers

Ferramenta :: IE CacheView

- Autor: Nirsoft
- S.O.: MS Windows

Free Software

http://www.nirsoft.net/utils/ie_cache_viewer.html



IECacheView: F:\Documents and Settings\Administrator\Local Settings\Temporary Inte...

Filename	Content Type	URL	Last Accessed
mozilla_cache_vie...	text/html	http://www.nirsoft.net/utils/mozilla_cache_viewer.html	06/10/2007 09:
mozilla_history_vi...	text/html	http://www.nirsoft.net/utils/mozilla_history_view.html	06/10/2007 09:
mozillacacheview[...	image/gif	http://www.nirsoft.net/utils/mozillacacheview.gif	06/10/2007 09:
mozillacacheview...	image/gif	http://www.nirsoft.net/utils/mozillacacheview_icon.gif	06/10/2007 09:
mozillahistoryview...	image/gif	http://www.nirsoft.net/utils/mozillahistoryview.gif	06/10/2007 09:
mozillahistoryview...	image/gif	http://www.nirsoft.net/utils/mozillahistoryview_icon.gif	06/10/2007 09:
mspass[1].gif	image/gif	http://www.nirsoft.net/utils/mspass.gif	05/10/2007 19:
mspass[1].htm	text/html	http://www.nirsoft.net/utils/mspass.html	05/10/2007 19:
mspass_icon[1].gif	image/gif	http://www.nirsoft.net/utils/mspass_icon.gif	05/10/2007 19:
myuninst[1].htm	text/html	http://www.nirsoft.net/utils/myuninst.html	14/09/2007 13:
registered_dll_vie...	text/html	http://www.nirsoft.net/utils/registered_dll_view.html	04/10/2007 11:
shexview[1].gif	image/gif	http://www.nirsoft.net/utils/shexview.gif	06/10/2007 06:
shexview[1].htm	text/html	http://www.nirsoft.net/utils/shexview.html	06/10/2007 06:

2254 item(s), 1 Selected

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

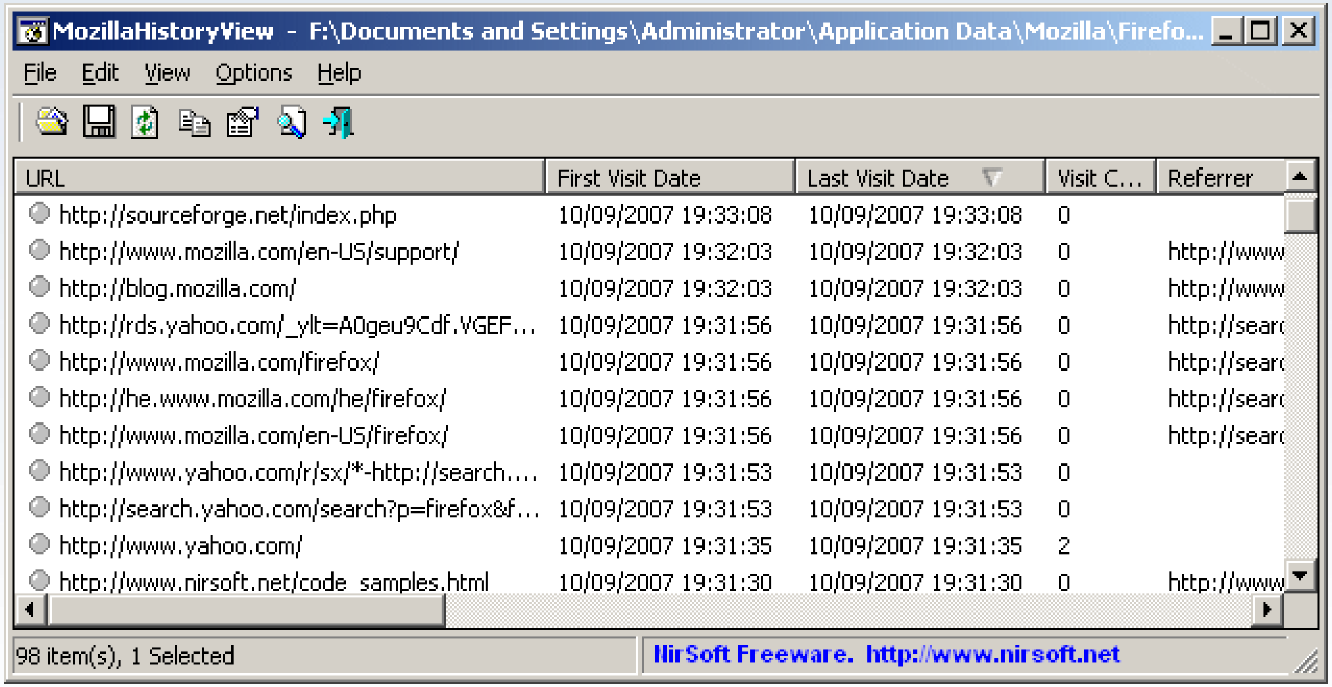
Computação Forense em Web Browsers

Ferramenta :: Mozilla HistoryView

- Autor: Nirsoft
- S.O.: MS Windows

Free Software

http://www.nirsoft.net/utils/mozilla_history_view.html



MozillaHistoryView - F:\Documents and Settings\Administrator\Application Data\Mozilla\Firefo...

URL	First Visit Date	Last Visit Date	Visit C...	Referrer
http://sourceforge.net/index.php	10/09/2007 19:33:08	10/09/2007 19:33:08	0	
http://www.mozilla.com/en-US/support/	10/09/2007 19:32:03	10/09/2007 19:32:03	0	http://www
http://blog.mozilla.com/	10/09/2007 19:32:03	10/09/2007 19:32:03	0	http://www
http://rds.yahoo.com/_ylt=A0geu9Cdf.VGEF...	10/09/2007 19:31:56	10/09/2007 19:31:56	0	http://searc
http://www.mozilla.com/firefox/	10/09/2007 19:31:56	10/09/2007 19:31:56	0	http://searc
http://he.www.mozilla.com/he/firefox/	10/09/2007 19:31:56	10/09/2007 19:31:56	0	http://searc
http://www.mozilla.com/en-US/firefox/	10/09/2007 19:31:56	10/09/2007 19:31:56	0	http://searc
http://www.yahoo.com/r/sx/*-http://search....	10/09/2007 19:31:53	10/09/2007 19:31:53	0	
http://search.yahoo.com/search?p=firefox&f...	10/09/2007 19:31:53	10/09/2007 19:31:53	0	
http://www.yahoo.com/	10/09/2007 19:31:35	10/09/2007 19:31:35	2	
http://www.nirsoft.net/code_samples.html	10/09/2007 19:31:30	10/09/2007 19:31:30	0	http://www

98 item(s), 1 Selected

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

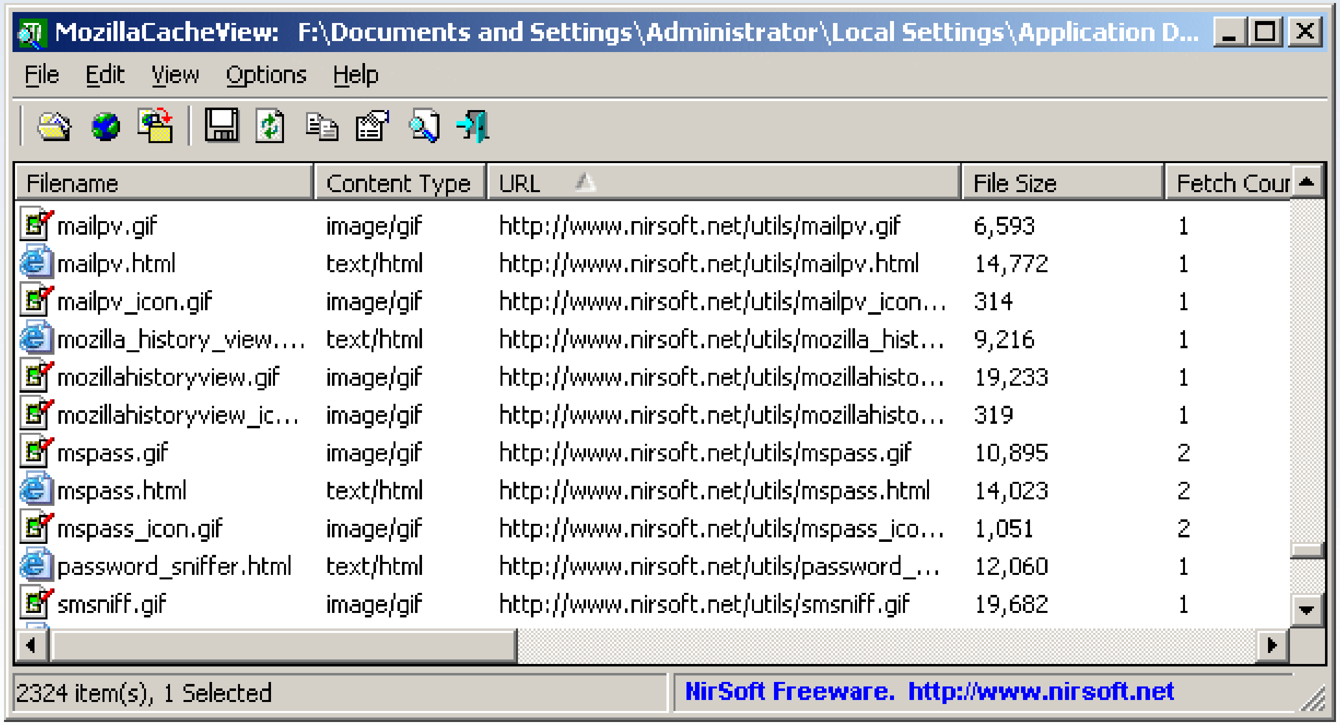
Computação Forense em Web Browsers

Ferramenta :: Mozilla CacheView

- Autor: Nirsoft
- S.O.: MS Windows

Free Software

http://www.nirsoft.net/utils/mozilla_cache_viewer.html



MozillaCacheView: F:\Documents and Settings\Administrator\Local Settings\Application D...

Filename	Content Type	URL	File Size	Fetch Cour
mailpv.gif	image/gif	http://www.nirsoft.net/utils/mailpv.gif	6,593	1
mailpv.html	text/html	http://www.nirsoft.net/utils/mailpv.html	14,772	1
mailpv_icon.gif	image/gif	http://www.nirsoft.net/utils/mailpv_icon...	314	1
mozilla_history_view....	text/html	http://www.nirsoft.net/utils/mozilla_hist...	9,216	1
mozillahistoryview.gif	image/gif	http://www.nirsoft.net/utils/mozillahisto...	19,233	1
mozillahistoryview_ic...	image/gif	http://www.nirsoft.net/utils/mozillahisto...	319	1
mspass.gif	image/gif	http://www.nirsoft.net/utils/mspass.gif	10,895	2
mspass.html	text/html	http://www.nirsoft.net/utils/mspass.html	14,023	2
mspass_icon.gif	image/gif	http://www.nirsoft.net/utils/mspass_ico...	1,051	2
password_sniffer.html	text/html	http://www.nirsoft.net/utils/password_...	12,060	1
smsniff.gif	image/gif	http://www.nirsoft.net/utils/smsniff.gif	19,682	1

2324 item(s), 1 Selected

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

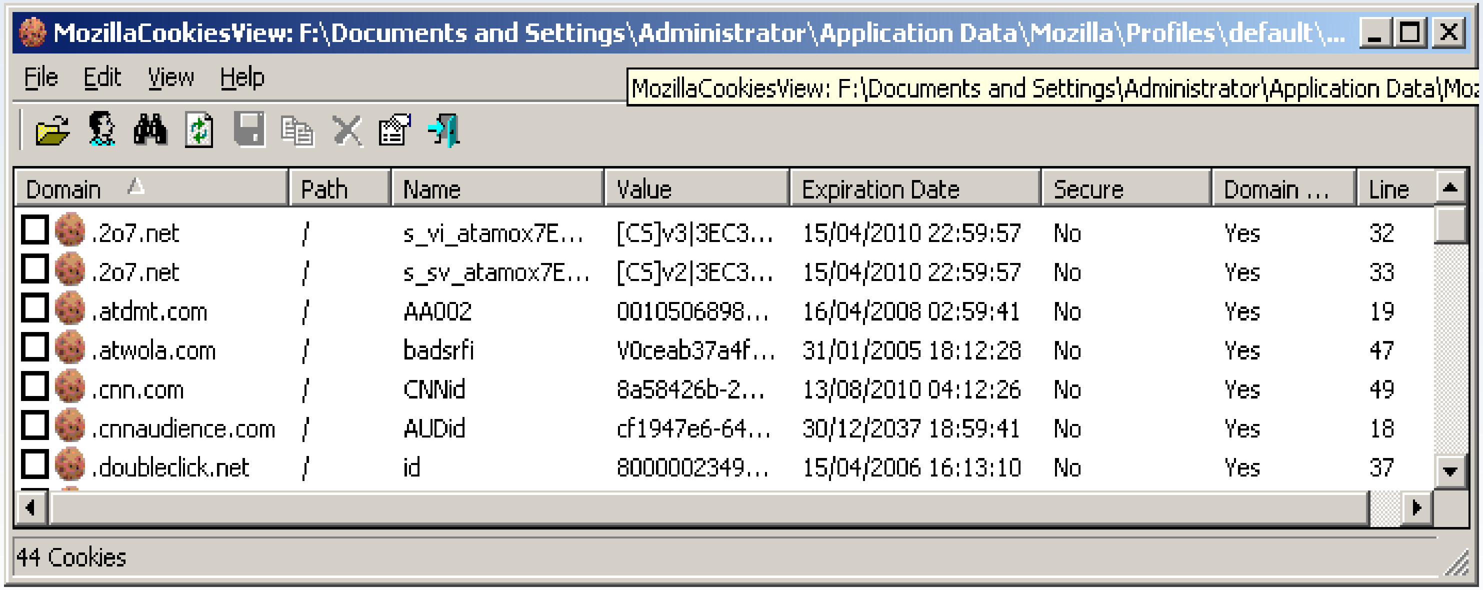
Computação Forense em Web Browsers

Ferramenta :: Mozilla CookiesView

- Autor: Nirsoft
- S.O.: MS Windows

Free Software

http://www.nirsoft.net/utils/mzcv.html



MozillaCookiesView: F:\Documents and Settings\Administrator\Application Data\Mozilla\Profiles\default\...

MozillaCookiesView: F:\Documents and Settings\Administrator\Application Data\Moz

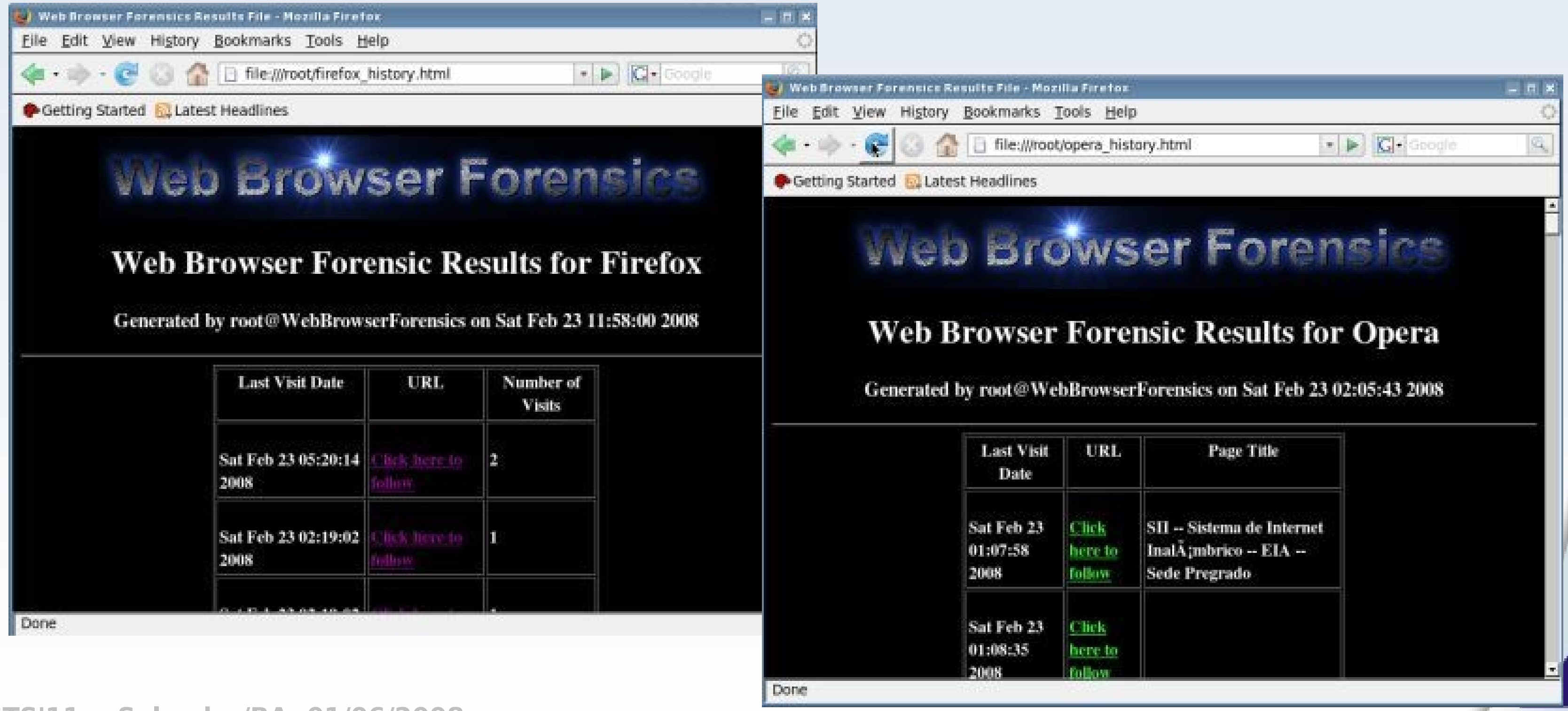
	Domain	Path	Name	Value	Expiration Date	Secure	Domain ...	Line
□	.2o7.net	/	s_vi_atamox7E...	[CS]v3|3EC3...	15/04/2010 22:59:57	No	Yes	32
□	.2o7.net	/	s_sv_atamox7E...	[CS]v2|3EC3...	15/04/2010 22:59:57	No	Yes	33
□	.atdmt.com	/	AA002	0010506898...	16/04/2008 02:59:41	No	Yes	19
□	.atwola.com	/	badsrfi	V0ceab37a4f...	31/01/2005 18:12:28	No	Yes	47
□	.cnn.com	/	CNNid	8a58426b-2...	13/08/2010 04:12:26	No	Yes	49
□	.cnnaudience.com	/	AUDid	cf1947e6-64...	30/12/2037 18:59:41	No	Yes	18
□	.doubleclick.net	/	id	8000002349...	15/04/2006 16:13:10	No	Yes	37

44 Cookies

Computação Forense em Web Browsers
Ferramenta :: wbf (Web Browser Forensics)

- Autor: Manuel Santander
- Foco principal: Análise de arquivos de Histórico
- Versões para Windows (Cygwin) e Linux

http://manuel.santander.name/wbf.html



Web Browser Forensics Results File - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///root/firefox_history.html
Google
Getting Started
Latest Headlines
Web Browser Forensics
Done

Web Browser Forensic Results for Firefox

Generated by root@WebBrowserForensics on Sat Feb 23 11:58:00 2008

Last Visit Date	URL	Number of Visits
Sat Feb 23 05:20:14 2008	Click here to follow	2
Sat Feb 23 02:19:02 2008	Click here to follow	1

Web Browser Forensics Results File - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///root/opera_history.html
Google
Getting Started
Latest Headlines
Web Browser Forensics
Done

Web Browser Forensic Results for Opera

Generated by root@WebBrowserForensics on Sat Feb 23 02:05:43 2008

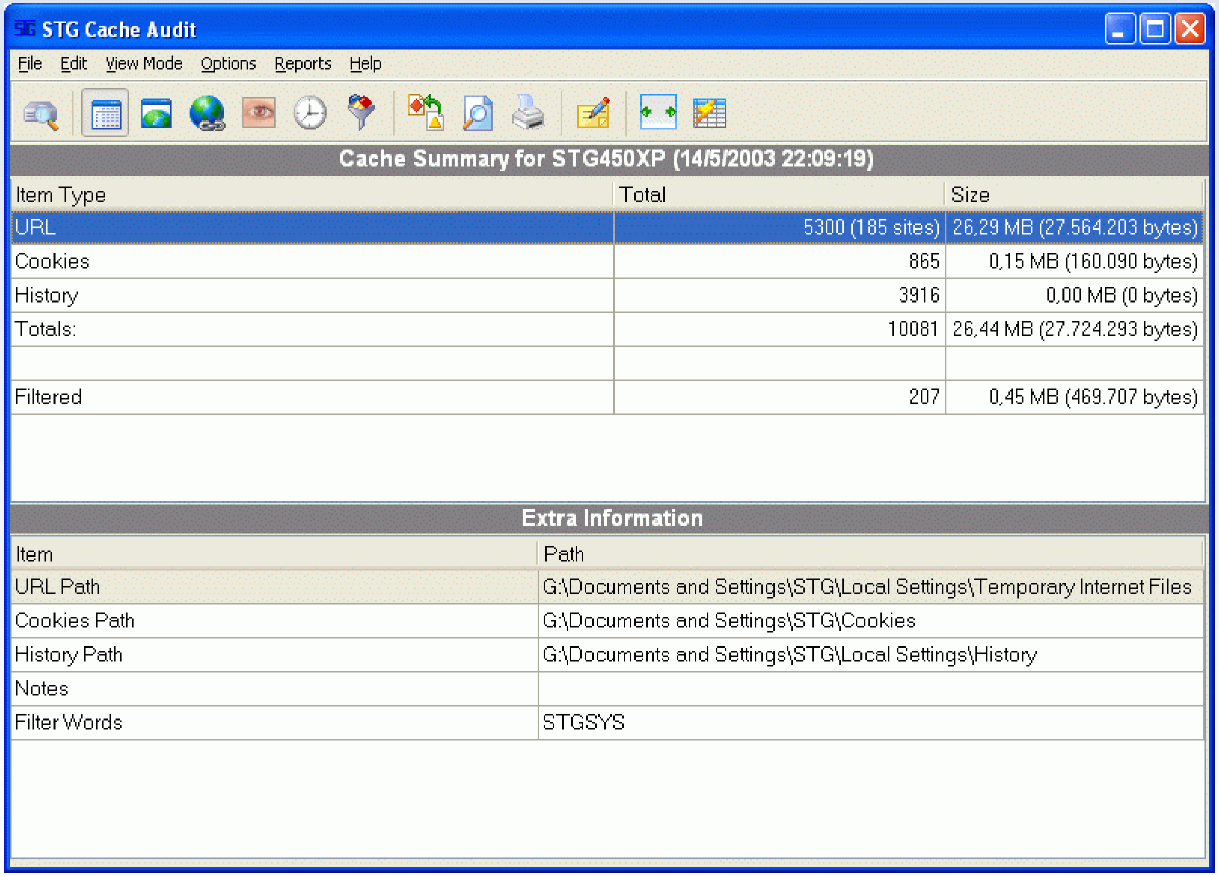
Last Visit Date	URL	Page Title
Sat Feb 23 01:07:58 2008	Click here to follow	SII -- Sistema de Internet InalÃ¡mbrico -- EIA -- Sede Pregrado
Sat Feb 23 01:08:35 2008	Click here to follow	

Computação Forense em Web Browsers

Ferramenta :: STG Cache Audit

- Autor: Starglider Systems
- S.O.: MS Windows
- http://www.stgsys.com/audit.asp

Free Software



Cache Summary for STG450XP (14/5/2003 22:09:19)

Item Type	Total	Size
URL	5300 (185 sites)	26,29 MB (27.564.203 bytes)
Cookies	865	0,15 MB (160.090 bytes)
History	3916	0,00 MB (0 bytes)
Totals:	10081	26,44 MB (27.724.293 bytes)
Filtered	207	0,45 MB (469.707 bytes)

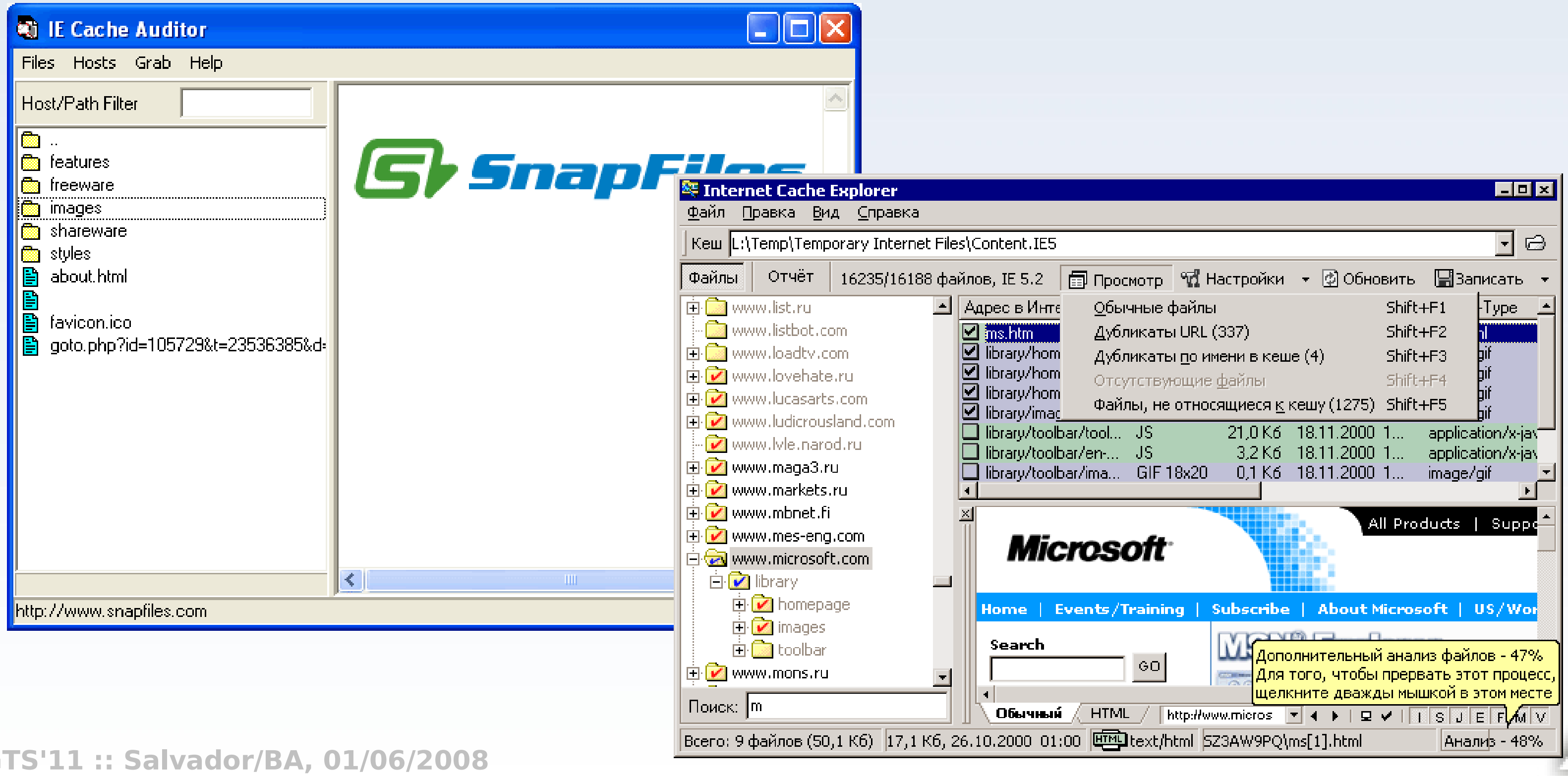
Extra Information

Item	Path
URL Path	G:\Documents and Settings\STG\Local Settings\Temporary Internet Files
Cookies Path	G:\Documents and Settings\STG\Cookies
History Path	G:\Documents and Settings\STG\Local Settings\History
Notes	
Filter Words	STGSYS

Computação Forense em Web Browsers

Outras Ferramentas

- **Cache Monitor**
  - http://www.enigmaticsoftware.com/cachemonitor/index.html
- **IE Cache Auditor**
  - http://www.softempire.com/cache-auditor-simple-ie-cache-viewer.html
- **Internet Cache Explorer**
  - http://www.risingresearch.com/ru/icache/



IE Cache Auditor

Host/Path Filter

..
features
freeware
images
shareware
styles
about.html
favicon.ico
goto.php?id=105729&t=23536385&d=

http://www.snapfiles.com

Internet Cache Explorer

Кеш L:\Temp\Temporary Internet Files\Content.IE5

16235/16188 файлов, IE 5.2

Обычные файлы Shift+F1
Дубликаты URL (337) Shift+F2
Дубликаты по имени в кеше (4) Shift+F3
Отсутствующие файлы Shift+F4
Файлы, не относящиеся к кешу (1275) Shift+F5

www.list.ru
www.listbot.com
www.loadtv.com
www.lovehate.ru
www.lucasarts.com
www.ludicrousland.com
www.lvle.narod.ru
www.maga3.ru
www.markets.ru
www.mbnet.fi
www.mes-eng.com
www.microsoft.com
library
homepage
images
toolbar
www.mons.ru

Адрес в Инте				Type
☑ ms.htm				nl
☑ library/hom				gif
☑ library/hom				gif
☑ library/hom				gif
☑ library/imag				gif
□ library/toolbar/tool...	JS	21,0 Кб	18.11.2000 1...	application/x-jav
□ library/toolbar/en-...	JS	3,2 Кб	18.11.2000 1...	application/x-jav
□ library/toolbar/ima...	GIF 18x20	0,1 Кб	18.11.2000 1...	image/gif

Microsoft
All Products | Suppo
Home | Events/Training | Subscribe | About Microsoft | US/Wor
Search
GO

Дополнительный анализ файлов - 47%
Для того, чтобы прервать этот процесс,
щелкните дважды мышкой в этом месте

Поиск: m

Всего: 9 файлов (50,1 Кб) | 17,1 Кб, 26.10.2000 01:00 | text/html | SZ3AW9PQ\ms[1].html | Анализ - 48%

Computação Forense em Web Browsers

Ferramenta :: Web Cache Illuminator

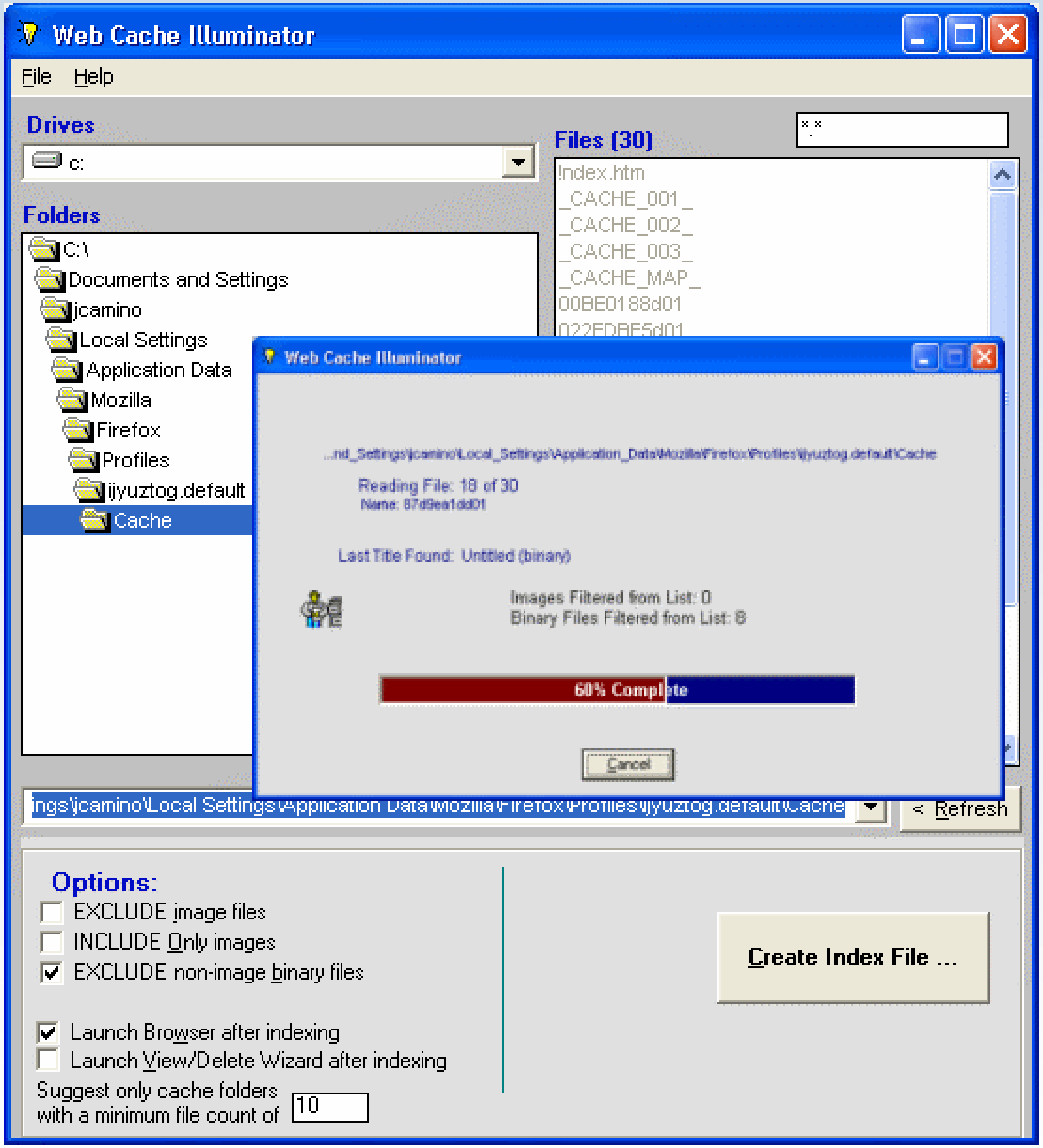
~ $ 30

- Autor: NorthStar Solutions
- Foco principal: Análise de arquivos de Cache
- S.O.: MS Windows (todos os browsers)
- Realiza buscas por arquivos ocultos
- Funcionalidade “anti-forense” (apagar pastas do cache e/ou arquivos selecionados)

http://www.nstarsolutions.com/wci/

Computação Forense em Web Browsers

Ferramenta :: Web Cache Illuminator



Drives: c:

Filter: *.*

Folders:
- C:\
- Documents and Settings
- jcamino
- Local Settings
- Application Data
- Mozilla
- Firefox
- Profiles
- ijyuztog.default
- Cache

Files (30):
- Index.htm
- _CACHE_001_
- _CACHE_002_
- _CACHE_003_
- _CACHE_MAP_
- 00BE0188d01
- 022FDBE5d01

...nd_Settings\jcamino\Local_Settings\Application_Data\Mozilla\Firefox\Profiles\ijyuztog.default\Cache

Reading File: 18 of 30
Name: 87d9ea1dd01

Last Title Found: Untitled (binary)

Images Filtered from List: 0
Binary Files Filtered from List: 8

60% Complete

ings\jcamino\Local Settings\Application Data\Mozilla\Firefox\Profiles\ijyuztog.default\Cache

Options:
- ☐ EXCLUDE image files
- ☐ INCLUDE Only images
- ☑ EXCLUDE non-image binary files
- ☑ Launch Browser after indexing
- ☐ Launch View/Delete Wizard after indexing

Suggest only cache folders with a minimum file count of 10

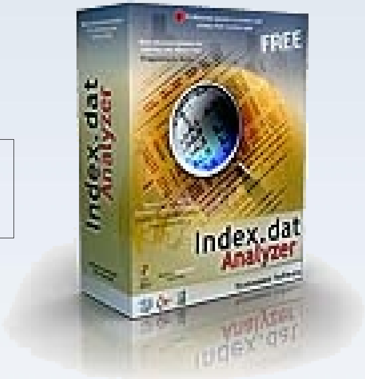
Computação Forense em Web Browsers

Ferramenta :: Index.dat Analyzer

- **Ferramenta "Anti-Forense" Web**
- **Tem como opções deletar:**
  - History – Current User
  - Cookies – Current User
  - Cache – Current User

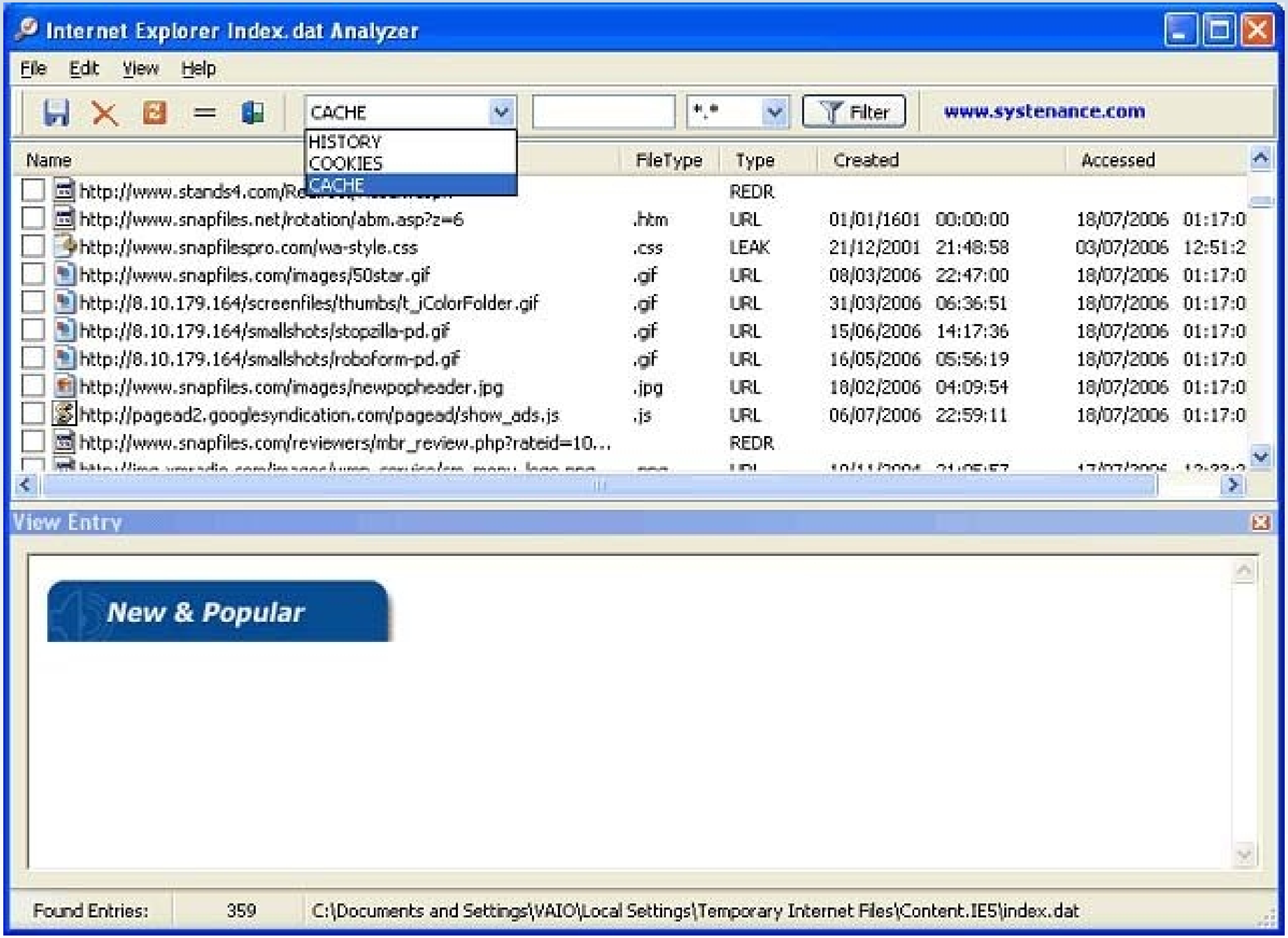
Free Software

`http://www.systenance.com/indexdat.php`



Computação Forense em Web Browsers

Ferramenta :: Index.dat Analyzer



	Name	FileType	Type	Created	Accessed
□	http://www.stands4.com/Re		REDR		
□	http://www.snapfiles.net/rotation/abm.asp?z=6	.htm	URL	01/01/1601 00:00:00	18/07/2006 01:17:0
□	http://www.snapfilespro.com/wa-style.css	.css	LEAK	21/12/2001 21:48:58	03/07/2006 12:51:2
□	http://www.snapfiles.com/images/50star.gif	.gif	URL	08/03/2006 22:47:00	18/07/2006 01:17:0
□	http://8.10.179.164/screenfiles/thumbs/t_iColorFolder.gif	.gif	URL	31/03/2006 06:36:51	18/07/2006 01:17:0
□	http://8.10.179.164/smallshots/stopzilla-pd.gif	.gif	URL	15/06/2006 14:17:36	18/07/2006 01:17:0
□	http://8.10.179.164/smallshots/roboform-pd.gif	.gif	URL	16/05/2006 05:56:19	18/07/2006 01:17:0
□	http://www.snapfiles.com/images/newpopheader.jpg	.jpg	URL	18/02/2006 04:09:54	18/07/2006 01:17:0
□	http://pagead2.googlesyndication.com/pagead/show_ads.js	.js	URL	06/07/2006 22:59:11	18/07/2006 01:17:0
□	http://www.snapfiles.com/reviewers/mbr_review.php?rateid=10...		REDR		

Found Entries: 359 C:\Documents and Settings\VAIO\Local Settings\Temporary Internet Files\Content.IE5\index.dat

Computação Forense em Web Browsers

Ferramenta :: IE History Manager

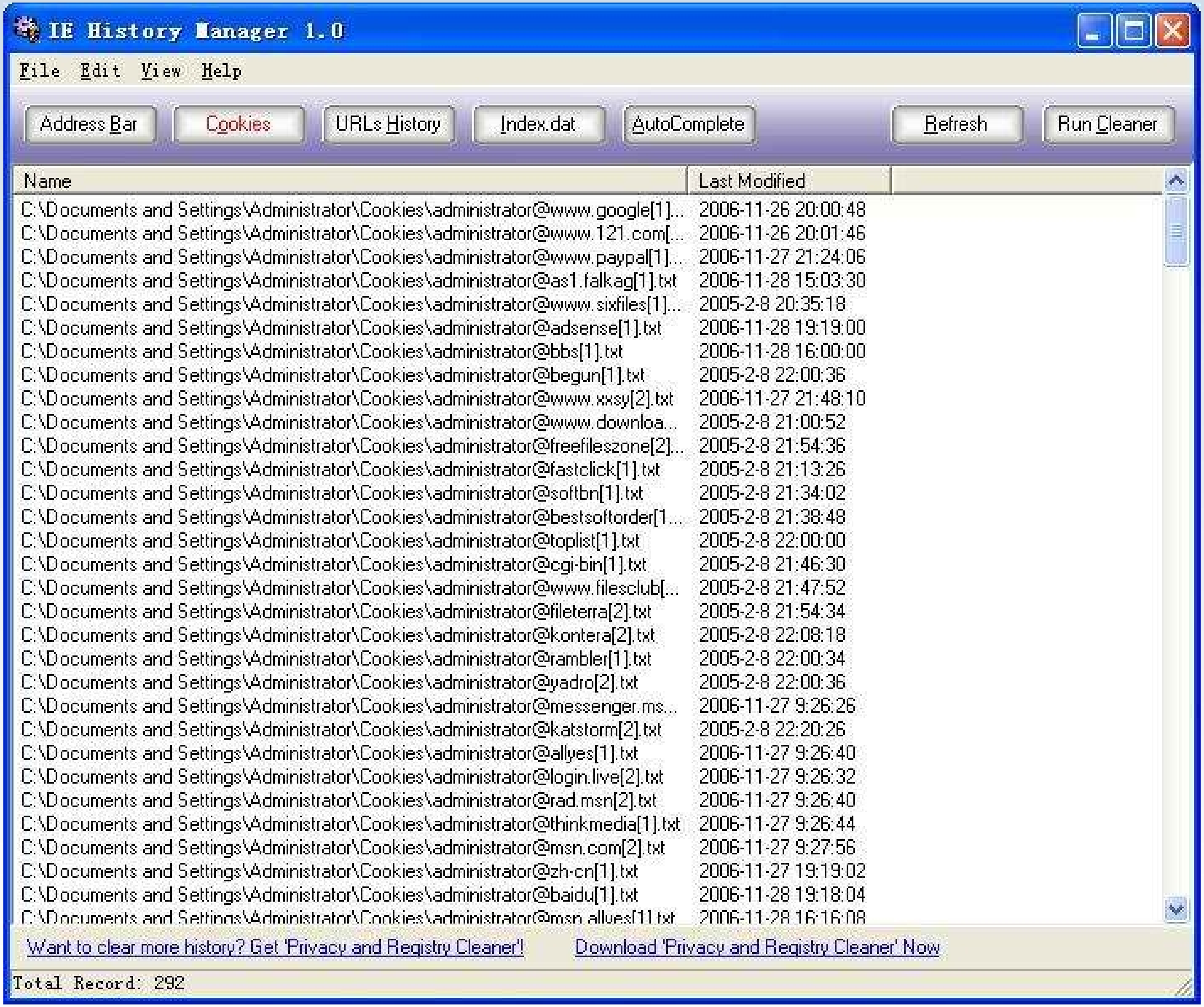
- **Ferramenta "Anti-Forense" Web**
- **S.O.: Windows 9x/Me/NT/2000/XP/2003**
- **Lista informações do Histórico...**
- **...e habilita a deleção dos "rastros":**
  - cache, cookies, history, autocomplete memory e arquivos index.dat

Free Software

```
http://www.cleanersoft.com/iehistory/iehistory.htm
```

Computação Forense em Web Browsers

Ferramenta :: IE History Manager



Name	Last Modified
C:\Documents and Settings\Administrator\Cookies\administrator@www.google[1]...	2006-11-26 20:00:48
C:\Documents and Settings\Administrator\Cookies\administrator@www.121.com[...	2006-11-26 20:01:46
C:\Documents and Settings\Administrator\Cookies\administrator@www.paypal[1]...	2006-11-27 21:24:06
C:\Documents and Settings\Administrator\Cookies\administrator@as1.falkag[1].txt	2006-11-28 15:03:30
C:\Documents and Settings\Administrator\Cookies\administrator@www.sixfiles[1]...	2005-2-8 20:35:18
C:\Documents and Settings\Administrator\Cookies\administrator@adsense[1].txt	2006-11-28 19:19:00
C:\Documents and Settings\Administrator\Cookies\administrator@bbs[1].txt	2006-11-28 16:00:00
C:\Documents and Settings\Administrator\Cookies\administrator@begun[1].txt	2005-2-8 22:00:36
C:\Documents and Settings\Administrator\Cookies\administrator@www.xxsy[2].txt	2006-11-27 21:48:10
C:\Documents and Settings\Administrator\Cookies\administrator@www.downloa...	2005-2-8 21:00:52
C:\Documents and Settings\Administrator\Cookies\administrator@freefileszone[2]...	2005-2-8 21:54:36
C:\Documents and Settings\Administrator\Cookies\administrator@fastclick[1].txt	2005-2-8 21:13:26
C:\Documents and Settings\Administrator\Cookies\administrator@softbn[1].txt	2005-2-8 21:34:02
C:\Documents and Settings\Administrator\Cookies\administrator@bestsoftorder[1...	2005-2-8 21:38:48
C:\Documents and Settings\Administrator\Cookies\administrator@toplist[1].txt	2005-2-8 22:00:00
C:\Documents and Settings\Administrator\Cookies\administrator@cgi-bin[1].txt	2005-2-8 21:46:30
C:\Documents and Settings\Administrator\Cookies\administrator@www.filesclub[...	2005-2-8 21:47:52
C:\Documents and Settings\Administrator\Cookies\administrator@fileterra[2].txt	2005-2-8 21:54:34
C:\Documents and Settings\Administrator\Cookies\administrator@kontera[2].txt	2005-2-8 22:08:18
C:\Documents and Settings\Administrator\Cookies\administrator@rambler[1].txt	2005-2-8 22:00:34
C:\Documents and Settings\Administrator\Cookies\administrator@yadro[2].txt	2005-2-8 22:00:36
C:\Documents and Settings\Administrator\Cookies\administrator@messenger.ms...	2006-11-27 9:26:26
C:\Documents and Settings\Administrator\Cookies\administrator@katstorm[2].txt	2005-2-8 22:20:26
C:\Documents and Settings\Administrator\Cookies\administrator@allyes[1].txt	2006-11-27 9:26:40
C:\Documents and Settings\Administrator\Cookies\administrator@login.live[2].txt	2006-11-27 9:26:32
C:\Documents and Settings\Administrator\Cookies\administrator@rad.msn[2].txt	2006-11-27 9:26:40
C:\Documents and Settings\Administrator\Cookies\administrator@thinkmedia[1].txt	2006-11-27 9:26:44
C:\Documents and Settings\Administrator\Cookies\administrator@msn.com[2].txt	2006-11-27 9:27:56
C:\Documents and Settings\Administrator\Cookies\administrator@zh-cn[1].txt	2006-11-27 19:19:02
C:\Documents and Settings\Administrator\Cookies\administrator@baidu[1].txt	2006-11-28 19:18:04
C:\Documents and Settings\Administrator\Cookies\administrator@msn.allyes[1].txt	2006-11-28 16:16:08

Want to clear more history? Get 'Privacy and Registry Cleaner'!   Download 'Privacy and Registry Cleaner' Now

Total Record: 292

Computação Forense em Web Browsers

Ferramentas Genéricas (não específicas p/web)

- FTK (Forensic Tool Kit)
- Encase
- Autopsy / Sleuthkit (sucessor do TCT)

- Kits
  - **Helix** (recomendado)
    - http://www.e-fense.com/helix/
  - **Professional Hackers Linux Assault Kit (PHLAK)**
    - http://www.phlak.org
  - **Knoppix security tools distribution (Knoppix-std)**
    - http://www.knoppix-std.org
  - **Penguin Sleuth Kit Bootable CD**
    - http://www.linux-forensics.com
  - **Forensic and Incident Response Environment Bootable CD (FIRE)**
    - http://fire.dmzs.com/

Computação Forense em Web Browsers
Dica para Praticar o Uso de Ferrramentas

- Caso hipotético disponível em artigo da Securityfocus
  - Web Browser Forensics (Parts 1 and 2)
    - Descrição:
      - http://www.securityfocus.com/infocus/1827
    - Material para prática:
      - http://downloads.securityfocus.com/downloads/JSchmo-InternetActivity.zip

Centro Federal de Educação Tecnológica do Rio Grande do Norte
Unidade de Ensino Descentralizada de Currais Novos
Departamento Acadêmico em Gestão Tecnológica

CEFET-RN

Perícia Forense em Web Browsers

Ricardo Kléber Martins Galvão
rk@cefetrn.br
http://www.ricardokleber.com.br

RN
CEFET

GTS
Grupo de Trabalho em Segurança

Salvador/BA, 01/06/2008