Internet Activity Analysis

Cybercrime Lab

U.S. Department of Justice

Computer Crime and intellectual Property Section

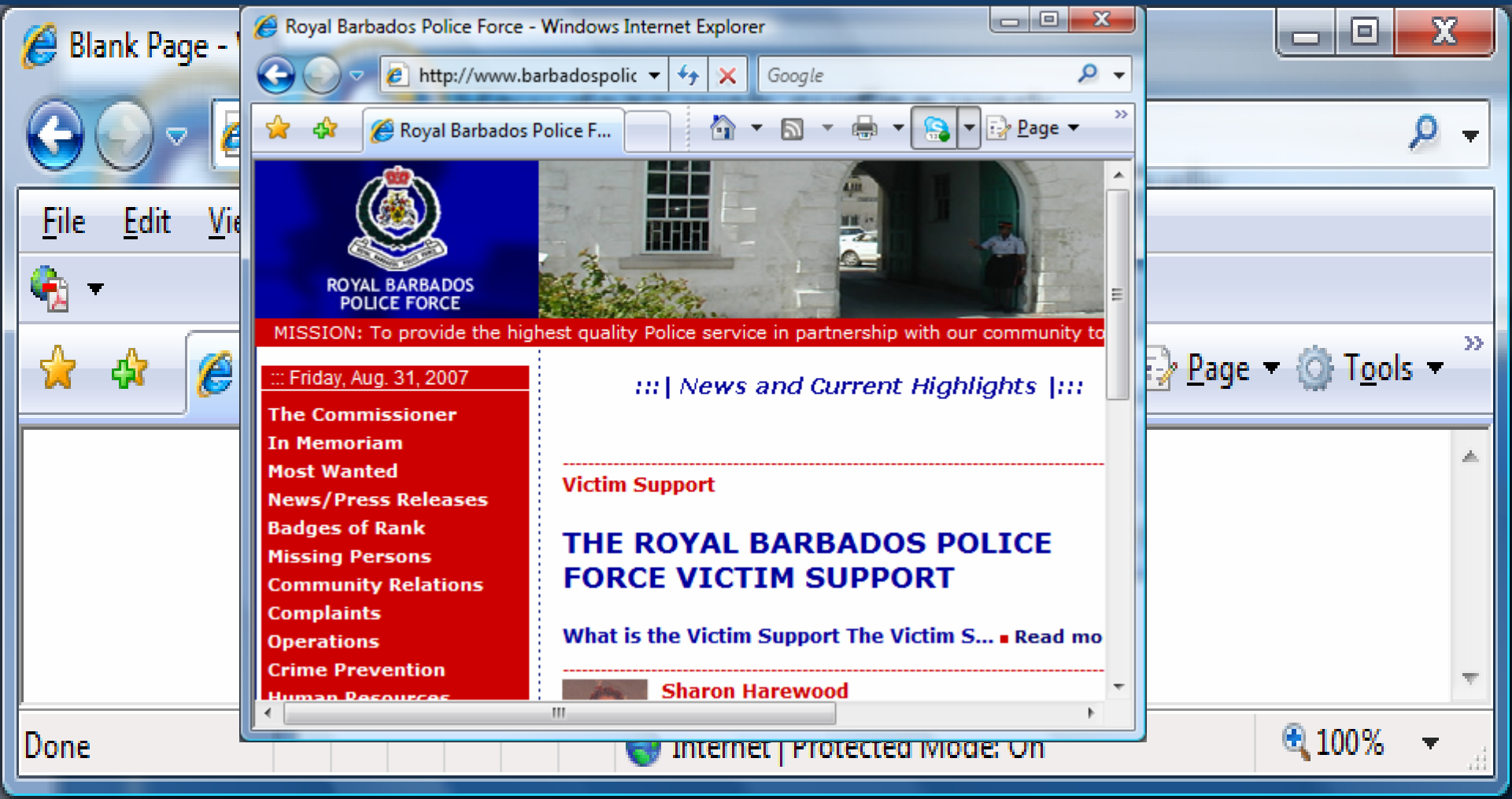
Internet Activity Analysis

Agenda

- How does web surfing works
- Where to Find Evidence of Web Surfing Activity
- Internet Activity Analysis and Tools needed.
  - User computer
  - Web server
  - Internet Service Provider (ISP)

How does web surfing work

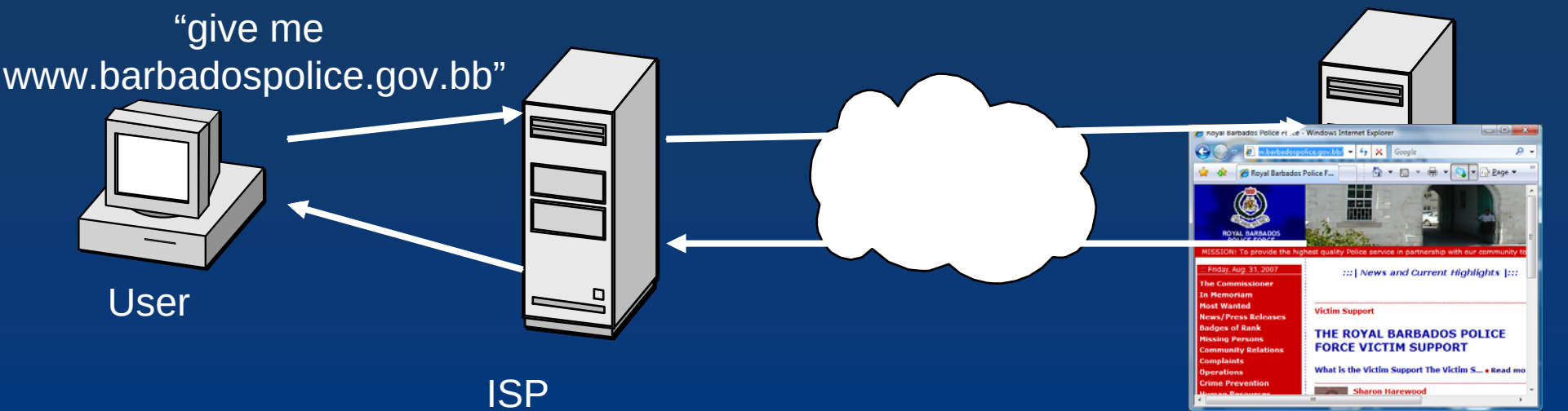
Visit www.barbadospolice.gov.bb



How does web surfing work

What Happens

- Our browser sends a request to the web server
- The web server sends files that makes up the webpage to our computer



Where to Find Web Surfing Evidence

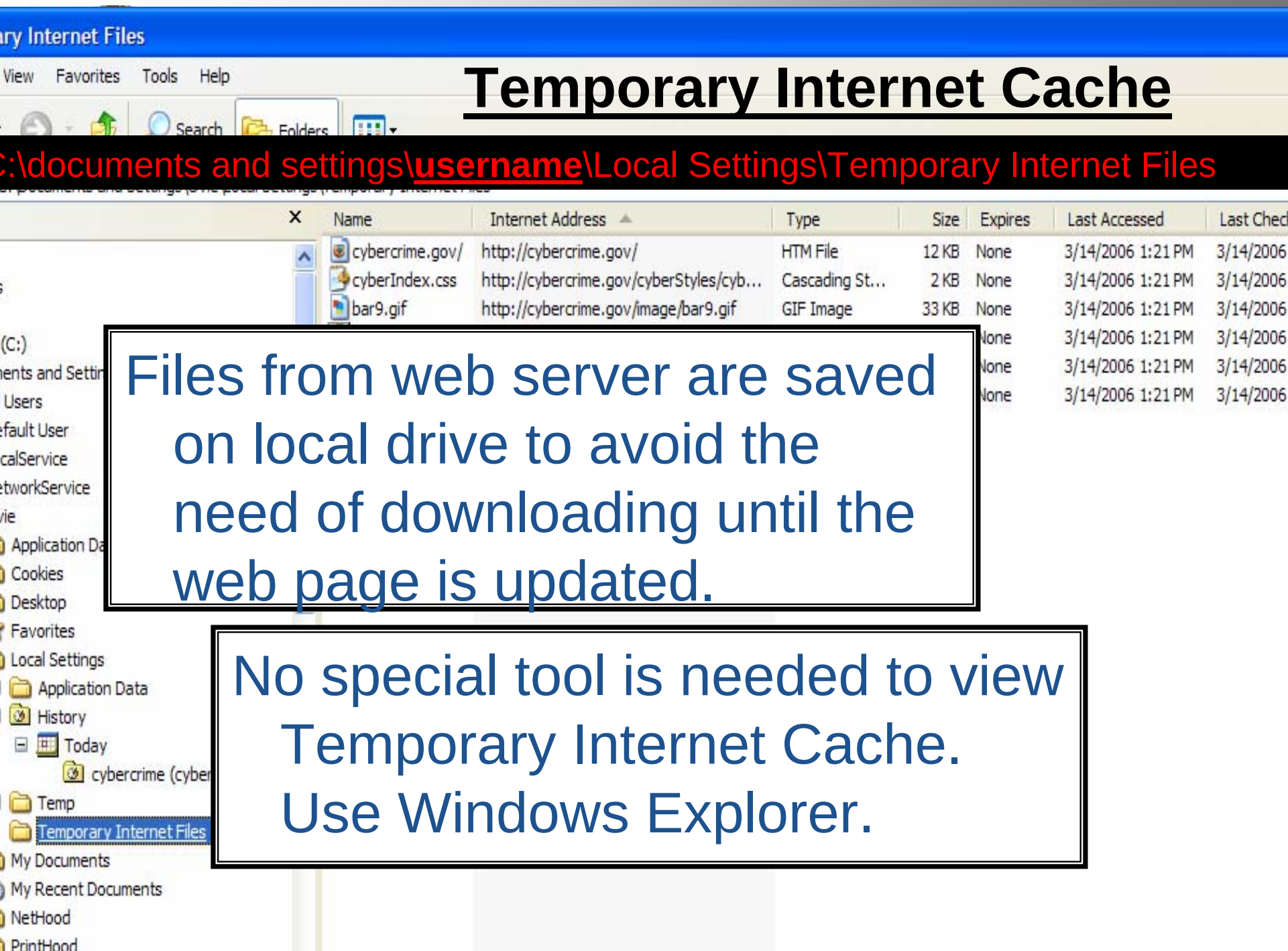
- User Computer:
  - Temporary Internet Files, index.dat, cookies, favorites, html pages and images in un-allocated space.
  - C:\Documents and Settings\<user>\Local Settings\History
  - Files from web sites, ftp programs and logs
- Web Server:
  - Site Content, Access logs, Error Logs, FTP Logs
  - Log Reporting Tools: Ana-log, web-analyzer, etc.
- Intermediate Sites (ISP)
  - Firewall logs, Anti-virus server logs, spam filter logs, web filtering logs (Web Sense)

Evidence on user computer

- Temporary Internet Cache
- History
- Index.dat
- Cookies
- Registry

Temporary Internet Cache

C:\documents and settings**username**\Local Settings\Temporary Internet Files

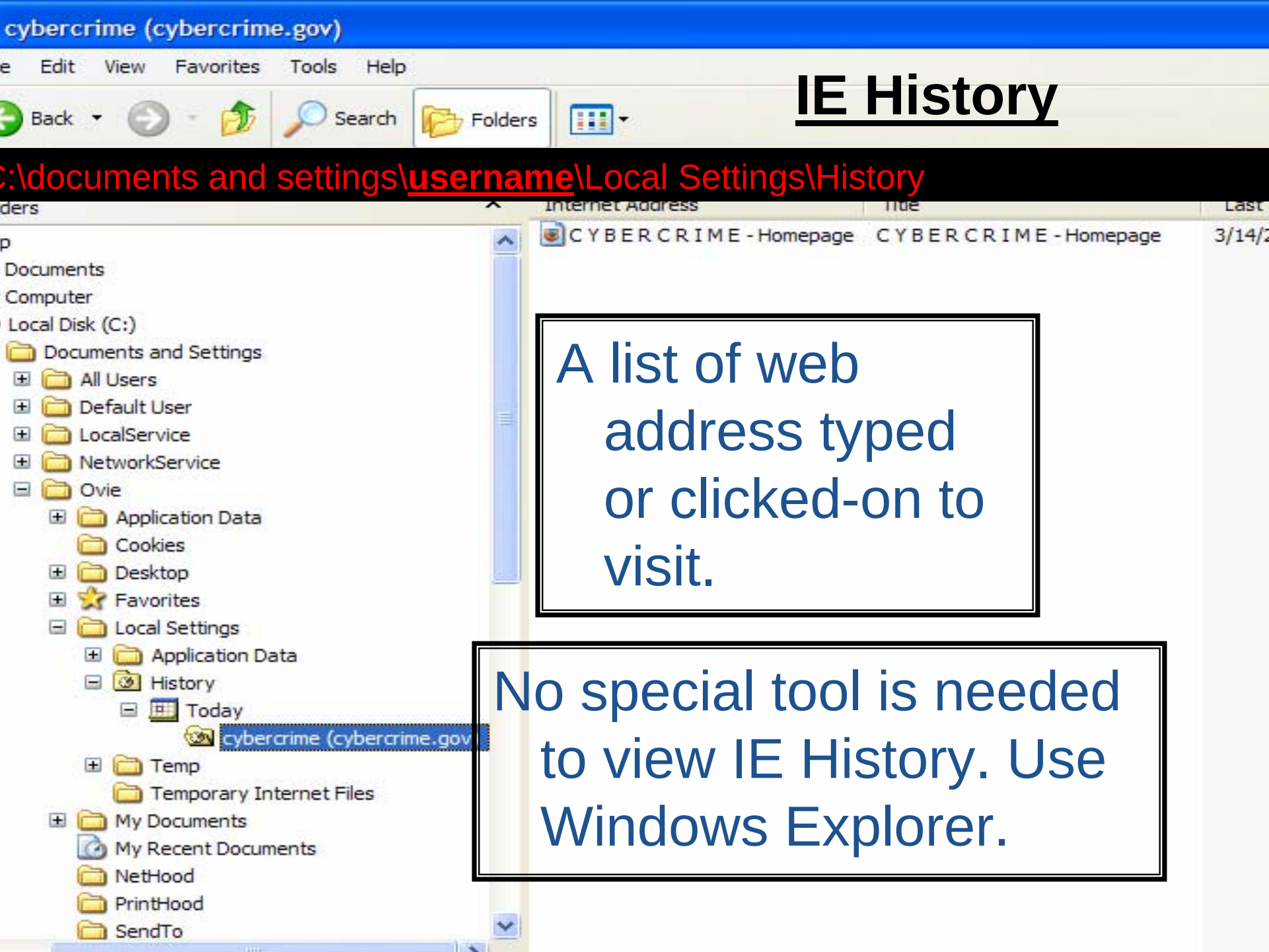


Files from web server are saved on local drive to avoid the need of downloading until the web page is updated.

No special tool is needed to view Temporary Internet Cache. Use Windows Explorer.

IE History

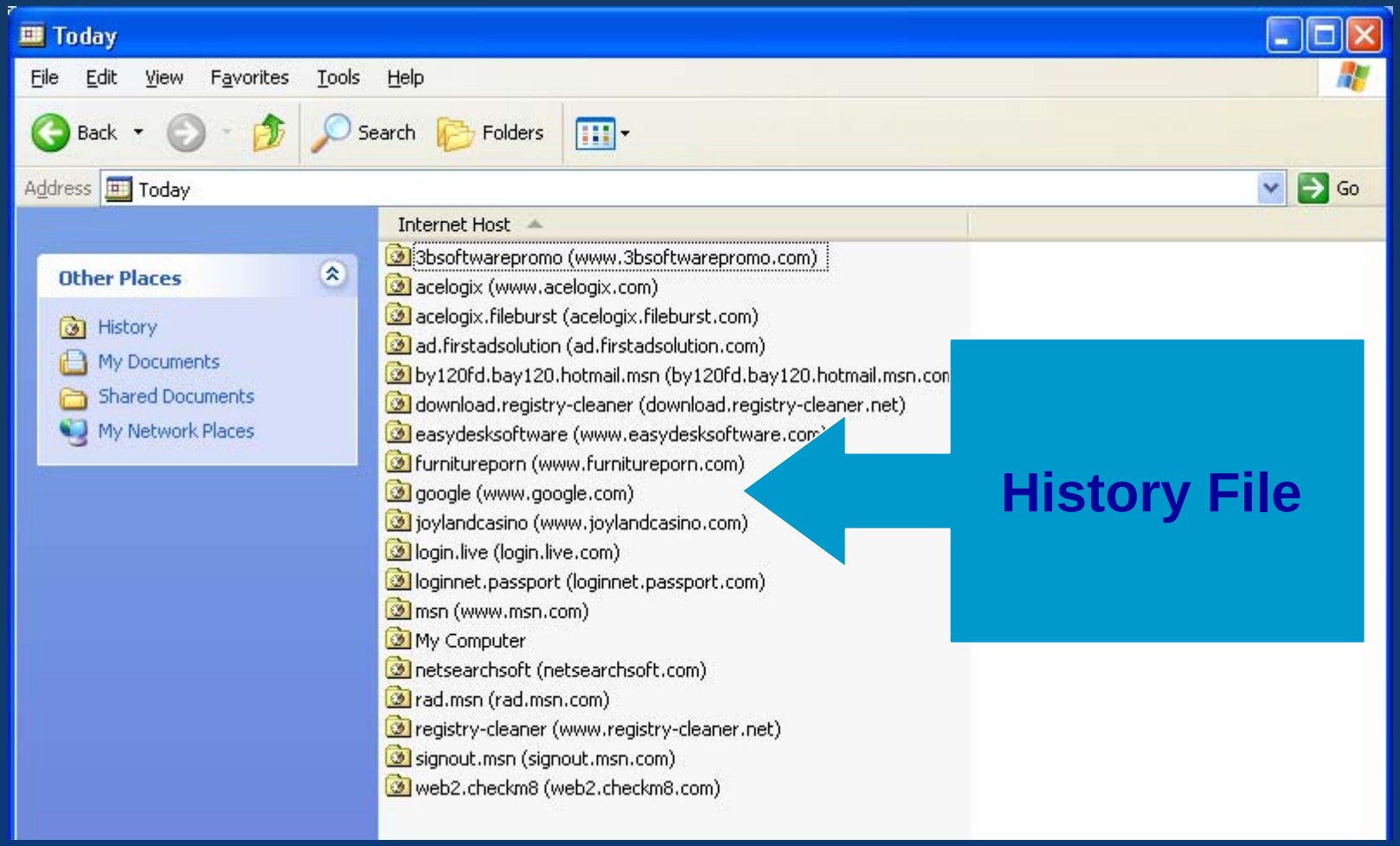
C:\documents and settings**username**\Local Settings\History



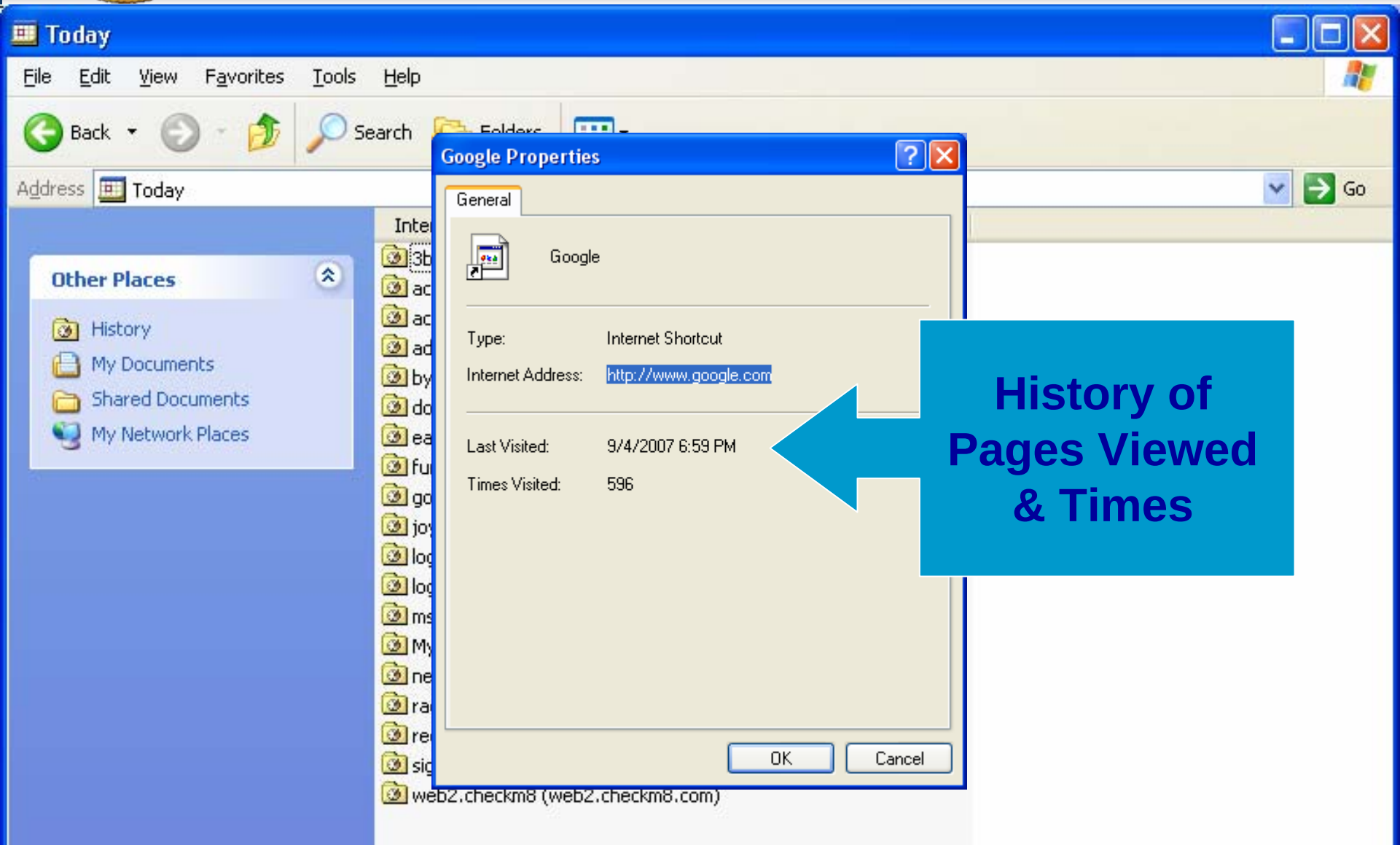
A list of web address typed or clicked-on to visit.

No special tool is needed to view IE History. Use Windows Explorer.

IE History


Today
File Edit View Favorites Tools Help
Back Search Folders
Address Today Go
Other Places
History
My Documents
Shared Documents
My Network Places
Internet Host
3bsoftwarepromo (www.3bsoftwarepromo.com)
acelogix (www.acelogix.com)
acelogix.fileburst (acelogix.fileburst.com)
ad.firstadsolution (ad.firstadsolution.com)
by120fd.bay120.hotmail.msn (by120fd.bay120.hotmail.msn.con
download.registry-cleaner (download.registry-cleaner.net)
easydesksoftware (www.easydesksoftware.com)
furnitureporn (www.furnitureporn.com)
google (www.google.com)
joylandcasino (www.joylandcasino.com)
login.live (login.live.com)
loginnet.passport (loginnet.passport.com)
msn (www.msn.com)
My Computer
netsearchsoft (netsearchsoft.com)
rad.msn (rad.msn.com)
registry-cleaner (www.registry-cleaner.net)
signout.msn (signout.msn.com)
web2.checkm8 (web2.checkm8.com)
History File

History



History of Pages Viewed & Times

Evidence on User Computer

Index.dat

- Contain a log all files makes up all the web pages visited.
- Needs special tools to decode this file.
  - IE history viewer
  - Net Analysis
- Reside in Folder “Documents and Settings\<User>\Local settings\Temporary Internet Files\Content.IE5” for Internet Explorer, Windows XP

Evidence on User Computer

Analyzing Index.dat

- Special tool is needed to view Index.dat file.

Paraben Net Analysis
www.logon-int.com

Analyzing Index.dat Using IEhistory Viewer

IEHistoryView: c:\documents and settings\Administrator\Local Settings\History

File Edit View Help

URL	Hits	Modified Date	Expiration Date
about:Home		2006 12:59:01 AM	N/A

Select User Profile

User Profile:

- Administrator
- CCIPS
- Default User
- LocalService
- NetworkService
- Ovie

1 item(s)

Analyzing Index.dat Using IEhistory Viewer

IEHistoryView: C:\Documents and Settings\CCIPS\Local Settings\History

File Edit View Help

URL	Hits	Modified Date	Expiration Date	User Name
http://cyberspeak.libsyn.com/index.php?post_id=155453&comments=on	11	11/27/2006 9:05:19 PM	12/23/2006 9:05:20 PM	CCIPS
http://cyberspeak.libsyn.com/index.php?post_id=155453&comments=on	10	11/27/2006 9:05:19 PM	12/23/2006 9:05:20 PM	CCIPS
http://cyberspeak.libsyn.com/rss	5	11/27/2006 9:05:19 PM	12/23/2006 9:05:20 PM	CCIPS
http://cyberspeak.libsyn.com	10	11/27/2006 9:05:16 PM	12/23/2006 9:05:18 PM	CCIPS
http://cyberspeak.libsyn.com/index.php?post_id=153162&comments=on	11	11/27/2006 9:03:59 PM	12/23/2006 9:04:00 PM	CCIPS
http://cyberspeak.libsyn.com/rss	2	11/27/2006 9:03:58 PM	12/23/2006 9:04:00 PM	CCIPS
http://cyberspeak.libsyn.com/index.php?post_id=153162&comments=on	2	11/27/2006 9:03:58 PM	12/23/2006 9:04:00 PM	CCIPS
http://cyberspeak.libsyn.com	7	11/27/2006 9:03:54 PM	12/23/2006 9:03:56 PM	CCIPS
http://www.cybercrime.gov	7	11/27/2006 9:03:43 PM	12/23/2006 9:03:44 PM	CCIPS
http://news.com.com/2547-1_3-0-20.xml	1	11/27/2006 9:03:29 PM	12/23/2006 9:03:30 PM	CCIPS
http://search.live.com/results.aspx?q=www.news.cnet.com&src=IE-Address	7	11/27/2006 9:03:15 PM	12/23/2006 9:03:16 PM	CCIPS
http://search.live.com/results.aspx?q=www.news.cnet.com&format=rss	1	11/27/2006 9:03:14 PM	12/23/2006 9:03:16 PM	CCIPS
http://local.live.com/i/spacer.gif	1	11/27/2006 9:00:14 PM	12/23/2006 8:53:06 PM	CCIPS
http://local.live.com/favicon.ico	3	11/27/2006 8:59:57 PM	12/23/2006 8:52:48 PM	CCIPS
http://local.live.com	1	11/27/2006 8:59:56 PM	12/23/2006 8:52:48 PM	CCIPS
https://lms.digitalthink.com/lms/com/digitalthink/lms/tk/jspDriver/lms_driver.jsp;LMSJSESSIONID=Fq42...	22	11/27/2006 8:59:47 PM	12/23/2006 8:52:38 PM	CCIPS
file:///C:/Documents%20and%20Settings/CCIPS/Desktop/Internet%20Analysis.ppt	1	11/27/2006 8:56:16 PM	12/23/2006 8:56:18 PM	CCIPS
file:///C:/Documents%20and%20Settings/CCIPS/Desktop/iehv_lng.ini	1	11/27/2006 8:34:46 PM	12/23/2006 8:34:48 PM	CCIPS
file:///C:/Documents%20and%20Settings/CCIPS/Desktop/iehv_spanish.zip	1	11/27/2006 8:34:02 PM	12/23/2006 8:34:04 PM	CCIPS
file:///C:/Documents%20and%20Settings/CCIPS/Desktop/Info%20Tools/iehv_lng.txt	2	11/27/2006 8:31:13 PM	12/23/2006 8:24:04 PM	CCIPS

677 item(s)

Internet Tracks

Internet Address	Last Accessed
http://by120fd.bay120.hotmail.msn.com/cgi-bin/getmsg?msg=8B5CFCCE-552A-498B-8D02-D8968EEDC790&start=0&len=192&m...	8/12/2006 4:31 PM
http://gfx2.hotmail.com/i.p.fwd.gif	8/12/2006 4:31 PM
http://gfx2.hotmail.com/i.p.printv.gif	8/12/2006 4:31 PM
http://gfx2.hotmail.com/i.p.reply.d.gif	8/12/2006 4:31 PM
http://gfx2.hotmail.com/i.p.replyall.d.gif	8/12/2006 4:31 PM
http://gfx2.hotmail.com/i.p.next.gif	8/12/2006 4:31 PM
http://gfx2.hotmail.com/i.p.previous.gif	8/12/2006 4:31 PM
http://gfx2.hotmail.com/crs_2716.gif	
http://gfx2.hotmail.com/crs_60.gif	
http://b.global.msad[illegible].net/ads/8707/0000008707_00000000000000[illegible]	
http://www.google.com/search?hl=en&q=Furniture+Porn	
http://www.furnitureporn.com/banners/banner20.gif	
http://www.furnitureporn.com/chairlie01.html	
http://www.vgg.com/furnitureporn/graphics/ca8.jpg	
http://www.furnitureporn.com/chairlie02.html	
http://www.vgg.com/furnitureporn/graphics/ca6.jpg	:33 PM
http://www.furnitureporn.com/chairlie03.html	4:33 PM
http://www.vgg.com/furnitureporn/graphics/ca12.jpg	06 4:33 PM
http://www.furnitureporn.com/chairlie04.html	06 4:33 PM
http://www.vgg.com/banners/banner4.gif	06 4:33 PM
http://www.vgg.com/furnitureporn/graphics/ca4.jpg	06 4:33 PM
http://www.furnitureporn.com/chairlie05.html	06 4:34 PM
http://www.vgg.com/furnitureporn/graphics/ca20.jpg	06 4:34 PM
http://www.furnitureporn.com/chairlie06.html	8/12/2006 4:34 PM
http://www.vgg.com/banners/banner21.gif	8/12/2006 4:34 PM
http://www.vgg.com/furnitureporn/graphics/ca26.jpg	8/12/2006 4:34 PM
http://www.furnitureporn.com/chairlie07.html	8/12/2006 4:34 PM

Clicks into Charlie's Angel's Pages

Clicks into EACH photo

Name	Internet Address	Last Accessed	Last Checked
935762.5.1??PID=3232842&...	http://b.global.msads.net/ads/8707		
search?hl=en&q=Furniture+P...	http://www.google.com/search?hl=		
banner20.gif	http://www.furnitureporn.com/bann		
chairlie01.html	http://www.furnitureporn.com/chair		
ca8.jpg	http://www.vgg.com/furnitureporn/		
chairlie02.html	http://www.furnitureporn.com/chair		

http://by120fd.bay120.hotmail.msn.com/cgi-bin/hmhome?fti=yes&c 000%2d0000%2d0000%2d0000%2d0000000..
http://hm.msn.com/FC/!8L3`W[C{KR[_]A{MURF.jpg
http://ads.msn.com/ads/pronws/HM010804msnbutton.gif
http://global.msads.net/ads/363/0000000363_00000000000
http://by120fd.bay120.hotmail.msn.com/cgi-bin/HoTMail?c 2d0000%2d0000%2d0000%2d000000000001&a..
http://spe.atdmt.com/images/pixel.gif
http://by120fd.bay120.hotmail.msn.com/cgi-bin/compose?8curmbox=00000000%2d0000%2d0000%2d0000%2d000000000001...
http://by120fd.bay120.hotmail.msn.com/cgi-bin/HoTMaiL?curmbox=00000000%2d0000%2d0000%2d0000%2d000000000001&a..
http://spe.atdmt.com/ds/AAAVEBBUYBB7/FY07_BTS_Phase2/bts_pc_phase2_desktop1_728x90_v1_NoSurv.swf?ver=1&clickTag1..
http://global.msads.net/ads/363/0000000363_00000000000000324074.gif
http://global.msads.net/ads/8013/0000008013_00000000000000296819.gif
http://ad.doubleclick.net/adj/N3285.msn-dm/B1714331.74;dcadv=895178;abr=!ie;sz=160x600;
http://ad.doubleclick.net/adj/N3285.msn-dm/B1714331.74;dcadv=895178;sz=160x600;ord=1
http://m.2mdn.net/895178/lmb_lre_PassStRtCredWireHseBord15sec_484TP_0606_160x600.swf?ct=US&s
http://by120fd.bay120.hotmail.msn.com/cgi-bin/HoTMail a18c73cb40fa0d6c1871f7695316b1d4daf6
http://gfx2.hotmail.com/i.F42AB.gif
http://rmd.atdmt.com/tl//DocumentDotWrite.
http://spe.atdmt.com/ds/MSMSNMATCD Adoor.swf?ver=1&clickTag1=http://clk.atdmt.com/go/ms..
http://global.msads.net/ads/8013/0000008 6818.gif
http://spe.atdmt.com/b/CJCNTCINGCIN/3 160x600.gif
http://by120fd.bay120.hotmail.msn.c in/c msg=14FB5ECD-C8BE-4B9A-90C0-ECC75B2AADFE&start=0&len=1031..
http://gfx2.hotmail.com/i.n.send.gif

Composes An Email

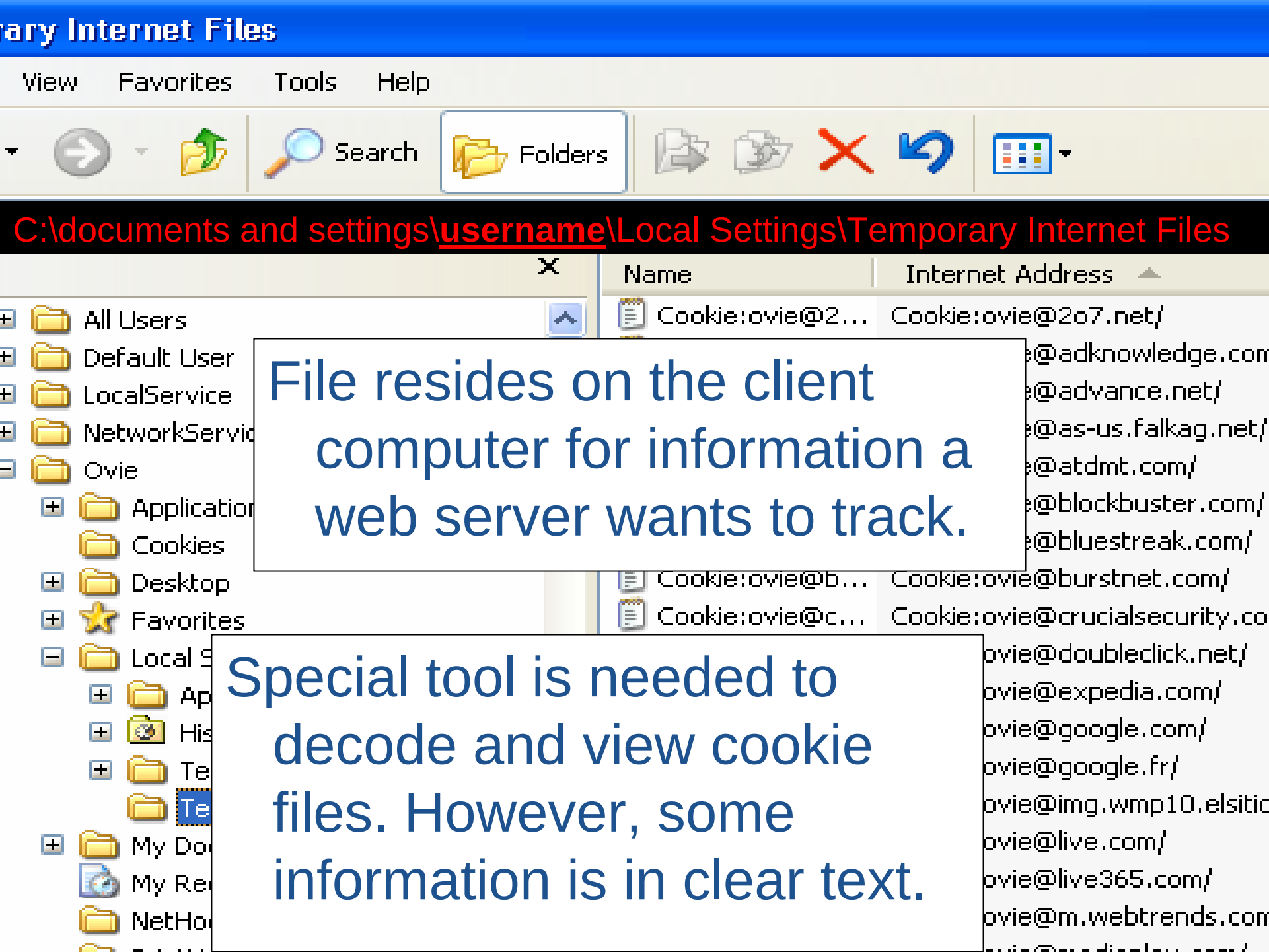
Goes Back To HOTMAIL

Sends The Email

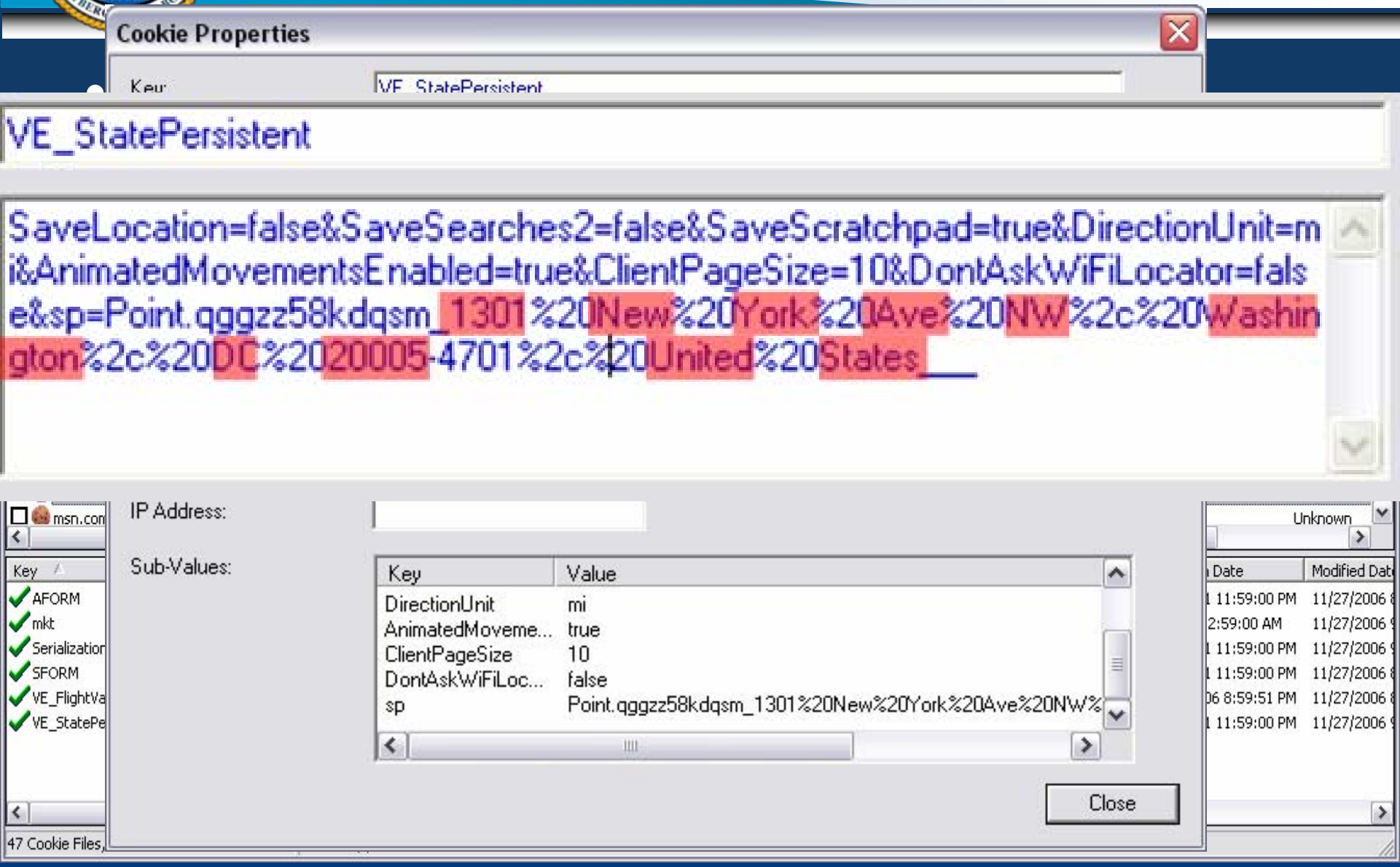
http://gfx2.hotmail.com/i.F42B5.gif
http://gfx2.hotmail.com/i.1EF9B0.gif
http://ad.doubleclick.net/adj/N3285.msn-dm/B1714331.61;dcadv=895178;abr=!ie;sz=728x90;ord=117479559?click=http://clk.a...
... http://global.msads.net/ads/363/0000000363_00000000000000000324076.gif
... http://global.msads.net/ads/8373/0000008373_00000000000000000245374.gif
... http://global.msads.net/ads/33/0000000033_00000000000000000261548.gif
http://ad.doubleclick.net/adj/N3285.msn-dm/B1714331.61;dcadv=895178;sz=728x90;ord=117479559?click=http://clk.atdmt.co...
http://m.2mdn.net/879366/DartRichMedia_1_03.js
... http://spe.atdmt.com/b/MSMSNMATCVZD/VZ_OfferOnly_1495_HSI_Modem_160x600.gif
... http://m.2mdn.net/895178/lmb_lre_PassStRtCredWirehseBrd15s_CW510_1698TP_0706_728x90.swf?ct=US&st=VA&ac=703&zp...
http://gfx2.hotmail.com/sbtnbk.gif
http://gfx2.hotmail.com/icon_checkmark.gif
.. http://global.msads.net/defaultads/ads/defaultads/1402.g
.. http://b.global.msads.net/ads/8707/0000008 ... sn.com&clickTAG=http%3A//g.ms...
http://www.furnitureporn.com/
http://www.furnitureporn.com/warning.html
http://www.furnitureporn.com/banners/banner.js
http://www.furnitureporn.com/graphics/enterfp.gif
http://www.furnitureporn.com/graphics/exitfp.gif
http://www.furnitureporn.com/banners/banner4.gif
http://www.furnitureporn.com/bond1.html
http://www.vgg.com/banners/banner9.gif
http://www.vgg.com/furnitureporn/graphics/bond2.jpg
http://www.furnitureporn.com/bond2.html
http://www.vgg.com/furnitureporn/graphics/bond5.jpg
http://www.furnitureporn.com/bond3.html
http://www.vgg.com/furnitureporn/graphics/bond6.jpg
http://www.furnitureporn.com/bond4.html

Returns to Surfing Furniture Porn

bond6.jpg	http://www.vgg.com/furnitureporn/graphics/bond6.jpg	8/12/2006 4:45 PM
bond4.html	http://www.furnitureporn.com/bond4.html	8/12/2006 4:45 PM


rary Internet Files
View
Favorites
Tools
Help
Search
Folders
C:\documents and settings\username\Local Settings\Temporary Internet Files
Name
Internet Address
All Users
Default User
LocalService
NetworkServic
Ovie
Application
Cookies
Desktop
Favorites
Local S
My Do
My Re
NetHo
Cookie:ovie@2...
Cookie:ovie@2o7.net/
Cookie:ovie@b...
Cookie:ovie@burstnet.com/
Cookie:ovie@c...
Cookie:ovie@crucialsecurity.co
File resides on the client computer for information a web server wants to track.
Special tool is needed to decode and view cookie files. However, some information is in clear text.

IECookiesView



Registry

Registry Editor

File Edit View Favorites Help

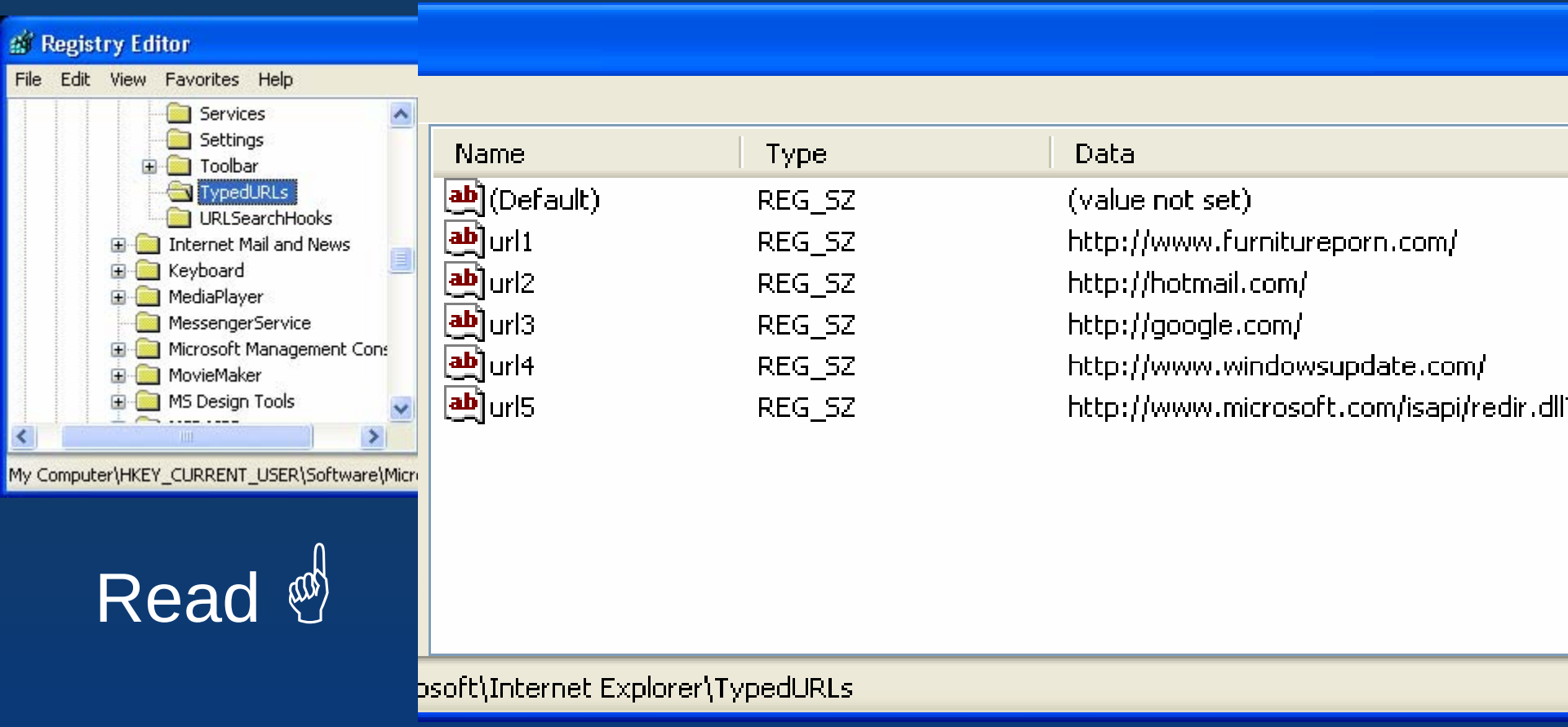
- File Manager
- FTP
- GDIPlus
- IMEJP
- IMEMIP
- Installer
- Internet Account Manager
- Internet Connection Wizard
- Internet Explorer
  - Default HTML Editor
  - Default MHTML Editor
  - Desktop
  - Document Windows
  - Download
  - Explorer Bars
  - Extensions
  - Help_Menu_URLs
  - IntelliForms
  - International
  - Main
  - Media
  - MenuExt
  - New Windows
  - SearchUrl
  - Security
  - Services
  - Settings
  - Toolbar
  - TypedURLs
  - URLSearchHooks

Name	Type	Data
(Default)	REG_SZ	(value not set)
url1	REG_SZ	http://www.hidemyass.com/
url2	REG_SZ	http://google.com/
url3	REG_SZ	http://www.cybercrime.gov/

My Computer\HKEY_USERS\S-1-5-21-1801674531-1326574676-839522115-1003\Software\Microsoft\Internet Explorer\TypedURLs

Registry

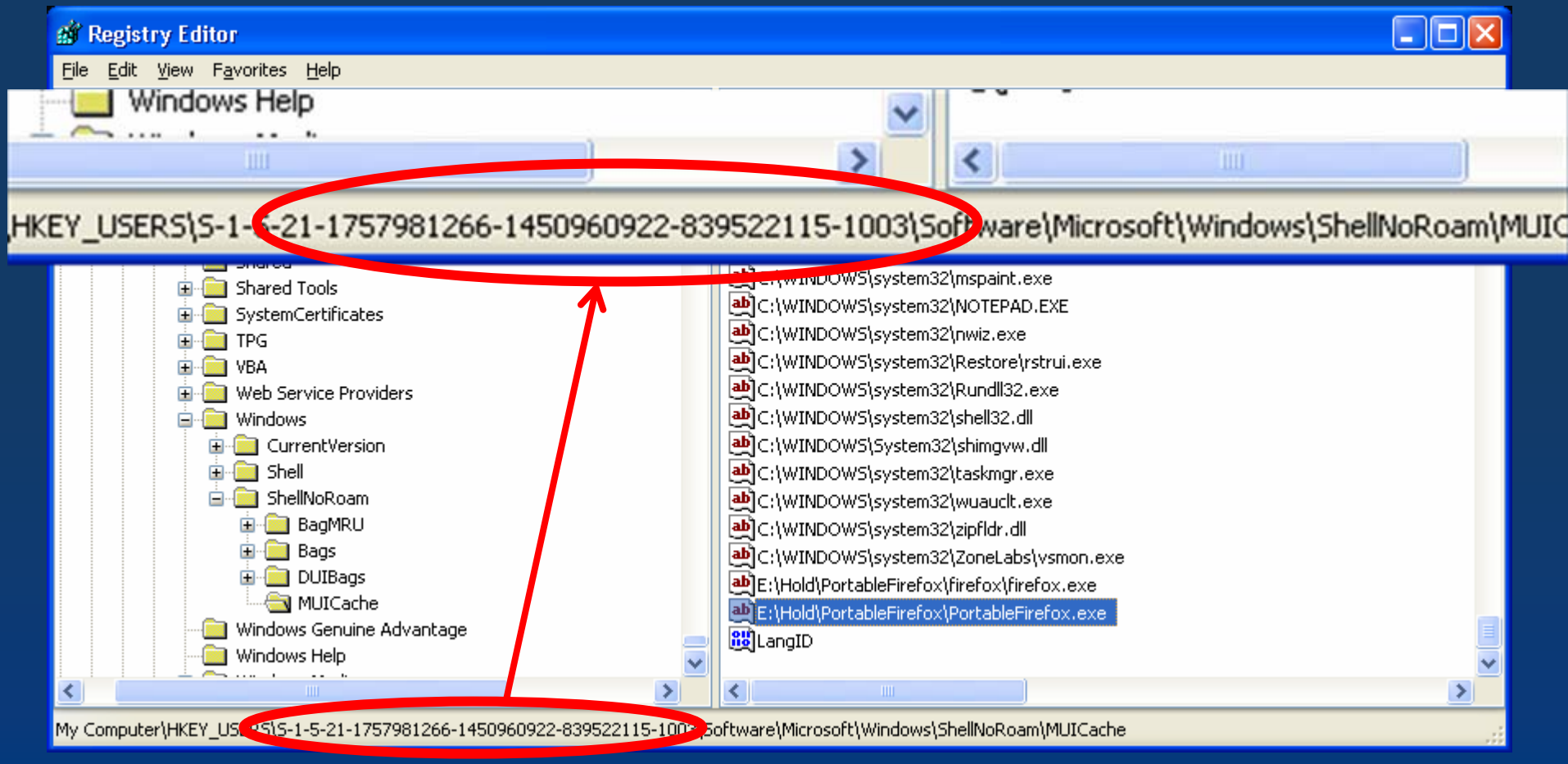
- Human Typed URL's



Read

Registry

- Also tracked by User Security Identifier (SID)



Why do we care about user's computer?

- Can be seized for evidence
- Can be used as an undercover investigation tool

Evidence: Web Server

- Web access logs.
- The illegal contents web server provides to Internet users.

Evidence: Web Server

Sample Web Server Logs: each entry represents a request to the sever

199.202.74.125 - - [25/Apr/2006:09:16:23:48 -0500] “GET /index.html /HTTP/1.0” 200 6248 “http://www.catsrus.com/links.htm” “Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98;+Win+9x+4.90)

199.202.74.125 - - [25/Apr/2006:09:16:24:01 -0500] “GET **/wordpress/seduction.jpg** /HTTP/1.0” 200 47178 “http://www.google.com/search?hl=en&q=kitty+porn” “Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98;+Win+9x+4.90)

IP of requesting computer

Request (file requested)

Date/time of request (as seen by web server)

Bytes transferred

Referrer URL (the referring page)

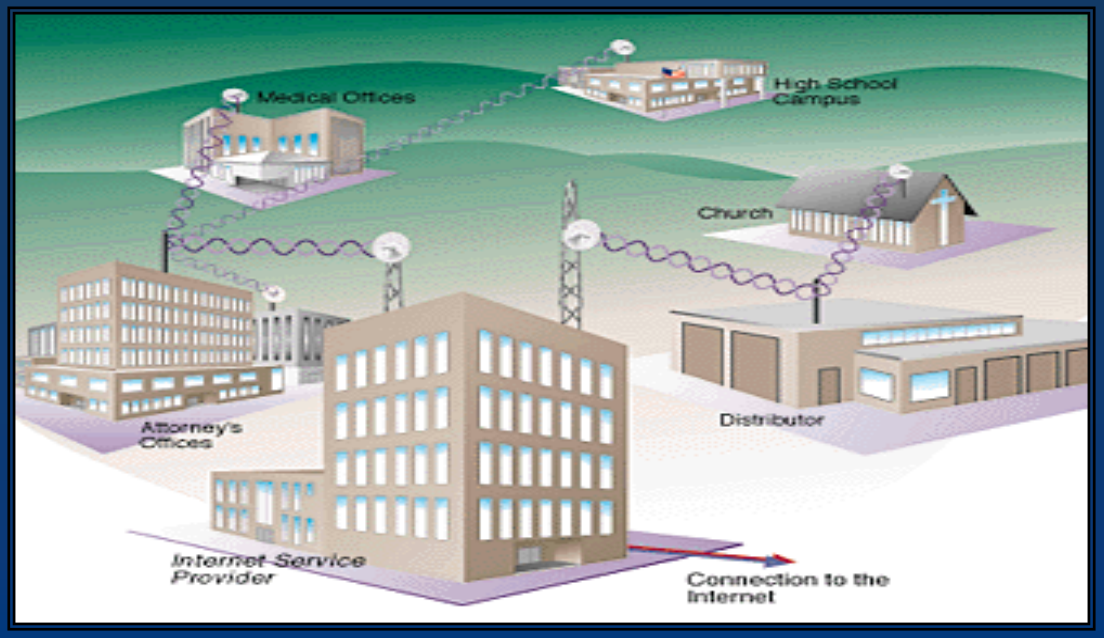
User Agent (browser, operating system)

Why do we care about web servers?

- Criminals using a web server will obtain information about the undercover computer
- If law enforcement can run the web server, we can obtain this information about targets

Evidence: ISP

- ISP can provide LE account information to full content of a user's activity



Evidence: ISP

- Sample response to pen-trap order

	A	B	C	D	E	F	G	H	I
1	TCP	Node1 Name	Node1 Bytes Sent	Node2 Name	Node2 Bytes Sent	Start Time	Stop Time	Total Bytes	Duration (secs.)
2	TCP	109.211.87.22	52	197.239.153.148	72	12/9/2005 5:17	12/9/2005 5:17	124	0
3	TCP	109.211.87.22	49	21.160.166.14	74	12/9/2005 5:17	12/9/2005 5:17	123	2
4	TCP	109.211.87.22	44	101.91.157.13	103	12/9/2005 5:17	12/9/2005 5:17	147	0
5	TCP	109.211.87.22	59	21.160.166.14	83	12/9/2005 5:17	12/9/2005 5:17	142	1
6	TCP	109.211.87.22	2273	115.198.117.225	417	12/9/2005 5:17	12/9/2005 5:17	2690	0
7	TCP	109.211.87.22	2257	115.198.117.225	3457	12/9/2005 5:17	12/9/2005 5:17	5714	0
8	TCP	109.211.87.22	48	102.110.252.202	77	12/9/2005 5:17	12/9/2005 5:17	125	0
9	TCP	109.211.87.22	54	249.142.242.201	199	12/9/2005 5:16	12/9/2005 5:17	253	0
10	TCP	109.211.87.22	423	71.54.97.105	1176	12/9/2005 5:16	12/9/2005 5:16	1599	0
11	TCP	109.211.87.22	49	2.135.238.65	81	12/9/2005 5:16	12/9/2005 5:16	130	0
12	TCP	254.84.58.65	0	109.211.87.22	0	12/9/2005 5:15	12/9/2005 5:15	0	8
13	TCP	109.211.87.22	9541	119.202.55.44	18344	12/9/2005 5:11	12/9/2005 5:18	27885	382
14	TCP	109.211.87.22	6	169.192.178.164	0	12/9/2005 5:11	12/9/2005 5:16	6	300
15	TCP	109.211.87.22	24	189.130.109.116	120	12/9/2005 5:11	12/9/2005 5:17	144	360
16	TCP	109.211.87.22	24	176.31.58.35	120	12/9/2005 5:11	12/9/2005 5:17	144	360
17	TCP	231.196.103.72	114	109.211.87.22	6	12/9/2005 5:11	12/9/2005 5:18	120	419
18	TCP	82.177.26.187	2711	109.211.87.22	296	12/9/2005 5:01	12/9/2005 5:18	3007	1028

Evidence: ISP

Sample of Full Content Monitoring / Capturing

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.205.161	212.24.243.2	HTTP	GET http://www.myspace.com/ HTTP/1.1
2	0.349072	212.24.243.2	172.16.205.161	TCP	http > 1392 [ACK] Seq=0 Ack=435 Win=65535 Len=0
3	1.027083	212.24.243.2	172.16.205.161	HTTP	[TCP Previous segment lost] Continuation or non-HTTP traffic
4	1.027143	172.16.205.161	212.24.243.2	TCP	1392 > http [ACK] Seq=435 Ack=0 Win=17040 Len=0
5	1.045529	212.24.243.2	172.16.205.161	HTTP	[TCP Retransmission] HTTP/1.0 200 OK (text/html)
6	1.046004	172.16.205.161	212.24.243.2	TCP	1392 > http [ACK] Seq=435 Ack=2823 Win=14217 Len=0
7	1.046308	172.16.205.161	212.24.243.2	TCP	[TCP Window Update] 1392 > http [ACK] Seq=435 Ack=2823 Win=17040 Len=0
8	1.052130	212.24.243.2	172.16.205.161	HTTP	Continuation or non-HTTP traffic
9	1.052269	172.16.205.161	212.24.243.2	TCP	1392 > http [ACK] Seq=435 Ack=3825 Win=16039 Len=0
10	1.053099	172.16.205.161	212.24.243.2	TCP	1392 > http [FIN, ACK] Seq=435 Ack=3825 Win=16039 Len=0
11	1.072755	172.16.205.161	212.24.243.2	HTTP	GET http://x.myspace.com/js/myspace.js HTTP/1.1
12	1.279441	212.24.243.2	172.16.205.161	TCP	[TCP ZeroWindow] http > 1392 [ACK] Seq=3825 Ack=436 Win=0 Len=0
13	1.364067	212.24.243.2	172.16.205.161	HTTP	[TCP Previous segment lost] Continuation or non-HTTP traffic
14	1.364119	172.16.205.161	212.24.243.2	TCP	1393 > http [ACK] Seq=382 Ack=0 Win=17040 Len=0
15	1.365754	212.24.243.2	172.16.205.161	TCP	[TCP Retransmission] [TCP segment of a reassembled PDU]
16	1.366213	172.16.205.161	212.24.243.2	TCP	1393 > http [ACK] Seq=382 Ack=2840 Win=14200 Len=0
17	1.366451	172.16.205.161	212.24.243.2	TCP	[TCP Window Update] 1393 > http [ACK] Seq=382 Ack=2840 Win=17040 Len=0
18	1.373631	212.24.243.2	172.16.205.161	HTTP	Continuation or non-HTTP traffic

```
⊞ Frame 1 (489 bytes on wire, 489 bytes captured)
⊞ Ethernet II, Src: IntelCor_2e:46:08 (00:13:ce:2e:46:08), Dst: LannerEl_06:c2:4c (00:90:0b:06:c2:4c)
⊞ Internet Protocol, Src: 172.16.205.161 (172.16.205.161), Dst: 212.24.243.2 (212.24.243.2)
⊞ Transmission Control Protocol, Src Port: 1392 (1392), Dst Port: http (80), Seq: 0, Ack: 0, Len: 435
⊟ Hypertext Transfer Protocol
  ⊟ GET http://www.myspace.com/ HTTP/1.1\r\n
      Request Method: GET
      Request URI: http://www.myspace.com/
      Request Version: HTTP/1.1
    Host: www.myspace.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.1) Gecko/20060111 Firefox/1.5.0.1\r\n
```

```
0030  42 90 1b 25 00 00 47 45  54 20 68 74 74 70 3a 2f   B..%..GE T http:/
0040  2f 77 77 77 2e 6d 79 73  70 61 63 65 2e 63 6f 6d   /www.mys pace.com
0050  2f 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   / HTTP/1 .1..Host
0060  3a 20 77 77 77 2e 6d 79  73 70 61 63 65 2e 63 6f   : www.my space.co
0070  6d 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   m..User- Agent: M
0080  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 57 69 6e 64   ozilla/5 .0 (wind
0090  6f 77 73 3b 20 55 3b 20  57 69 6e 64 6f 77 73 20   ows; U;  Windows
00a0  4e 54 20 35 2e 31 3b 20  65 6e 2d 55 53 3b 20 72   NT 5.1;  en-US; r
00b0  76 3a 31 2e 38 2e 30 2e  31 29 20 47 65 63 6b 6f   v:1.8.0. 1) Gecko
```

Questions

Cybercrime Lab
Computer Crime and
Intellectual Property Section
United States Department of Justice

Phone: 202-514-1026

Web: ww.cybercrime.gov