

SEARCH



2012 San Diego International Conference on Child and Family Maltreatment

Field Search



What is SEARCH?

- Non-profit based in Sacramento, CA
- Funded to offer assistance to law enforcement throughout the country

The screenshot shows the SEARCH website homepage. The header features the SEARCH logo and tagline "The online resource for justice and public safety decision makers". Navigation links include HOME, CAREERS, CONTACT US, ABOUT SEARCH, PRODUCTS & SERVICES, PROGRAMS, PUBLICATIONS, and CALENDAR. A search bar is located in the top right. The main content area includes a 40th anniversary banner, a "Register Today! 2011 Winter Membership Meeting" call to action, a "SEARCH News" section, and a "Quick Links" sidebar with items like CRIMINAL HISTORY RECORDS, HIGH-TECH INVESTIGATIVE GUIDES, IDENTITY THEFT, ISP LIST, JIEM@ TOOL, PODCASTS, PUBLIC SAFETY ISSUE BRIEFS, SEARCH INVESTIGATIVE TOOLBAR, SEX OFFENDER REGISTRIES, and SURVEYS. A central "In the Spotlight" section highlights "SEARCH Offers High-Tech Crime Investigative Resources" with a "LEARN MORE" button. A video player is visible at the bottom of the spotlight section.



What is SEARCH?

www.search.org

- Low-cost (or free) law enforcement training around the U.S.
 - Introduction to Computer Crime
 - Cell Phone Data Recovery
 - Advanced Responders: Search and Seizure of Networks
 - Social Networking Website Investigations
 - Peer-to-Peer



What is SEARCH?

- Free technical assistance to federal, tribal, state and local LE
- Other resources
 - SEARCH ISP List
 - SEARCH Investigative Toolbar
 - Whitepapers
 - LE conference speakers



Who We Are

Chris Armstrong

High-Tech Crime Training Specialist

carmstrong@search.org



Who We Are

Timothy Lott

High-Tech Crime Training Specialist

tim@search.org



Field Search

- Field Search is a suite of software products developed by the National Law Enforcement and Corrections Technology Center (NLECTC).
- Field Search was designed specifically for use in the field by non-technical criminal justice personnel to allow them to quickly and efficiently search a target computer and create a detailed report of findings.
- Originally designed to assist probation and parole officers in sex offender management, the Field Search suite is equally effective in first responder situations or in examining computers for evidence of other crimes.



Field Search

- Keep In Mind that Field Search is **not** a forensically sound tool
 - It will change the USB time and date stamps.
- Field Search was designed for quick preview type search.
- Field Search will quickly find evidence such as Internet histories, images, multimedia files and results from text searches.
- Creating a report of your findings is easy.



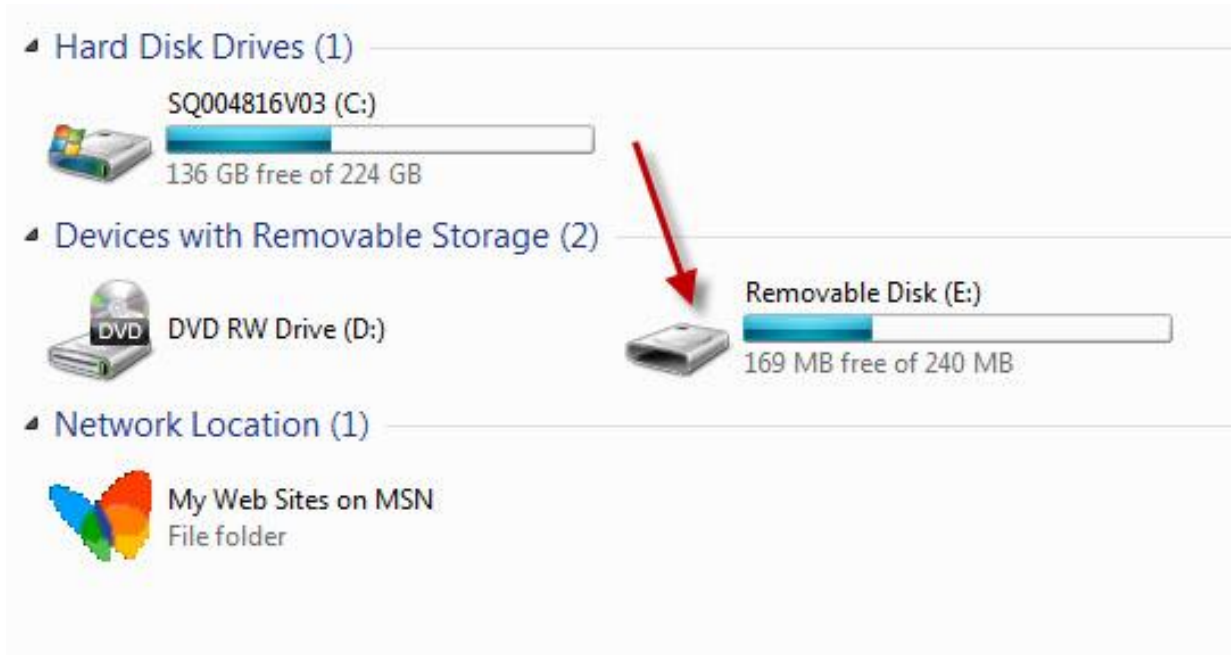
Field Search

- How to Get Your Copy of Field Search
- Current Versions:
 - **FS Win, Version 3.0.35: Released May 2009**
 - **FS Mac: Released September 2008**
- Field Search is available to public sector criminal justice agencies only. There is no charge for the software.
- In order to gain access to the various versions of Field Search, manuals and the training video, please follow this link:
 - <https://fieldsearch.justnet.org/request.asp>



Field Search

- The Windows version of Field Search has been provided to you on a USB flashdrive.
- Insert the flashdrive to access the Field Search software.
- Double left click on the flashdrive to access the files.





Field Search

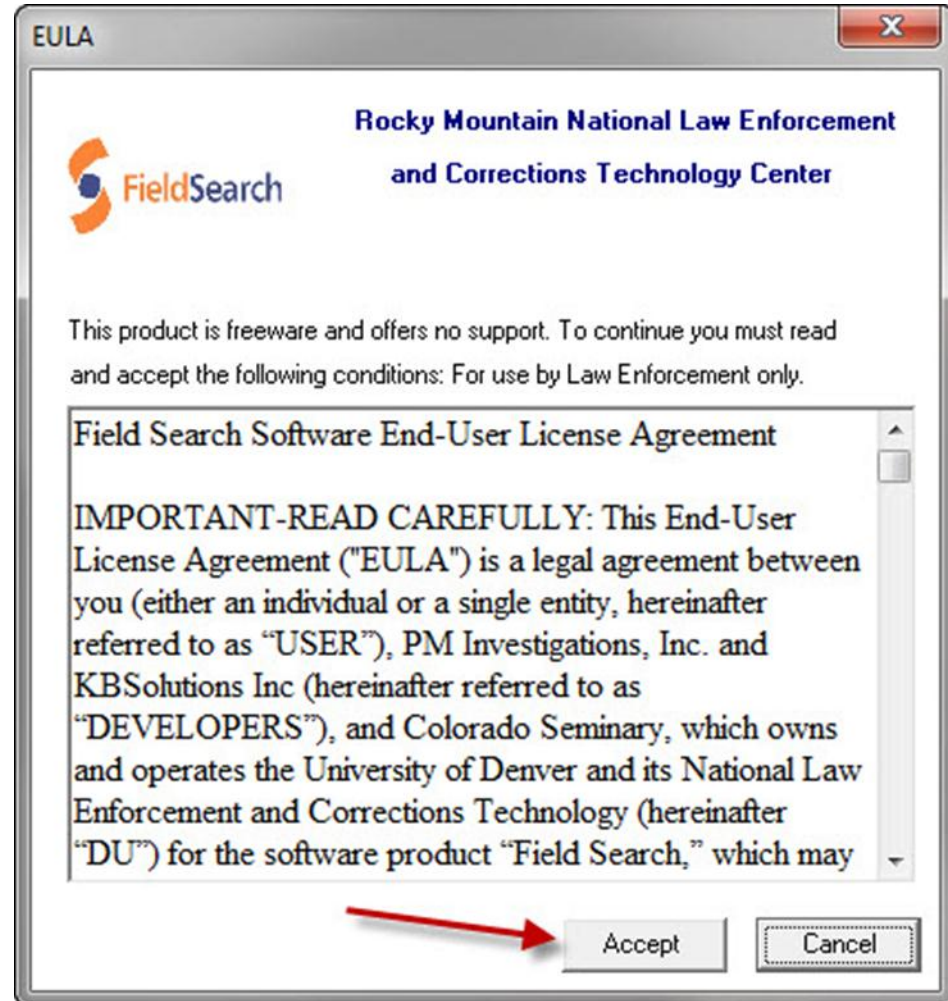
- Field Search executable file.
- Left clicking on the executable file starts Field Search.

Name	Date modified	Type	Size
help	10/28/2009 4:11 PM	File folder	
config	2/25/2011 10:50 AM	XML Document	2 KB
FSWin	4/8/2009 11:47 AM	Application	1,145 KB
FSWin.frx	6/6/2008 3:42 PM	FRX File	170 KB
FSWin	2/25/2011 10:50 AM	Text Document	15 KB
FSWin	6/3/2008 11:31 PM	XML Document	1 KB
FSWin-FAT.frx	5/10/2008 11:14 AM	FRX File	170 KB
keyword	2/25/2011 10:06 AM	XML Document	2 KB
libmcl.dll	5/17/2006 11:05 PM	Application extens...	4,862 KB
paths	10/28/2009 5:16 PM	XML Document	1 KB
sqlite3.dll	3/6/2009 12:03 AM	Application extens...	392 KB



Field Search

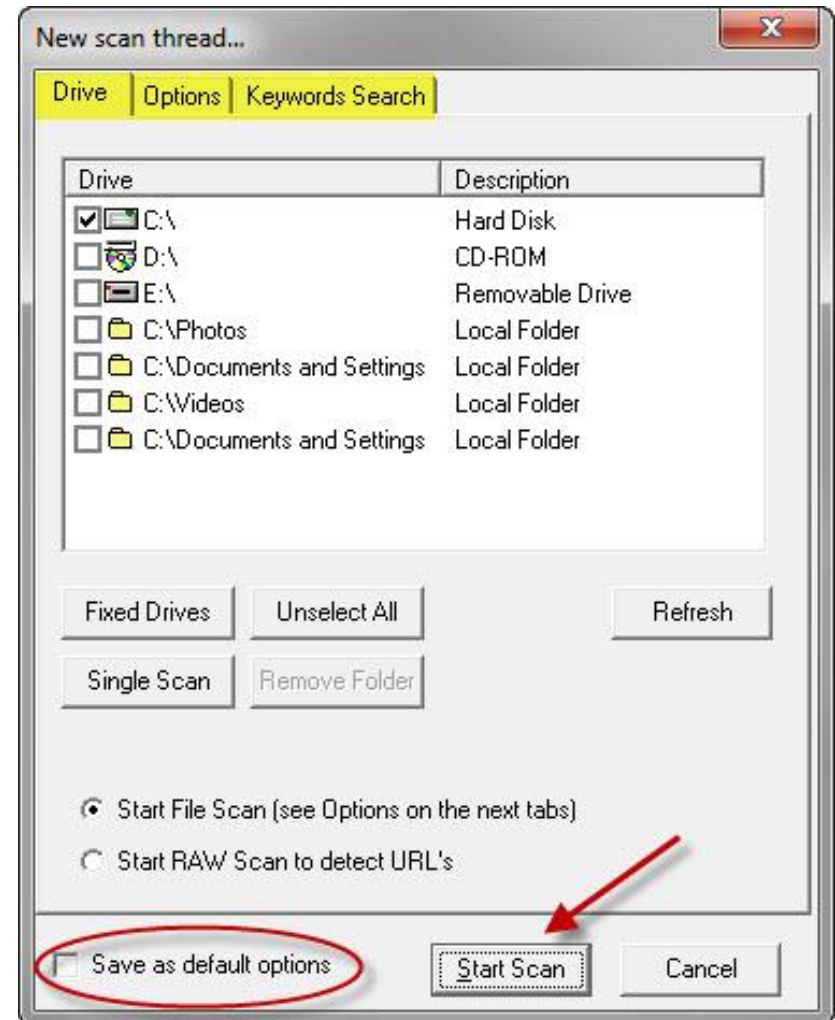
As Field Search starts you will be prompted to Accept their EULA.





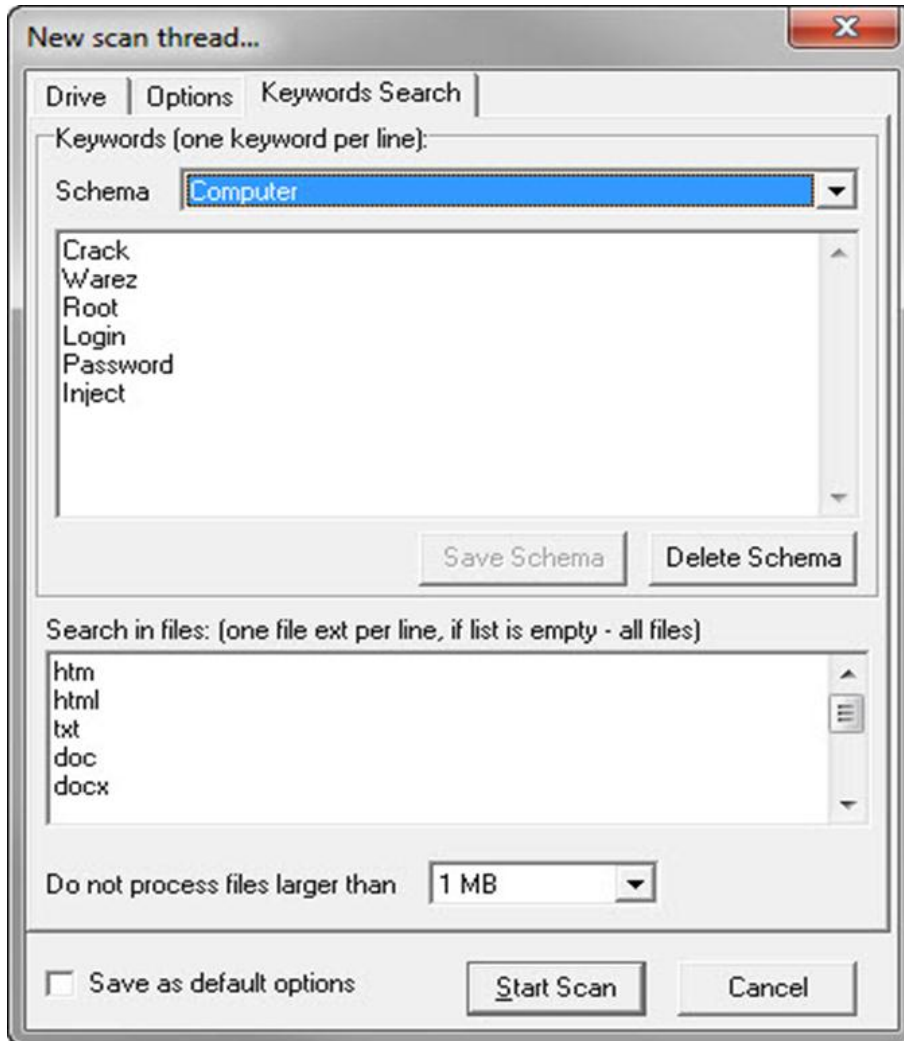
Field Search

- Searching Configuration
 - Drives you wish to search
 - Options
 - Keywords
- Configure the settings then save as the default options.
- Click “Start Scan” to begin.





Field Search



- Keywords
- There are options to create your own keyword list.
- Click on the down arrow to create your own list.



Field Search

Searches

- Field Search does a good job with image and video searches.
- It will also provide you with Browser results, Most Recently Used (MRU) file results and information about what's in the Recycle Bin.



Field Search

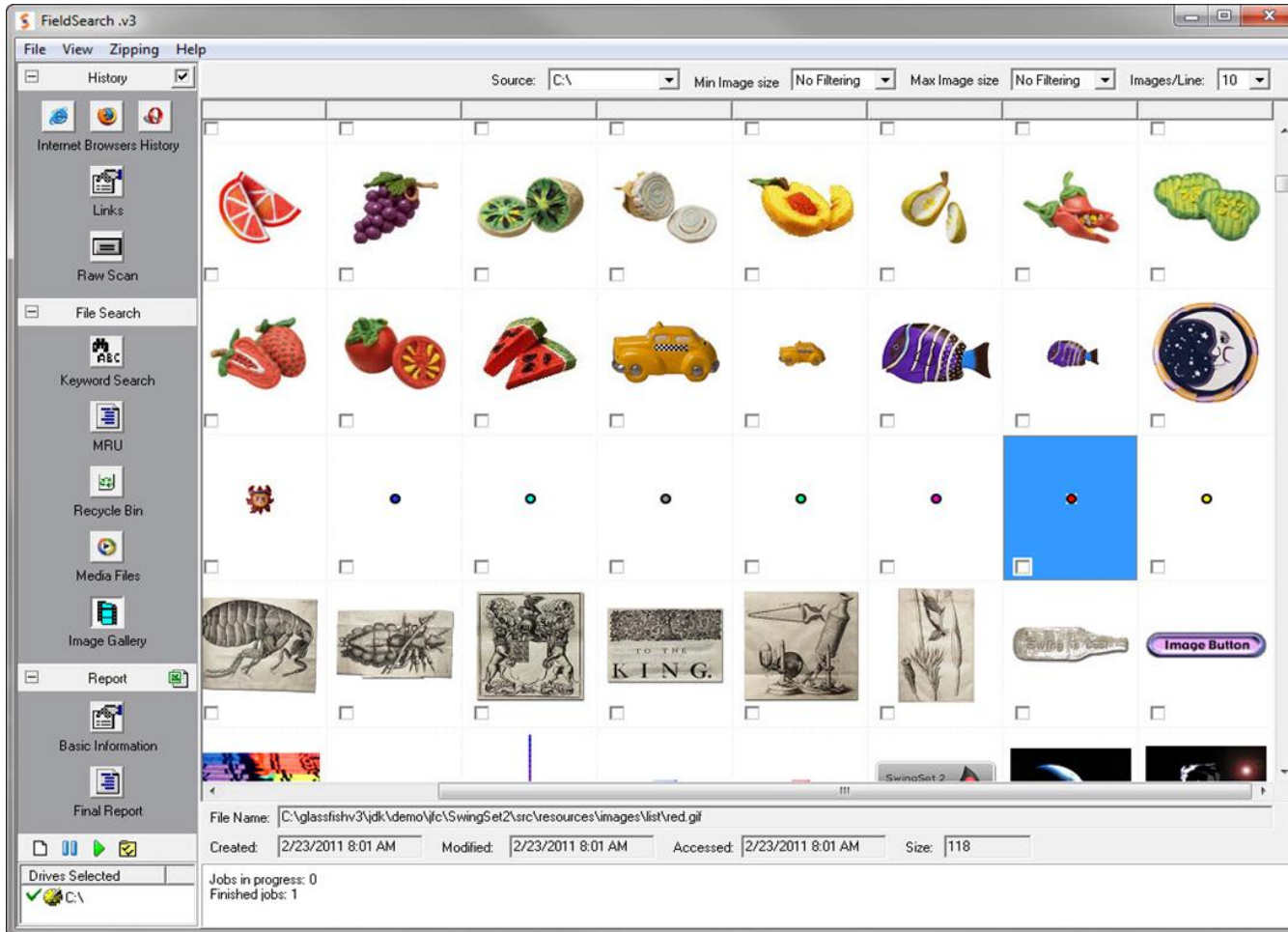


Image Gallery Search Results

Click in the small square next to the image to bookmark the image for the Final Report.



Field Search

Media File Search Results

Click on the arrow to play the media file.

Click in the box to bookmark the file.

The screenshot shows the FieldSearch.v3 application window. The main pane displays a list of search results with columns for File Name, Size, Created, Modified, and Accessed. A red arrow points to the play button in the media player control bar at the bottom of the window. The media player is currently displaying a video of a waterfall.

File Name	Size	Created	Modified	Accessed
C:\Windows\winsxs\x86_microsoft-windows-winsatmediamples_31bf3856ad364e35_6.1.7600.16385_non...	3 MB	7/13/2009 3:23...	6/10/2009 1:48...	7/13/2009 3:23 PM
C:\Windows\winsxs\x86_microsoft-windows-winsatmediamples_31bf3856ad364e35_6.1.7600.16385_non...	4 MB	6/10/2009 1:48...	6/10/2009 1:48...	6/10/2009 1:48 PM
C:\Windows\winsxs\x86_microsoft-windows-winsatmediamples_31bf3856ad364e35_6.1.7600.16385_non...	3 MB	7/13/2009 3:23...	6/10/2009 1:48...	7/13/2009 3:23 PM
C:\Windows\winsxs\x86_microsoft-windows-winsatmediamples_31bf3856ad364e35_6.1.7600.16385_no...	3 MB	7/13/2009 3:23...	6/10/2009 1:48...	7/13/2009 3:23 PM
C:\Windows\winsxs\x86_microsoft-windows-winsatmediamples_31bf3856ad364e35_6.1.7600.16385_no...	9 MB	7/13/2009 3:23...	6/10/2009 1:48...	7/13/2009 3:23 PM
C:\Windows\winsxs\x86_microsoft-windows-winsatmediamples_31bf3856ad364e35_6.1.7600.16385_no...	8 MB	7/13/2009 3:23...	6/10/2009 1:48...	7/13/2009 3:23 PM
C:\Windows\winsxs\x86_microsoft-windows-videosamples_31bf3856ad364e35_6.1.7600.16385_none_f583...	25 MB	6/10/2009 1:41...	6/10/2009 1:41...	6/10/2009 1:41 PM
C:\Windows\winsxs\x86_microsoft-windows-tabletpc-inputpanel_31bf3856ad364e35_6.1.7600.16385_none...	189 KB	7/13/2009 12:4...	6/10/2009 1:28...	7/13/2009 12:49 PM
C:\Windows\winsxs\x86_microsoft-windows-tabletpc-inputpanel_31bf3856ad364e35_6.1.7600.16385_non...	217 KB	7/13/2009 12:4...	6/10/2009 1:28...	7/13/2009 12:49 PM
C:\Windows\winsxs\x86_microsoft-windows-tabletpc-inputpanel_31bf3856ad364e35_6.1.7600.16385_non...	219 KB	7/13/2009 12:4...	6/10/2009 1:28...	7/13/2009 12:49 PM
C:\Windows\winsxs\x86_microsoft-windows-tabletpc-inputpanel_31bf3856ad364e35_6.1.7600.16385_non...	192 KB	7/13/2009 12:4...	6/10/2009 1:28...	7/13/2009 12:49 PM
C:\Windows\winsxs\x86_microsoft-windows-tabletpc-inputpanel_31bf3856ad364e35_6.1.7600.16385_non...	61 KB	7/13/2009 12:4...	6/10/2009 1:28...	7/13/2009 12:49 PM
C:\Windows\winsxs\x86_microsoft-windows-tabletpc-inputpanel_31bf3856ad364e35_6.1.7600.16385_non...	32 KB	7/13/2009 12:4...	6/10/2009 1:28...	7/13/2009 12:49 PM
C:\Windows\winsxs\x86_microsoft-windows-tabletpc-inputpanel_31bf3856ad364e35_6.1.7600.16385_non...	31 KB	7/13/2009 12:4...	6/10/2009 1:28...	7/13/2009 12:49 PM
C:\Windows\winsxs\x86_microsoft-windows-tabletpc-inputpanel_31bf3856ad364e35_6.1.7600.16385_non...	87 KB	6/10/2009 1:28...	6/10/2009 1:28...	6/10/2009 1:28 PM
C:\Windows\winsxs\x86_microsoft-windows-t.flicklearningwizard_31bf3856ad364e35_6.1.7600.16385_non...	1 MB	6/10/2009 1:47...	6/10/2009 1:47...	6/10/2009 1:47 PM
C:\Windows\winsxs\x86_microsoft-windows-o.tyle-resizingpanels_31bf3856ad364e35_6.1.7600.16385_non...	529 KB	7/13/2009 1:03...	6/10/2009 1:45...	7/13/2009 1:03 PM
C:\Windows\winsxs\x86_microsoft-windows-o.tyle-resizingpanels_31bf3856ad364e35_6.1.7600.16385_non...	531 KB	7/13/2009 1:03...	6/10/2009 1:45...	7/13/2009 1:03 PM
C:\Windows\winsxs\x86_microsoft-windows-o.iadisc-style-travel_31bf3856ad364e35_6.1.7600.16385_non...	223 KB	7/13/2009 1:03...	6/10/2009 1:45...	7/13/2009 1:03 PM
C:\Windows\winsxs\x86_microsoft-windows-o.iadisc-style-travel_31bf3856ad364e35_6.1.7600.16385...	55 KB	7/13/2009 1:03...	6/10/2009 1:45...	7/13/2009 1:03 PM



Field Search

IE Internet History

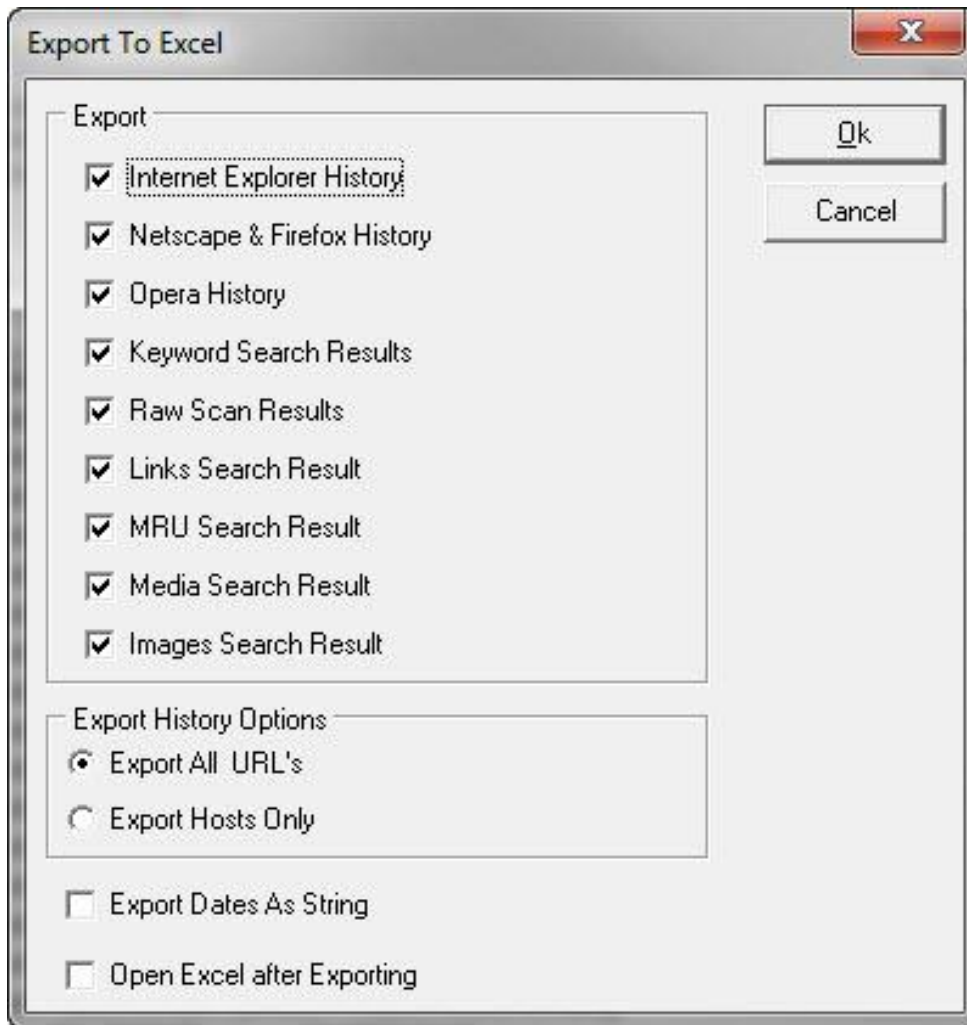
Found 17 history files

Internet Explorer, version: 8.0.7600.16385

History File Name - Site - Pages ▲	Created	Modified	Accessed
C:\Users\Chris\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat	8/19/2010 7:31...	2/24/2011 11:0...	8/19/2010 7:31 AM
C:\Users\Chris\AppData\Local\Microsoft\Feeds Cache\index.dat	8/6/2010 11:34...	2/24/2011 11:0...	8/6/2010 11:34 AM
C:\Users\Chris\AppData\Local\Microsoft\Internet Explorer\DOMStore\index.dat	2/4/2011 12:42...	2/4/2011 12:42...	2/4/2011 12:42 PM
C:\Users\Chris\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012011013120110207\index.dat	2/8/2011 7:35 ...	2/8/2011 7:35 ...	2/8/2011 7:35 AM
C:\Users\Chris\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012011020720110214\index.dat	2/15/2011 10:3...	2/15/2011 10:3...	2/15/2011 10:35 AM
C:\Users\Chris\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012011021420110221\index.dat	2/22/2011 8:57...	2/22/2011 8:57...	2/22/2011 8:57 AM
C:\Users\Chris\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012011022220110223\index.dat	2/22/2011 8:57...	2/22/2011 4:44...	2/22/2011 8:57 AM
C:\Users\Chris\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012011022320110224\index.dat	2/23/2011 7:32...	2/23/2011 7:57...	2/23/2011 7:32 AM
C:\Users\Chris\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012011022420110225\index.dat	2/24/2011 8:01...	2/24/2011 8:00...	2/24/2011 8:01 AM
C:\Users\Chris\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012011022520110226\index.dat	2/25/2011 8:09...	2/25/2011 9:36...	2/25/2011 8:09 AM
C:\Users\Chris\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat	8/6/2010 11:34...	2/25/2011 9:35...	8/6/2010 11:34 AM
C:\Users\Chris\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012010081920100820\index.dat	8/19/2010 7:31...	8/19/2010 7:31...	8/19/2010 7:31 AM
C:\Users\Chris\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat	8/19/2010 7:31...	2/24/2011 11:0...	8/19/2010 7:31 AM
C:\Users\Chris\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat	8/6/2010 11:34...	2/25/2011 9:35...	8/6/2010 11:34 AM
C:\Users\Chris\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\index.dat	8/19/2010 7:31...	2/24/2011 11:0...	8/19/2010 7:31 AM
C:\Users\Chris\AppData\Local\Temp\Temporary Internet Files\Content.IE5\index.dat	8/31/2010 9:18...	2/13/2011 9:34...	8/31/2010 9:18 AM
C:\Users\Chris\AppData\Roaming\Microsoft\Windows\Cookies\index.dat	8/6/2010 11:34...	2/25/2011 9:35...	8/6/2010 11:34 AM



Field Search



Field Search gives you the ability to export your search results to Excel.



Field Search

- The Field Search Final Report is a collection of items bookmarked by the Investigator.
- The Final Report is generated automatically by Field Search when you click on the Final Report Link button.





Field Search

Field Search

Final Report

Computer User's Name: Chris
 Examiner's Name: Chris Armstrong
 Computer: Toshiba Tecra -
 Location: 7311 Greenhaven Dr. # 145
 Sacramento, CA 95831
 Comments:

ProductId:
 Owner: Microsoft, Organization: Microsoft
 Operating System: Windows 7 Professional 6.1.7600
 Windows Installed Date: 1/1/1970 12:00 AM
 Time Zone (Standard Time Setting): @tzres.dll,-212

Found Images

	File Name	Created	Accessed
#1	C:\Program Files (x86)\Shareaza\Data\Splash.png	10/6/2010 6:46 AM	10/7/2010 6:51 AM
#2	C:\Program Files (x86)\Shareaza\Data\Splash2.png	10/6/2010 6:46 AM	10/7/2010 6:51 AM
#3	C:\Program Files (x86)\Shareaza\Skins\BlueStreak\BlueStreak.bmp	10/6/2010 6:46 AM	10/7/2010 6:51 AM
#4	C:\Program Files (x86)\Shareaza\Skins\ShareazaOS\sos_main.bmp	10/6/2010 6:46 AM	10/7/2010 6:51 AM
#5	C:\Program Files (x86)\Shareaza\Skins\ShareazaOS\sos_main_2.bmp	10/6/2010 6:46 AM	10/7/2010 6:51 AM
#6	C:\Program Files (x86)\Shareaza\Skins\ShareazaOS\sos_main_old.bmp	10/6/2010 6:46 AM	10/7/2010 6:51 AM
#7	C:\Program Files (x86)\Yahoo!\Messenger\Media\FriendIcon\balloon.png	1/4/2010 8:53 AM	1/4/2010 8:53 AM
#8	C:\Program Files (x86)\Yahoo!\Messenger\Media\FriendIcon\dog.png	1/4/2010 8:53 AM	1/4/2010 8:53 AM
#9	C:\Program Files (x86)\Yahoo!\Messenger\Media\FriendIcon\golf.png	1/4/2010 8:53 AM	1/4/2010 8:53 AM
#10	C:\Program Files (x86)\Yahoo!\Messenger\Media\FriendIcon\snowman.png	1/4/2010 8:53 AM	1/4/2010 8:53 AM
#11	C:\Program Files (x86)\Yahoo!\Messenger\Media\FriendIcon\soccer.png	1/4/2010 8:53 AM	1/4/2010 8:53 AM
#12	C:\Program Files (x86)\Yahoo!\Messenger\Profiles\ca8920\My Icons\ypt38A8.png	1/4/2010 8:56 AM	1/4/2010 8:56 AM

Thumbnails



Media Files

	File Name	Created	Accessed
#1	C:\Windows\winsxs\amd64_microsoft-windows-videosamples_31bf3856ad364e35_6.1.7600.1	6/10/2009 1:01 PM	6/10/2009 1:01 PM
#2	C:\Windows\winsxs\amd64_microsoft-windows-tabletpc-inputpanel_31bf3856ad364e35_6.1.7	7/13/2009 12:39 PM	7/13/2009 12:39 PM
#3	C:\Windows\winsxs\amd64_microsoft-windows-tabletpc-inputpanel_31bf3856ad364e35_6.1.7	7/13/2009 12:39 PM	7/13/2009 12:39 PM
#4	C:\Windows\winsxs\amd64_microsoft-windows-tabletpc-inputpanel_31bf3856ad364e35_6.1.7	7/13/2009 12:39 PM	7/13/2009 12:39 PM
#5	C:\Windows\winsxs\amd64_microsoft-windows-tabletpc-inputpanel_31bf3856ad364e35_6.1.7	6/10/2009 12:47 PM	6/10/2009 12:47 PM



Field Search

- To save your report click on the disk icon to the upper left of the report. The report saves in an .rtf format which can be opened with any text editor.
- To print your report click on the printer icon.

A screenshot of a web browser window displaying a 'Computer Exam Report'. The browser's address bar shows 'Report: FSWin'. The report content includes:

Computer Exam Report

Page 1 of 1
Created Monday, February 28, 2011 at 2:05 PM
Computer: WIN-4PP1AH1B2E1 - User: Chris

ProductId:
Owner: Microsoft, Organization: Microsoft
Operating System: Windows 7 Professional 6.1 7600
Windows Installed Date: 1/1/1970 12:00 AM
Time Zone (Standard Time Setting): @tzres.dll,-212

Computer User's Name: Chris
Examiner's Name: Chris Armstrong
Computer: Toshiba Tecra -
Location: 7311 Greenhaven Dr. # 145
Sacramento, CA 95831
Comments:

A red arrow points to the save icon (a floppy disk) in the browser's toolbar.



Questions ?