NLECTC NIJ
Criminal Justice
Electronic Crime Technology
Center of Excellence

Internet Evidence Finder

Version 5.6.0

EVALUATION REPORT

November 2012

NLECTC NIJ
Criminal Justice
Electronic Crime Technology
Center of Excellence

NIJ Electronic Crime Technology Center of Excellence
550 Marshall St., Suite B
Phillipsburg, NJ 08865
www.ECTCoE.org

NIJ ECTCOE TESTING AND EVALUATION PROJECT STAFF

Robert J. O'Leary, CFCE; DFCP
Russell Yawn, CFCE
Chester Hosmer
Mark Davis, Ph.D.
Michael Terminelli, ACE
Randy Becker, CFCE
Jacob Fonseca
Victor Fay-Wolfe, Ph.D.
Kristen McCooey, CCE; ACE
Laurie Ann O'Leary

Table of Contents

This report is current at the time of writing. Please be sure to check the vendor website for the latest version and updates. All software and trademarks are property of their respective companies and owners.

Introduction

The National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTCoE) has been assigned the responsibility of conducting electronic crime and digital evidence tool, technology and training testing and evaluations in support of the NIJ Research, Development, Testing and Evaluation (RDT&E) process.

The NIJ RDT&E process helps ensure that NIJ's research portfolios are aligned to best address the technology needs of the criminal justice community. The rigorous process has five phases:

- **Phase I: Determine technology needs principally in partnership with the Law Enforcement and Corrections Technology Advisory Council (LECTAC) and the appropriate Technology Working Group (TWG).** NIJ identifies criminal justice practitioners' functional requirements for new tools and technologies. (For more information on LECTAC and the TWGs, visit http://www.justnet.org.)
- **Phase II: Develop technology program plans to address those needs.** NIJ creates a multiyear research program to address the needs identified in Phase I. One of the first steps is to determine whether products that meet those needs currently exist or whether they must be developed. If a solution is already available, Phases II and III are not necessary, and NIJ moves directly to demonstration, testing and evaluation in Phase IV. If solutions do not currently exist, they are solicited through annual, competitively awarded science and technology solicitations and TWG members help review the applications.
- **Phase III: Develop solutions**. Appropriate solicitations are developed and grantees are selected through an open, competitive, peer-reviewed process. After grants are awarded, the grantee and the NIJ program manager then work collaboratively to develop the solutions.
- **Phase IV: Demonstrate, test, evaluate and adopt potential solutions into practice.** A potential solution is tested to determine how well it addresses the intended functional requirement. NIJ then works with first-adopting agencies to facilitate the introduction of the solution into practice. After adoption, the solution's impact on practice is evaluated. During the testing and evaluation process, performance standards and guides are developed (as appropriate) to ensure safety and effectiveness; not all new solutions will require the publication of new standards or guides.
- **Phase V: Build capacity and conduct outreach to ensure that the new tool or technology benefits practitioners.** NIJ publishes guides and standards and provides technology assistance to second adopters.[1]

The High Priority Criminal Justice Technology Needs are organized into five functional areas:

- Protecting the Public.
- Ensuring Officer Safety.
- Confirming the Guilty and Protecting the Innocent.
- Improving the Efficiency of Justice.
- Enabling Informed Decision-Making.

The NIJ ECTCoE tool, technology and training evaluation and testing reports support the NIJ RDT&E process, which addresses high priority needs for criminal justice technology.

[1] *National Institute of Justice High-Priority Criminal Justice Technology Needs,* March 2009 NCJ 225375.

Overview

Product Information

Internet Evidence Finder (IEF) from Magnet Forensics is a forensics grade software application that is designed for investigators to easily discover Internet artifacts.

From the products brochure:

> Internet Evidence Finder (IEF) is a digital forensics solution that can search a hard drive, live RAM captures or files for Internet-related evidence. IEF was designed with digital forensics examiners/investigators in mind. IEF is also used by IT security professionals, litigation support personnel, incident response teams, cyber security specialists and corporate investigators.
>
> IEF can recover evidence left behind within social networking artifacts, instant messaging chat histories, popular webmail applications, Web-browsing history and peer-to-peer file sharing applications.

Product Description

IEF comes in two different versions, a standard and a triage version. From the product brochure:

> IEF Standard Edition:
>
> IEF software comes on a USB dongle and can be installed on as many computers as necessary. The dongle holds the license key. Simply plug the USB dongle into the computer on which you're running IEF and install the software. This dongle approach allows the flexibility to use IEF on different workstations, but it can only run on a single computer at a time.
>
> IEF Triage Edition:
>
> The Triage Edition offers all the functionality of the Standard Edition. In addition, with Triage you get the following:
>
> - Automated check for disk encryption.
> - Built-in live RAM capture.
> - Built-in drive imaging.
> - Mount and search volume shadow copies.
> - Ability to save all results on the dongle.

Special Features

The following special features of IEF are taken from the product's website:

- IEF recovers more types of Internet-related data.
  - ❏ Social networking artifacts.
  - ❏ Instant messenger chat history.
  - ❏ Webmail.
  - ❏ Full Web-browser artifacts.
  - ❏ P2P file-sharing applications.
  - ❏ Cloud-based applications.
- IEF searches in more places.
  - ❏ Entire logical or physical drives: .E01/dd images.
  - ❏ Carves in unallocated space/deleted space.
  - ❏ Selected files (pagefile.sys/hiberfil.sys files, and more).

  - Live RAM captures and network PCAP files.
  - Entire user-selected folders and subfolders.
- IEF finds more relevant and accurate data.
  - Patent-pending data recovery process.
  - Single search for more than 60 artifacts.
  - Customize your search by artifact(s) and locations to search.
  - Ability to search multiple drives, images, files and folders in a single search.
- IEF offers rich and comprehensive reporting.
  - Import keyword lists to search, including preset lists.
  - Search, filter, sort and export results.
  - Search and filter data with multiple keywords simultaneously.
  - Search alert capabilities for keyword matches.
  - View search results in real-time, including estimated time to completion.
  - All artifact locations map to a physical sector or file offset.

IEF will recover artifacts generated by the following sources:

- Cloud artifacts.
  - Dropbox.
  - SkyDrive.
  - Google Docs.
  - Google Drive.
  - Flickr.
- Social networking.
  - Facebook.
  - Twitter.
  - Bebo.
  - Myspace.
  - Google Plus.
  - LinkedIn.
- Instant messenger chats.
  - GoogleTalk.
  - Yahoo.
  - MSN/Windows Live Messenger.
  - Messenger Plus.
  - AOL Instant Messenger (AIM).
  - mIRC.
  - Skype.
  - ICQ.
  - World of Warcraft.
  - Second Life.
  - Trillian.
- Webmail applications.
  - Gmail.
  - Yahoo webmail.
  - Hotmail webmail.
- P2P file sharing applications.
  - Limewire.
  - FROSTWIRE.props files.
  - GigaTribe.
  - Ares P2P.
  - Shareaza.
  - eMule.
  - Torrent.

- Web browsers.
  - Internet Explorer.
  - Firefox.
  - Google Chrome.
  - Apple Safari.
  - Opera.

The newest version of IEF will also reconstruct Web pages from local cached images and process iOS backup files for evidence.

Evaluation and Testing of Internet Evidence Finder

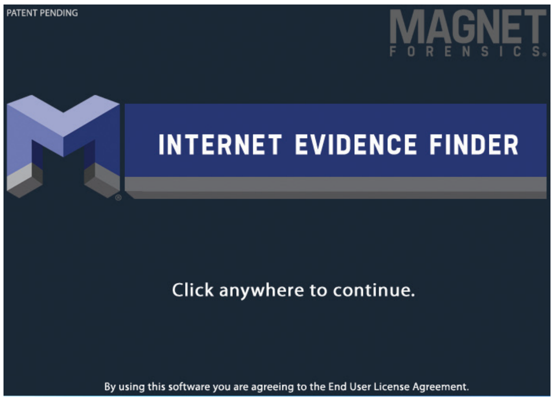
A download link for the IEF setup file was provided by Magnet Forensics to the ECTCoE. A key file was emailed that was copied to an external USB dongle. The setup executable was executed on several examination machines with the default settings.

In preparation for evaluating IEF, the user manual included with the product download was reviewed. The user manual is extremely detailed, providing general usage tips and a comprehensive list of artifacts that IEF can discover with a detailed explanation of IEF's recovery capabilities for each artifact. IEF was not tested against every artifact, but a sampling is included in this report.

IEF was tested on several different systems and drives. Regardless of the target, IEF was always successful in finding artifacts. To demonstrate the standard operation of IEF, it was installed in a Windows 7 VMware session. This VMware session has been used minimally for testing software and capturing screenshots. The following steps are a walkthrough of usage of IEF:

1. Google Chrome was used to download the latest version of IEF. It was installed with default settings. The USB token containing the license key was inserted in a USB slot of the host computer and told to connect to the VMware session. The IEF icon that was placed on the desktop was double-clicked to launch IEF.

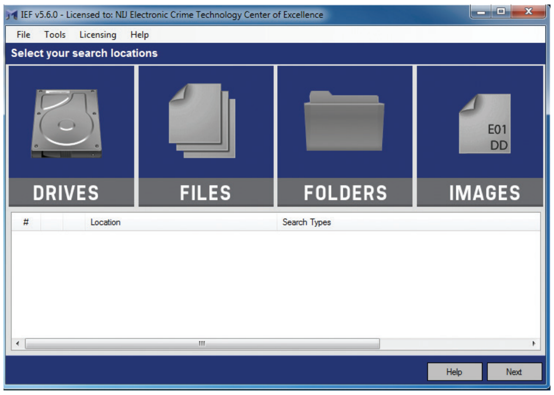
2. The splash screen for IEF was displayed. The window was left-clicked.



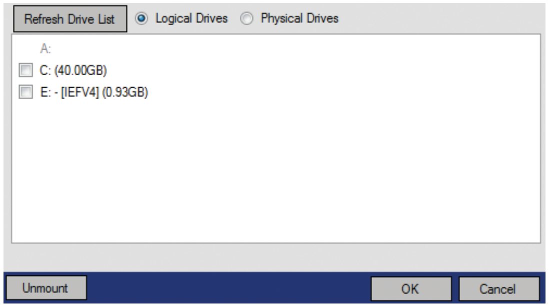
Click anywhere to continue.

By using this software you are agreeing to the End User License Agreement.

3. The following screen was displayed. This screen allows the user to direct IEF to search a drive, certain files, folders or forensics Images. E01 (Encase Format) and dd (raw bitstream images) are both supported.


IEF v5.6.0 - Licensed to: NIJ Electronic Crime Technology Center of Excellence
File
Tools
Licensing
Help
Select your search locations
E01
DD
DRIVES
FILES
FOLDERS
IMAGES
#
Location
Search Types
Help
Next

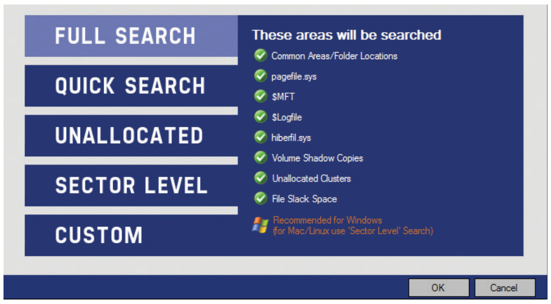
4. For this demonstration, “Drives” was selected and the following screen was displayed. The “C:” drive was selected, and “Logical Drive” was left selected. If the investigation would require searching lost partitions or full drives for deleted or other information, “Physical” should be selected.



● Logical Drives ○ Physical Drives

A:
□ C: (40.00GB)
□ E: - [IEFV4] (0.93GB)

5. Once OK was pressed, the following screen was displayed asking what type of search should be performed on the drive.



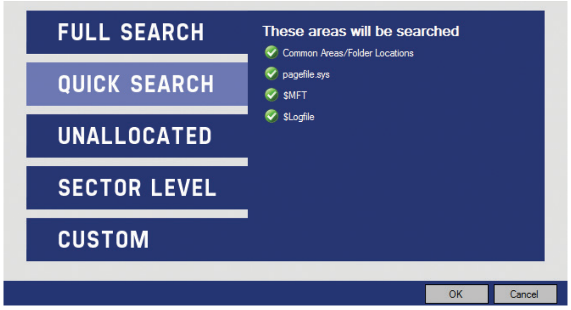
These areas will be searched
- ✓ Common Areas/Folder Locations
- ✓ pagefile.sys
- ✓ $MFT
- ✓ $Logfile
- ✓ hiberfil.sys
- ✓ Volume Shadow Copies
- ✓ Unallocated Clusters
- ✓ File Slack Space

Recommended for Windows
(for Mac/Linux use 'Sector Level' Search)

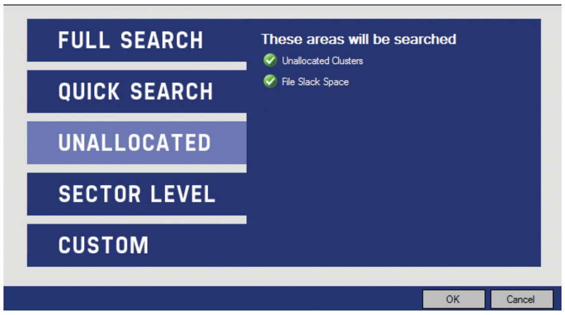
From the IEF User Guide:

> After choosing a drive/folder/file/image to search, you are shown a list of areas to search and “presets” are available. You can either customize which areas (or files/folders) you’d like to search, or use a preset to select predefined areas.
>
> For a comprehensive search, the Full Search is recommended as it will search all relevant areas of a drive for artifacts, and process fragmented files more effectively. To search non-NTFS/FAT drives (i.e. Mac and Linux), use the Sector Level search.

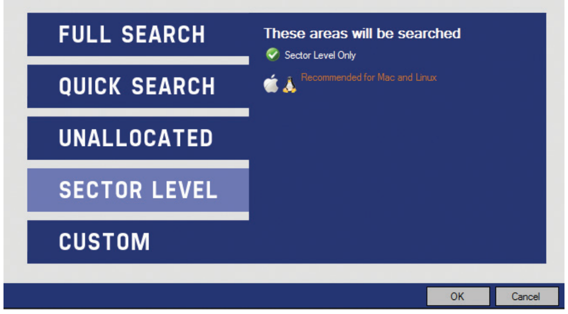
The following screenshots show the remaining preset options available for searching. For this demonstration “Quick Search” was selected.



These areas will be searched
- ✓ Common Areas/Folder Locations
- ✓ pagefile.sys
- ✓ $MFT
- ✓ $Logfile

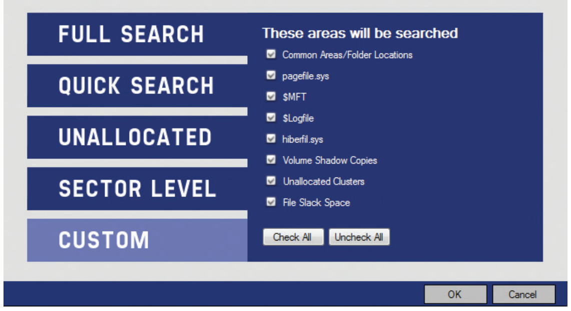


These areas will be searched
- ✓ Unallocated Clusters
- ✓ File Slack Space



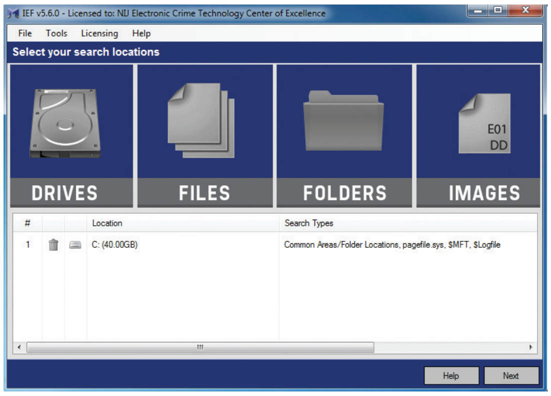
These areas will be searched
- ✓ Sector Level Only

Recommended for Mac and Linux



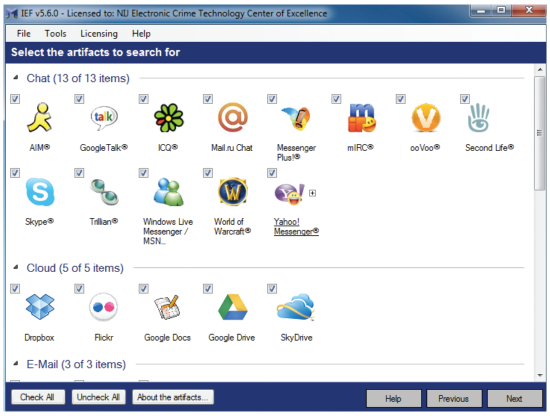
These areas will be searched
- ☑ Common Areas/Folder Locations
- ☑ pagefile.sys
- ☑ $MFT
- ☑ $Logfile
- ☑ hiberfil.sys
- ☑ Volume Shadow Copies
- ☑ Unallocated Clusters
- ☑ File Slack Space

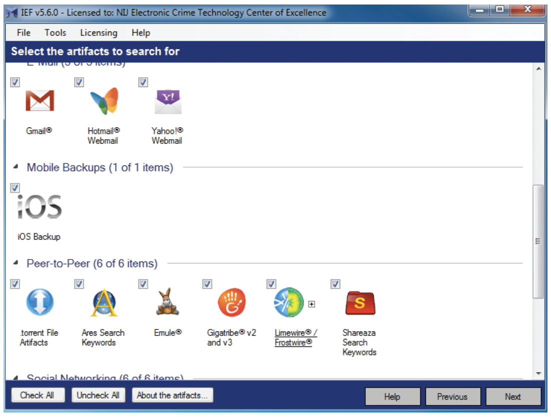
6. Once “Ok” was pressed the main screen was displayed again with the selected drive.

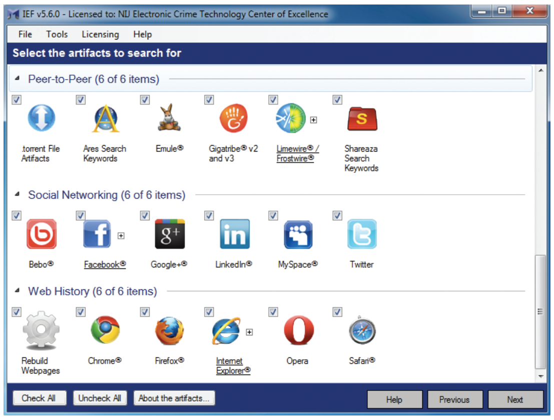

IEF v5.6.0 - Licensed to: NIJ Electronic Crime Technology Center of Excellence
File Tools Licensing Help
Select your search locations
DRIVES
FILES
FOLDERS
E01
DD
IMAGES
Help
Next

#			Location	Search Types
1			C: (40.00GB)	Common Areas/Folder Locations, pagefile.sys, $MFT, $Logfile

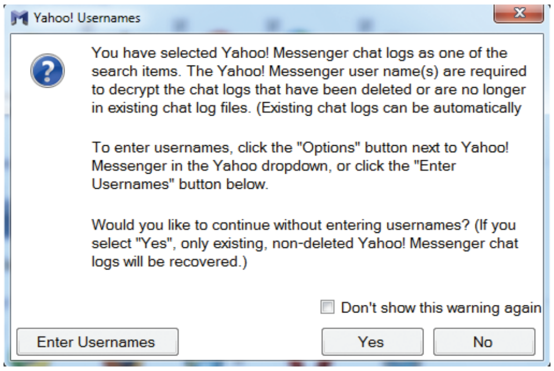
7. Once next was clicked, the following screen was displayed. Note: This screen is in multiple screenshots since it required scrolling to see all of the options. From this screen, the artifacts to search for can be selected. All of the options were left checked, and next was clicked.




IEF v5.6.0 - Licensed to: NIJ Electronic Crime Technology Center of Excellence
File Tools Licensing Help
Select the artifacts to search for
E-Mail (3 of 3 items)
☑ Gmail®
☑ Hotmail® Webmail
☑ Yahoo!® Webmail
Mobile Backups (1 of 1 items)
☑ iOS Backup
Peer-to-Peer (6 of 6 items)
☑ torrent File Artifacts
☑ Ares Search Keywords
☑ Emule®
☑ Gigatribe® v2 and v3
☑ Limewire® / Frostwire®
☑ Shareaza Search Keywords
Social Networking (6 of 6 items)
Check All
Uncheck All
About the artifacts...
Help
Previous
Next



8. The following screen about Yahoo Messenger decryption was displayed. In order to properly display Yahoo Messenger chat logs, the Yahoo username is required. “Yes” was selected to continue without entering usernames.

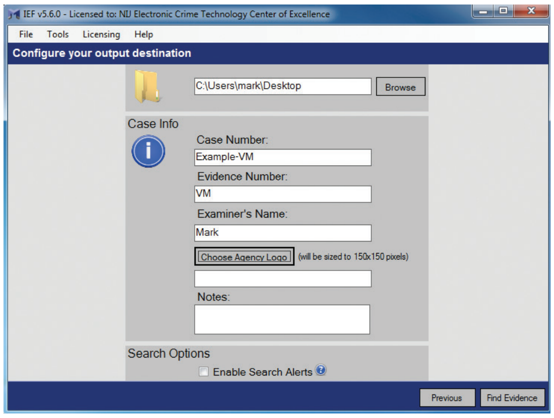


You have selected Yahoo! Messenger chat logs as one of the search items. The Yahoo! Messenger user name(s) are required to decrypt the chat logs that have been deleted or are no longer in existing chat log files. (Existing chat logs can be automatically

To enter usernames, click the "Options" button next to Yahoo! Messenger in the Yahoo dropdown, or click the "Enter Usernames" button below.

Would you like to continue without entering usernames? (If you select "Yes", only existing, non-deleted Yahoo! Messenger chat logs will be recovered.)

9. The following screen was displayed to enter information about the case. There is also an option to enter “Search Alerts,” which can email the investigator if IEF encounters those items during processing. It was completed as follows.


IEF v5.6.0 - Licensed to: NIJ Electronic Crime Technology Center of Excellence
File Tools Licensing Help
Configure your output destination
Browse
Choose Agency Logo
Previous
Find Evidence

C:\Users\mark\Desktop

Case Info

Case Number: Example-VM

Evidence Number: VM

Examiner's Name: Mark

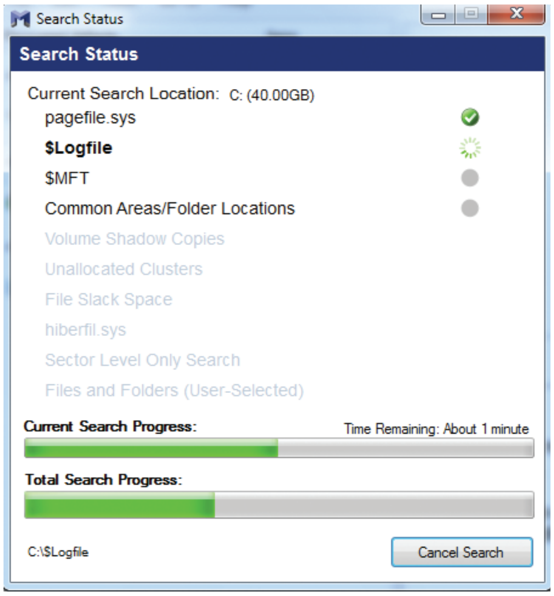
(will be sized to 150x150 pixels)

Notes:

Search Options

□ Enable Search Alerts

10. A status window was displayed indicating the items being processed and the approximate time remaining.



Current Search Location: C: (40.00GB)

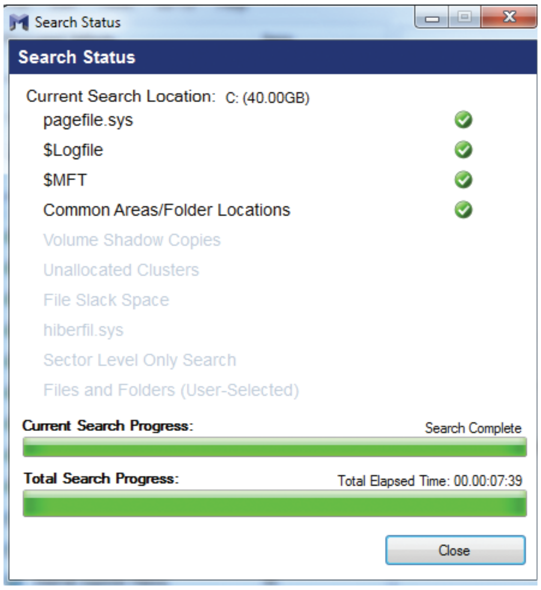
pagefile.sys	✓
$Logfile	
$MFT	●
Common Areas/Folder Locations	●
Volume Shadow Copies	
Unallocated Clusters	
File Slack Space	
hiberfil.sys	
Sector Level Only Search	
Files and Folders (User-Selected)	

Current Search Progress: Time Remaining: About 1 minute

Total Search Progress:

C:\$Logfile

11. Once the processing was completed, the progress window could be closed.



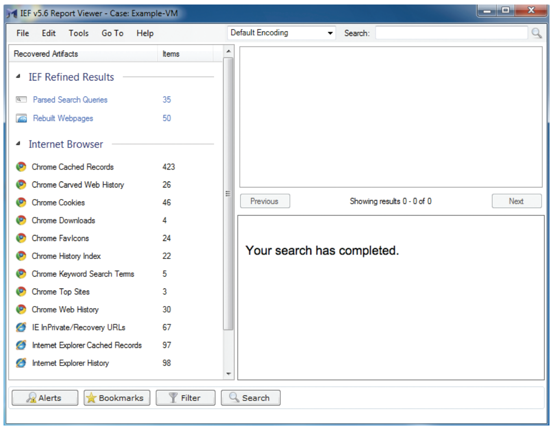
Current Search Location: C: (40.00GB)

pagefile.sys	✓
$Logfile	✓
$MFT	✓
Common Areas/Folder Locations	✓
Volume Shadow Copies	
Unallocated Clusters	
File Slack Space	
hiberfil.sys	
Sector Level Only Search	
Files and Folders (User-Selected)	

Current Search Progress: Search Complete

Total Search Progress: Total Elapsed Time: 00:00:07:39

12. Once closed, the IEF report viewer window was displayed. This window included a summary of all of the artifacts found on the left side.

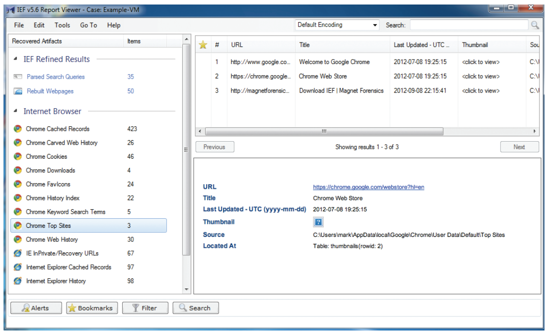


Recovered Artifacts	Items
IEF Refined Results	
Parsed Search Queries	35
Rebuilt Webpages	50
Internet Browser	
Chrome Cached Records	423
Chrome Carved Web History	26
Chrome Cookies	46
Chrome Downloads	4
Chrome FavIcons	24
Chrome History Index	22
Chrome Keyword Search Terms	5
Chrome Top Sites	3
Chrome Web History	30
IE InPrivate/Recovery URLs	67
Internet Explorer Cached Records	97
Internet Explorer History	98

Showing results 0 - 0 of 0

Your search has completed.

13. Selecting an artifact name in the left pane populates the two right panes: the top one with a summary of the data found, and the bottom pane with details of the line items. All panes are adjustable if additional viewing space is required. In the screenshot, "Chrome Top Sites" was selected.



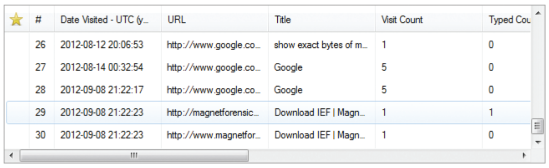
Recovered Artifacts	Items
IEF Refined Results	
Parsed Search Queries	35
Rebuilt Webpages	50
Internet Browser	
Chrome Cached Records	423
Chrome Carved Web History	26
Chrome Cookies	46
Chrome Downloads	4
Chrome FavIcons	24
Chrome History Index	22
Chrome Keyword Search Terms	5
Chrome Top Sites	3
Chrome Web History	30
IE InPrivate/Recovery URLs	67
Internet Explorer Cached Records	97
Internet Explorer History	98

★	#	URL	Title	Last Updated - UTC ...	Thumbnail	Sou
	1	http://www.google.co...	Welcome to Google Chrome	2012-07-08 19:25:15	<click to view>	C:\
	2	https://chrome.google...	Chrome Web Store	2012-07-08 19:25:15	<click to view>	C:\
	3	http://magnetforensic...	Download IEF | Magnet Forensics	2012-09-08 22:15:41	<click to view>	C:\

Showing results 1 - 3 of 3

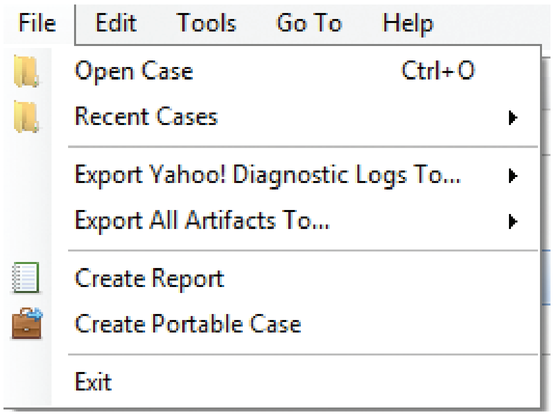
URL	https://chrome.google.com/webstore?hl=en
Title	Chrome Web Store
Last Updated - UTC (yyyy-mm-dd)	2012-07-08 19:25:15
Thumbnail	
Source	C:\Users\mark\AppData\local\Google\Chrome\User Data\Default\Top Sites
Located At	Table: thumbnails(rowid: 2)

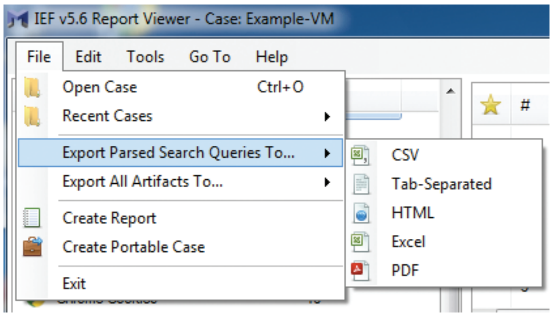
14. The following screenshot shows the "Chrome Carved Web History" selected. The date visited, URL and other information are readily available. Items can be selected and added to bookmarks.



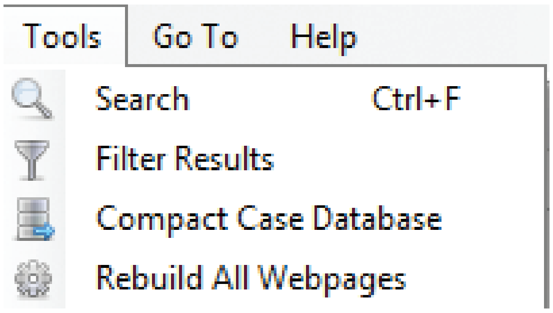
★	#	Date Visited - UTC (y...	URL	Title	Visit Count	Typed Cou
	26	2012-08-12 20:06:53	http://www.google.co...	show exact bytes of m...	1	0
	27	2012-08-14 00:32:54	http://www.google.co...	Google	5	0
	28	2012-09-08 21:22:17	http://www.google.co...	Google	5	0
	29	2012-09-08 21:22:23	http://magnetforensic...	Download IEF | Magn...	1	1
	30	2012-09-08 21:22:23	http://www.magnetfor...	Download IEF | Magn...	1	0

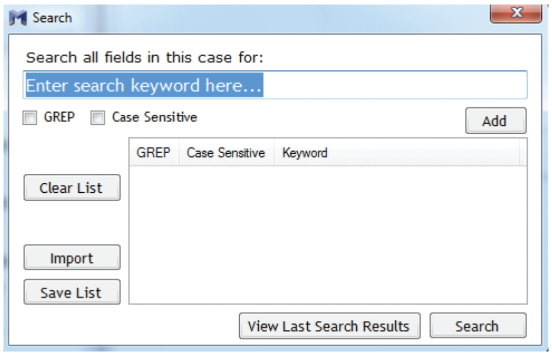
15. The report viewer has several other options in the menu bar. The file menu includes report generation and artifact exporting capabilities. Items can be exported in a number of different formats including CSV, PDF, HTML, Excel Formatted and Tab-Separated.



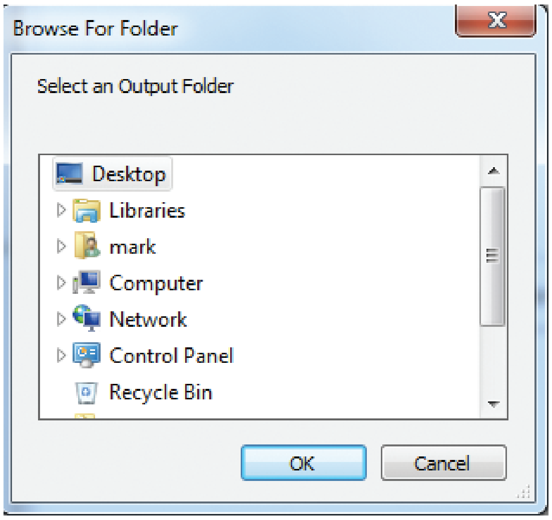


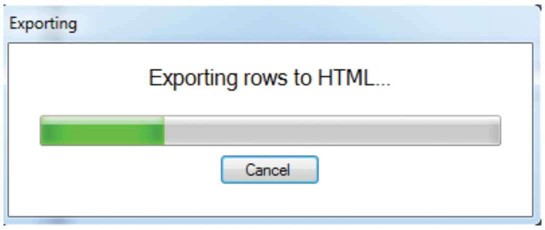
16. The Tools menu has several options, including the search option, which can be used to access the search dialog, where keywords can be entered.





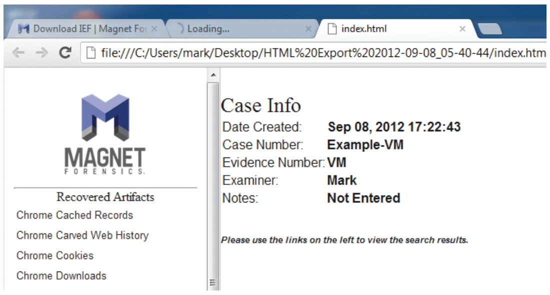
17. A report can be generated from the File menu. “Click Report” was selected. A file dialog for where to save the report was displayed, and once information was entered, a status bar was displayed to indicate the progress of the report being generated.





Exporting rows to HTML...

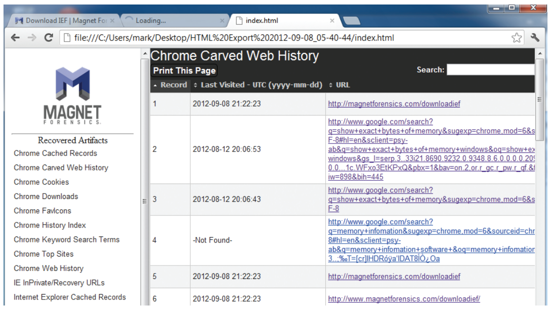
18. The report was opened with Google Chrome and viewed. The report is laid out similar to the report viewer, with artifact lists on the left side and details on the right.



Case Info

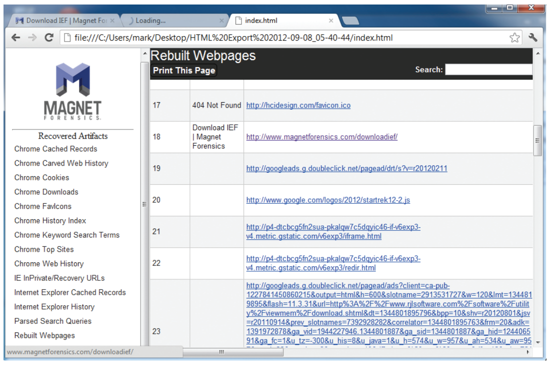
Date Created:	Sep 08, 2012 17:22:43
Case Number:	Example-VM
Evidence Number:	VM
Examiner:	Mark
Notes:	Not Entered

Please use the links on the left to view the search results.


Download IEF | Magnet For
Loading...
index.html
file:///C:/Users/mark/Desktop/HTML%20Export%202012-09-08_05-40-44/index.html
MAGNET FORENSICS
Recovered Artifacts
Chrome Cached Records
Chrome Carved Web History
Chrome Cookies
Chrome Downloads
Chrome Favicons
Chrome History Index
Chrome Keyword Search Terms
Chrome Top Sites
Chrome Web History
IE InPrivate/Recovery URLs
Internet Explorer Cached Records
Print This Page
Search:

Chrome Carved Web History

Record	Last Visited - UTC (yyyy-mm-dd)	URL
1	2012-09-08 21:22:23	http://magnetforensics.com/downloadief
2	2012-08-12 20:06:53	http://www.google.com/search?q=show+exact+bytes+of+memory&sugexp=chrome,mod=6&sF-8#hl=en&sclient=psy-ab&q=show+exact+bytes+of+memory+windows&oq=show+exwindows&gs_l=serp.3..33i21.8690.9232.0.9348.8.6.0.0.0.0.200.0...1c.WFxo3EtKPxQ&pbx=1&bav=on.2,or.r_gc.r_pw.r_qf.&iw=898&bih=445
3	2012-08-12 20:06:43	http://www.google.com/search?q=show+exact+bytes+of+memory&sugexp=chrome,mod=6&sF-8
4	-Not Found-	http://www.google.com/search?q=memory+infomation&sugexp=chrome,mod=6&sourceid=chr8#hl=en&sclient=psy-ab&q=memory+infomation+software+&oq=memory+infomatior3..;‰T=[cr]IHDRóÿa'IDAT8ÍÒ¿Oa
5	2012-09-08 21:22:23	http://magnetforensics.com/downloadief
6	2012-09-08 21:22:23	http://www.magnetforensics.com/downloadief/


Download IEF | Magnet For
Loading...
index.html
file:///C:/Users/mark/Desktop/HTML%20Export%202012-09-08_05-40-44/index.html
MAGNET FORENSICS
Recovered Artifacts
Chrome Cached Records
Chrome Carved Web History
Chrome Cookies
Chrome Downloads
Chrome Favicons
Chrome History Index
Chrome Keyword Search Terms
Chrome Top Sites
Chrome Web History
IE InPrivate/Recovery URLs
Internet Explorer Cached Records
Internet Explorer History
Parsed Search Queries
Rebuilt Webpages
Print This Page
Search:
www.magnetforensics.com/downloadief/

Rebuilt Webpages

17	404 Not Found	http://hcidesign.com/favicon.ico
18	Download IEF | Magnet Forensics	http://www.magnetforensics.com/downloadief/
19		http://googleads.g.doubleclick.net/pagead/drt/s?v=r20120211
20		http://www.google.com/logos/2012/startrek12-2.js
21		http://p4-dtcbcg5fn2sua-pkalqw7c5dqyic46-if-v6exp3-v4.metric.gstatic.com/v6exp3/iframe.html
22		http://p4-dtcbcg5fn2sua-pkalqw7c5dqyic46-if-v6exp3-v4.metric.gstatic.com/v6exp3/redir.html
23		http://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-1227841450860215&output=html&h=600&slotname=2913531727&w=120&lmt=1344819895&flash=11.3.31&url=http%3A%2F%2Fwww.rjlsoftware.com%2Fsoftware%2Futility%2Fviewmem%2Fdownload.shtml&dt=1344801895796&bpp=10&shv=r20120801&jsv=r20110914&prev_slotnames=7392928282&correlator=1344801895763&frm=20&adk=1391972878&ga_vid=1944227946.1344801887&ga_sid=1344801887&ga_hid=124406591&ga_fc=1&u_tz=-300&u_his=8&u_java=1&u_h=574&u_w=957&u_ah=534&u_aw=95

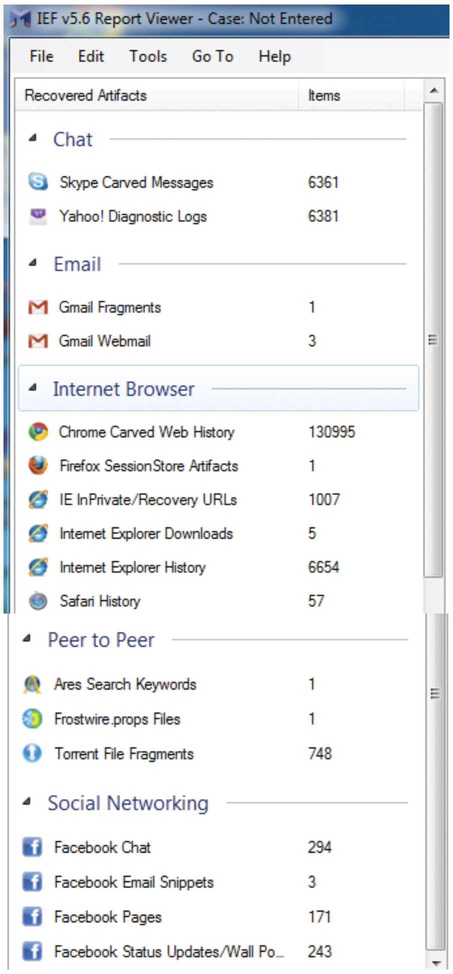
Results

IEF is extremely simple to use. This VMware session was going to be used primarily to capture screenshots of a quick walkthrough of IEF's functionally. However, IEF surprisingly turned up a number of artifacts, including the Internet history of downloading and installing IEF. Software installation was simple. Executing the program and navigating the results of the test were both easy and intuitive. Report generation was quick and simple and the layout of the report was easy to read.

Test – Live Case Data

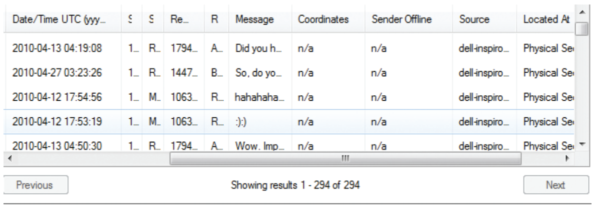
This test was performed on a 160 GB drive image of an actual investigative case. This drive was failing and experienced many read errors. This drive was imaged with the program "dcfldd" from a Backtrack 5 Live CD. Once imaged, IEF was configured to perform a sector level search. The case involved online chat and it was determined this would be a good test for IEF. Note that many of the fields displayed on the following screenshots have been shortened or obfuscated to protect individuals involved in the case; however, it is easy to see what IEF found.

Once IEF processed the case, the entire IEF folder was copied to another machine for review. IEF was started and the case opened. Immediately, it was noticed that IEF discovered a number of chat-based artifacts, including Skype and Facebook chat messages, along with extensive Web history from both IE and Google Chrome.



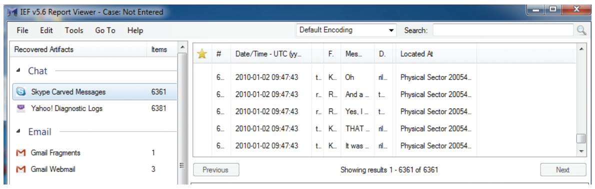
Recovered Artifacts	Items
Chat	
Skype Carved Messages	6361
Yahoo! Diagnostic Logs	6381
Email	
Gmail Fragments	1
Gmail Webmail	3
Internet Browser	
Chrome Carved Web History	130995
Firefox SessionStore Artifacts	1
IE InPrivate/Recovery URLs	1007
Internet Explorer Downloads	5
Internet Explorer History	6654
Safari History	57
Peer to Peer	
Ares Search Keywords	1
Frostwire.props Files	1
Torrent File Fragments	748
Social Networking	
Facebook Chat	294
Facebook Email Snippets	3
Facebook Pages	171
Facebook Status Updates/Wall Po...	243

Examining the details of these chat messages revealed the sender, the recipients(s), the message, the date and time in UTC format, and the physcial sector where the information was found. Again, note that some fields have been shortened to not display the full information of the case for this report.



Date/Time UTC (yyy...	S	S	Re...	R	Message	Coordinates	Sender Offline	Source	Located At
2010-04-13 04:19:08	1...	R...	1794...	A...	Did you h...	n/a	n/a	dell-inspiro...	Physical Se
2010-04-27 03:23:26	1...	R...	1447...	B...	So, do yo...	n/a	n/a	dell-inspiro...	Physical Se
2010-04-12 17:54:56	1...	M...	1063...	R...	hahahaha...	n/a	n/a	dell-inspiro...	Physical Se
2010-04-12 17:53:19	1...	M...	1063...	R...	:):)	n/a	n/a	dell-inspiro...	Physical Se
2010-04-13 04:50:30	1...	R...	1794...	A...	Wow. Imp...	n/a	n/a	dell-inspiro...	Physical Se

Showing results 1 - 294 of 294

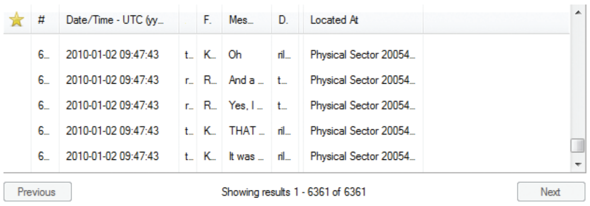


IEF v5.6 Report Viewer - Case: Not Entered

Recovered Artifacts	Items
Chat	
Skype Carved Messages	6361
Yahoo! Diagnostic Logs	6381
Email	
Gmail Fragments	1
Gmail Webmail	3

☆	#	Date/Time - UTC (yy...		F.	Mes...	D.	Located At
	6...	2010-01-02 09:47:43	t...	K...	Oh	ril...	Physical Sector 20054...
	6...	2010-01-02 09:47:43	r...	R...	And a ...	t...	Physical Sector 20054...
	6...	2010-01-02 09:47:43	r...	R...	Yes, I ...	t...	Physical Sector 20054...
	6...	2010-01-02 09:47:43	t...	K...	THAT ...	ril...	Physical Sector 20054...
	6...	2010-01-02 09:47:43	t...	K...	It was ...	ril...	Physical Sector 20054...

Showing results 1 - 6361 of 6361



☆	#	Date/Time - UTC (yy...		F.	Mes...	D.	Located At
	6...	2010-01-02 09:47:43	t...	K...	Oh	ril...	Physical Sector 20054...
	6...	2010-01-02 09:47:43	r...	R...	And a ...	t...	Physical Sector 20054...
	6...	2010-01-02 09:47:43	r...	R...	Yes, I ...	t...	Physical Sector 20054...
	6...	2010-01-02 09:47:43	t...	K...	THAT ...	ril...	Physical Sector 20054...
	6...	2010-01-02 09:47:43	t...	K...	It was ...	ril...	Physical Sector 20054...

Showing results 1 - 6361 of 6361

Results

IEF was able to locate the relevant chat information to the case, despite the drive containing errors. With a sector level search, IEF recovered over 12,000 individual chat messages from the drive image.

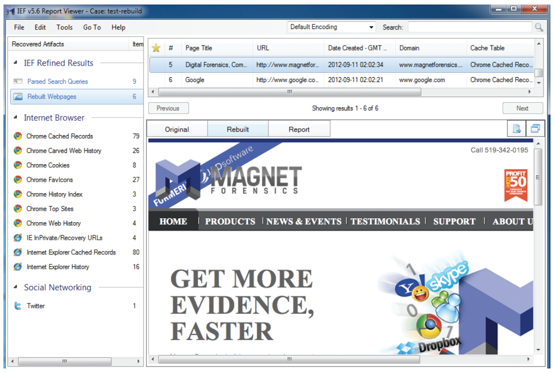
Test – Rebuilding Web Pages

One of the newest features of IEF is the ability to use cached items such as pictures in conjunction with the Internet history to rebuild Web pages. This option is selected during the artifact acquisition. To test this feature, the following steps were performed:

1. A clean VMware was loaded. Using both Internet Explorer and Google Chrome, both magnetforensics.com and ectcoe.net were loaded. Both Web browsers were closed.
2. Using a Backtrack 5 ISO file as the VMware CD drive, the VMware session was rebooted, imaged to an external hard drive using the program "dcfldd" and disconnected.
3. The drive was then plugged into a Windows 7 computer with IEF installed. This computer was not connected to the Internet. The image file was mounted using FTK Imager.
4. IEF was executed, and told to perform a quick search on mounted image files.
5. Once completed, the results were viewed using IEF's report viewer.

Results

IEF rebuilt six Web pages, including the four that were browsed to during the test setup. The rebuilt Web pages can be seen in the screenshots below. Upon close examination, it was determined that these Web pages exactly matched the browsed Web pages. Since the examination computer was not connected to the Internet, these Web pages could only have been rebuilt from the local cache file.

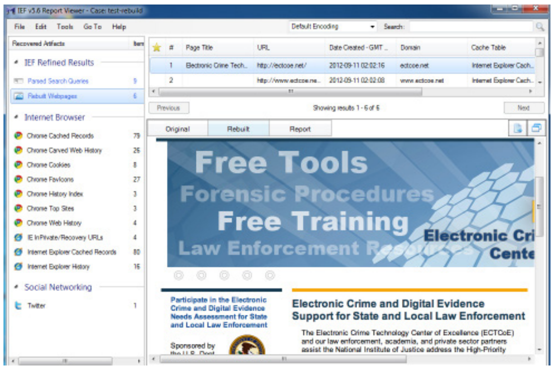


IEF v5.6 Report Viewer - Case: test-rebuild

Recovered Artifacts	Item
IEF Refined Results	
Parsed Search Queries	9
Rebuilt Webpages	6
Internet Browser	
Chrome Cached Records	79
Chrome Carved Web History	26
Chrome Cookies	8
Chrome FavIcons	27
Chrome History Index	3
Chrome Top Sites	3
Chrome Web History	4
IE InPrivate/Recovery URLs	4
Internet Explorer Cached Records	80
Internet Explorer History	16
Social Networking	
Twitter	1

☆	#	Page Title	URL	Date Created - GMT ...	Domain	Cache Table
	5	Digital Forensics, Com...	http://www.magnetfor...	2012-09-11 02:02:34	www.magnetforensics....	Chrome Cached Reco...
	6	Google	http://www.google.co...	2012-09-11 02:02:21	www.google.com	Chrome Cached Reco...

Showing results 1 - 6 of 6



IEF v5.6 Report Viewer - Case: test-rebuild

Recovered Artifacts	Item
IEF Refined Results	
Parsed Search Queries	9
Rebuilt Webpages	6
Internet Browser	
Chrome Cached Records	79
Chrome Carved Web History	26
Chrome Cookies	8
Chrome FavIcons	27
Chrome History Index	3
Chrome Top Sites	3
Chrome Web History	4
IE InPrivate/Recovery URLs	4
Internet Explorer Cached Records	80
Internet Explorer History	16
Social Networking	
Twitter	1

☆	#	Page Title	URL	Date Created - GMT ...	Domain	Cache Table
	1	Electronic Crime Tech...	http://ectcoe.net/	2012-09-11 02:02:16	ectcoe.net	Internet Explorer Cach...
	2		http://www.ectcoe.ne...	2012-09-11 02:02:08	www.ectcoe.net	Internet Explorer Cach...

Showing results 1 - 6 of 6

Original
Rebuilt
Report
Free Tools
Forensic Procedures
Free Training
Law Enforcement Resources
Electronic Cri
Cente
Participate in the Electronic Crime and Digital Evidence Needs Assessment for State and Local Law Enforcement
Sponsored by the U.S. Dept

Electronic Crime and Digital Evidence Support for State and Local Law Enforcement

The Electronic Crime Technology Center of Excellence (ECTCoE) and our law enforcement, academia, and private sector partners assist the National Institute of Justice address the High-Priority

Test – Cloud Artifacts

This test was performed to determine IEF's collection capability of cloud artifacts. The following steps were performed:

1. Using the same VMware session as in the rebuilding Web pages test, the application installer for Skydrive and Google Drive were downloaded and installed.

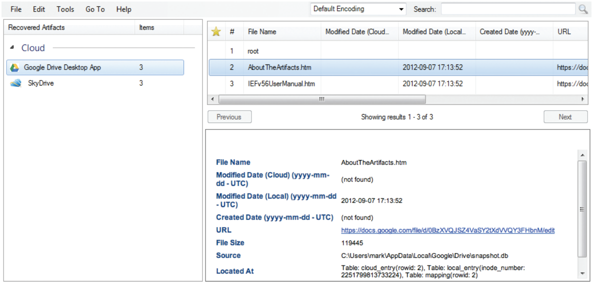
2. The IEF manual PDF file was copied into each of the locally configured shared drives, and the applications were allowed to fully sync.

4. The VMware session was shut down, imaged with Backtrack 5 as before and mounted on an IEF investigation machine using FTK imager.

5. IEF was configured to perform a full search, selecting only the cloud-based artifacts. Once completed, the results were examined.

Results

IEF's report viewer reported results for Google Drive and Skydrive. Google drive returned the best results as can be seen in the screenshot below.



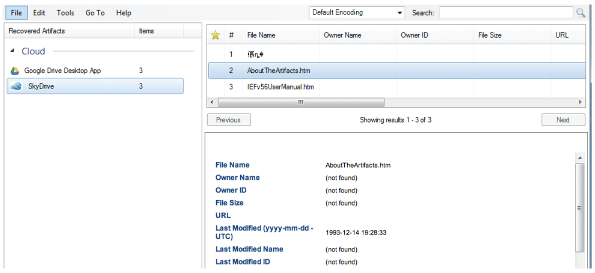
Recovered Artifacts	Items
Cloud	
Google Drive Desktop App	3
SkyDrive	3

#	File Name	Modified Date (Cloud...	Modified Date (Local...	Created Date (yyyy-...	URL
1	root				
2	AboutTheArtifacts.htm		2012-09-07 17:13:52		https://doc
3	IEFv56UserManual.htm		2012-09-07 17:13:52		https://doc

Showing results 1 - 3 of 3

File Name	AboutTheArtifacts.htm
Modified Date (Cloud) (yyyy-mm-dd - UTC)	(not found)
Modified Date (Local) (yyyy-mm-dd - UTC)	2012-09-07 17:13:52
Created Date (yyyy-mm-dd - UTC)	(not found)
URL	https://docs.google.com/file/d/0BzXVQJSZ4VaSY2tXdVVQY3FHbnM/edit
File Size	119445
Source	C:\Users\mark\AppData\Local\Google\Drive\snapshot.db
Located At	Table: cloud_entry(rowid: 2), Table: local_entry(inode_number: 2251799813733224), Table: mapping(rowid: 2)

IEF reported Skydrive items results with less fleshed out information.



Recovered Artifacts	Items
Cloud	
Google Drive Desktop App	3
SkyDrive	3

#	File Name	Owner Name	Owner ID	File Size	URL
1	俵ŋ♦				
2	AboutTheArtifacts.htm				
3	IEFv56UserManual.htm				

Showing results 1 - 3 of 3

File Name	AboutTheArtifacts.htm
Owner Name	(not found)
Owner ID	(not found)
File Size	(not found)
URL	
Last Modified (yyyy-mm-dd - UTC)	1993-12-14 19:28:33
Last Modified Name	(not found)
Last Modified ID	(not found)

During development of this report, it was also discovered that Magnet Forensics is actively developing additional enhancements to other cloud artifact recovery, including the popular application Dropbox. Furthermore, during this test, IEF said that a new version of IEF (5.6.2) was available for download. This is a strong indication that the vendor is actively working to maintain and upgrade IEF's functionality.

Test – iPhone Backup

The test was performed to test one of IEF's newest features, the extraction of information from an iPhone backup. To perform this test, the following steps were performed.

1. The VMware image used in the previous tests was used to backup an iPhone 3G.

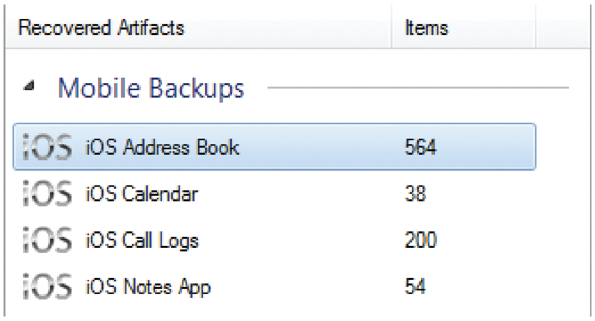
2. The VMware session was shut down, imaged with Backtrack 5, and the image mounted on an IEF investigation machine using FTK imager.

3. IEF was instructed to perform a drive full search with only the 'iOS Backup' artifact selected. Once completed, the results were examined.

Results

IEF recovered several iOS artifacts as shown in the screenshot below, including notes, address book, call logs and calendar information. Each artifact includes details about all of the items discovered. Details have been purposely omitted from this report since they are related to an ongoing investigation.

IEF not only discovered the iPhone backup on the image, but parsed data that could aid an investigation.



Recovered Artifacts	Items
Mobile Backups	
iOS Address Book	564
iOS Calendar	38
iOS Call Logs	200
iOS Notes App	54

Conclusion

In every instance that IEF was run, it was able to discover Internet artifacts. IEF consistently found information that was not expected to be found. IEF provides a very clear idea of how the computer under examination has been used over a long period of time. IEF also discovers evidence that an investigator may have not thought to initially look for. Manually performing the searches that IEF automatically performs would take an investigator a great deal of time, effort and knowledge. IEF clearly demonstrates a tool that would enhance the efficiency of justice. There is no doubt IEF is a superior tool and should be a part of every investigator's toolbox.

During the review, IEF's staff was informed of any issues and quickly addressed them. Magnet Forensics is constantly updating IEF. This tool will only continue to improve over time and provide a large return on investment to law enforcement investigating digital evidence.