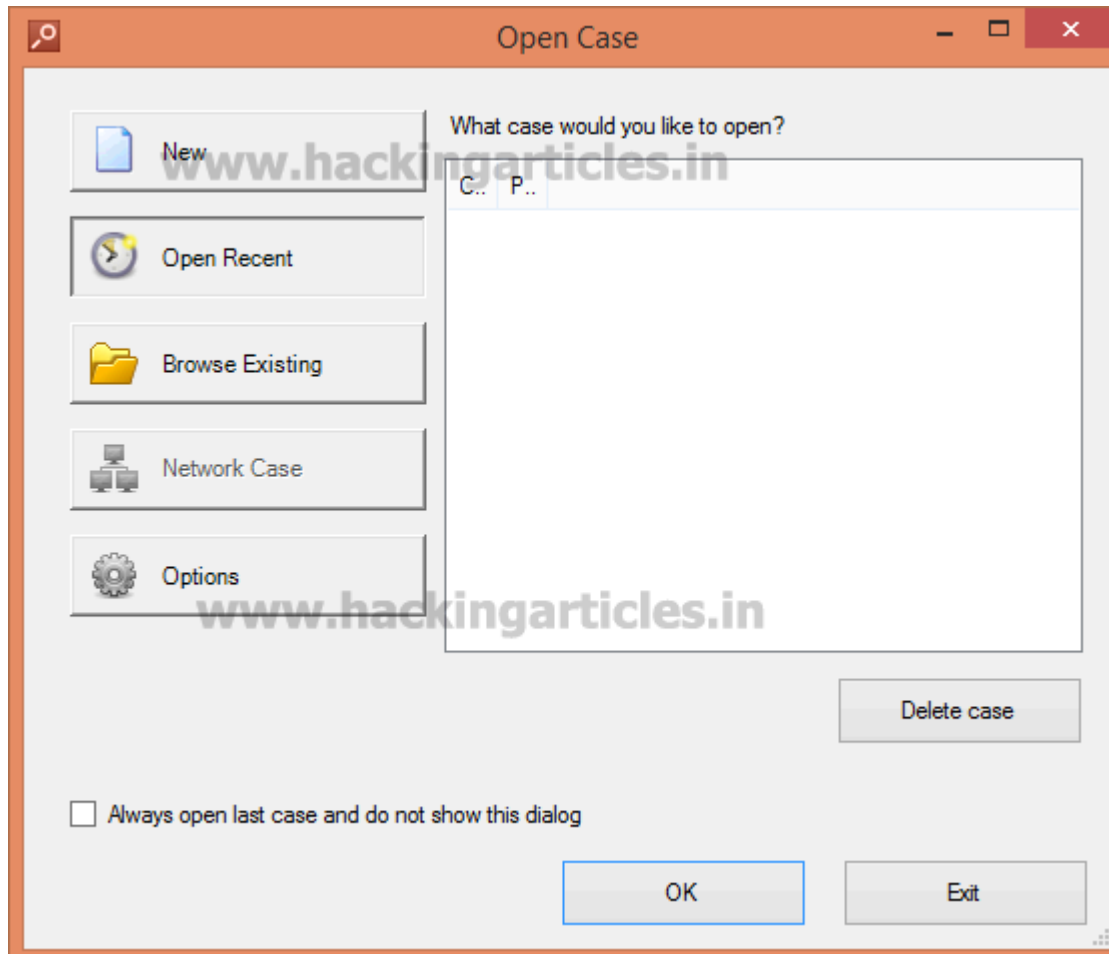


# Forensic Investigation of RAW Images using Belkasoft Evidence Center

July 13, 2015 By Raj Chandel

First of all, download the Belkasoft Evidence Center ultimate from this link.

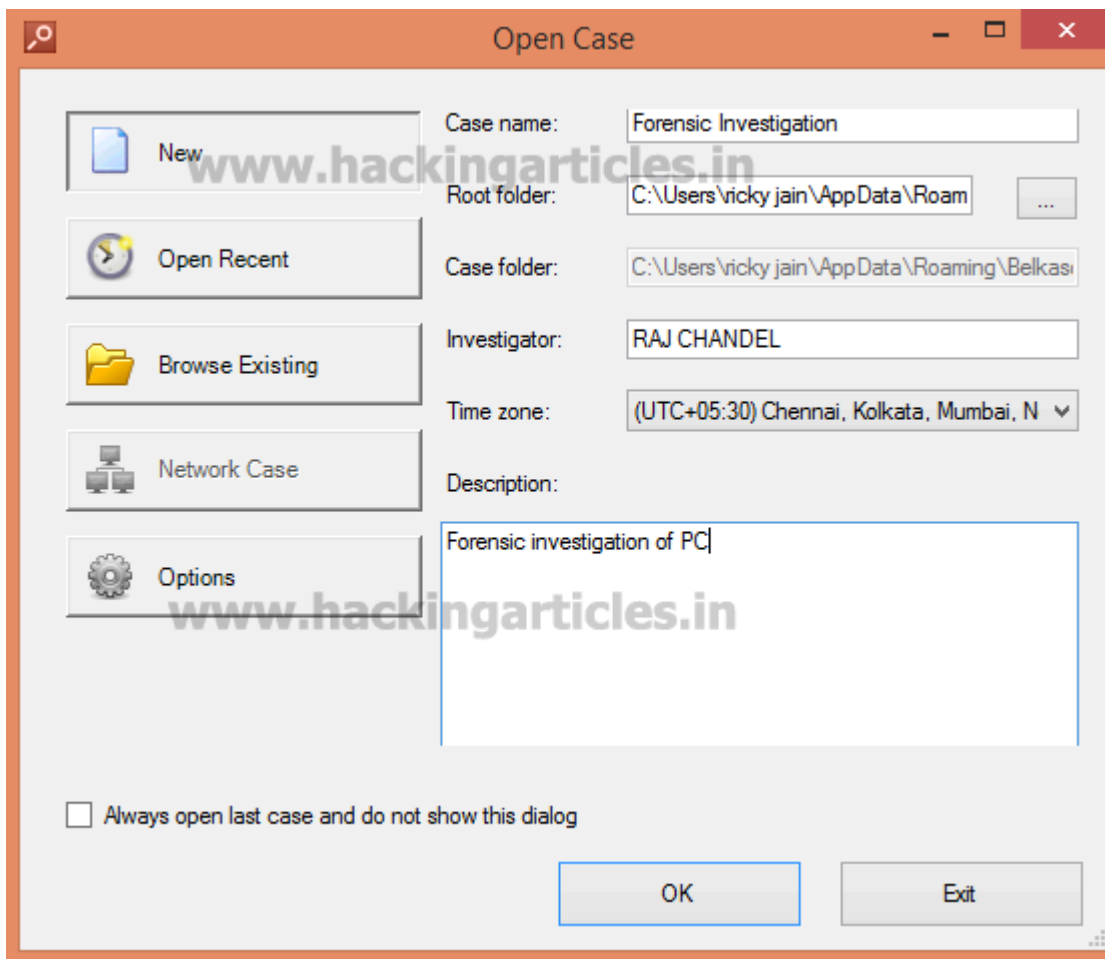
Click on New Option to select the Raw Image.



Enter the Case Name.

Select the Root folder where Forensic Evidence will be created.

Then type the name of the investigator and Case Description. Click Ok.



Now select the Raw Image and Check the Option Analyze Data Source. Click on Next.

**Add data source**

**What sources would you like to analyze?**

Select drive, image, dump, device or other source to include to the case

Available types of data sources

☒ Drive image file or virtual machine disk

G:\vivek pc\v.001 ...

☐ Logical drive

...

☐ Physical drive

...

☐ Mobile backup file, UFED image, chip-off or JTAG dump

... ..

☐ Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)

... ..

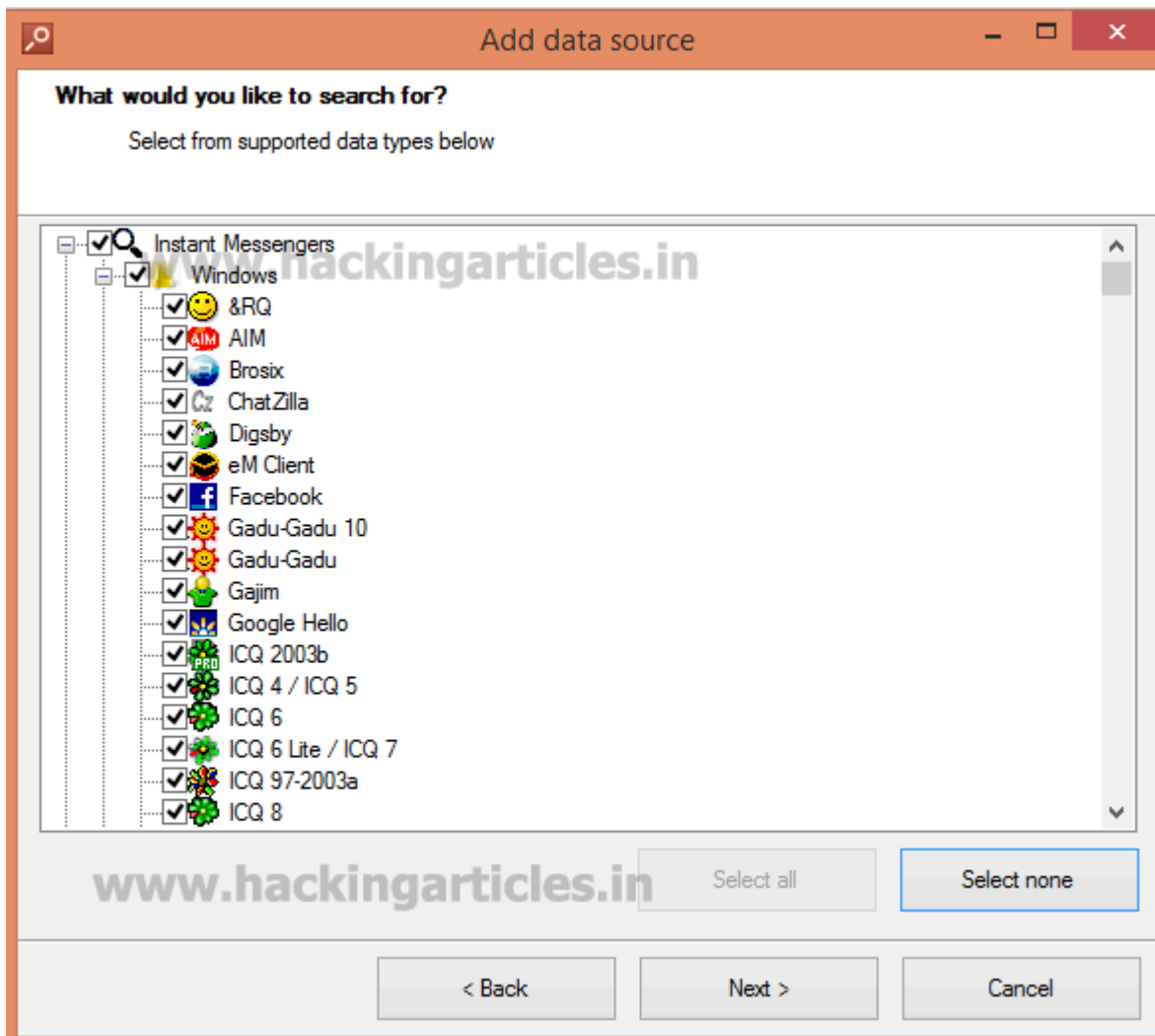
☐ Selected folder

C:\Program Files (x86)\Belkasoft Evidence Center Ultimate\Samples ...

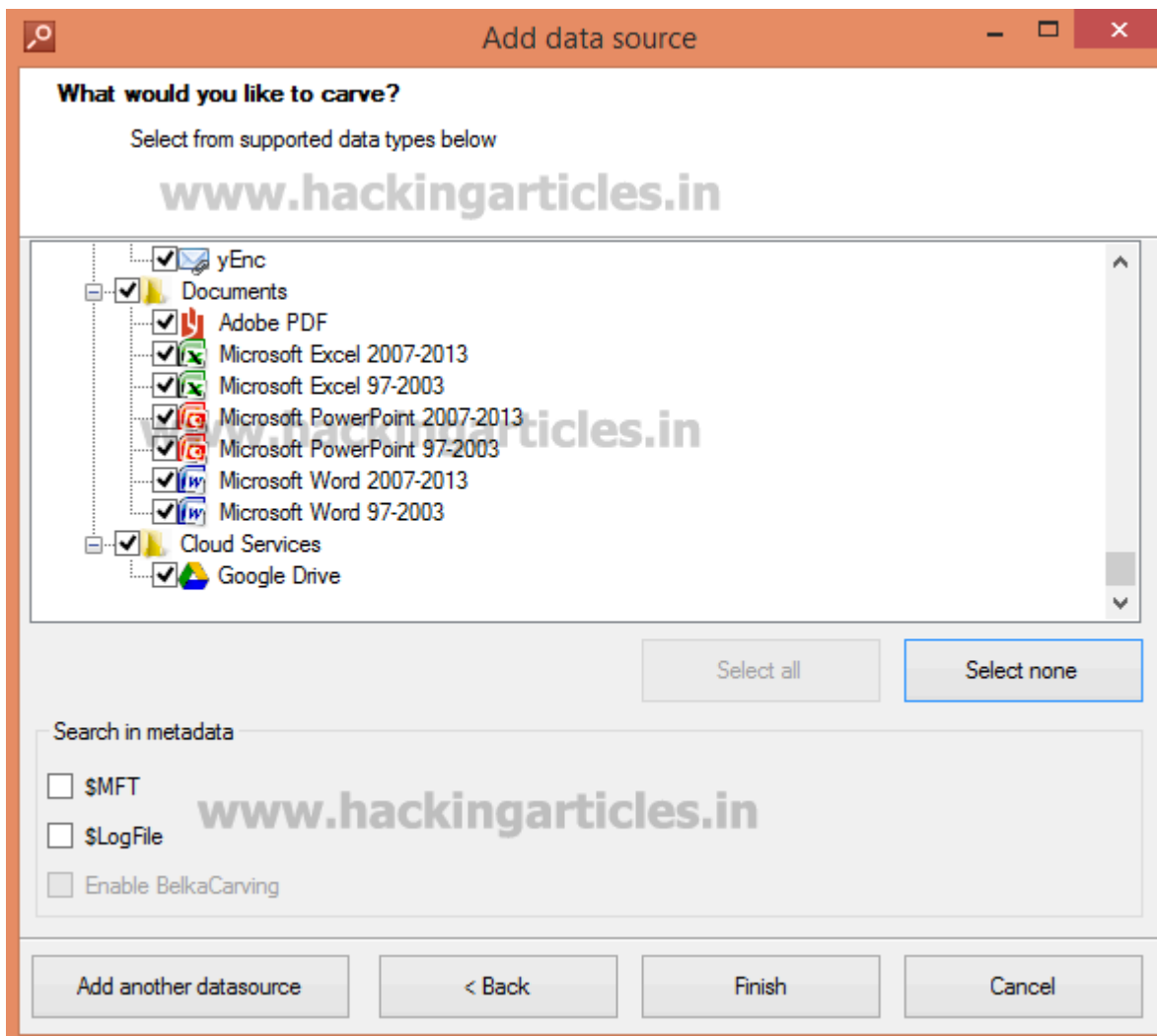
☒ Analyze data source

Next > Cancel

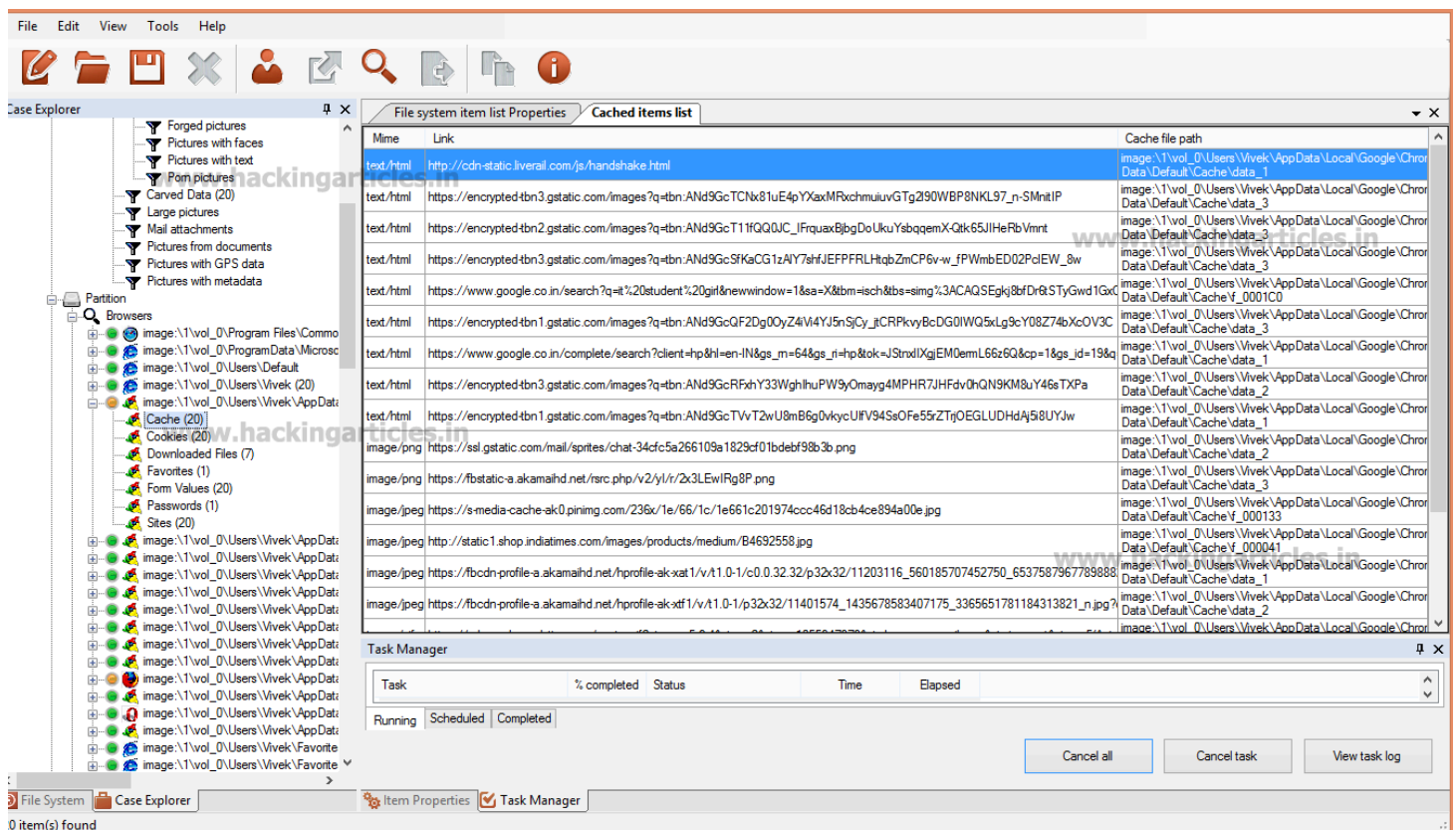
Now Select from supported data types and click on Next.



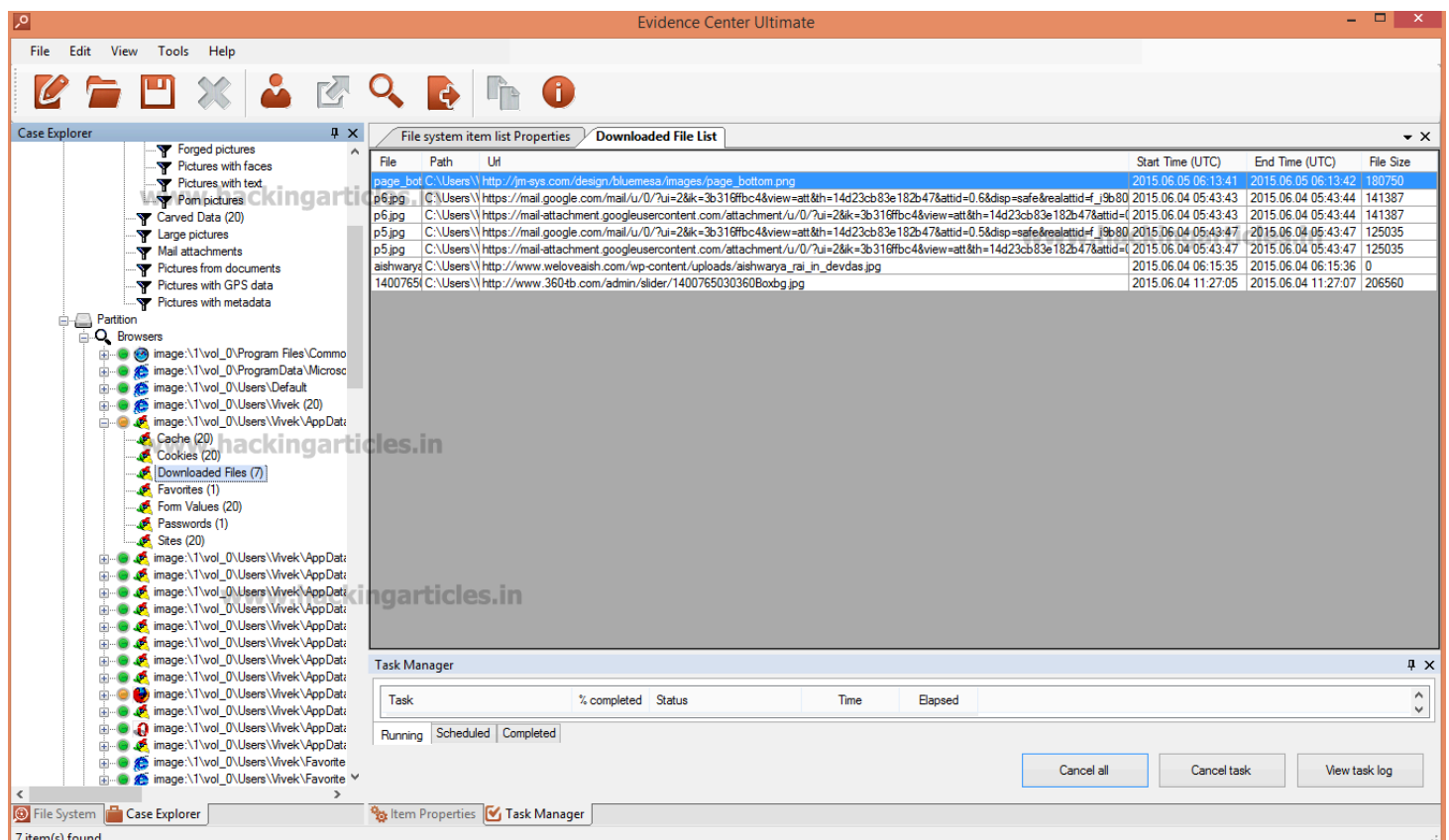
Now Select all and Click on Finish.



To visualize the cached sites exactly as seen by the user, Click on Cache in Browsers option.



To see Downloaded file list, click on Downloaded Files.



To Check the List of Sites Visited by the user, select Sites Option.

File Edit View Tools Help

Case Explorer

File system item list Properties URL List

Last visit (UTC)	URL	Title
2015.06.04 05:03:02	https://www.google.com/	Google
2015.06.04 05:24:15	https://www.google.co.in/url?sa=t&ct=j&q=&esrc=s&source=web&cd=7&cad=rja&uact=8&ved=0CFcQFjAG&url=http://www.mysmartpr	
2015.06.04 05:23:18	https://www.google.co.in/url?sa=t&ct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0CFAQFjAF&url=http://www.smartprix.c	
2015.06.04 05:24:07	https://www.google.co.in/url?sa=t&ct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0CDsQFjAC&url=http://www.91mobiles	
2015.06.04 05:22:36	https://www.google.co.in/search?client=psy-ab&site=&source=hp&q=micromax&oq=&gs_l=&pbx=1&toJSON=undefined&bav=on.2.or.8	micromax - Google Search
2015.06.04 05:23:07	https://www.google.co.in/search?newwindow=1&biw=1280&bih=899&noj=1&q=micromax x353 price&oq=micromax x353&gs_l=serp.1.1.0.10.13707.27737.0.30136.5.5.0.0.0.0.147.719.0.5.5.0...0...1c.1.64.serp..0.5.718.AXzqe_flbD8	micromax x353 price - Google Search
2015.06.04 05:03:02	https://www.google.co.in/?gfe_rd=cr&ei=BbcvVYCvD8-CoAOunYG4CA	Google
2015.06.04 05:23:56	https://www.facebook.com/r.php	Sign up for Facebook   Facebook
2015.06.04 05:23:56	https://www.facebook.com/l.php?u=/r.php&h=8AQGKyBnG	Sign up for Facebook   Facebook
2015.06.04 05:23:56	https://www.facebook.com/campaign/landing.php?campaign_id=779780378771330&partner_id=inmobi&placement=149ca0e288b64	Sign up for Facebook   Facebook
2015.06.04 05:23:51	http://www.youradexchange.com/ad/display.php?r=376975?i=20000	
2015.06.04 05:23:52	http://www.youradexchange.com/ad/display.php?k=556fe0e90a6424971584.7799421&h=d43db1deb6f379fde29fd3653159ec6d6d	
2015.06.04 05:23:53	http://www.trafficoptimiser.com/redirect?target=http://apx.trck.avazutracking.net/click/redirect.php?apxcode=449444&id=KU25KRjMW	
2015.06.04 05:23:19	http://www.smartprix.com/mobiles/micromax-x353-p1101824w3pn	Micromax X353 Best Price in India

To see Cookie List, Click on Cookies Option.

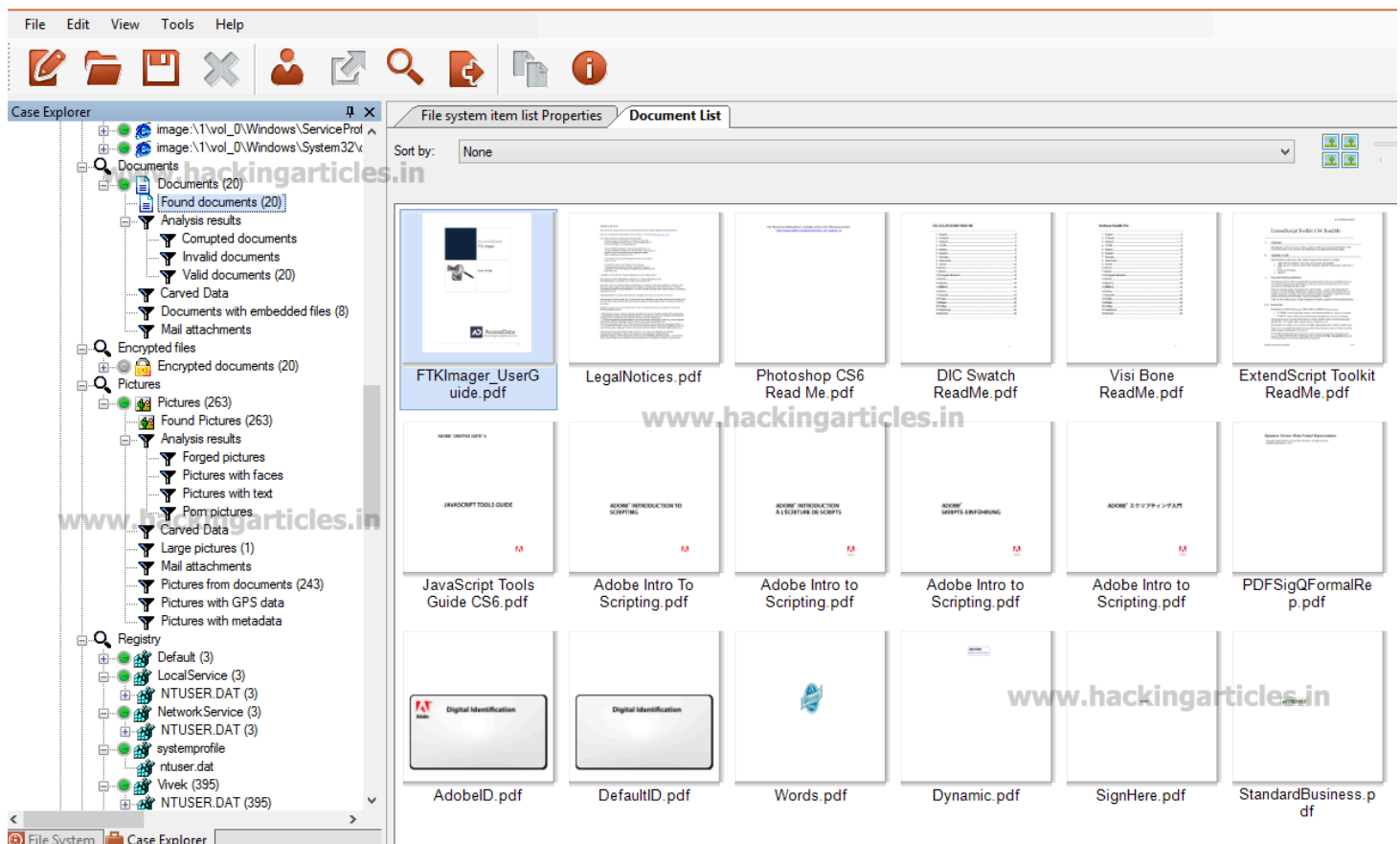
File Edit View Tools Help

Case Explorer

File system item list Properties Cookie list

Host	Expire date (UTC)	Modified date (UTC)	Key	Value
google.co.	2015.09.14 11:46:47	2015.03.15 11:58:27	NID	
google.co.	2017.03.14 11:46:57	2015.03.15 11:58:27	PREF	
java.com	2016.03.14 11:47:11	2015.03.15 11:58:27	ORA_FLE	
mozilla.org	2025.03.12 11:48:43	2015.03.15 11:58:27	optimizely	
mozilla.org	2025.03.12 11:48:43	2015.03.15 11:58:27	optimizely	
mozilla.org	2025.03.12 11:48:43	2015.03.15 11:58:27	optimizely	
mozilla.org	2015.03.15 11:58:46	2015.03.15 11:58:27	__utmt	
24605913	2025.03.12 11:48:47	2015.03.15 11:58:27	end_user	
mozilla.org	2017.03.14 11:48:48	2015.03.15 11:58:27	__utma	
mozilla.org	2015.03.15 12:18:48	2015.03.15 11:58:27	__utmb	
mozilla.org	2015.09.13 23:48:48	2015.03.15 11:58:27	__utmz	
java.com	2015.04.14 11:51:16	2015.03.15 11:58:27	s_nr	
java.com	2015.03.15 12:21:16	2015.03.15 11:58:27	gpName	
java.com	2015.03.15 12:21:16	2015.03.15 11:58:27	gpChanne	
java.com	2015.03.15 12:21:16	2015.03.15 11:58:27	gpServer	
oracle.112	2017.03.14 11:51:17	2015.03.15 11:58:27	s_vl	
browserch	2055.12.31 10:27:47	2015.03.15 11:58:27	page_visi	
qualys.com	2015.03.15 12:02:11	2015.03.15 11:58:27	_gat_UA-	
qualys.com	2017.03.14 11:53:00	2015.03.15 11:58:27	_ga	
browserch	2016.03.14 11:53:04	2015.03.15 11:58:27	scan opti	

Now click on Documents option and Then Select Found Documents option to see all the office Documents files found in user pc.



To see all the encrypted files, click on Found Encrypted files option. It will detect more than 150 types of encrypted files. It is also possible to decrypt all these encrypted files with in this product by installing Passware kit Forensic integrated with Belkasoft Product.



Evidence Center Ultimate

File Edit View Tools Help

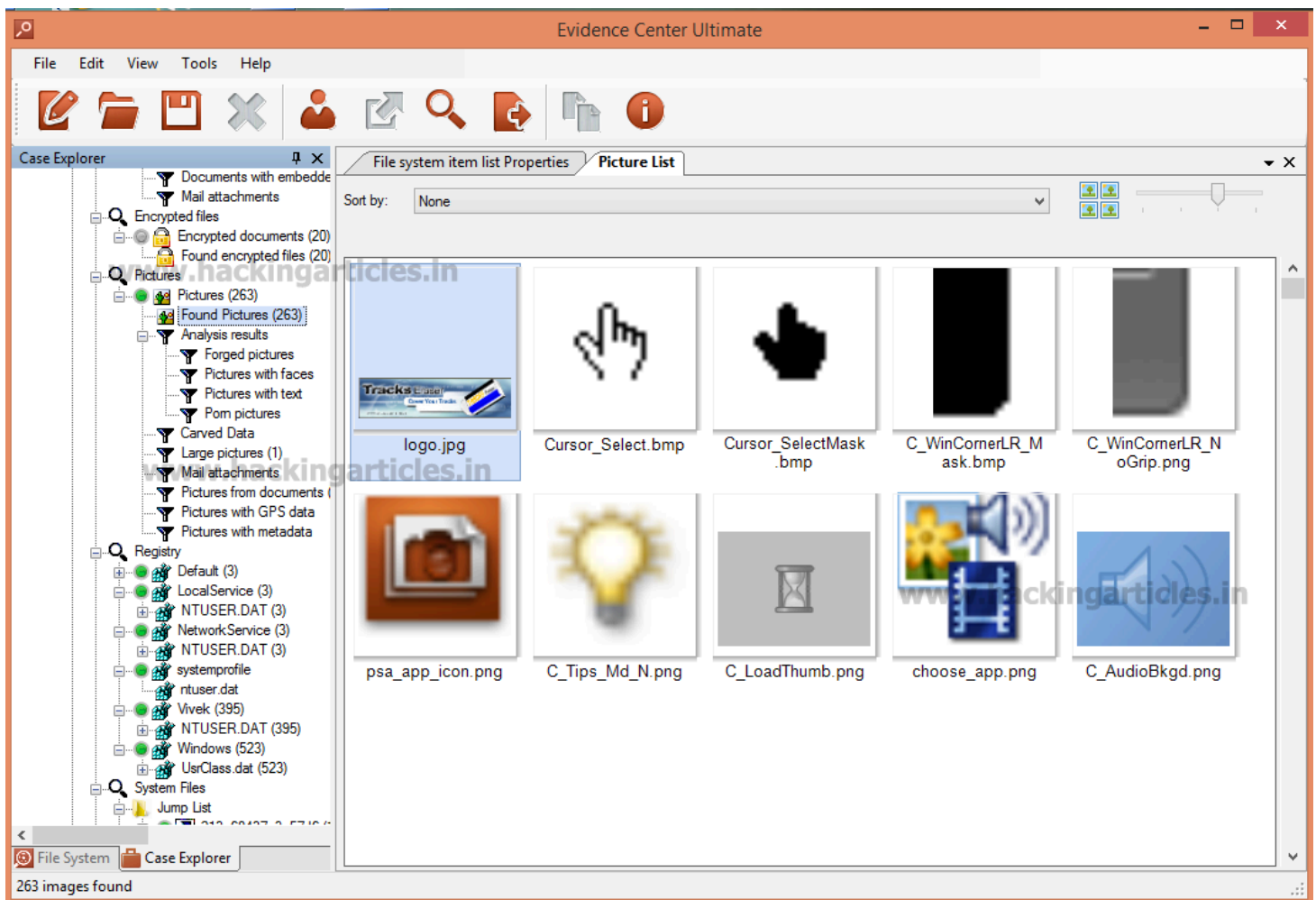
Case Explorer

File system item list Properties Encrypted File List

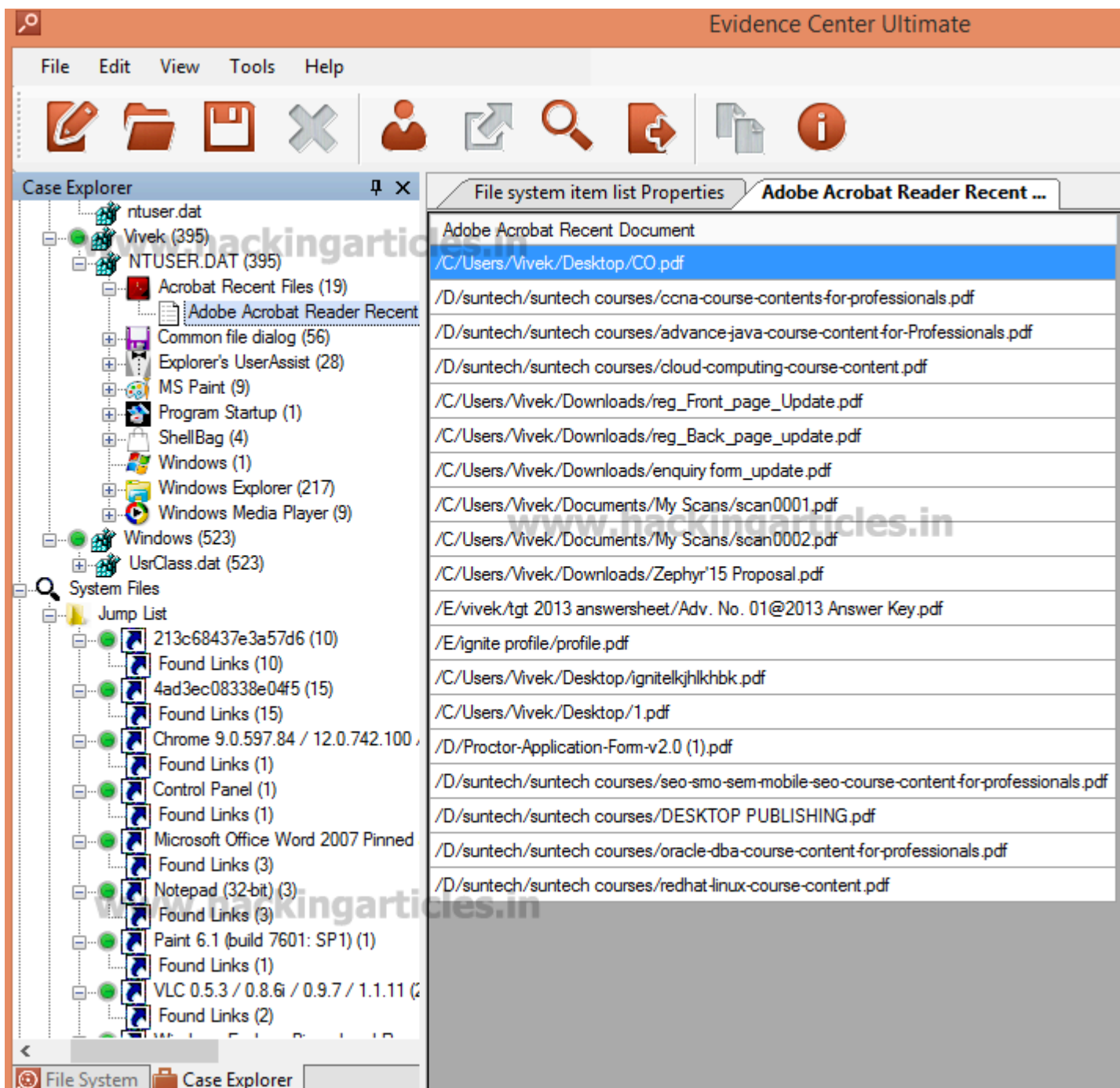
File	File type	Md5	Complexity	Protection features	Recovery options	File-open password	Path
HTML_XLAM	MS Excel 2007	36089CC3	Instant	VBA Project; VBA Password			image:\1\vol_0\Progr Files\Microsoft Office\Office12\Libra
EXPTOOWS.XI	MS Excel 97-2003	F684C292	Instant	VBA Project; Add-in			image:\1\vol_0\Progr Files\Microsoft
GB.pdf	Acrobat 7.0	B9769998	Instant	Permissions Password; RC4 Encryption	File patching required		image:\1\vol_0\Progr Files\Core\Core\DR\ Graphics Suite X5\Languages\EN\H
IFE_1.pdf	Acrobat 7.0	A4ACAA7	Instant	Permissions Password; RC4 Encryption	File patching required		image:\1\vol_0\Progr Files\Core\Core\DR\ Graphics Suite
IFE_2.pdf	Acrobat 7.0	CD147D7	Instant	Permissions Password; RC4 Encryption	File patching required		image:\1\vol_0\Progr Files\Core\Core\DR\ Graphics Suite
IFE_3.pdf	Acrobat 7.0	9EDF9A7	Instant	Permissions Password; RC4 Encryption	File patching required		image:\1\vol_0\Progr Files\Core\Core\DR\ Graphics Suite
IFE_4.pdf	Acrobat 7.0	08C148E7	Instant	Permissions Password; RC4 Encryption	File patching required		image:\1\vol_0\Progr Files\Core\Core\DR\ Graphics Suite
IFE_5.pdf	Acrobat 7.0	7D2439D4	Instant	Permissions Password; RC4 Encryption	File patching required		image:\1\vol_0\Progr Files\Core\Core\DR\ Graphics Suite
IFE_6.pdf	Acrobat 7.0	5E28D454	Instant	Permissions Password; RC4 Encryption	File patching required		image:\1\vol_0\Progr Files\Core\Core\DR\ Graphics Suite
IFE_7.pdf	Acrobat 7.0	C2BF0B15	Instant	Permissions Password; RC4 Encryption	File patching required		image:\1\vol_0\Progr Files\Core\Core\DR\ Graphics Suite
dr_1.pdf	Acrobat 7.0	4196DCE9	Instant	Permissions Password; RC4 Encryption	File patching required		image:\1\vol_0\Progr Files\Core\Core\DR\ Graphics Suite X5\Languages\EN\T
dr_3.pdf	Acrobat 7.0	4D7BF638	Instant	Permissions Password; RC4 Encryption	File patching required		image:\1\vol_0\Progr Files\Core\Core\DR\ Graphics Suite X5\Languages\EN\T

File System Case Explorer

To Find Picture List, Select **Found Pictures** in **Pictures** Option. To Detect Forgery in Picture. Right click on Picture, Select **Analyze Pictures** and Click on **Detect Forgery** Tab.



To find the recent files opened by Acrobat Reader, Click on Adobe Acrobat Reader Recent Option.



To See Recent applications run by user, Click on Last Application and Paths in NTUSER.DAT Option. NTUSER.DAT is a registry file in Windows Operating System .Every user profile contains an NTUSER.DAT file. It contains a unique Documents Folder, Start menu Configuration, Desktop properties and browsing history

Evidence Center Ultimate

File Edit View Tools Help

Case Explorer

- ntuser.dat
- Vivek (395)
  - NTUSER.DAT (395)
    - Acrobat Recent Files (19)
    - Adobe Acrobat Reader Recent
    - Common file dialog (56)
    - Last applications and paths (7)
    - Last selected files (49)
    - Explorer's UserAssist (28)
    - MS Paint (9)
    - Program Startup (1)
    - ShellBag (4)
    - Windows (1)
    - Windows Explorer (217)
    - Windows Media Player (9)
  - Windows (523)
  - UsrClass.dat (523)
- System Files
  - Jump List
    - 213c68437e3a57d6 (10)
    - Found Links (10)
    - 4ad3ec08338e04f5 (15)
    - Found Links (15)
    - Chrome 9.0.597.84 / 12.0.742.100
    - Found Links (1)
    - Control Panel (1)
    - Found Links (1)
    - Microsoft Office Word 2007 Pinned
    - Found Links (3)
    - Notepad (32-bit) (3)
    - Found Links (3)
    - Paint 6.1 (build 7601: SP1) (1)
    - Found Links (1)

File system item list Properties
Case properties

Order	Application	Last path
1	chrome.exe	
2	CorelDRW.exe	
3	{13F1931C-0850-4E39-B19B-9BFF69EC2D1F}	
4	notepad.exe	{031e4825-7b94-4dc3-b131-e946b44c8dd5}\???
1	Photoshop.exe	
2	3dsmax.exe	
3	notepad++.exe	website

To see last Selected Files by the user, Click on Last Selected Files.

Evidence Center Ultimate

File Edit View Tools Help

Case Explorer

File system item list Properties Last selected files

Overall order	File type	By type order	Text
	cdr	1	Project Training banner.cdr
	docx	1	Project Training mail.docx
	html	1	Jeena_Kya_Hai_Jaana_Maine.html
2	jpg	1	11329551_898488720189632_1975930465_n.jpg
3	jpg	2	ignite_banner7.jpg
7	jpg	3	ignite_banner5.jpg
8	jpg	4	ignite_banner4.jpg
10	jpg	5	ignite_banner3.jpg
11	jpg	6	ignite_banner2.jpg
12	jpg	7	ignite_banner0.jpg
13	jpg	8	ignite_banner1.jpg
	jpg	9	Salman-Khan.jpg
	jpg	10	882369-salmankhan-1430984366.jpg
	jpg	11	anshu.jpg
	jpg	12	11334372_898428136862357_60577406_n.jpg
	jpg	13	vivek.jpg
	jpg	14	{20d04fe0-3aea-1069-a2d8-08002b30309d}\D:\IMG_20150412_110916.jpg
	jpg	15	10407116_1456072921370751_1140920357509327201_n.jpg
	jpg	16	1400765030360Boxbg.jpg
	jpg	17	icecream1 (1).jpg
	jpg	18	3791.jpg
	jpg	19	live project traning.jpg
	jpg	20	12_10_2013_14_51_00_npp5sdma9tqntls6suvbujkdh1_im2gmg2127.jpg
5	png	1	poster13-big.png
9	png	2	logo001.png

To check the recent files opened by user, Click on Recent files option.

Evidence Center Ultimate

File Edit View Tools Help

Case Explorer

Program Startup (2)

Programs (2)

Windows (1)

LocalService (3)

NTUSER.DAT (3)

Program Startup (2)

Programs (2)

Windows (1)

NetworkService (3)

NTUSER.DAT (3)

systemprofile

ntuser.dat

Vivek (395)

NTUSER.DAT (395)

Acrobat Recent Files (19)

Adobe Acrobat Reader Recent

Common file dialog (56)

Last applications and paths (7)

Last selected files (49)

Explorer's UserAssist (28)

User Assist (28)

MS Paint (9)

Recent files (9)

Program Startup (1)

ShellBag (4)

Windows (1)

Windows Explorer (217)

Windows Media Player (9)

Windows (523)

UsrClass.dat (523)

System Files

Jump List

213c68437e3a57d6 (10)

File system item list Properties

Recent files

Order	Text
1	C:\Users\Vivek\Desktop\live-project-training-in-ahmedabad_53450810c06f4_w1500.png
2	C:\Users\Vivek\Desktop\007.jpg
3	D:\Shikhankit BSES\Rajni Jain Pan.jpg
4	C:\Users\Vivek\Desktop\2 - Copy.png
5	C:\Users\Vivek\Desktop\enquiry form0 - Copy.png
6	C:\Users\Vivek\Desktop\banne_fb banner.png
7	C:\Users\Vivek\Desktop\ignite_logo.png
8	C:\Users\Vivek\Desktop\website\banner4.jpg
9	C:\Users\Vivek\Desktop\website\Fb_ad2.jpg

File System

Case Explorer

To detect latest searches by the user, click on Searches option.



File Edit View Tools Help

Case Explorer

File system item list Properties Recent searches

Order Text

1	receipt
2	ignite
3	rec
4	latter head
5	latter
6	out
7	ignite lo
8	logo
9	banner
10	cous
11	feed
12	.doc
13	coun
14	course
15	coures
16	fee
17	feedback
18	2
19	ceh
20	ignite banner
21	alien

21 item(s) found

To find the latest accessed files by the user , click on Recently accessed documents.

File Edit View Tools Help



## Case Explorer

- Vivek (395)
  - NTUSER.DAT (395)
    - Acrobat Recent Files (19)
      - Adobe Acrobat Reader Recent
    - Common file dialog (56)
      - Last applications and paths (7)
      - Last selected files (49)
    - Explorer's UserAssist (28)
      - User Assist (28)
    - MS Paint (9)
      - Recent files (9)
    - Program Startup (1)
      - Programs (1)
    - ShellBag (4)
      - ShellBag (4)
    - Windows (1)
      - Windows Explorer (217)
        - Recent searches (21)
        - Recently accessed documents
        - RunMRU - recent inputs in the
    - Windows Media Player (9)
  - Windows (523)
    - UsrClass.dat (523)
- System Files
  - Jump List
    - 213c68437e3a57d6 (10)
      - Found Links (10)
    - 4ad3ec08338e04f5 (15)
      - Found Links (15)
    - Chrome 9.0.597.84 / 12.0.742.100
      - Found Links (1)
    - Control Panel (1)
      - Found Links (1)

## File system item list Properties

## Recently accessed documents

Overall order	File type	By type order	Text
	.10	1	banner_print2.10
	.10	2	banner2.10
	.4	1	fb_banner_19.4
	.ai	1	page4.ai
15	.apk	1	Meri Sex Video.apk
100	.avi	1	mg (2).avi
101	.avi	2	Comp.avi
145	.avi	3	Indian Desi Bhabhi Blowjob And Hardcore Sex with Dirty Hindi.avi
147	.avi	4	Indian Desi Recent Hot Homemade Video Clips 20min.avi
149	.avi	5	Indian Wife Fucked Hard In Doggy And Had Anal By Her Husband
	.avi	6	Very Hot Indian Desi Self Made Exclusive 4 Video Clip Set.avi
35	.cdr	1	Project Training banner.cdr
42	.cdr	2	Backup_of_Backup_of_ignite_Courses.cdr
48	.cdr	3	fb banner.cdr
50	.cdr	4	2.2_ignite.cdr
62	.cdr	5	receipt.cdr
95	.cdr	6	banner24.cdr
98	.cdr	7	banner_update_20.05.2015.cdr
111	.cdr	8	Backup_of_new banner.cdr
117	.cdr	9	new banner.cdr
118	.cdr	10	new banner_front.cdr
	.cmx	1	hoding00111.cmx
	.css	1	style3.css
125	.doc	1	Radio Proposals-100Spots.doc
126	.doc	2	Radio Proposals-80Spots.doc

File System Case Explorer