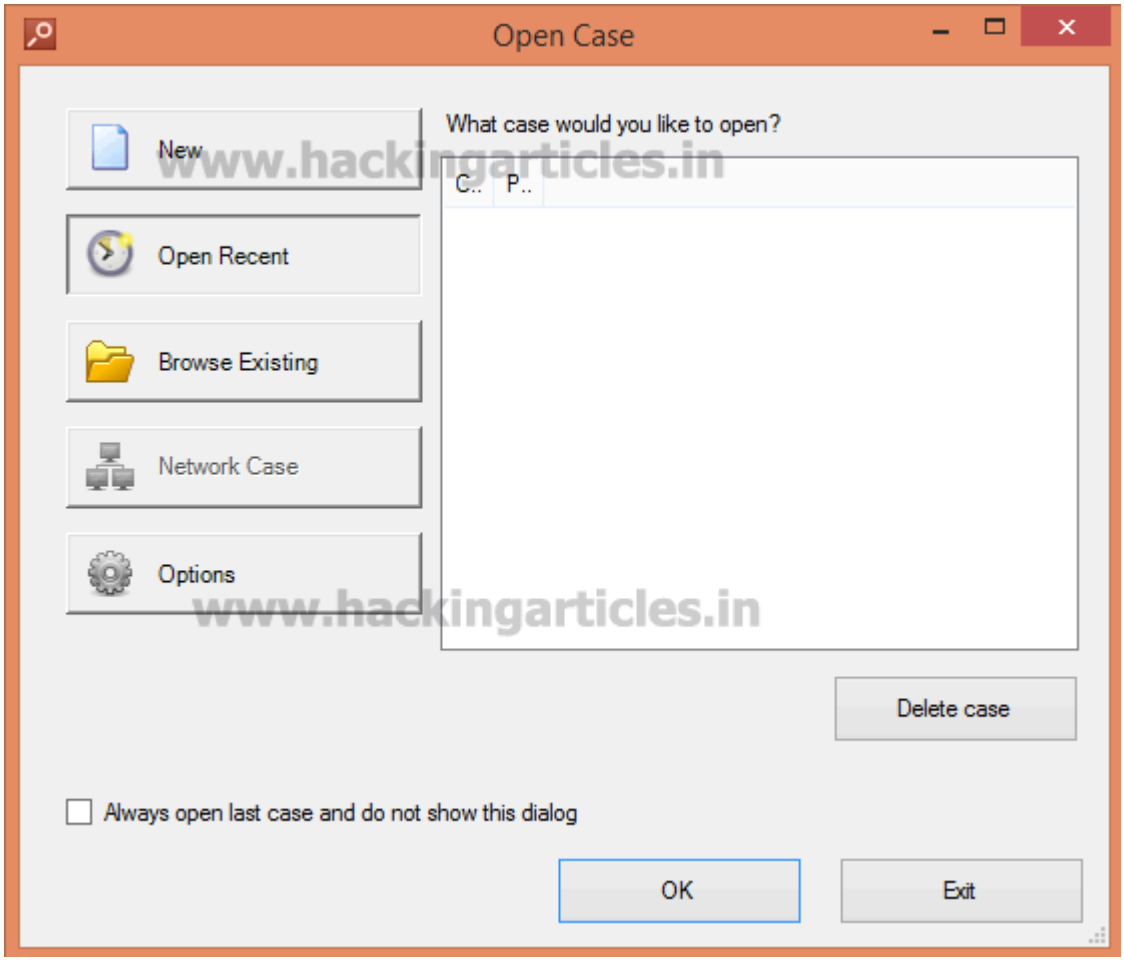
Forensic Investigation of RAW Images using Belkasoft Evidence Center

July 13, 2015 By Raj Chandel

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

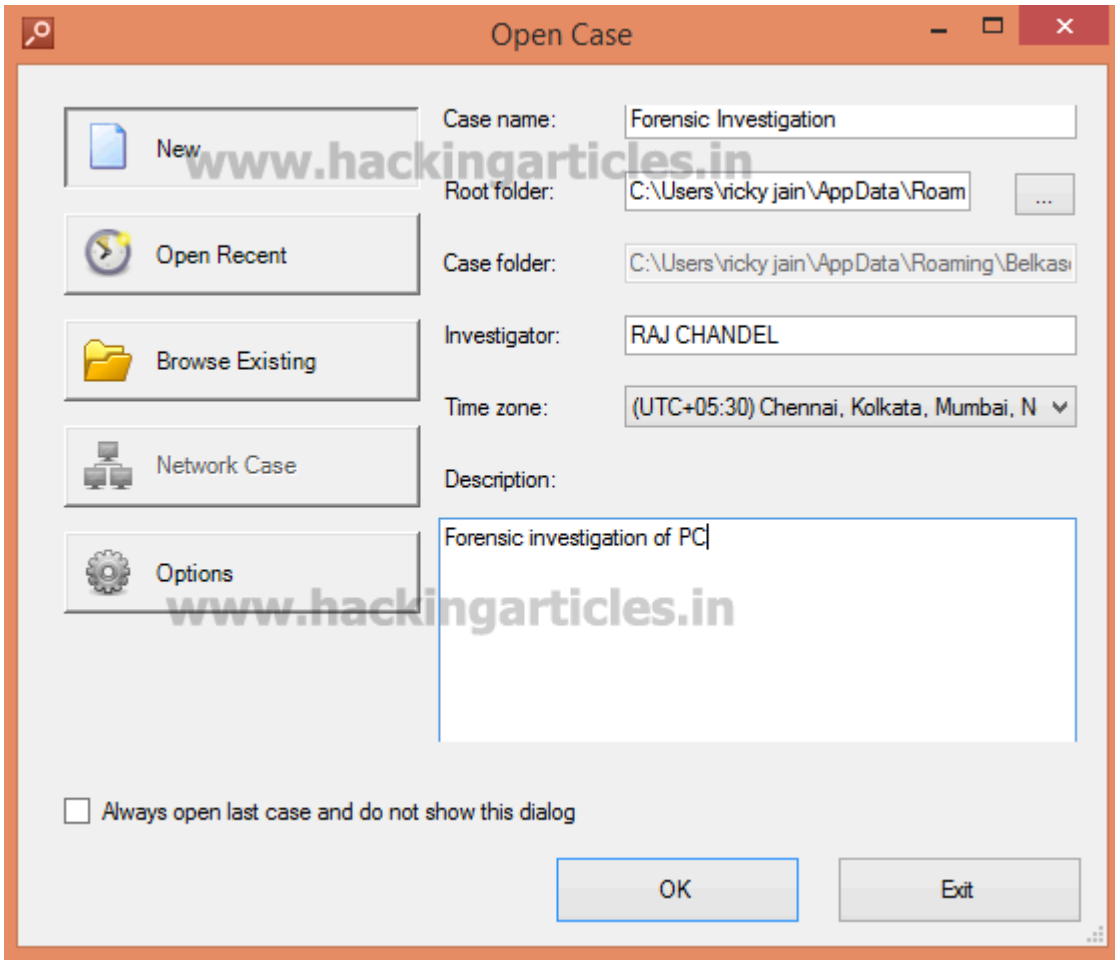
Click on New Option to select the Raw Image.



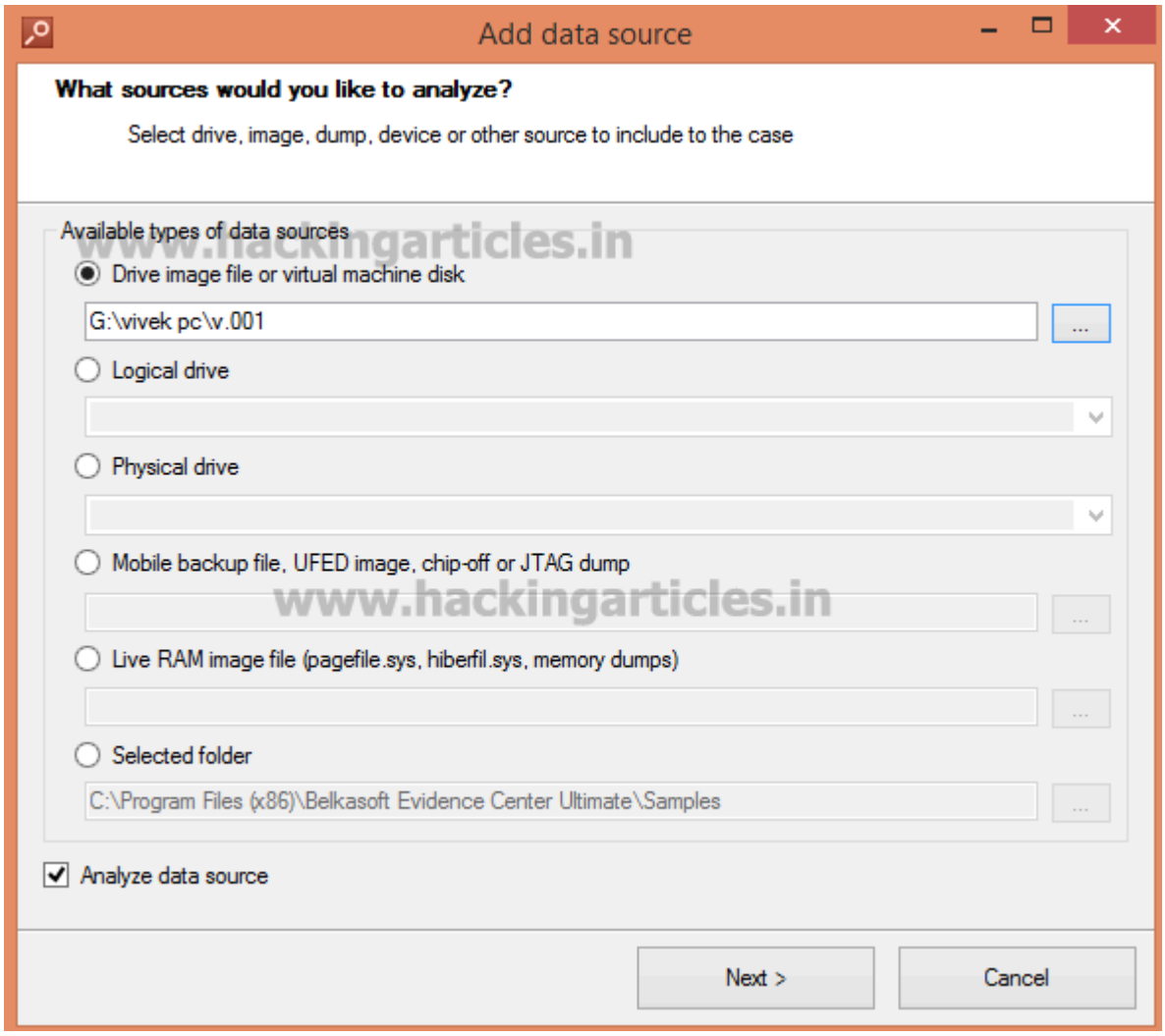
Enter the Case Name.

Select the Root folder where Forensic Evidence will be created.

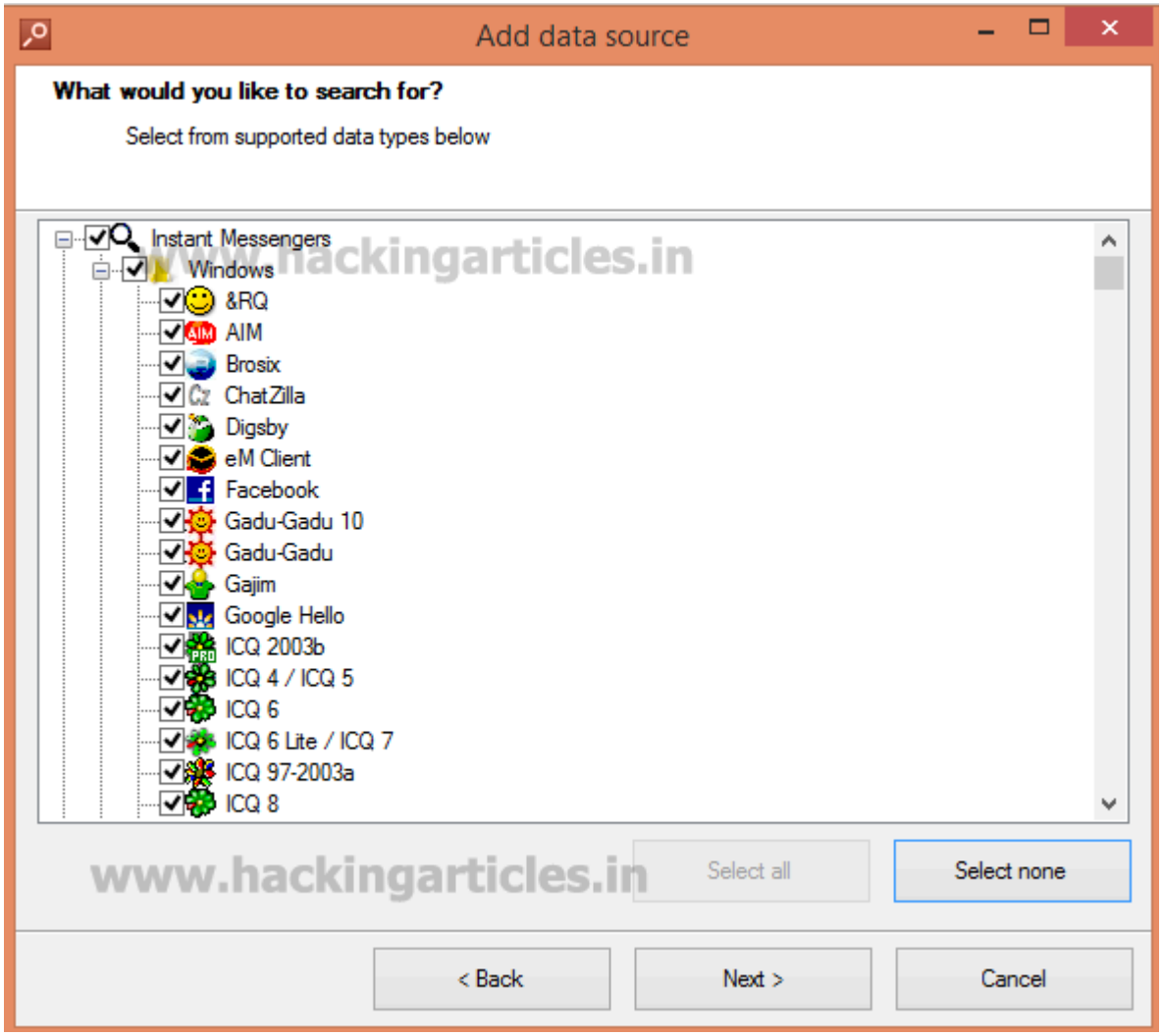
Then type the name of the investigator and Case Description. Click Ok.



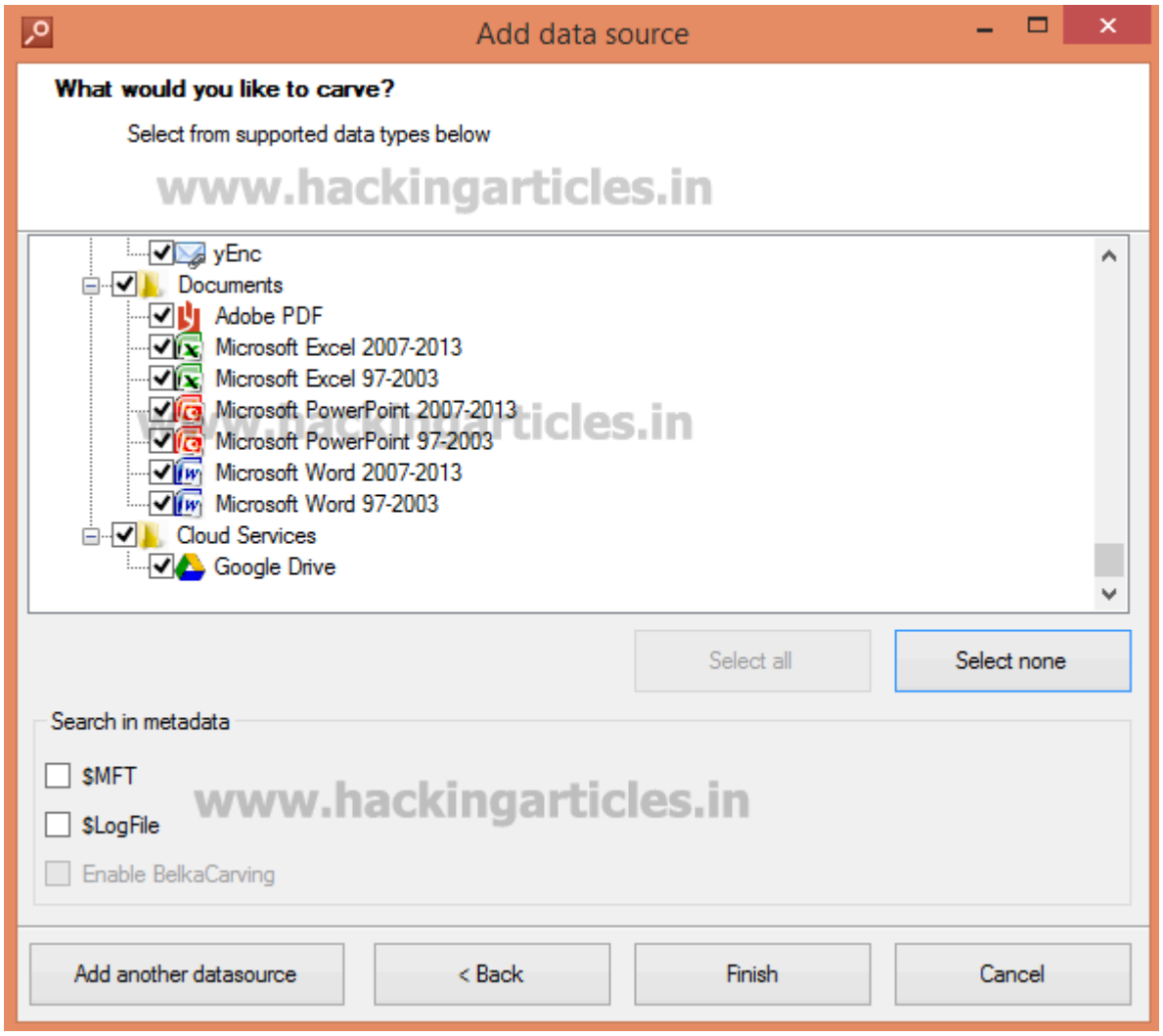
Now select the Raw Image and Check the Option Analyze Data Source. Click on Next.



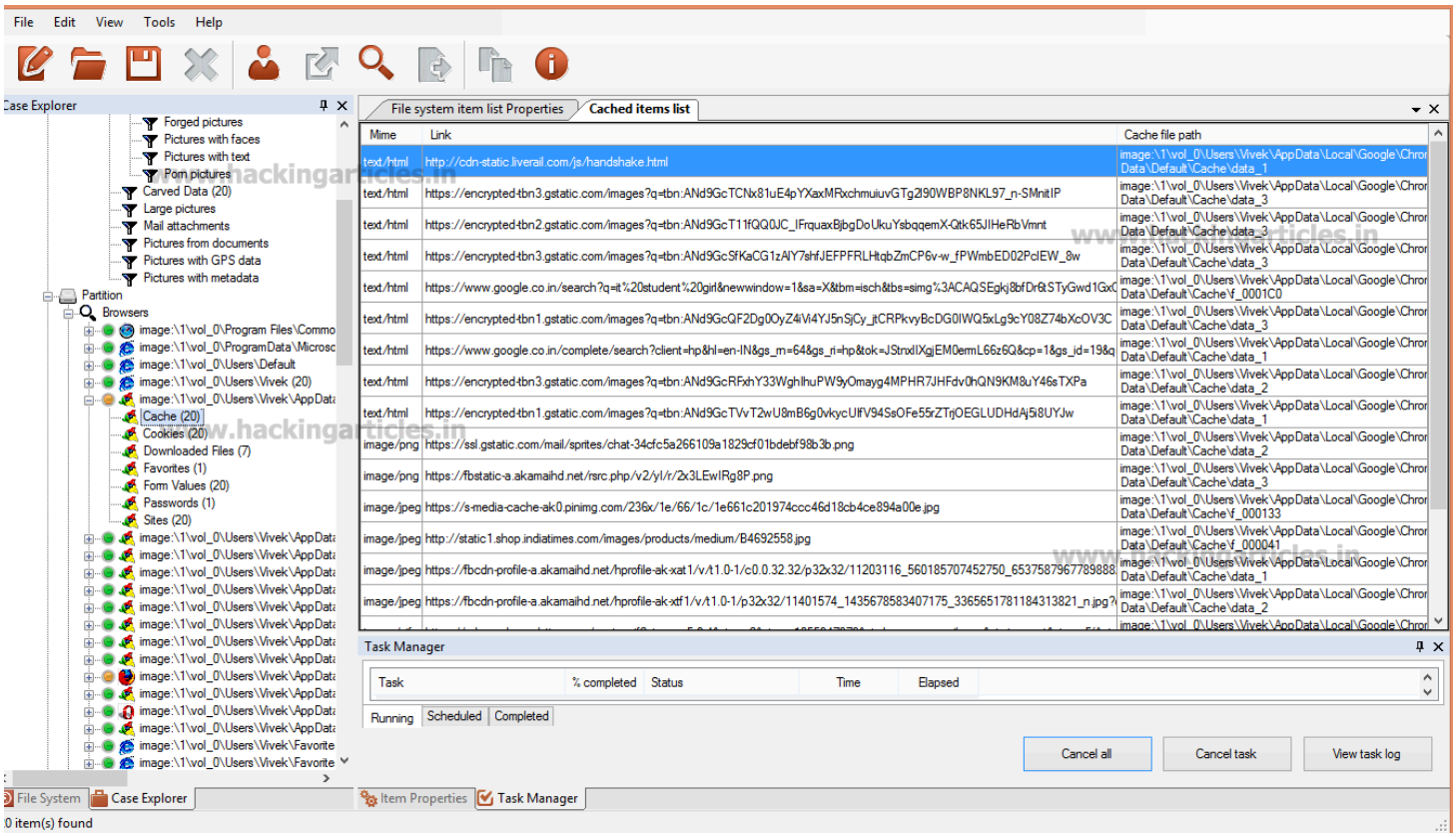
Now Select from supported data types and click on Next.



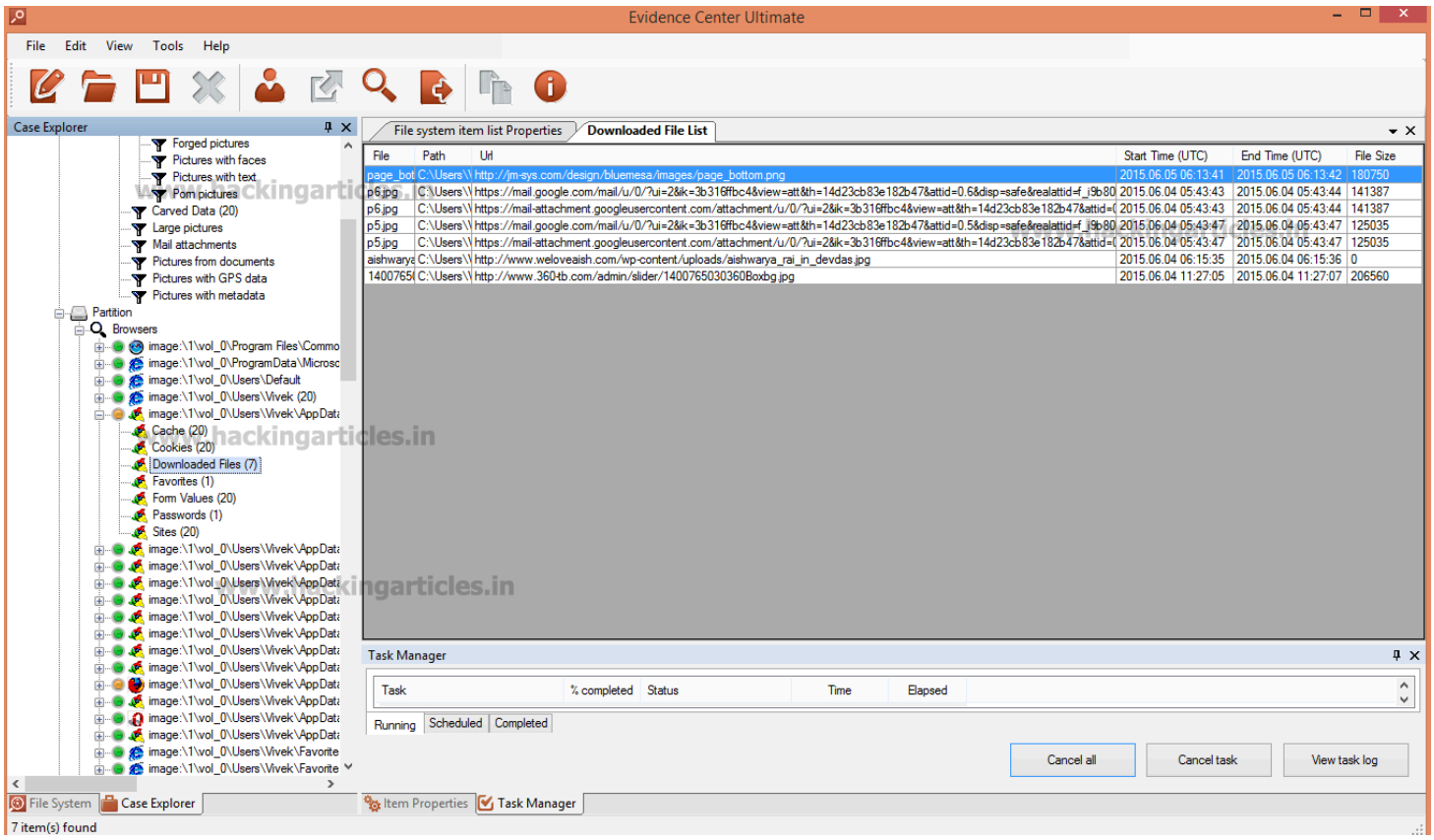
Now Select all and Click on Finish.



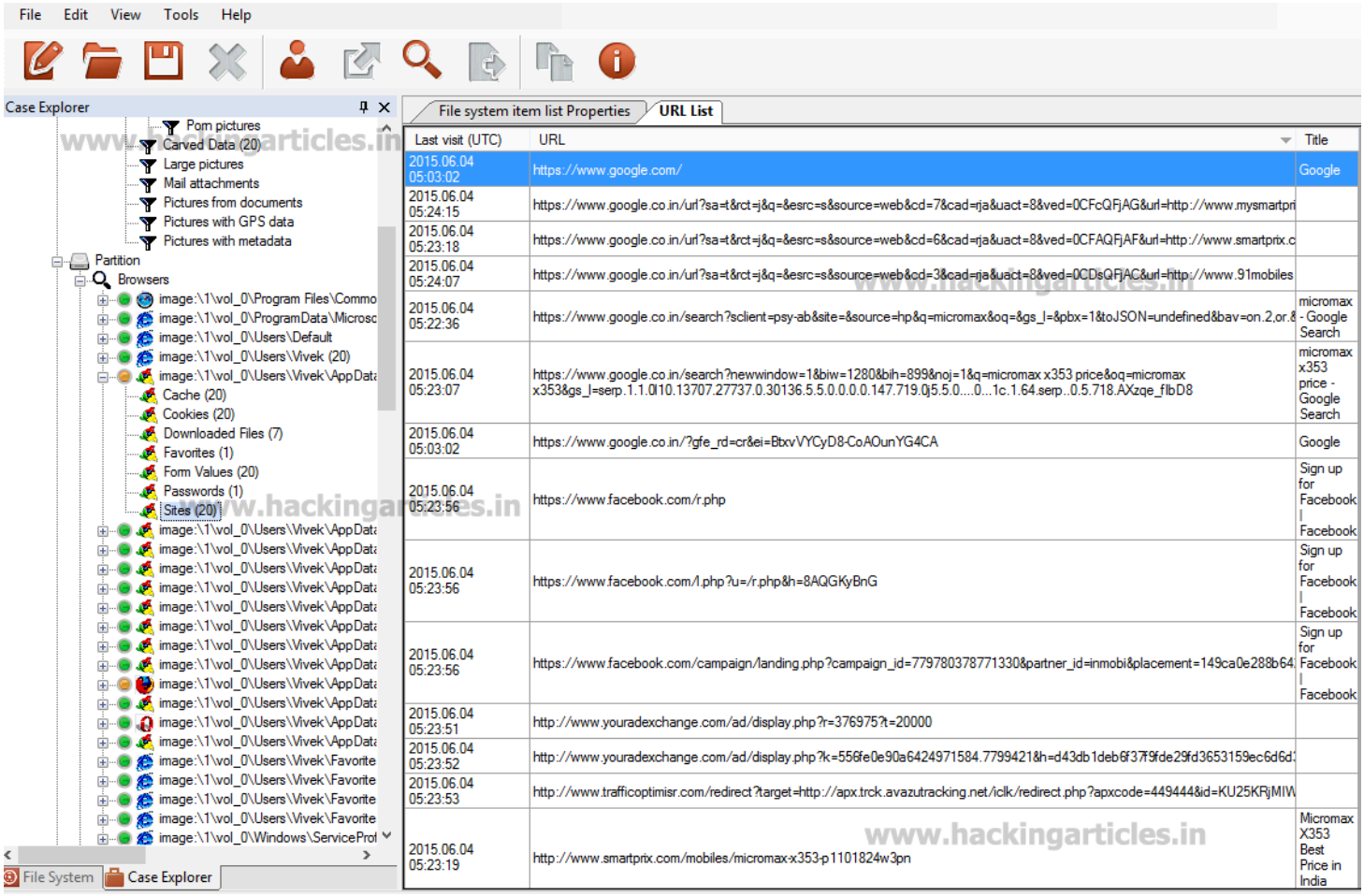
To visualize the cached sites exactly as seen by the user, Click on Cache in Browsers option.



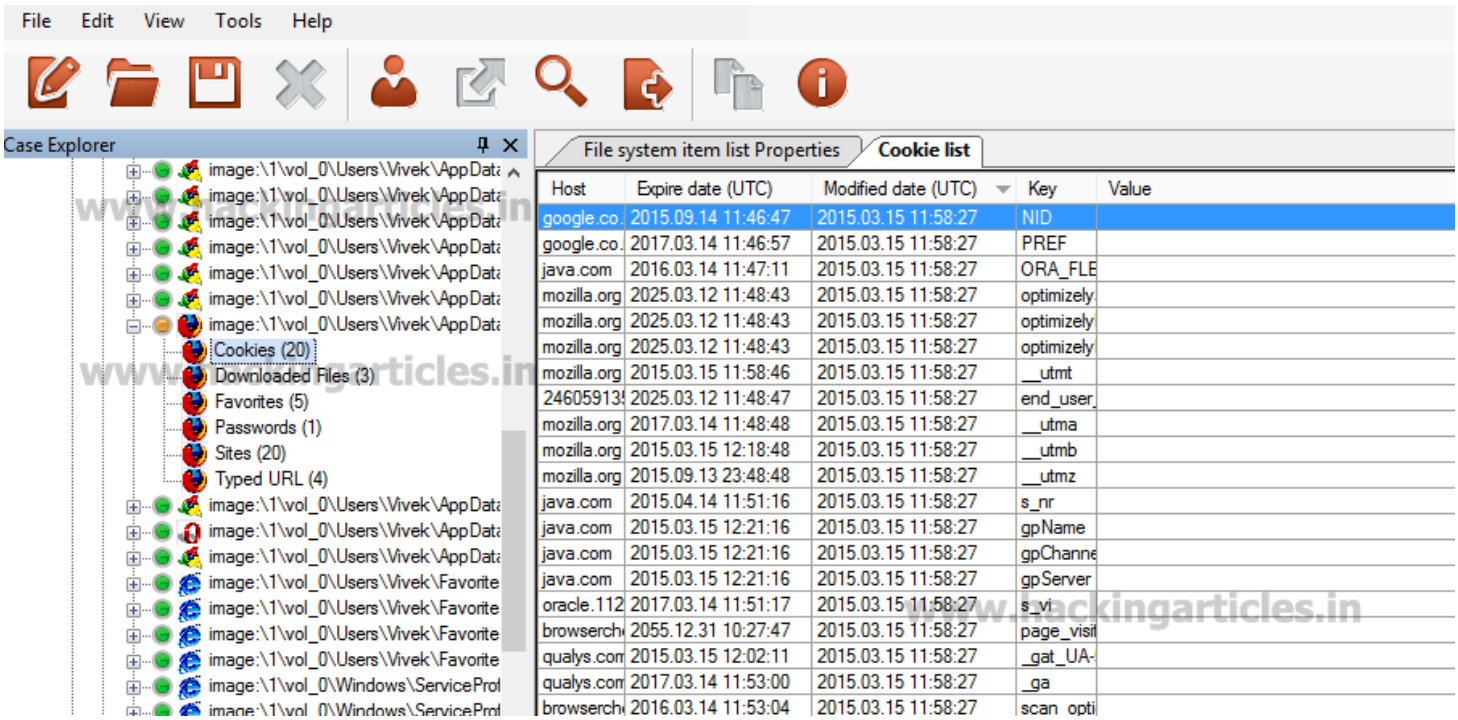
To see Downloaded file list, click on Downloaded Files.



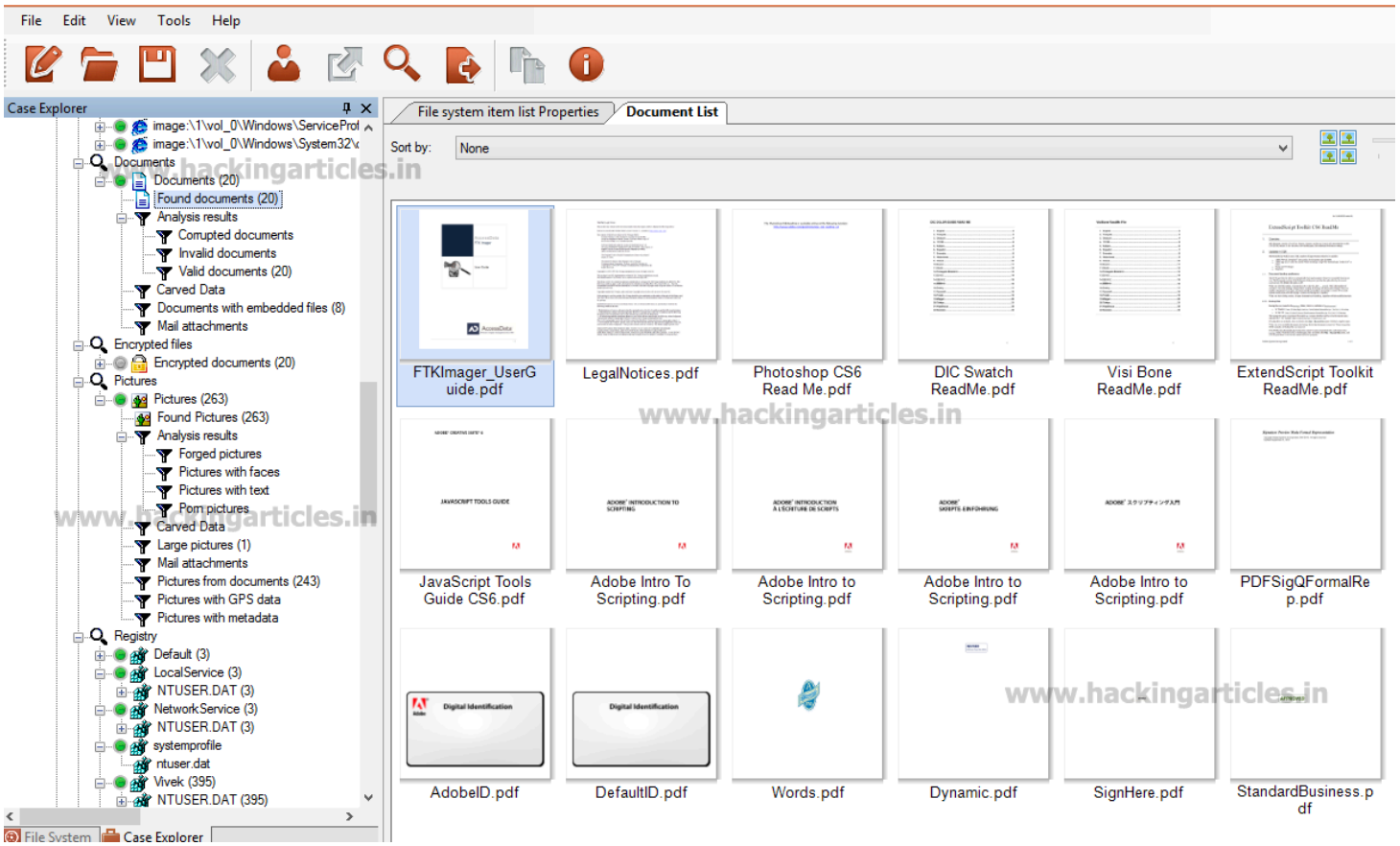
To Check the List of Sites Visited by the user, select Sites Option.



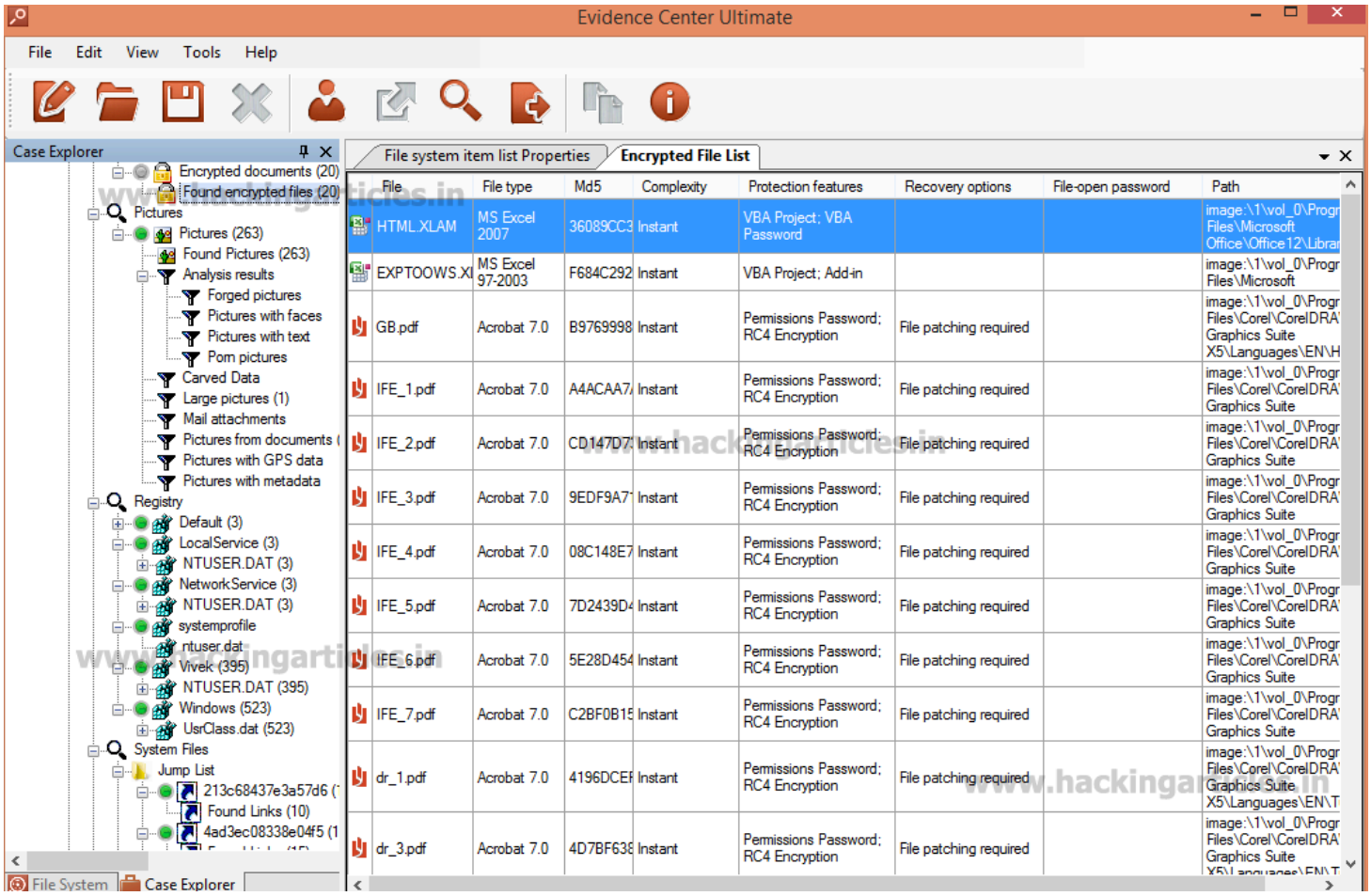
To see Cookie List, Click on Cookies Option.



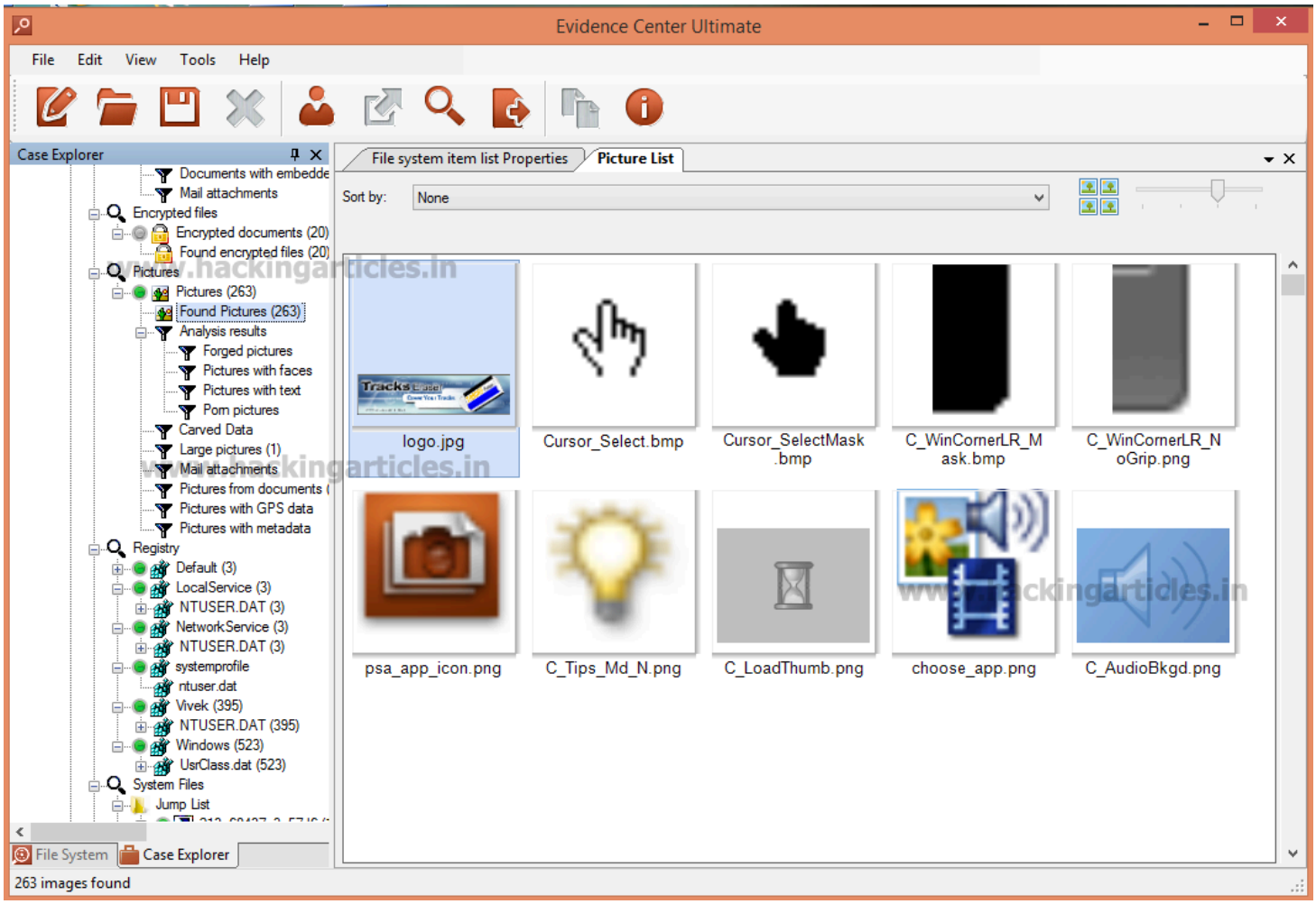
Now click on Documents option and Then Select Found Documents option to see all the office Documents files found in user pc.



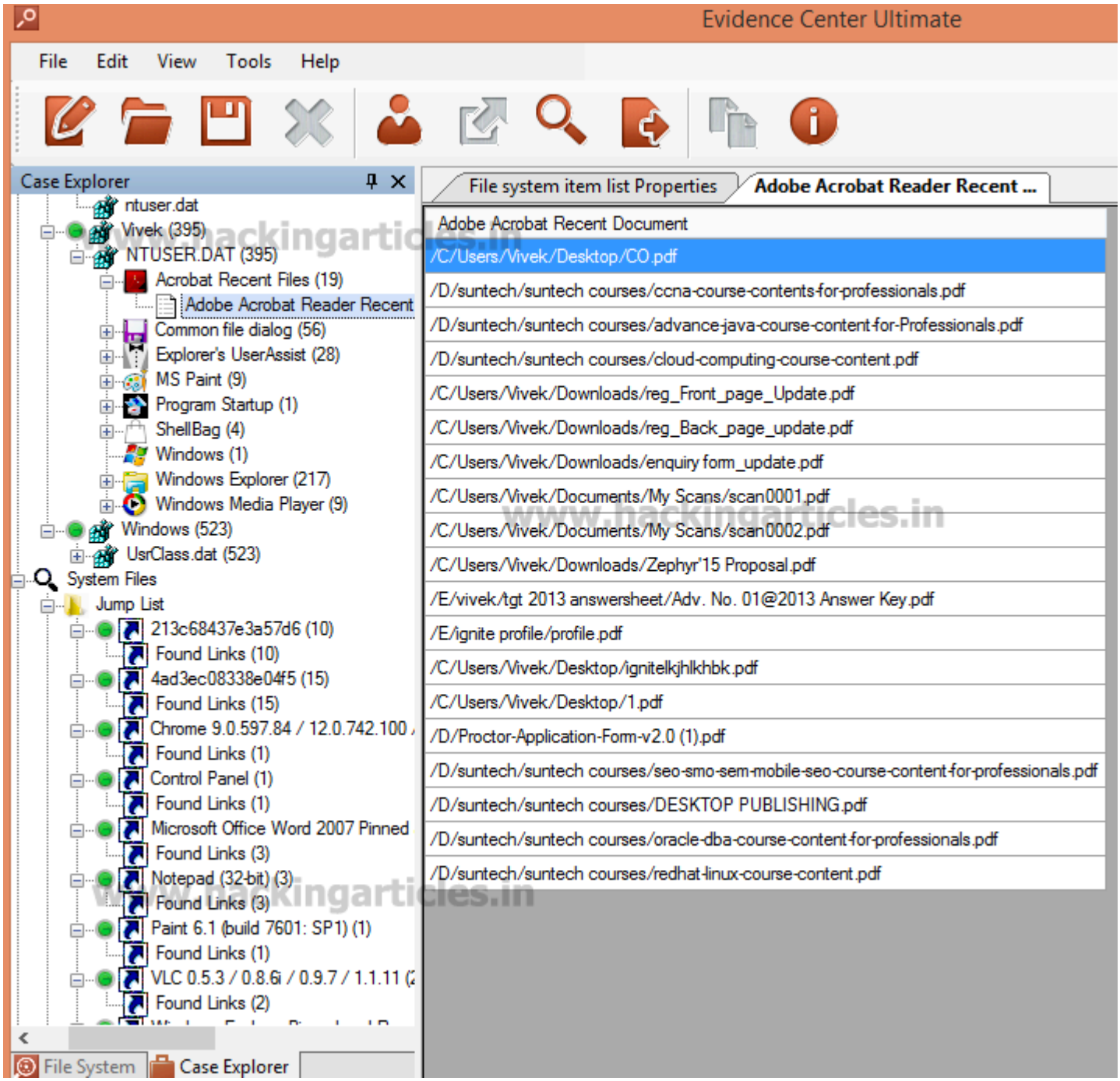
To see all the encrypted files, click on Found Encrypted files option. It will detect more than 150 types of encrypted files. It is also possible to decrypt all these encrypted files with in this product by installing Passware kit Forensic integrated with Belkasoft Product.



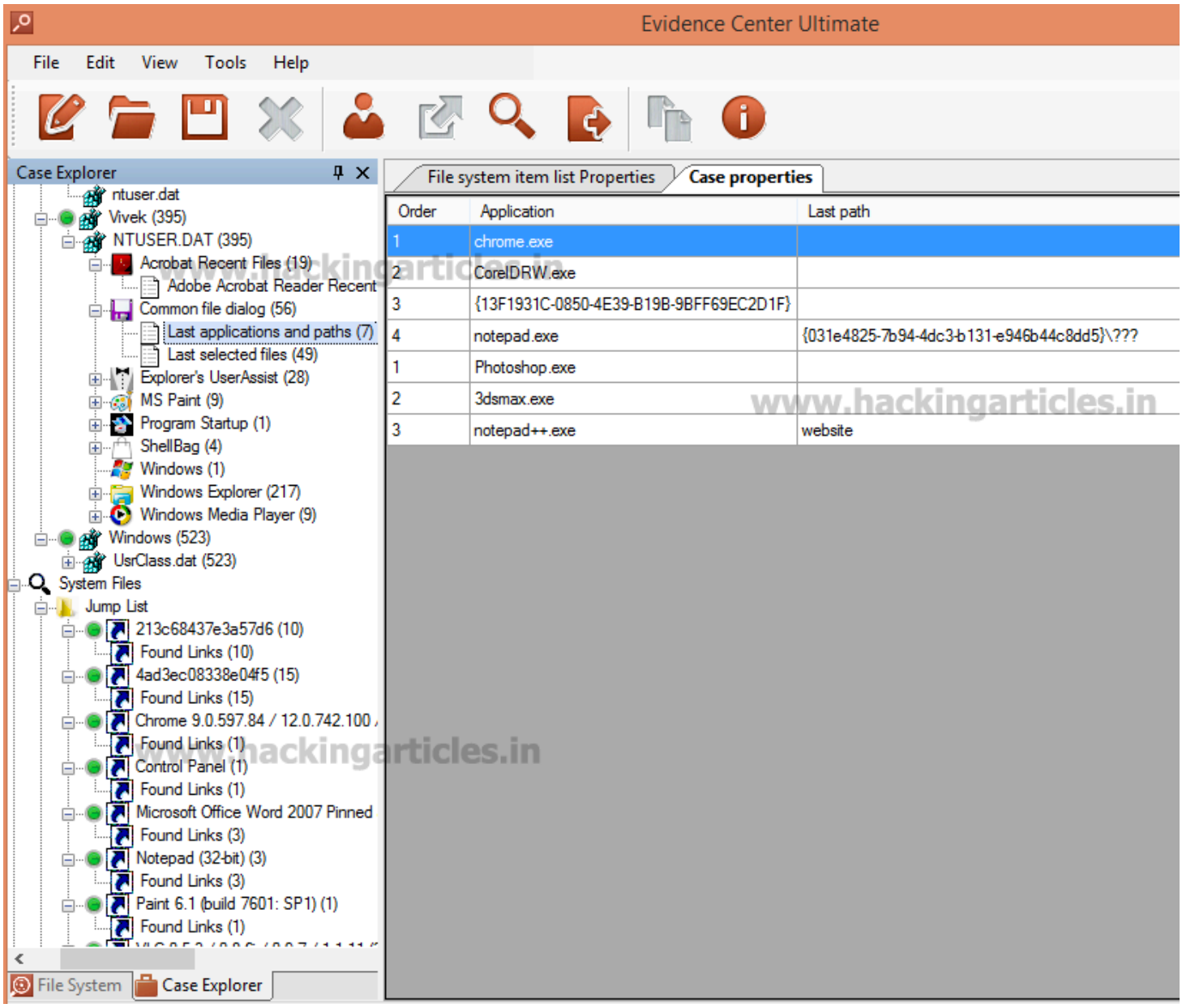
To Find Picture List, Select **Found Pictures** in **Pictures** Option. To Detect Forgery in Picture. Right click on Picture, Select **Analyze Pictures** and Click on **Detect Forgery** Tab.



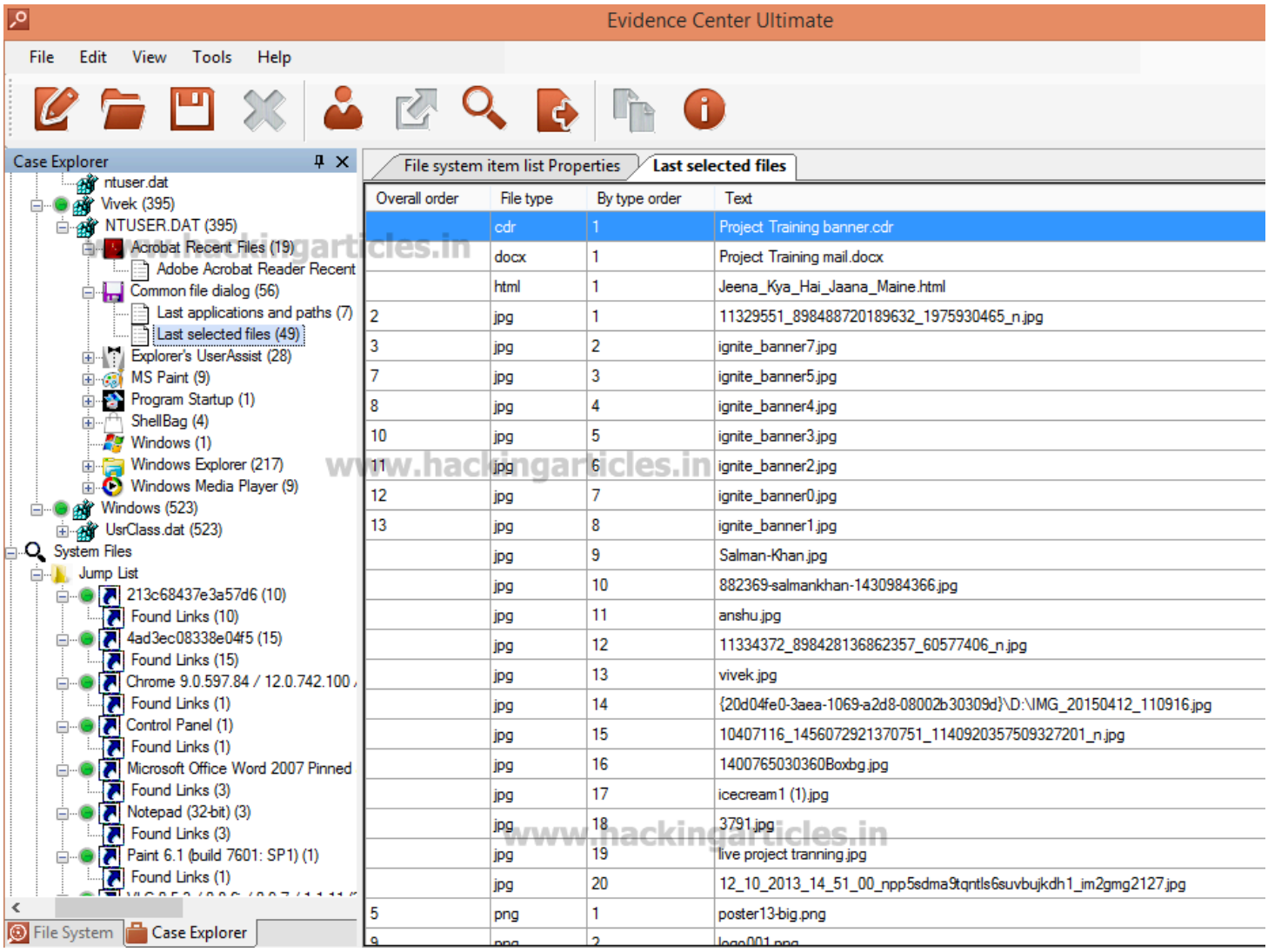
To find the recent files opened by Acrobat Reader, Click on Adobe Acrobat Reader Recent Option.



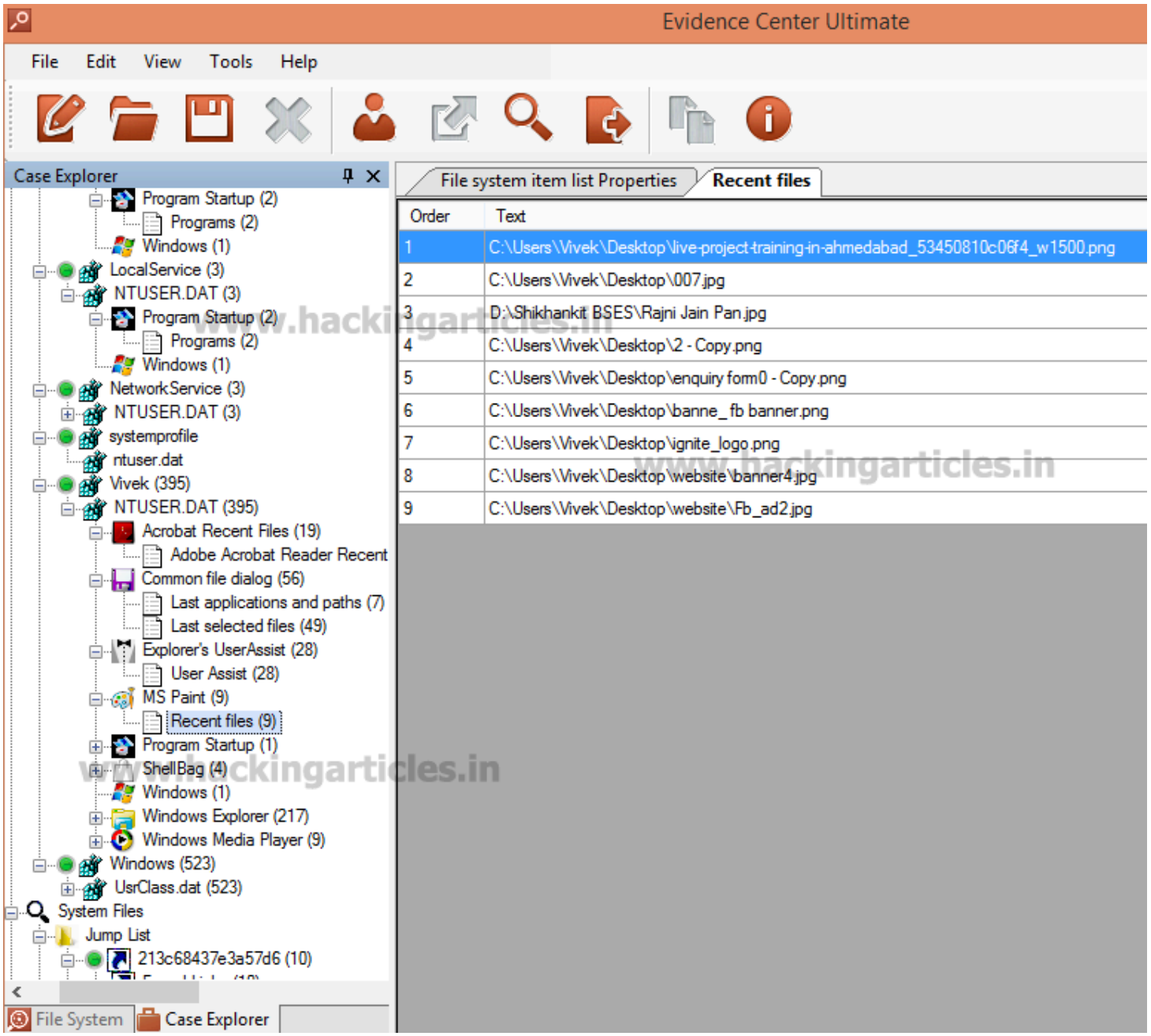
To See Recent applications run by user, Click on Last Application and Paths in NTUSER.DAT Option. NTUSER.DAT is a registry file in Windows Operating System .Every user profile contains an NTUSER.DAT file. It contains a unique Documents Folder, Start menu Configuration, Desktop properties and browsing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



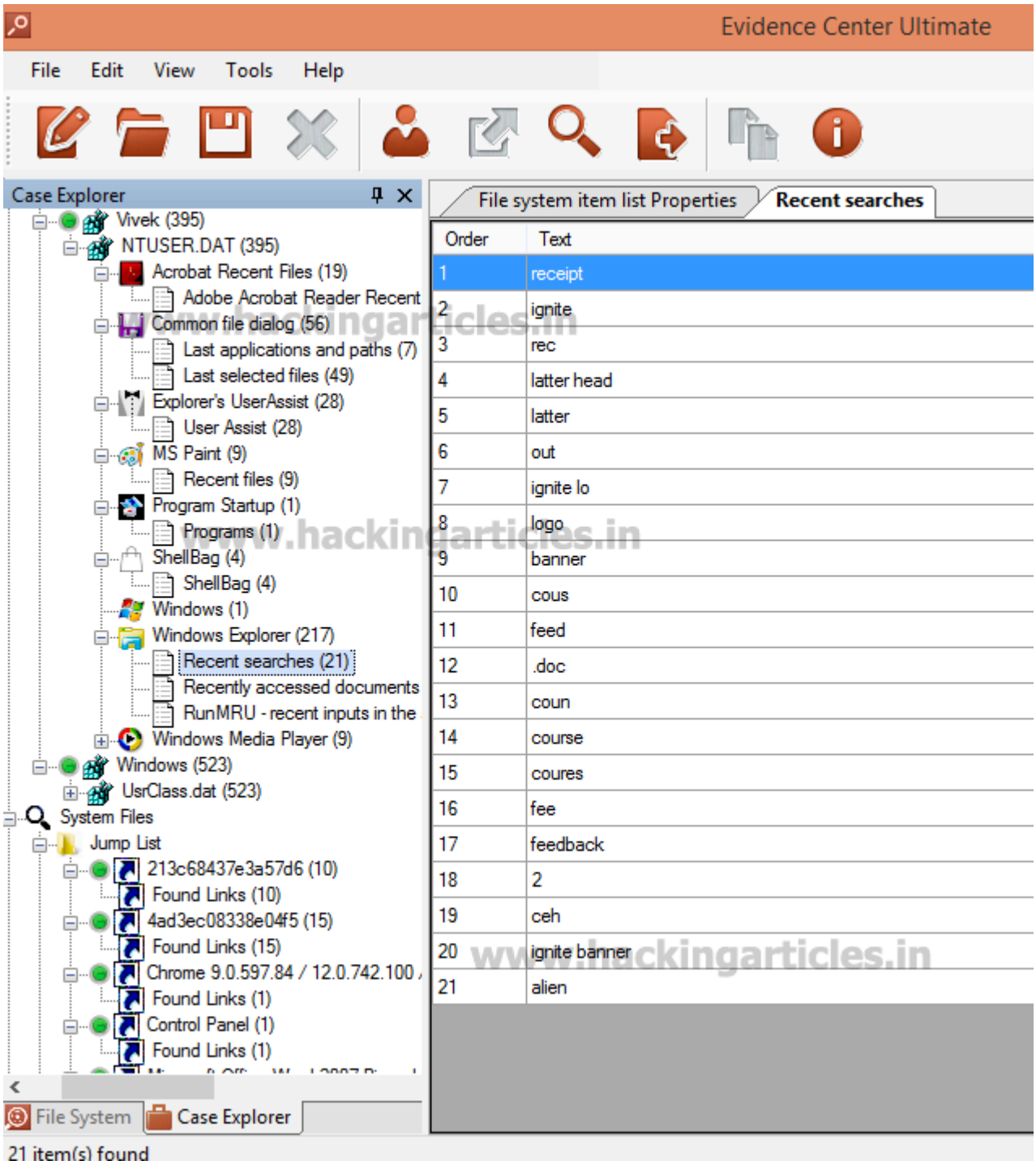
To see last Selected Files by the user, Click on Last Selected Files.



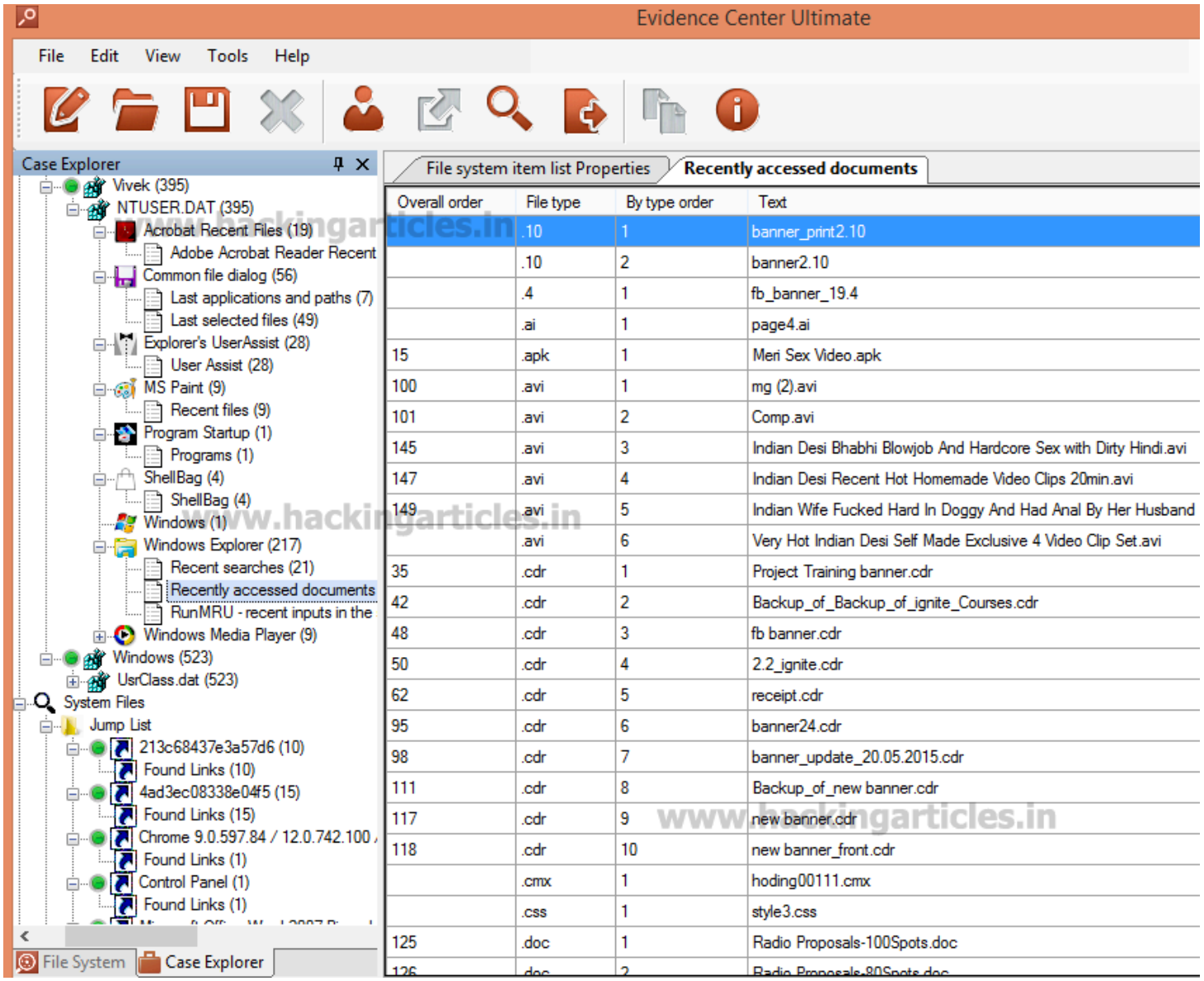
To check the recent files opened by user, Click on Recent files option.



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



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


Evidence Center Ultimate
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
Case Explorer
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
www.hackingarticles.in