

Alat za digitalnu forenzičku istragu - Thumbnail pretraživač

Dipl. ing. Uglješa Georgijević master diplomac,
e-mail: ugljesageorg@gmail.com
Doc. dr. Gojko Grubor
e-mail: ggrubor@singidunum.ac.rs

Sažetak: U ovom radu je opisan programski realizovani pomoćni alat za digitalnu forenzičku istragu - Thumbnail pretraživač. Alat se specifično koristi u fazi pretrage i pred-istražnih radnji za pretraživanje fajlova sličica, *Thumbs* .db fajlova, po čvrstom disku ispitivanog računara i za prikazivanje njihovog sadržaja.

Ključne reči: forenzički alat, pred-istražna analiza, pretraga sličica, Thumbnails pretraživač

1. Uvod

Digitalna forenzička istraga kompjuterskog kriminala podrazumeva primenu principa digitalne forenzičke nauke, upotrebu potvrđenih forenzičkih tehnika, modernih tehnologija kao i najnovijih digitalnih forenzičkih alata. Uobičajena je sledeća taksonomija alata za digitalnu forenzičku istragu, u odnosu na više različitih kriterijuma [3]:

Prema načinu implementacije na:

- hardverske alate i
- programske (softverske) alate.

Prema oblasti upotrebe na:

- alate za forenziku računarske mreže,
- alate za forenziku računarskog sistema,
- alate za analizu drugih digitalnih uređaja (npr. PDA, mobilnih telefona, itd.) i
- alate za forenziku softvera (malicioznih kodova),

Prema tipu koda, na:

- programske alate otvorenog koda (Open source) i
- licencirane programske alate.

Prema platformi na kojoj rade:

- alate koji rade na Windows platformi i
- alate koji rade na Linux i drugim platformama.

Prema fazi procesa koji obavljaju u forenzičkoj istrazi, na:

- alate za pravljenje sterilnih medijuma,
- alate za pravljenje fizičke kopije čvrstog diska (imidža, miror slike HD),
- alate za oporavak podataka,
- alate za dešifrovanje podataka (razbijanje šifara i pasvorda),
- alate za analizu digitalnog materijala i
- alate za dokumentovanje.

Jedan alat može spadati i pod više različitih grupa. U oblasti korporacijske digitalne forenzike najčešće se koriste *programski forenzički alati* za upravljanje i istragu kompjuterskog incidenta, tipično sa ciljem da će slučaj završiti na sudu, što znači sa potpunom primenom principa, tehnika i alata digitalne forenzičke nauke [2]. Opšte prihvaćeno mišljenje je da svi programski alati za digitalnu forenzičku istragu trebaju biti otvorenog koda, ali tako ne misle i proizvođači programa, jer bi tim konkurencija imala uvid u određene prednosti nekog programskog alata. Principi digitalne forenzičke nauke zahtevaju da određeni delovi programa alata treba da budu otvorenog koda, ako ne ceo program, jer se time postiže da forenzičari mogu proveriti da li program radi kako treba, da li možda pogrešno interpretira neke rezultate itd. Takođe, što više ljudi vidi kod programa, moguće je poboljšanje istog, kao i ispravka postojećih grešaka, jer, kao što je poznato, nijedan program nije bez grešaka (*bagova*). Deo koda koji treba otkriti javnosti je deo programa koji je zadužen za pravljenje *imidža* uređaja sa kojeg se vrši akvizicija dokaza, jer je ovo osnovni korak koji mora da se radi bez greške. Ukoliko se akvizicija dokaza ne obavi na pravilan način, dokazi će biti nevažeći, a samim tim i ceo slučaj može biti odbačen na sudu. Zato je od velike važnosti da neki delovi programa budu *open source*. *Open source* programski alati se ne plaćaju, većina radi na Linux platformi i obično ne pokrivaju sve oblasti digitalne forenzičke istrage, tačnije, nisu namenjeni za sve apstraktne slojeve ispitivanog uređaja. Uglavnom nemaju dobru podršku i servise. Licencirani programi se prave uglavnom za Windows platformu, imaju veći broj modula integrisanih u jedan program i samim tim pokrivaju više oblasti digitalne forenzičke istrage. Plaćaju se i nisu nimalo jeftini. I jedni i drugi mogu da se koriste u zvaničnim i korporacijskim istragama. U zavisnosti od kupljenih modula zavisi i stepen korišćenja alata kod licenciranih alata. Uprkos činjenici da su na raspolaganju brojni setovi alata, koji obezbeđuju veći komfor forenzičarima u radu, ali su često nedovoljni za izvršavanje svih zadataka, mora se koristiti više različitih, specijalizovanih alata u većini slučajeva [1].

2. Windows *Thumbnail cache*

Na Windows operativnim sistemima (od verzije Windows 98), *thumbnail cache* je fajl koji u sebi sadrži *thumbnail* (sličica-umanjena verzija originalne slike) slike za *Windows explorer thumbnail view*. Ovakav pristup skladištenja *thumbnail* slike u fajl omogućava brži prikaz *thumbnail*-ova slike koje se nalaze u folderu, jer ne moraju da se prerađuju svaki put kada korisnik pristupi nekom folderu koji sadrži slike.

Windows smešta *thumbnail*-ove grafičkih fajlova i određenih dokumenata, kao i filmova u *Thumbnail Cache* fajl, uključujući i sledeće formate: JPEG, BMP, GIF, PNG, TIFF, AVI, PDF, PPT i HTML.

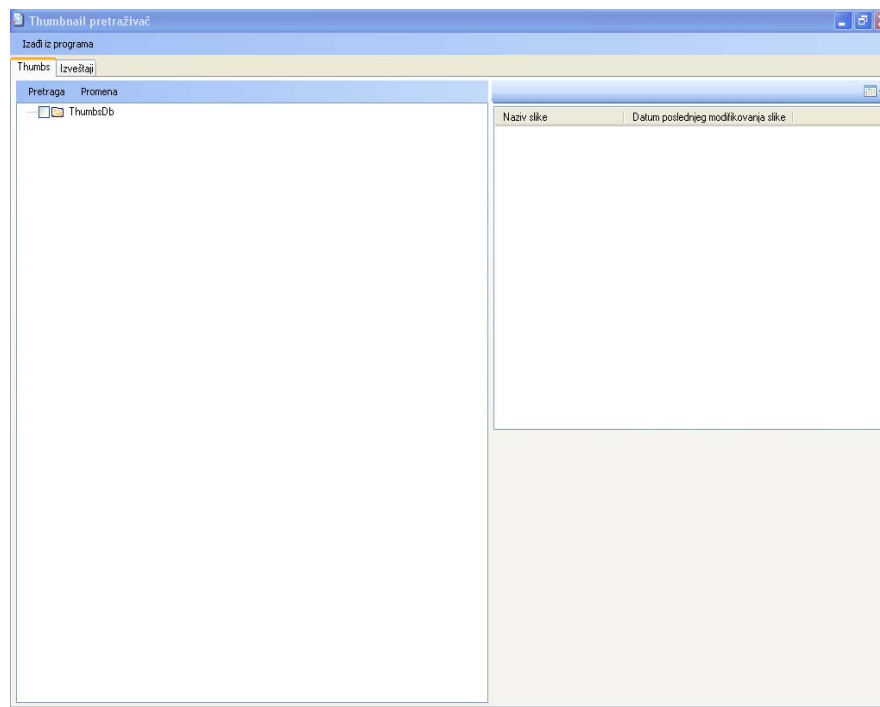
2.1. *Thumbs.db*

Thumbs.db fajlovi su smešteni u svaki direktorijum koji sadrži slike ili filmove na *Microsoft Windows NT* verzijama operativnih sistema pre *Viste*. Operativni sistem kreira fajl lokalno. Za svaku sliku koja se nalazi u direktorijumu pravi se njena umanjena kopija koja se smešta u *Thumbs.db* fajl kao mali JPEG fajl, bez obzira na format slike koje se nalaze u direktorijumu [4]. Ove slike se smanjuju na maksimalno 96×96 *pixels*, ili na proporcionalnu minijaturu njihovog originalnog oblika (ovo je kod slike koje nisu kvadratnog oblika) sa 96 *pixels* na dužoj strani. Svaki folder u kojem su fajlovi prikazani kao *Thumbnails* ili *Filmstrip* u *Windows Exploreru* sadržaće i *Thumbs.db* fajl. *Thumbs.db* fajl je “*OLE Compound Document format*” [5]. Ovaj format koriste mnogi Microsoft Office proizvodi.

3. Funkcionalnosti *Thumbnail* pretraživača

Neki forenzički digitalni alati ne poseduju modul za pregledanje *thumbs.db* fajlova tj. njihovog sadržaja. *ThumbnailViewer* je napravljen kao dodatna (pomoćna) alatka tim forenzičkim alatima. *ThumbnailViewer* pronalazi sve *thumbs.db* fajlove koji se nalaze na kompjuteru, a ima mogućnost pretrage samo određenih delova kompjutera, kao i prikazivanje sadržaja pojedinačnog *thumbs.db* fajla.

Početni ekran *Thumbnails* pretraživača

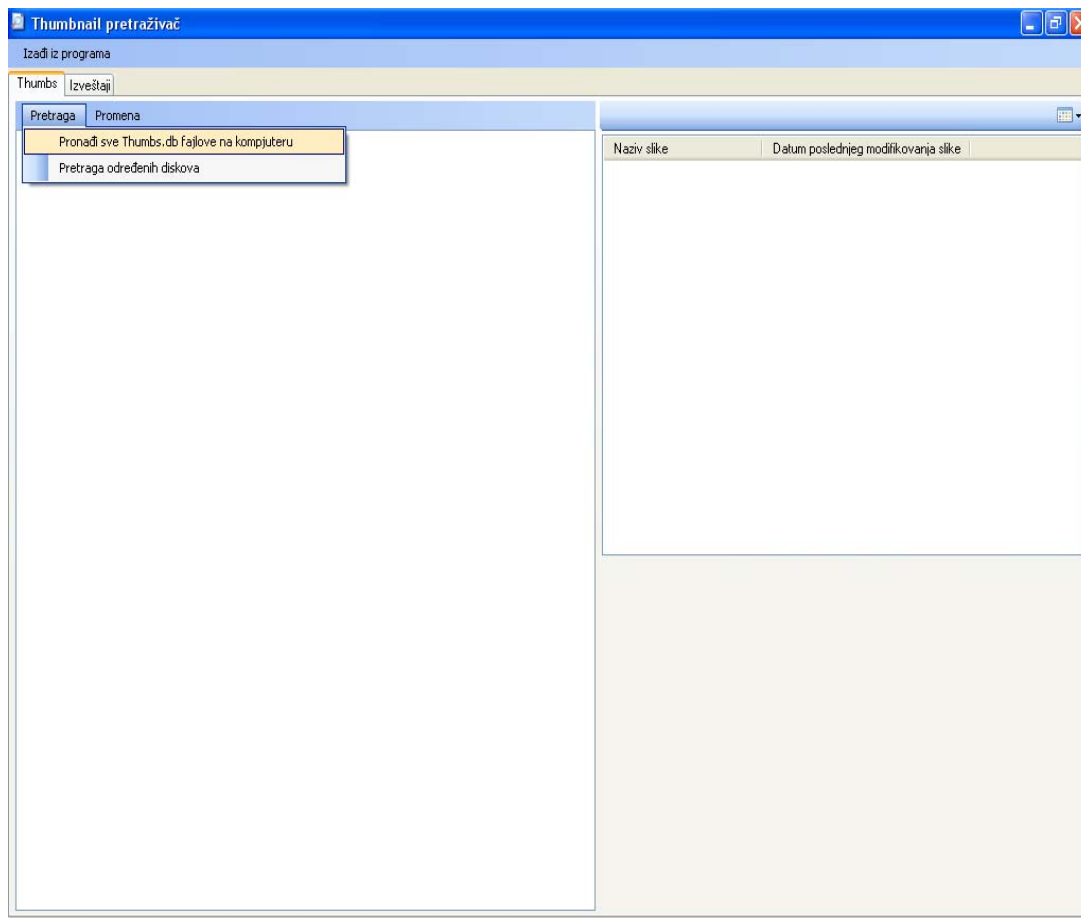


3.1. Osnovne funkcionalnosti *Thumbnails* pretraživača

Izborom opcije **pretraga** prikazuje se padajući meni u kojem se mogu izabrati 2 vrste pretrage:

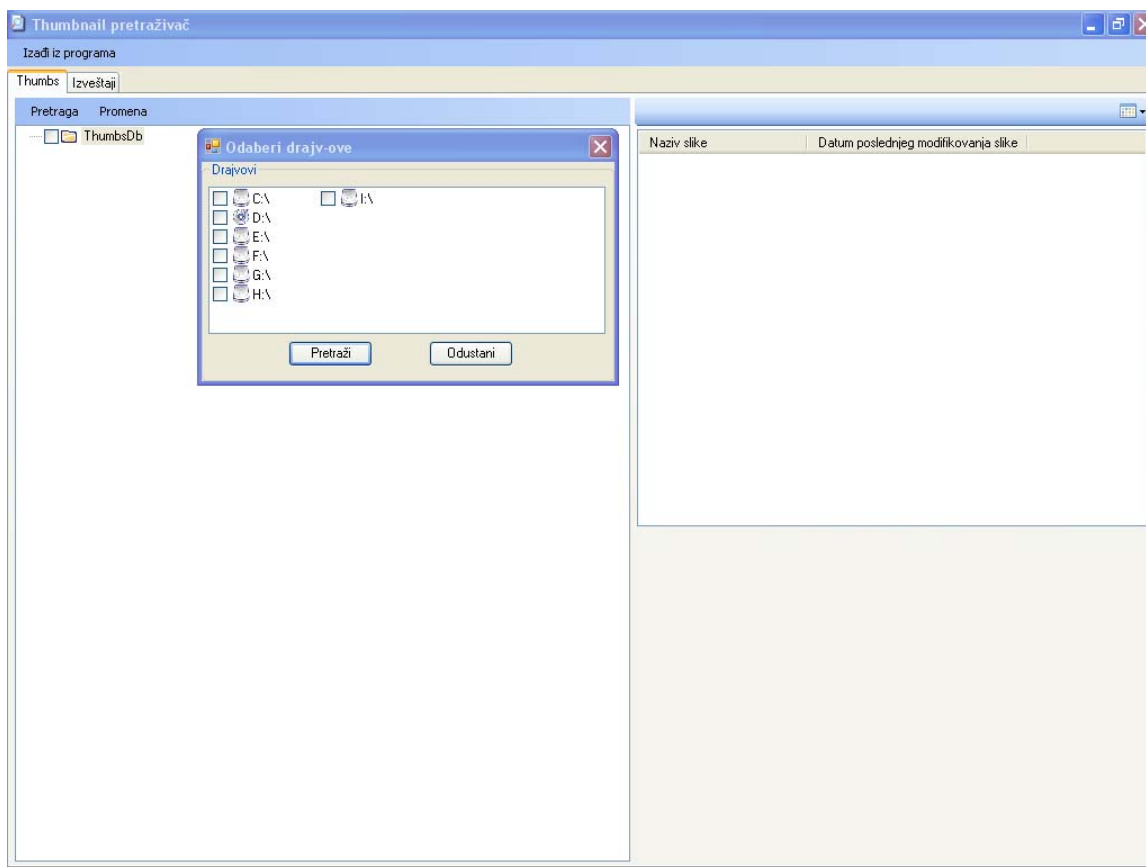
1. pretraga celog računara, svih HD, CD-ova, USB-uređaja koji su prikačeni na računar ili
2. pretraga određenih delova računara.

Pretraga svih uređaja iz računara prikazana je na slici 1.



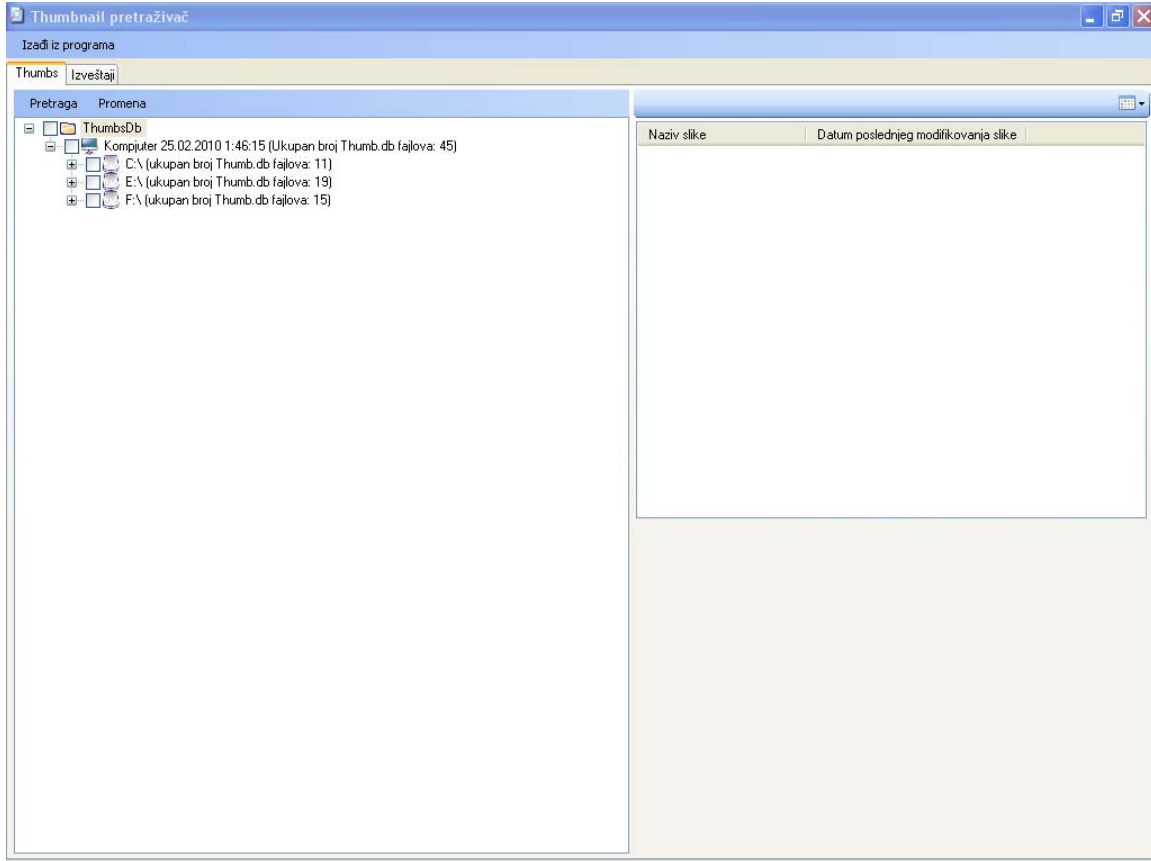
Sl.1. Pretraga celog računara

Pretraga izabranih uređaja iz računara prikazana je na slici 2.



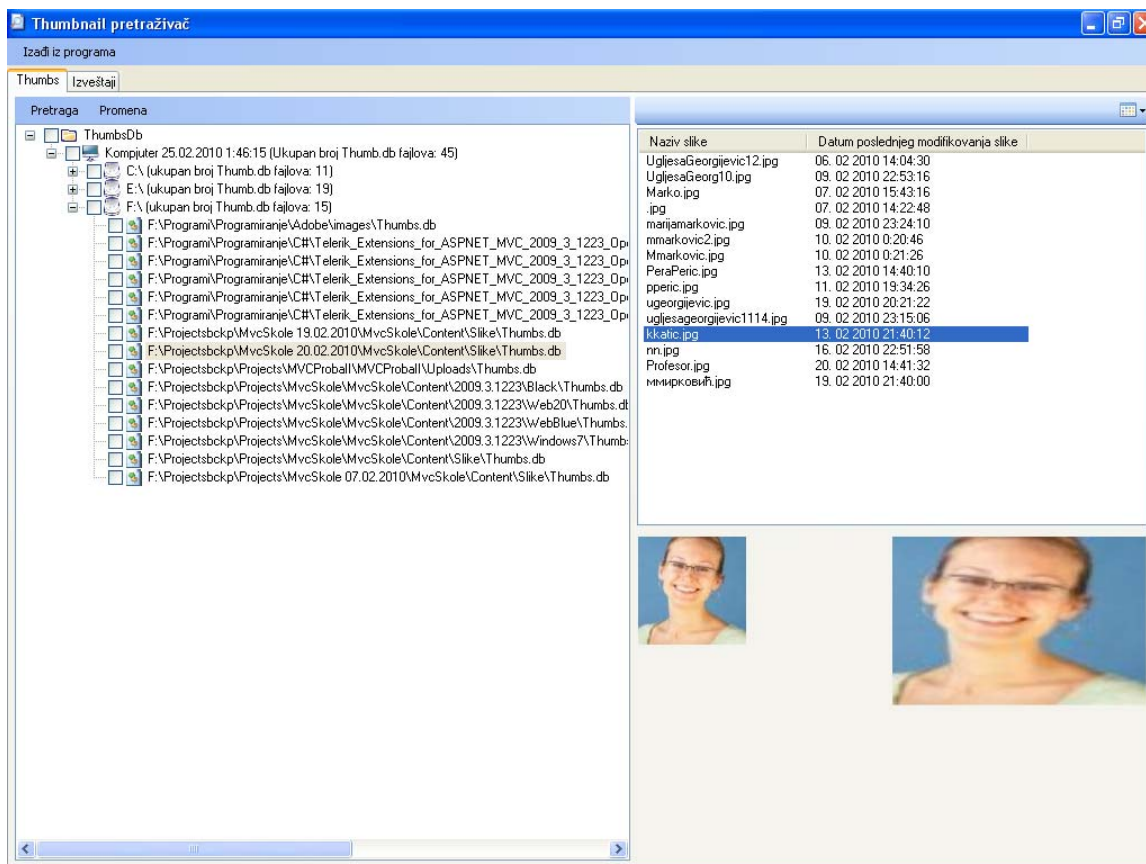
Sl.2. Pretraga izabranih uređaja iz računara

Posle izabranih opcija sledi prikaz pretrage (slika 3.):



Sl.3. Prikaz pretrage

Prikazuju se datum i vreme pretrage, ukupan broj pronađenih *thumbs.db* fajlova i uređaji koji su pronađeni i koliko u kojem od njih ima *thumbs.db* fajlova. Odabirom diska prikazuju se svi *thumbs.db* fajlovi na tom disku (putanje fajlova). Odabirom nekog *thumbs.db* fajla prikazuje se sadržaj tog fajla u desnom prozoru programa. Prikazuje se naziv fajla i vreme kada je fajl poslednji put bio modifikovan, a u donjem desnom delu prozora prikazuje se *thumbnail* slika kao i njena uvećana verzija (slika 4.).



Sl.4. Prikaz thumbnail slike i njene uvećane verzije

Na osnovu prikaza svih slika sa izabranog, istraživanog medija, forenzičar može izvršiti selektivnu sliku koje podržavaju osnovanu sumnju za istragu (npr., dečije pornografije, terorističkih aktivnosti itd.). Ovom operacijom forenzičar bitno smanjuje vreme analize imidža, kao i zahtevanu veću procesorsku snagu za analizu *thumbnails*.

4. Zaključak

Neki alati za digitalnu forenzičku istragu ne poseduju opciju za pregledanje sadržaja *Thumbs.db* fajlova (X-Way,...).

Thumbnail pretraživač je alatka koja može da se koristi u korelaciji sa alatima za digitalnu forenzičku istragu koji nemaju opciju čitanja sadržaja *Thumbs.db* fajlova, a može da se koristi i kao specijalizovan alat, jer ima ugrađene mehanizme pretrage svih uređaja (HDD,CD,USB...) na računaru.

Postoje i drugi alati koji pretražuju *Thumbs.db* fajlove, neki su komercijalni (20-40\$), a neki besplatni. Ovaj alat je napravljen kao deo šireg projekta poboljšanja funkcionalnosti raspoloživih forenzičkih alata.

5. Literatura

1. Bunting, S., Wei, W., Encase Certified Examiner Study Guide, WileyPublishing 2006.
2. Grance, T., Chevalier, S., Kent, K., Dang, H., *Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response*, National Institute of Standards and Technolog, 2007.
3. Milosavljević, M., Grubor, G., *Istraga kompjuterskog kriminala – metodološko tehnološke osnove*, Univerzitet Singidunum, 2009.

Internet izvori:

1. <http://www.forensicswiki.org/wiki/Thumbs.db>
2. http://www.forensicswiki.org/wiki/OLE_Compound_File

Digital Investigation Tool - Thumbnail Viewer

Abstract

This paper describes designed programm of the Thumbnail Viewer, a tool for digital forensic investigation. This tool is specificaly designed to search Thumbs.db files and show their contents in a prewiev of HD investigated computer.

Key words: *forensic tool, pre-investigation analysis, Thumbnails search, Thumbnails viewer*