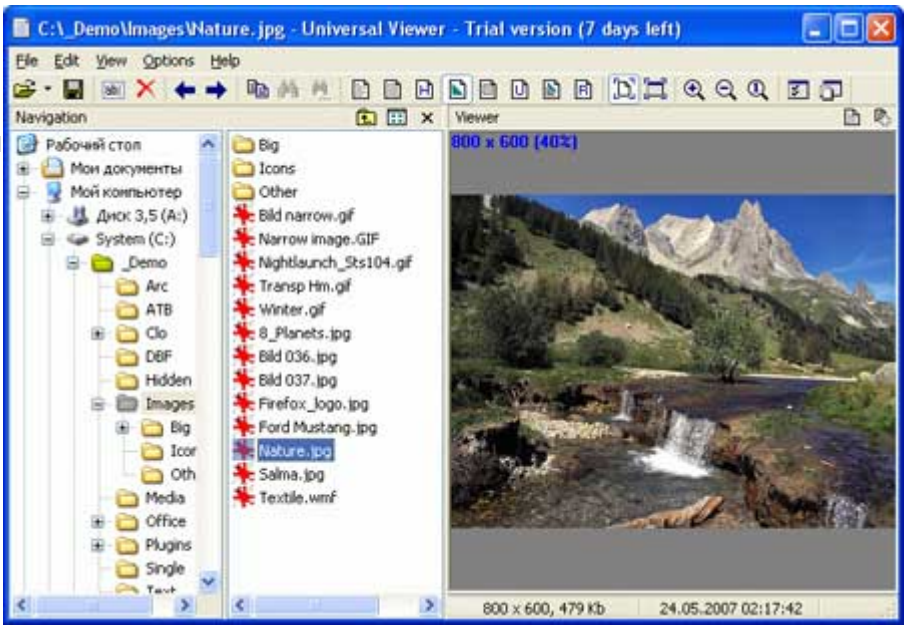
Analiza dokaza

Postupak analize dokaza je dijelom znanost, a dijelom umjetnost. Istražitelj treba razviti osjećaj za analizu, otkud početi i što tražiti. S druge strane, potrebno je poznavanje operacijskog sustava kojeg se istražuje. Što se tiče samog pregledavanja podataka, postoje mnogi alati koji će obaviti posao. Slijedi pregled tipova alata koji se koriste u procesu računalne forenzike.

`Most computer forensics tool sets include utilities that create device copies and calculate checksums where appropriate. If you are using the Unix operating system, you can obtain and use the md5sum utility to calculate checksums.`

File viewers



Preglednici datoteka prikazuju malu sliku sadržaja datoteke. Ovaj tip programa radi tako da skenira mapu za datoteke koje odgovaraju traženom kriteriju i prikazuju malu sliku sadržaja. Iako ih većina radi tako da gleda samo ekstenzije datoteka, neki od sofisticiranijih alata gledaju i zaglavlje datoteke (saznaj više o važnosti zaglavlja). Preglednici datoteka mogu biti korisni u situaciji gdje istražitelj treba pretražiti puno slika da bi pronašao inkriminirajuće dokaze.

Extension checkers

Ovaj tip alata provjerava poklapaju li se ekstenzija i zaglavlje datoteke. U slučaju kad počinitelj želi sakriti neku sliku, npr. `oblak.jpg`, mogao bi promijeniti ekstenziju tako da istražitelj u mapi vidi `oblak.wav` ili pak nešto posve besmisleno kao npr. `iR3.544`. Neovisno o tome kako je ekstenzija promijenjena, ukoliko je zaglavlje datoteke netaknuto ovaj alat će dojaviti nepodudarnost.

Unerase tools

Jednostavni alati za povratak izbrisanih datoteka postoje od početka DOS-a i Windowsa. Noviji operacijski sustavi kompliciraju postupak povraćanja podataka.

Alati za pretraživanje

Forenzički istražitelji često trebaju proći kroz veliki broj datoteka tražeći određene ključne riječi ili izraze. U takvim slučajevima dobro dođu alati koji će uštedjeti istražitelju vrijeme i stres.