Čuvanje dokaza

- **SLIKA SUSTAVA**
  Kako bi istražitelj mogao “kopati” po podacima na preuzetim medijima, a ipak na sudu mogao dokazati da nije ništa promijenio, potrebno je napraviti “sliku” sustava. To se može postići računanjem *hash* vrijednosti. *Hash* algoritam nepovratno stvara sažetak fiksne duljine (ovisno o tipu algoritma). Ako istražitelj napravi jedan sažetak sustava prije nego što poduzme išta drugo te jedan nakon analize, može dokazati da ništa nije promijenjeno (ako su sažeci jednaki).

- **WRITE BLOCKERS**
  Kako bi spriječio slučajno mijenjanje podataka, istražitelj može koristiti *write-blocking* uređaj prilikom analize sustava. Može birati između softverskog i hardverskog rješenja. Softverski, onemogućava se operacijski sustav od pisanja na medij. Hardverski, fizički se onesposobljava kabel koji prenosi instrukcije pisanja. Drugu opciju je lakše opravdati na sudu.
  Ako se ne može koristiti ni jedno od dva spomenuta rješenja, medij se može *mountati* u *read-only* načinu. U tom slučaju je potrebno u detalje opisati korištene postupke i opcije kako bi se na sudu moglo dokazati da nije bilo dopušteno pisanje na disk.

- **OČUVANJE STANJA DOKAZA**
  Nakon *mountanja* istraživanog medija, prvi korak je računanje MD5 *hash* sažetka. To pruža referentnu točku inicijalnog stanja medija. Drugi korak je *bit-by-bit* kopija medija. Sve daljnje akcije će biti obavljane na kopiji medija, ne na originalu. Nakon toga je original potrebno pohraniti na sigurno mjesto.

  ```
  Take extra precautions to protect the original media and the initial
  hash. You will need both at the time of trial so that you can ensure
  that evidence you find is admissible. Even if your investigation does
  not lead to court, being able to prove that your activities made no
  changes to a disk drive is extremely helpful. You'll need the initial
  hash to prove such a claim.
  ```