Forenzika podataka

Istražitelj ovdje pokušava pronaći, spasiti ili rekonstruirati što više podataka može. Istražuju se:

- Izbrisane datoteke
  - u košu za smeće (eng. *Recycle Bin*),
  - u *cache* memoriji,
  - u nedodijeljenom prostoru (eng. *unallocated space*) – to je prostor koji se smatra slobodnim za pohranjivanje novih datoteka iako možda nije prazan (formatiran) nego sadrži izbrisane datoteke preko kojih će se pisati novi podaci,
  - u neiskorištenom prostoru pojedinih klastera (eng. *slack space*) – s obzirom da postoji minimalna veličina klastera (za Windows XP – 7 NTFS je to 4 KB), u slučaju kad je datoteka manja od klastera, preostali prostor se smatra neiskorištenim i može sadržavati stare izbrisane datoteke.
- Nedostupni prostor
  Svaki medij ima određen prostor kojem operacijski sustav ne može pristupiti (zato npr. USB stick od 8GB ima iskoristiv prostor od 7.4GB). Taj se prostor obično nalazi na fizičkom kraju uređaja i može mu se pristupiti jedino pomoću heksadecimalnog uređivača (eng. *hex editor*).
- Radna memorija (RAM)
  Ukoliko je računalo nad kojim se provodi istraživanje upaljeno pri dolasku istražitelja, bitno je prvo uzeti sliku radne memorije (eng. *image file*) da se ne izgube privremeni podaci koji mogu odati sve što je korisnik radio od zadnjeg paljenja računala.
- Windows registri (eng. *Registry*)
  - Informacije o lozinkama,
  - podaci o programima koji se pokredu prilikom uključivanja računala (eng. *startup application*),
  - popis trenutno i ranije priključenih uređaja (eng. *storage devices*),
  - SSID (identifikatori) bežičnih mreža na koje se računalo spajalo,
  - informacije o unesenim URL adresama i o lokacijama gdje su preuzimane datoteke (eng. *download path*),
  - broj nepročitanih e-mail poruka na korisnikovom e-mail računu.