Forenzika dokumenata

Prilikom forenzičke analize dokumenata, istražitelj obraća pažnju na metapodatke dokumenta te na povezanost zaglavlja i ekstenzije. Tek kad se dovrši analiza nad svim tim podacima se može reći da je neki dokument uistinu ono što korisnik tvrdi da jest, te da ništa ne skriva.

Metapodaci

Metapodaci, odnosno „podaci o podacima“ su bitan izvor informacija. Sadrže podatke kao što su:

- Autor,
- organizacija,
- revizije - uz dnevnik revizija (eng. *log*), mogu biti pohranjeni i autori prethodnih revizija i lokacija na kojoj je datoteka bila pohranjena,
- prethodni autori,
- korišteni predložak (eng. *template*),
- naziv računala na kojem je datoteka stvorena,
- tvrdi disk i lokaciju (eng. *path*),
- ime mrežnog poslužitelja ako je datoteka bila pohranjena na poslužitelju,
- vrijeme trajanja obrade,
- izbrisani tekst,
- Visual Basic objekti,
- vremenske oznake, ovisne o vremenskim oznakama na OS-u – uključuju trenutke stvaranja, pristupa i promjena dokumenta (CAM - *Create, Access, Modify*),
- podaci o vremenu ispisivanja (eng. *printed*).

Na slici ispod je prikazan primjer metapodataka MS Word dokumenta u stvaranju. Kako prilikom razmjene dokumenata na webu korisnik ne bi slao i metapodatke (iz sigurnosnih razloga), mogu se koristiti razni alati (npr. iScrub) koji „čiste“ dokumente od metapodataka.

Zaglavlja i ekstenzije dokumenata

Osim metapodataka, bitno je obratiti pažnju na to da ekstenzija i zaglavlje dokumenta odgovaraju jedno drugome (svaki tip dokumenta ima točno određeno zaglavlje). Ako bi, na primjer, korisnik htio sakriti sliku (ekstenzija .JPEG) koja bi ga mogla inkriminirati (npr. optužen je zbog pregledavanja dječje pornografije), on može promijeniti ekstenziju datoteke .JPEG u .MP3. Na taj način istražitelj prilikom površne pretrage može isključiti taj dokument kao nebitan ako filtrira podatke po ekstenziji. No zaglavlje dokumenta još uvijek odgovara .JPEG dokumentu te se on još uvijek može otvoriti alatom za uređivanje slika. Postoje forenzički programi koji uspoređuju ekstenziju sa zaglavljem i javljaju ako je došlo do diskrepancije. No čak i kad zaglavlje i ekstenzija odgovaraju jedno drugome, ne znači da korisnik nije izmijenio oboje kako bi sakrio datoteku istražitelju „pod nosom“. Ako se takva datoteka pokuša otvoriti, računalo će javiti da je došlo do greške. U tom trenutku istražitelj mora znati koje zaglavlje treba ubaciti u dokument da bi ga mogao otvoriti (standardna zaglavlja se mogu pronaći na Internetu). Uz to, istražitelj treba obratiti pažnju na dokumente koji su otvarani i mijenjani nedavno ili relativno često.