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.

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.

Mrežna forenzika

Mrežna forenzika uključuje analizu mrežne opreme kao što su usmjeritelji, preklopnici (eng. *switch*), koncentratori (eng. *hub*), NIC (eng. *Network Interface Card*), samo računalo te razni mediji poput parica, optičkih kablova i sl. Konkretni podaci se mogu naći na sljedećim uređajima:

- Računalo domaćin (eng. *host*)
  Riječ je o “standardnom” prikupljanju podataka. Obuhvaća slike (eng. *image*) uređaja za pohranjivanje, sadržaj radne memorije i bilo kakve statičke podatke unutar dohvata računala koji se mogu slati preko mreže. Tu se ne broje samo pojedina računala već i svi poslužitelji na mreži (e-mail, datotečni, s bazama podataka, poslužitelji pisača)

- Usmjeritelj (eng. *router*)
  Usmjeriteljski zapisi mogu sadržavati greške do kojih je došlo tijekom usmjeravanja, detalje o komponentama usmjeritelja (npr. sučelja) te sumnjive aktivnosti (ovisno o postavkama zapisa). Osim toga, usmjeritelji čuvaju tablice IP i MAC adresa prema kojima usmjeravaju promet.

- Vatrozid (eng. *firewall*)
  Vatrozid pohranjuje detaljne zapise aktivnosti sustava kao što su prepoznati napadi, odbačeni paketi, aplikacije kojima je dopušten ulaz ili izlaz te popisuje sve sumnjive aktivnosti.

- Preklopnik (eng. *switch*)
  Preklopnici ne stvaraju zapise, ali su korisni za postavljanje prisluškivača ili tzv. zrcala kako bi se kopirali nadolazeći podaci u stvarnom vremenu. No u CAM memoriji (eng. *Content Addressable Memory*) se mogu pronaći podaci o MAC adresama povezanih s određenim portovima, kao i podaci o virtualnim lokalnim mrežama (VLAN – eng. *Virtual Local Area Network*).

- IDS (eng. *Intrusion Detection System*)
  Zapisnici IDS-a sadrže sve što se smatra imalo sumnjivim. Jedna od funkcija IDS-a je zapisivanje događaja za kasniju analizu kako bi se spriječilo ponavljanje incidenta. IDS-ovi su osmišljeni da budu pasivni i mogu se smatrati protuprovalnim alarmom kod računala. Zapisuju se podaci kao što su:
    - skenovi portova,

    - nadolazeći promet iz sumnjivih portova (npr. portovi koji ne bi trebali biti otvoreni, a jesu) ili protokola (npr. protokol koji koristi krivi port),
    - poznate prijetnje poput crva ili virusa koji pokušavaju prodrijeti u mrežu,
    - anonimni pokušaji korištenja FTP ili drugih servisa u mreži,
    - IP adrese izvora napada,
    - iskorištenost veze (eng. *bandwidth usage*).

- IPS (eng. *Intrusion Prevention System*)
  IPS-u je svrha blokirati ili isključiti svaku uočenu prijetnju u mreži. Zapisuje mnoge događaje kao i IDS, ali glavna mu je funkcija analizirati podatke na mreži u stvarnom vremenu. Ako se IDS može usporediti sa protuprovalnim alarmom, IPS bi pozvao policiju i blokirao vrata.

- Mrežni pisač (eng. *network printer*)
  Moderni pisači često pohranjuju zapise o ispisivanim dokumentima zajedno s metapodacima tih dokumenata.

- Mrežni uređaji za kopiranje (eng. *network copier*)
  Kao i pisači, pohranjuju zapise o kopiranim i ispisanim dokumentima.

- WAP (eng. *Wireless access point*)
  WAP zapisuje sve što i normalni "žičani" usmjeritelj uz podatke specifične za bežični promet kao što su SSID identifikatori mreža.

Forenzika mobilnih uređaja

Ova grana računalne forenzike predstavlja najteže područje zbog prirode mobilnih uređaja da se iz godine u godinu potpuno mijenjaju. Od starih "cigli" koje su služile samo za pozive do današnjih *smartphone* uređaja koji gotovo mogu zamijeniti prijenosno računalo, ne samo po performansama nego i po količini memorije. Jedini način na koji istražitelj može pristupiti istrazi mobilnih uređaja je da konstantno bude u toku sa svim modernim čudima. U ovu kategoriju se ubrajaju:

- mobiteli,
- *smartphone* uređaji,
- GPS uređaji (eng. *Global Positioning System*),
- PDA uređaji (eng. *Personal Digital Assistant*),
- iPod i slični uređaji za reproduciranje audio signala,
- digitalne kamere i fotoaparati,
- digitalni diktafoni, …

Mobiteli se danas koriste za mnogo više od samih poziva. Analizom adresara može se vidjeti s kim je osoba bila u kontaktu. Nedavni pozivi govore s kim je nedavno kontaktirala, a kalendar može pokazati s kim se i gdje našla. Stoga ne čudi što su istražiteljima veoma zanimljivi podaci koji se mogu pronaći na mobilnim uređajima kao što su:

- povijest poziva,
- kontakti (adresar),
- SMS poruke,
- MMS poruke,
- IM poruke,
- podaci u kalendaru (sastanci, rođendani, …),

- slike,
- video zapisi,
- audio zapisi,
- memorijske kartice,
- pa čak i povijest pregledavanja web stranica (više o ovome u poglavlju o web forenzici).

E-mail i web forenzika

Web forenzika je područje koje se bavi analizom aktivnosti web preglednika (eng. web browser), elektroničke pošte te Instant Messaging komunikacije. Vedina korisnika, i poslovnih i privatnih, najvedi dio vremena provedenog za računalom provodi online. Lako je shvatiti koliko forenzičar može saznati o korisniku samo pregledavajudi njegovu aktivnost na Internetu. Bilo da je riječ o otkrivanju najposjedenijeg portala s kojeg korisnik čita vijesti uz jutarnju kavu, ilegalno preuzete glazbe i filmova, pornografskih slika ili razgovora između dva zaposlenika o tome kako de se osvetiti zlom šefu, činjenica je da web aktivnost može mnogo toga otkriti o osobi.

U sklopu analize web aktivnosti, istražitelj će obratiti pažnju na:

- web preglednik (eng. *browser*)
  - povijest pregledavanja stranica (eng. *browsing history*)
  - kolačiće (eng. *cookies*)
  - preuzete datoteke (eng. *download history*)
  - podatke iz formulara (eng. *form history*)
- webmail
  - podaci u zaglavljima poruka (eng. *header*)
- IM (eng. *Instant Messaging*)
  - podaci o kontaktima
  - sačuvani razgovori (eng. *chat history*)

Saznaj više o analizi web aktivnosti
Saznaj više o podacima u e-mailu
Saznaj više o Instant Messagingu