Računalna forenzika

Pišući o alatima za spašavanje podataka (*dd_rescue*, *testdisk* i *photorec*), suzdržavao sam se da ih ne zovem forenzičkim alatima. Ipak se radilo o primjerima koji pokazuju kako sistemac može svojim korisnicima pomoći da se sačuvaju podaci pogubljeni na nepouzdanim medijima. No ova se tri izuzetno korisna programčića mogu koristiti i u računalnoj forenzici.

Koja je razlika između spašavanja podataka i forenzike? Kao između prijateljske pomoći i službene istrage. Naime forenziku će od nas zatražiti ako se nešto ozbiljno dogodilo, neki prekršaj zakona ili internih propisa, pa je potrebno prikupiti dokaze. Rezultati će možda jednog dana biti korišteni u sudskom procesu, zato cijeli posao treba odraditi profesionalno. Dobar odvjetnik može osporiti "klimave" dokaze ili lošu proceduru. Zato su nam prilikom prikupljanja dokaza potrebni svjedoci.

Prvo je pravilo forenzičke istrage da se dokazi moraju prikupiti tako da se sačuva nedirnuto "mjesto zločina". U našem slučaju to je korisnikovo računalo, ili poslužitelj ustanove. Ako računalo ugasimo, već smo nešto promijenili. Ako spustimo operativni sustav, izgubit ćemo sliku radne memorije, u kojoj mogu biti brojni dokazi. Nakon ponovnog podizanja, možda se neće aktivirati procesi koje je korisnik, ili provalnik, aktivirao. S druge strane, ako samo izvučemo kabel za napajanje, sačuvat ćemo barem swap particiju, ali opet gubimo radnu memoriju. Radi toga će istražitelj ostaviti računalo da radi, te forenzičkim alatima napraviti preslike radne memorije i tvrdog diska. Za to može poslužiti i naš *dd_rescue*. Dobijene datoteke treba spremiti na vanjski disk, opet zato da se ne naprave promjene na "mjestu zločina". Forenzičari nose sa sobom vanjske diskove velikog kapaciteta, pa odmah na licu mjesta naprave višestruke kopije, jer ne vjeruju u pouzdanost današnjih digitalnih medija. Čuo sam iskustvo jednog profesionalca kojeg je angažirala tvrtka u SAD. Otputovao je preko velike bare, pokupio dokaze, i vratio se kući, da na miru obavi istragu. Možete misliti njegovo razočaranje kad je ustanovio da mu je otkazao vanjski disk i da je sve bilo uzalud?

Da bi se kasnije moglo dokazati da se radi o izvornim podacima koji ni na koji način nisu izmijenjeni, te da dokazi nisu "podmetnuti", odmah se napravi kontrolna suma preslika, na primjer md5 hash. Napravi se zapisnik u kojem se zapiše dobijena kontrolna suma, a svjedoci svojim potpisima jamče da je sve obavljeno na ispravan način. Bilo kakve izmjene u preslikama izazvat će promjenu koja vodi do drugačije kontrolne sume, pa će se to lako otkriti.

Sama istraga može potrajati mjesecima. Forenzičar će izraditi radnu kopiju preslike na kojoj će raditi. Njegov posao će biti otkriti sve procese, iz radne memorije i diska izdvojiti datoteke koje mogu sadržavati dokaze, pronaći pobrisane datoteke itd. To se sve radi posebnim alatima, koji mogu biti izuzetno skupi. Na informatičkim konferencijama slušat ćete tvrtke koje nude forenzičke programe kako tvrde da se na sudu priznaju samo rezultati dobijeni programom koji košta 100 K$. Ali to nije istina, postoje i *open source* alati koje će sud priznati. To su obično na Linuxu zasnovane distribucije, na primjer Heelix ili FTK, Forensic Toolkit. Bitno je da se napravi doslovna kopija sadržaja diska, jamči njezin integritet pomoću md5 hasha, a onda se posebnim alatima mogu tražiti na primjer obrisani e-mailovi, logovi itd. Ako su počinitelji koristili enkripciju, tada će istražitelj možda pronaći i zaporku kojom se kriptirani sadržaji mogu "otključati".

No sama istraga je priča za sebe i njome se bavi certificirani sudski vještaci. Sistemac može taj posao obaviti ako ima dovoljno znanja i iskustva, ali samo za interne potrebe.

Povezani članci:
Spašavanje podataka s oštećenih medija [1]
Testdisk [2]
Photorec [3]

Spašavanje USB sticka [4]

pon, 2013-01-07 07:37 - Aco Dmitrović**Kuharice:** Linux [5]
Kategorije: Sigurnost [6]
Vote: 3.4

Vaša ocjena: Nema Average: 3.4 (5 votes)

Source URL: https://sysportal.carnet.hr/node/1177

Links
[1] https://sysportal.carnet.hr/node/1169
[2] https://sysportal.carnet.hr/node/1171
[3] https://sysportal.carnet.hr/node/1175
[4] https://sysportal.carnet.hr/node/1179
[5] https://sysportal.carnet.hr/taxonomy/term/17
[6] https://sysportal.carnet.hr/taxonomy/term/30