Arantza IRASTORZA GOÑI
UPV/EHUko Donostiako Informatika Fakultateko irakasle eta ikerlaria

Forentse informatikoak datuen uxarrean

Konputagailuen azterketa forentsea» konputagailutatik ebidentziak identifikatu eta gordetzen dituen teknologia eremua da. Zibersegurtasunak gailuen eta datuen babesarekin zerikusia duen bezala, teknologia honek datuak berreskuratzearekin du zerikusia. Zibersegurtasunak eraso zibernetikoak ez gertatzeko edo beren ondorioak txikitzeko neurriak jartzen ditu, eta azterketa forentseak, berriz, segurtasuneko gorabehera gertatu ondoren, hori aztertu eta arakatzen dihardu.

Konputagailuan burutzen diren ekintza ia guztiek aztarna utziko dute fitxategien sisteman: fitxategiaren aldaketa, fitxategia ezabatzea, disko eremua handitzea, memoriatik diskora idaztea, gertaeren lorratza aldatzea. "Forentse informatikoa"-ren lana froga edo ebidentzia digitalak bildu, analizatu eta aurkeztea da. Horretarako, oso teknika eta software tresna espezializatuak erabili beharko ditu, metodologia eta prozedura legalak zorrotz aplikatuz eta zaintza-kateak mantenduz, ebidentziak fidagarritzat eta baliozkotzat hartuak izan daitezen. Esaterako, konputagailu batean jasotako fitxategi sistemaren analisia egin beharko du, bere egitura sakonean arakatu eta ulertu beharko du, kontuan hartuz sistema eragile bakoitzak bere fitxategi sistema duela (NTFS, EXT, etab.). Arakatzean, batzuetan datuak sakabanatuta egon daitezke eta dena berrantolatu behar izatea gerta daiteke, edo hondatutako fitxategi sistema konpondu behar izatea.

Forentse informatikoaren lana ebidentzia digitalak bildu, analizatu eta aurkeztea da. GETTY

Arakatze lan horretan beste teknika garrantzitsu bat da «metadatuen analisia». "Metadatuak", motzean esanda, datuen inguruko datuak dira, eta definizioa pixka bat osatuta, datuak antolatzeko eta erabilgarriago egiteko modu bat. Fitxategiak, hots, dokumentuak, argazkiak, bideoak... gordetzen dituenak agerian eta ikusgai dagoen eduki horretaz gain beste eduki estra edo ezkutu bat dauka, esaterako, fitxategia noiz sortu zen, nork eta zein aplikaziorekin sortu zuen, nor izan zen azkena fitxategia aldatzen, argazkia egin zeneko lekuaren kokapena, etab. Horrela, ordenagailuetan gordetako fitxategien gainean saguarekin eskuin-botoia klikatuz eta "Ezaugarriak" aukeratuz, beren metadatuak aztertu daitezke. Mezu elektroniko bat jasotzen denean bere iturburu kodea kopiatu eta Google-n "Messageheader" aplikazioarekin bere metadatua arakatu daiteke, mezua bidali duenaren domeinua, IP helbidea (goiburuko izenaz haragoko informazioa), edo mezua bidali denetik egin duen gailu zerbitzarietako ibilbidea. X-n (Twitter) txioa botatzen denean, bere inguruko metadatuak tresna egokiekin aztertu daitezke eta, esaterako, bere antzeko beste txio batzuk lortu.

Mezu elektronikoen, dokumentuen eta transakzioen inguruko metadatuak aztertzean, forentseak denbora-lerro zehatza ezar dezake, hots, mezu elektroniko baten dataren eta dokumentu baten sorrera-dataren arteko erlazioa ezar dezake. Eta korrelazio horretatik aztarna garrantzitsuak atzeman ditzake, epaitegietan froga moduan erabiltzeko. Hortaz, forentse informatikoaren lana izango da konputagailuekin lan egiterakoan ogi apurren moduan utzitako aztarnak atzematea eta ebidentzia moduan jasotzea. •