

Forenzična orodja za preiskave digitalnih medijev in naprav ter njihova zanesljivost³

Sodobni informacijsko komunikacijski sistemi predstavljajo temeljno infrastrukturo za delovanje organizacij, saj so v uporabi praktično na vseh področjih človekovega delovanja. Iz tega razloga informacijski sistemi pogosto vsebujejo tudi veliko število različnih digitalnih forenzičnih sledi. V primeru sumov kaznivih dejanj ali tim. varnostnih incidentov je s pomočjo tehnik digitalne forenzike te sledi mogoče analizirati. Z različnimi tehnikami digitalne forenzike je mogoče tudi obnavljati izbrisane podatke, zaradi česar je mogoče digitalno forenziko uporabiti tudi za obnavljanje ne samo namerno, pač pa tudi pomotoma izbranih podatkov izven sfere kazenskega prava.

Področje digitalne forenzike v ožjem smislu obsega iskanje digitalnih dokazov in podatkov ter predstavitev teh dokazov na sodišču. Pri slednjem pa trčimo na problem visoke kompleksnosti sodobnih informacijsko informacijskih sistemov. Posledica te kompleksnosti je zmanjšana transparentnost, saj je za razumevanje delovanja teh sistemov potrebno (pogosto obsežno) strokovno znanje. Posledica netransparentnosti je zato pogosto tudi manjše zaupanje v te sisteme in posledično v forenzične tehnike kar lahko privede do večje skepse pri obravnavi digitalnih dokazov.

Na področju digitalne forenzike, širše gledano pa tudi na področju informacijske varnosti, je zato izredno pomembno načelo odprtosti. To zahteva visoko transparentnost vseh postopkov, ter seveda njihovo ponovljivost in zanesljivost. Eden najbolj kritičnih, in zato tudi najpomembnejših delov vsake digitalno forenzične preiskave je ustrezen zajem digitalnih podatkov. Podatki morajo biti zajeti in shranjeni na način, da se zagotovi popolna integriteta podatkov. Integriteta, ali neokrnjenost podatkov pomeni, da je kopija forenzično zajetih podatkov povsem enaka originalu. Integriteta podatkov v praksi predstavlja zagotovilo, da podatki na digitalni kopiji niso bili spremenjeni, tako v smislu uničenja dokazov, kot tudi v smislu podtikanja lažnih dokazov.

Forenzični zajem digitalnih podatkov

Sodobne digitalno forenzične tehnike omogočajo zajem podatkov tako iz nosilcev podatkov namenjenim trajni hrampi podatkov (npr. trdih diskov, USB ključev, CD in DVD nosilcev, pomnilniških kartic, SIM kartic, itd.), kot tudi zajem tim. neobstoječih podatkov, oziroma zajem podatkov iz delovnega pomnilnika (RAM). Pri forenzičnem zajemu digitalnih podatkov se pogosto govori tudi o zajemu oz. analizi tim. mrtvega ali tim. živega sistema. O analizi tim. mrtvega sistema govorimo takrat, kadar podatke zajamemo iz nadzorovanega okolja, torej iz (glede na preiskovani sistem) zunanjega nadzorovanega operacijskega sistema in z uporabo zunanjih, nadzorovanih aplikacij ali strojne opreme. O analizi tim. živega sistema pa govorimo, kadar zajem digitalnih

1 dr. Matej Kovačič je zaposlen na *Fakulteti za družbene vede, Univerza v Ljubljani* ter je član strokovnega sveta *Inštituta za forenziko informacijskih tehnologij*. E-naslov: matej.kovacic@ifit.si

2 Delo je izdano pod Creative Commons licenco: "Priznanje avtorstva-Nekomercialno-Deljenje pod enakimi pogoji 2.5 Slovenija". Celotno pravno besedilo licence je dostopno na spletni strani: <<http://creativecommons.org/licenses/by-nc-sa/2.5/si/legalcode>>, ali na poštnem naslovu: Inštitut za intelektualno lastnino, Čufarjeva ulica 17, 1000 Ljubljana.

3 Prispevek za 1. konferenco kazenskega prava in kriminologije, sredo, 19. in četrtek, 20. november 2008, GH Bernardin, Portorož.

podatkov poteka znotraj samega sistema, ki ga preiskujemo. Najbolj idealna pa tudi v praksi najbolj razširjena je analiza tim. mrtvega sistema, saj se ob analizi tim. živega sistema izpostavljamo nevarnosti, da je na sistemu nameščena zlonamerna programska koda, ki prikriva nekatere digitalne dokaze. Je pa res, da analiza tim. mrtvega sistema ni vedno mogoča, poleg tega pa imajo nekatere tehnike analize živega sistema potencialno visoko vrednost pri zbiranju in nadaljnji analizi digitalnih dokazov, zato se bo v prihodnosti verjetno skušalo čim večkrat uporabljati obe vrsti digitalno-forenzičnih tehnik.

Kot rečeno, so najbolj razširjeni postopki zajema podatkov iz nosilcev podatkov namenjenim trajni hrampi podatkov. Pri tem se lahko uporabi tako programska, kot tudi posebna strojna oprema, ki preprečuje kakršnokoli pisanje podatkov na nosilce iz katerih podatke zajemamo ter s tem zagotavlja integriteto originalnih in zajetih podatkov.

Zajem podatkov iz aktivnega delovnega pomnilnika (zajem na tim. živem sistemu) je v tem smislu nekoliko bolj problematičen, saj ga je v praksi mogoče izvesti le z ustrezno programsko opremo, ki se jo v času delovanja računalnika (ali druge podobne naprave, npr. mobilnega telefona ali dlančnika) naloži v delovni pomnilnik in zažene. To pa seveda pomeni, da (poleg ostalih težav, ki jih ta tehnika prinaša) že s samim zajemom posežemo v integriteto originalnega nosilca podatkov, saj smo v nosilec podatkov naložili programsko aplikacijo namenjeno forenzičnemu zajemu podatkov.

Obstaja tudi tehnika zajema podatkov iz delovnega pomnilnika s pomočjo podatkovnega vmesnika FireWire (ki se ga pri sodobnih računalnikih praviloma uporablja za priklop zunanjih diskov ali digitalne videokamere). Specifikacija FireWire vmesnika namreč določa, da imajo zunanje naprave priključene nanj neposredni dostop do delovnega pomnilnika, kar je mogoče izkoristiti za forenzični zajem podatkov iz delovnega pomnilnika. Idejo forenzičnega zajema delovnega pomnilnika preko vmesnika FireWire so leta 2004 predstavili raziskovalci Michael Becher, Maximillian Dornseif in Christian N. Klein, danes pa je že na voljo posebna programska oprema s katero lahko s pomočjo prenosnega računalnika s FireWire vmesnikom izvedemo forenzični zajem delovnega pomnilnika na ciljnim računalniku. Kljub vsemu, se danes tehnika v praksi ne uporablja pogosto, saj ima določene pomanjkljivosti, med drugim predvsem to, da osebni računalniki danes večinoma niso opremljeni z ustreznim FireWire vmesnikom, zato tovrstnega zajema podatkov ne omogočajo.

Še novejše raziskave pa so pokazale, da je podatke mogoče zajeti tudi iz delovnega pomnilnika tim. "mrtvega" sistema, torej iz računalnika, ki je bil tik pred forenzičnim zajemom podatkov resetiran ali ugasnjen. Tehnika je bila prvič javno omenjena leta 2006 s strani varnostnega raziskovalca Douglasa MacIverja iz podjetja Microsoft, obsežnejšo raziskavo na to temo pa so aprila 2008 izvedli raziskovalci Princeton University. V raziskavi so ugotovili, da se vsebina pomnilniških modulov DRAM ne izgubi v trenutku ko računalnik ugasnemo, pač pa se (počasi) izgublja z časom. Vsebino DRAM modulov je tako mogoče prebrati še nekaj sekund, do nekaj minut po tem, ko je računalnik ugasnjen, ta čas pa je mogoče podaljšati (celo do nekaj ur) z ustreznim hlajenjem pomnilniških modulov. Raziskava, ki sva jo leta 2008 v zvezi s tem opravila Matej Kovačič in Jožko Škrablin je pokazala, da je takšen zajem podatkov mogoče opraviti s prosto dostopno programsko opremo, se pa zaradi omenjenega "izgubljanja" vsebine pomnilnika DRAM soočamo s tim. "bitnim razpadom" podatkov (naključnim spreminjanjem podatkov), zato je neposredna forenzična vrednost takšnih podatkov v dokaznem postopku lahko zelo vprašljiva. Kljub temu, da so tehnike zajema podatkov iz delovnega pomnilnika v praksi težko izvedljive njihova neposredna dokazna vrednost pa je nizka, pa nas tako zbrane digitalne sledi v nekaterih primerih lahko vodijo do pomembnih ugotovitev (npr. rekonstrukciji šifriranih ključev s katerimi nato odklenemo podatke na trdem disku), zato je pričakovati še nadaljnje raziskovanje v tej smeri. Kot drugod pa tudi tu

velja, da je izredno pomembno striktno dokumentiranje vseh postopkov ter uporaba transparentnih programskih orodij.

Zagotavljanje integritete digitalnih podatkov

Pri zagotavljanju integritete digitalnih podatkov se v sodobni digitalni forenziki uporabljajo različne metode računanja tim. kontrolnih vsot (ang. *hash*). Pri računanju kontrolnih vsot - gre za podatkovne oz. številске nize fiksne dolžine - se uporabljajo različne kriptografske funkcije, katerih lastnost je, da za kot vhodni podatek vzamejo poljubno dolg niz znakov, vrnejo pa število fiksne dolžine (npr. velikosti 128 bitov v primeru algoritma MD5).

Algoritmi za izračun kontrolne vsote podatkov morajo imeti dve pomembne lastnosti. Prva lastnost je, da omogočajo enosmerno preslikavo poljubnih podatkov v kontrolno vsoto (da torej obraten izračun, torej "rekonstrukcija" vhodnih podatkov iz kontrolne vsote ni mogoča, ali pa je vsaj zelo nepraktična), druga, predvsem za področje digitalne forenzike zelo pomembna lastnost pa je, da ne obstajata dva različna niza vhodnih podatkov, ki bi vrnila isto kontrolno vsoto, oziroma, da je verjetnost, da taka dva različna niza podatkov obstajata čim manjša. Z drugimi besedami, da torej ne obstaja oz. obstaja čim manjša možnost tim. kolizije.

Na področju digitalne forenzike, pa tudi informacijske varnosti (kontrolne vsote se uporabljajo tudi pri implementaciji digitalnega podpisa ter varnemu shranjevanju gesel) se trenutno največ uporabljata algoritma MD5 (Message-Digest algorithm 5) ter SHA-1 (Secure Hash Algorithm). Žal so nekatere raziskave v kriptografiji in matematiki v zadnjih letih pokazale, da ta dva algoritma vsebujeta določene matematične slabosti, ki lahko privedejo do kolizij. Tako sta raziskovalca Magnus Daum in Stefan Lucks leta 2005 na konferenci Eurocrypt 2005 predstavila posebno tehniko iskanja oz. generiranja kolizij v algoritmu MD5.

V praksi to pomeni, da je na podlagi enega niza vhodnih podatkov in njegove MD5 kontrolne vsote mogoče poiskati drug niz vhodnih podatkov z enako MD5 kontrolno vsoto. Z drugimi besedami, potencialni napadalec bi lahko na podlagi digitalne kopije forenzičnih podatkov in njihove MD5 kontrolne vsote ustvaril takšno spremenjeno (lažno) kopijo digitalnih podatkov, da preverjanje integritete podatkov z algoritmom MD5 ne bi pokazalo, da je prišlo do posega v integriteto podatkov.

Iz tega razloga bo na področju forenzičnega zajema digitalnih podatkov potrebno uporabljati izboljšane (novejše) zgoštevne algoritme, katerih slaba lastnost pa je podaljšan čas izračuna kontrolne vsote in s tem posledično tudi podaljšan čas ustreznega forenzičnega zajema digitalnih podatkov.

Pomen odprtosti in transparentnosti

Eden izmed pomembnih mehanizmov za zagotavljanje transparentnosti forenzičnih postopkov in s tem vzpostavljanje zaupanja vanje je njihova odprtost - tako v smislu odprtosti in dokumentiranosti vseh postopkov, kot tudi v smislu odprtosti programske kode.

Odprtost programske kode pomeni, da je mogoč dostop do izvorne kode računalniške aplikacije, torej skupka "navodil" napisanih v programskem jeziku. Za razliko od odprtega programja pri zaprtem programju dostop do izvorne programske kode ni mogoč, zato je pri takem programju težje, če že ne nemogoče natančno ugotoviti, kako točno takšna programska aplikacija deluje. Tipično zaprto programje je tim. lastniško programje, torej programje, katerega raba, razširjanje in/ali spreminjanje so prepovedani oziroma zahtevajo posebno dovoljenje, ni pa vsako lastniško programje tudi zaprto, saj nekateri proizvajalci programske opreme (navadno pod določenimi

pogoji) omogočajo vpogled v izvorno kodo njihovega programja. Odprta koda namreč ne pomeni nujno, da mora biti programska koda dostopna pod kakšno izmed prostih licenc (npr. GNU GPL), pač pa le, da mora biti omogočen prost dostop do kode za namene pregleda in testiranja.

Odprtost programske kode ustvarja osnovni predpogoj za zaupanje, da programska koda res počne tisto, kar naj bi počela. Da torej ne vsebuje skritih funkcij ali napak, ki bi v primeru forenzičnih preiskav lahko ogrozile integriteto digitalnih podatkov ali privedle do predstavitve neustreznih ali celo lažnih rezultatov.

Želja po čim večji transparentnosti postopkov digitalne forenzike je tako povsem razumljiva, hkrati pa je tudi povsem razumljiva želja proizvajalcev programske opreme za digitalno forenziko po nerazkritju programske kode njihovih produktov konkurentom, saj jim le-to predstavlja pomemben mehanizem za zagotavljanje tržne prednosti pred konkurenti.

To dilemo je mogoče rešiti na tak način, da se pri najbolj kritičnem delu forenzične preiskave - forenzičnem zajemu digitalnih podatkov in postopkih za zagotavljanje integritete zajetih podatkov striktno zahteva uporabo standardiziranih postopkov in odprtokodnih orodij. Pri sami forenzični analizi digitalnih podatkov v smislu *iskanja* digitalnih dokazov, pa sama transparentnost ni tako pomembna. Rezultat - obstoj nekega digitalnega dokaza, je namreč potem, ko ga poljubno forenzično orodje najde, mogoče vedno dokazati s fizičnim vpogledom na dano lokacijo v podatkovni strukturi, višjo stopnjo transparentnosti pa je mogoče doseči tudi s ponovljivostjo, torej z uporabo različnih analitičnih orodij različnih proizvajalcev, ki vsa privedejo do istega rezultata.

Prihodnost digitalne forenzike?

Kot rečeno, sodobni informacijski sistemi vsebujejo veliko število različnih digitalnih forenzičnih sledi. Mikroprocesorske tehnologije pa danes niso samo del osebnih računalnikov in strežniških sistemov, pač pa jih najdemo tudi v številnih drugih napravah, npr. v mobilnih telefonih ter njihovih komponentah (npr. SIM karticah). Digitalna forenzika se je zato že pred časom pričela usmerjati na nova področja, predvsem na področje mobilne telefonije in dlančnikov, v prihodnosti pa bo verjetno postala aktualna na vseh področjih kjer srečujemo informacijsko tehnologijo, npr. v avtomobilizmu ter na področju številnih drugih digitalnih naprav.

Žal se tehnike digitalne forenzike danes uporabljajo tudi v nezakonite namene - npr. obnavljanje izbrisanih podatkov z namenom kraje poslovnih informacij, osebnih podatkov ali finančnih podatkov posameznikov. Znani so primeri kriminalnih združb, ki so preko interneta kupovale rabljeno računalniško opremo, iz katere so nato z uporabo tehnik digitalne forenzike izluščile npr. digitalne certifikate bivših lastnikov, ki so jih uporabile za krajo njihovih finančnih sredstev. Tehnike je mogoče uporabiti tudi na ukradeni ali izgubljeni opremi, npr. prenosnih računalnikih, USB ključih, itd. Zato se čedalje več posameznikov zaveda pomena uporabe šifrirnih tehnik. Na voljo je čedalje več kvalitetnih - tudi prosto dostopnih in brezplačnih - programov namenjenih šifriranju podatkov. Možnosti šifriranja v zadnjem času postajajo del sodobnih operacijskih sistemov (npr. FileVault v okolju Mac, BitLocker v okolju Windows, LUKS v okolju Linux). In čedalje več posameznikov to programsko opremo uporablja z namenom varovanja svojih zasebnih ali poslovnih podatkov.

V primeru šifriranih podatkov večina tehnik digitalne forenzike seveda odpove, saj je brez ustreznega šifrirnega ključa nemogoča kakršnakoli analiza oz. iskanje digitalnih dokazov. Kljub temu pa je do splošne uporabe šifriranja verjetno še dolgo časa in vse do tedaj, bo digitalna forenzika ostala pomembno orodje v preiskovanju informacijskih sistemov.