Ekonomska upravičenost uporabe metod digitalne forenzike

LILJANA SELINŠEK

Povzetek

Članek skuša povezati področje ekonomske analize prava z uporabo digitalnih forenzičnih metod, ki so v sodobni informacijski družbi čedalje bolj uporabno sredstvo za dokazovanje znakov različnih kaznivih dejanj, pa tudi drugih pravno pomembnih dejstev. Avtorica izhaja iz temeljne (hipo)teze, da je dokazovanje z metodami digitalne forenzike primerno uporabiti le, kadar pričakovana korist od tako zbranih dokazov presega stroške digitalne forenzične preiskave. Hkrati opozarja, da so stroškovni vidiki digitalne forenzike izjemno kompleksni, saj segajo na področje bitke med komercialnimi in odprtokodnimi orodji za digitalne forenzične preiskave, kjer trčijo interesi tehnoloških podjetij, ki razvijajo forenzično programsko opremo, interesi policije in pravosodja ter interesi potrošnikov.

Ključne besede: • digitalna forenzika • kazenski postopek • ekonomska analiza prava • elektronski dokazi • stroškovni vidiki digitalne forenzike

KONTAKTNI NASLOV: Dr. Liljana Selinšek, docentka, Pravna fakulteta Univerze v Mariboru, Mladinska ulica 9, SI-2000 Maribor, Slovenija, e-pošta: liljana.selinsek@uni-mb.si.

ISSN 1855-7147 Tiskana izdaja / 1855-7155 Spletna izdaja
UDK: 330.13:[343.983.003.1:681.3]
Na svetovnem spletu dostopno na http://www.lexonomica.com

Economic Justification of Use of Digital Forensic Methods

LILJANA SELINŠEK

Abstract

The author is trying to connect the field of law and economics with the usage of digital forensic methods that are increasingly important evidence means in modern information society for proving of different criminal offences' elements as well as other important facts in legal proceedings. The basis of the article is the (hypo)thesis that digital forensic methods are proper evidence means only in cases where expected benefit from evidences collected with this methods is higher than the costs of digital forensic investigation. The author is pointing out also the fact that economic views of digital forensics are of complex nature because they interfere with the battle between commercial and open source tools for digital forensic investigations where many interests collide: those of technological companies that develop forensic software, of police, jurisdiction and consumers.

Keywords: • Digital forensics • criminal proceeding • electronic evidences • law and economics • costs of digital forensic methods

CORRESPONDENCE ADDRESS: Dr. Liljana Selinšek, Assistant Professor, University of Maribor, Faculty of Law, Mladinska ulica 9, SI-2000 Maribor, e-mail: liljana.selinsek@uni-mb.si.

ISSN 1855-7147 Print / 1855-7155 On-line
UDC: 330.13:[343.983.003.1:681.3]
Available on-line at http://www.lexonomica.com

1. Uvod

Pričujoči članek ima precej omejitev, pri čemer bi uvodoma izpostavila tri. Prva omejitev je ta, da ima članek zgolj enega avtorja oziroma avtorico, ki ni vešča ekonomije, ampak le prava. Druga omejitev je v tem, da članek ekonomsko analizo prava povezuje s področjem, ki je v različnih delih sveta na zelo različnih razvojnih stopnjah. Nekatere države (denimo v centralni Afriki) digitalne forenzike sploh ne poznajo, v nekaterih državah (denimo v Sloveniji) je ta disciplina kot znanstveno in praktično področje v povojih, v nekaterih državah (denimo v ZDA) pa se sodišča že ukvarjajo s tem, ali je izračun zgoščenih (hash) vrednosti trdega diska kazenska preiskava ali ne.[1] Tretja omejitev je povezana z drugo omejitvijo in se nadaljuje v tem, da tudi v državah, kjer digitalna forenzika vsaj približno uspe slediti hitremu tehnološkemu razvoju, ni obsežnejših analiz, razprav, diskusij, zapisov ali česa podobnega na temo stroškovnih vidikov te preiskovalne metode; oziroma te vsaj niso splošno dostopne. S približno enakimi temami kot ta prispevek, se ukvarja npr. članek »The Economics of Digital Forensics«, ki ga je napisal Tyler Moore iz računalniškega laboratorija univerze v Cambridgeu (Velika Britanija);[2] nekoliko širše pa podobna vprašanja obravnava Ross Anderson, prav tako iz računalniškega laboratorija univerze v Cambridgeu, v članku »Why Information Security is Hard – An Economic Perspective«.[3]

Navedene omejitve seveda pomenijo, da je ta članek v prvi vrsti namenjen izpostavljanju odprtih vprašanj in opozarjanju na pomembne vidike v povezavi digitalna forenzika – ekonomska analiza (prava). Za kakršna koli konkretnejša stališča bi bile potrebne raziskave in analize ter ustrezne povezave različnih faktorjev, o katerih bo govor tekom prispevka; izoblikovati pa bi bilo treba tudi vsaj približni cenik (posameznih delov) digitalne forenzične preiskave, kar ni enostavno, ker marsikje (tudi v Sloveniji) še kar ni jasno, kdo naj bi te preiskave sploh opravljal.

2. Beseda o digitalni forenziki

V poplavi definicij digitalne forenzike (uporabljajo se tudi izrazi računalniška forenzika, forenzično računalništvo ipd.) je težko izbrati najboljšo – med bolj

---

[1] Prim. sodbo United States of America v. Robert Elsworth Crist III (US District Court for the middle district of Pennsylvania), dostopno npr. na: http://arstechnica.com/news.media/USA_v._Crist,_order-1.pdf (obiskano 17.11.2008).

[2] Članek je dostopen na spletnem naslovu http://weis2006.econinfosec.org/docs/14.pdf.

[3] Članek je dostopen na spletnem naslovu: http://www.acsac.org/2001/abstracts/thu-1530-b-anderson.html.

nazornimi je npr. opredelitev forenzičnega računalništva, ki sta jo razvila Broucek in Turner. V sklop »forensic computing« uvrščata procese in postopke, ki vključujejo nadzorovanje, zbiranje, analizo in predstavitev digitalnih dokazov in so del *a priori* ali *post mortem* preiskave kaznivih, nelegalnih ali drugih neprimernih dejanj, izvršenih v medmrežju (on-line) (Broucek in Turner, 2006: 4). Seveda pa ni resnih zadržkov, da ne bi v pristojnost digitalne forenzike uvrstili tudi prepovedanih ravnanj, ki so izvršena izven medmrežja (off-line). Z drugimi besedami je digitalna forenzika metoda, s katero se za potrebe različnih sodnih postopkov (kazenskih, pa tudi civilnih) razkrivajo digitalni dokazi.[4]

Digitalna forenzika je mlada veda. Njeni začetki segajo v leto 1988, ko je Clifford Stoll objavil članek »Zalezovanje Wilyja Hackerja« (Stalking the Wily Hacker) in dve leti kasneje še knjigo Kukavičje jajce (The Cuckoo's Egg), v katerih je dokumentiran prvi primer organizirane oziroma sistematične preiskave kaznivega dejanja, storjenega s pomočjo takrat še ne zelo razširjene računalniške tehnologije. Pred približno desetimi leti so se pričeli bolj masovno pojavljati strokovni članki na to temo, večji proizvajalci programske opreme pa so pričeli razvijati prve komercialne programe za digitalne forenzične preiskave. Danes so na voljo različna forenzična orodja, ki omogočajo preiskave različnih segmentov računalnikov in drugih digitalnih naprav (mobilnih telefonov, dlančnikov, digitalnih kamer ipd).

Digitalno forenziko zaradi njene »mladosti« spremlja kup odprtih vprašanj, ki se povezujejo predvsem s forenzičnimi orodji za digitalne preiskave ter s potrebnimi znanji, izobrazbo oziroma izkušnjami digitalnih forenzikov, pa tudi uporabnikov rezultatov digitalne forenzične preiskave. Digitalna forenzika oziroma forenziki se srečujejo s problemom izjemne količine podatkov, ki jih je treba preveriti v posameznem primeru,[5] nagajajo jim anti-forenziki,[6] bremenijo jih prepiri glede uporabe odprtokodnih forenzičnih orodij; pa še pravniki jim grenijo življenje predvsem s svojim (pre)slabim

[4] Praktično gledano, je digitalni dokaz serija elektronskih impulzov, shranjenih v bolj ali manj stabilni obliki (prim. Scheetz, 2007: 26). Digitalni dokazi se v osnovi delijo v dve skupini: 1) na digitalne dokaze v obliki podatkov, shranjenih v elektronski (računalniški ipd.) obliki, in 2) na digitalne dokaze, ustvarjene s strani računalniškega programa ali operacijskega sistema.

[5] V zvezi s tem se pogosto navaja primerjava z 8848 metrov visokim Mount Everestom: podatki, sestavljeni iz enega milijona črk, natisnjeni predstavljajo cca. 200 strani. Kup 200 strani papirja je debel cca. 5 centimetrov. Podatki iz povprečnega prenosnega računalnika s 40 gigabajtnim diskom bi torej (pod predpostavko, da je disk polno zaseden) natisnjeni in zloženi na kup segali približno 2.000 metrov visoko; podatki iz povprečnega strežnika s 400 gigabajtnim diskom pa kar 20.000 metrov visoko, kar pomeni, da bi za skoraj 2,3-krat presegli Mount Everest.

[6] Boj je na tem področju precej podoben tistemu, ki se že dolga stoletja bije med šifrerji in razbijalci šifer (dešifrerji).

razumevanjem osnov informatike in s poskusi zaščititi pravico do zasebnosti v tudi informacijski dobi.

Skratka – področje digitalne forenzike je v vseh pogledih pestro, razgibano in kompliciranо. S tem prispevkom ga želimo še nekoliko bolj zakomplicirati s tem, da bomo v zapleteno zgodbo vpletli še stroškovni vidik.

3. Stroškovni vidiki digitalne forenzike

Digitalna forenzika je zanimivo področje tudi z ekonomskega vidika, oziroma natančneje rečeno, z vidika ekonomske analize prava. V klasičnem smislu se ekonomska analiza prava sicer definira kot teorija vedenja, ki napoveduje, kako se naslovniki zakona odzivajo na njegovo spremembo (Cooter in Ulen, 2005: 4), vendar pa iz vsebin, ki jih ta disciplina preučuje, izhaja, da je precej širša. Ni v nasprotju z ekonomsko analizo prava, če za potrebe tega prispevka postavimo naslednjo hipotezo: *dokazovanje z metodami digitalne forenzike je v konkretnem, recimo kazensko-pravnem primeru primerno uporabiti le, kadar pričakovana korist od tako zbranih dokazov presega stroške digitalne forenzične preiskave.*

V zvezi s to hipotezo je treba jasno zapisati, da naše kazensko procesno pravo zaenkrat na zakonski ravni ne dopušča odmikov od pravil dokazovanja zaradi stroškovnih razlogov. Določba 17. člena Zakona o kazenskem postopku[7] (v nadaljevanju ZKP) določa, da morajo sodišče in državni organi, ki sodelujejo v kazenskem postopku, po resnici in popolnoma ugotoviti dejstva, pomembna za izdajo zakonite odločbe (pri tem morajo enako pazljivo preizkusiti in ugotoviti tako dejstva, ki obdolženca obremenjujejo, kakor tudi dejstva, ki so mu v korist). Celoten dokazni sistem je v kazenskem postopku naravnan tako, da sodišče ne sme zavrniti dokaznega predloga katere od strank zato, ker je izvedba določenega dokaza predraga. Npr. zahtevo za pridobitev dokaza z metodami digitalne forenzike lahko sodišče zavrne le, če oceni, da izvedba tega dokaza ni potrebna, ker je stanje stvari tudi brez tega razčiščeno do te mere, da omogoča razsojanje. Vse navedbe in ugotovitve, vezane na slovensko pravo, je treba brati in razumeti v kontekstu tega splošnega pravila.

Digitalna forenzika je povsod po svetu draga reč, predvsem zato, ker je za njeno izvajanje potrebna strojna in programska oprema (cena te opreme se seveda dviguje sorazmerno s kakovostjo), pri čemer gre za kontinuiran

[7] Uradni list RS, št. 63/1994, 72/1998, 6/1999, 66/2000, 111/2001, 56/2003, 43/2004, 101/2005, 14/2007, UPB4: 32/2007), 68/2008.

strošek, ker je potrebno nenehno nadgrajevanje. Pozitivna stran pa je v tem, da je to opremo mogoče uporabiti za preiskavo večjega števila primerov. Tudi strošek dela je upošteven,[8] saj lahko digitalne forenzične preiskave terjajo ogromno časa (prim. opombo 5). Sicer pa se vprašanje stroška dela povezuje s še vedno odprtim vprašanjem, kdo naj bi opravljal ali smel opravljati digitalne forenzične preiskave za potrebe sodnih postopkov (ali strokovnjaka naredi izobrazba, znanje ali izkušnje ali morda vse troje?).

Države, ki si to lahko privoščijo, financirajo neprofitne laboratorije oziroma institucije za digitalne forenzične preiskave, ki so precejšen zalogaj za državni proračun. V Veliki Britaniji za kakovost teh institucij skrbijo tudi tako, da jih ne obremenjujejo z zadevami manjšega pomena. Tako se npr. enota za digitalno forenziko pri britanskem uradu za boj proti resnemu kriminalu (Serious Fraud Office's Digital Forensic Unit), ki razpolaga s cca. tremi milijoni funtov letnega proračuna, vključuje le v preiskave finančnih goljufij in drugih resnih oblik kriminala, pri katerih gre za sum protipravne premoženjske koristi vsaj v višini enega milijona funtov.[9] Dobro izšolani strokovnjaki, ki imajo na voljo vrhunsko strojno in programsko opremo, se torej ne ukvarjajo s kurjimi tatovi.

Države, ki si ne morejo privoščiti neprofitnega laboratorija za digitalno forenziko, digitalne forenzične preiskave bodisi prepuščajo bolj ali manj skromno opremljenim policijskim oddelkom, na ravni izvedenstva pa se vključuje predvsem zasebni sektor. Če pogledamo npr. Slovenijo, v kateri ni državne institucije za digitalno forenziko, so razmerja in vprašanja okrog tega, kdo naj opravlja digitalne forenzične preiskave odprta oziroma ovita v meglo. To v praksi pomeni, da se zapravljajo velike količine denarja ne da bi se vedelo, ali bodo rezultati preiskav sploh uporabni na sodišču. Na tem področju je vsekakor treba čim prej postaviti jasna pravila, kar ni le v interesu pravosodja, ampak tudi državnega proračuna.

Moore v zgoraj navedenem članku, ki je precej tehnično obarvan, ugotavlja, da mnoge pomembne omejitve digitalne forenzike niso tehnične, ampak ekonomske narave. Vsekakor so stroškovni vidiki eden od pomembnih

[8] O tem sicer obstajajo različna mnenja – Moore npr. čas, potreben za pridobivanje in analizo digitalnega dokaza, označuje za »marginal cost,« se pravi marginalen strošek, pri čemer osebo, ki to storitev opravlja, imenuje »officer« (uradnik).

[9] Delo te enote temelji na usklajenem multidisciplinarnem pristopu pri preiskovanju, kar v praksi pomeni, da so preiskovalne skupine za vsak konkreten primer sestavljene iz različnih strokovnjakov. Preiskovalno skupino vedno vodi tožilec, v njej pa sodelujejo agentje urada, pravniki, ena ali več policijskih enot, svetovalci, IT forenziki iz enote za digitalno forenziko, po potrebi pa tudi zunanji sodelavci (računovodje in podobno). Stroški take preiskave so seveda zelo visoki.

argumentov v odprtem sporu o tem, katera programska forenzična orodja so primerna za izvajanje digitalnih forenzičnih preiskav. Veliki proizvajalci, kot sta ameriški Guidance Software (med drugim razvija orodje EnCase) in Access Data (med drugim razvija orodje FTK), seveda stojijo na stališču, da bi se za potrebe pravosodja morala uporabljati (le) standardizirana in komercialna (torej njihova) orodja. Ta orodja so visokega cenovnega razreda (cena licence je okrog 3000 – 3500 USD za osnovno verzijo). Mnogi poleg cene vidijo pri teh orodjih težavo tudi v tem, da je programska koda tajna, zato nihče od zunanjih strokovnjakov ne more (legalno) preveriti postopka, ki ga to orodje izvaja pri svojem delovanju, kar pomeni, da so lahko v takem orodju tudi skrite funkcije ali celo napake, kar vpliva na verodostojnost dokazov. Na drugem polu pa so t. i. odprtokodna orodja (koda je javno dostopna vsem zainteresiranim), ki jih večinoma razvijajo nekomercialno usmerjene skupine entuziastov, nekatera pa tudi večji proizvajalci programske opreme. Odprtokodna orodja so praviloma brezplačna. Njihovi zagovorniki so prepričani, da ta orodja zagotavljajo transparentnost pri pridobivanju digitalnih dokazov, saj lahko vsakdo z dovolj znanja v vsakem trenutku preveri, na kakšnih principih tako orodje deluje; poudarjajo pa tudi ugoden stroškovni vidik. Vsekakor je mogoče reči, da se pomemben del bitke med komercialnimi in odprtokodnimi orodji za digitalne forenzične preiskave bije na ekonomskem področju, kjer trčijo interesi tehnoloških podjetij, ki razvijajo forenzično programsko opremo, interesi policije in pravosodja ter interesi potrošnikov. Pravzaprav področje digitalne forenzike pri tem niti ni tako zelo unikatno.

4. Sklep

Postavljene hipoteze, da je dokazovanje z metodami digitalne forenzike primerno uporabiti le, kadar pričakovana korist od tako zbranih dokazov presega stroške digitalne forenzične preiskave, v tem prispevku nismo dokazovali s številkami – to ostaja izziv za kakšno drugo priložnost, saj je treba za tovrstno analizo zbrati in pravilno ovrednotiti oziroma oceniti številne podatke. Hipoteza ima namreč dva povsem različna stroškovna pola – tehničnega (forenzičnega) in pravnega (pravosodnega) – ki ju lahko v ustrezen ekonomski kontekst verjetno postavi le interdisciplinaren strokovni tim.

Sklepna ugotovitev tega prispevka tako izhaja iz zdrave pameti, ki govori za zgoraj navedeno hipotezo. Če lahko določeno kaznivo dejanje dokažemo z dokazi, katerih zbiranje in analiza sta tehnološko in praktično nezahtevna in poceni, seveda ni nobenega razloga, da bi uporabljali drage in komplicirane postopke, katerih rezultati marsikje sploh še nimajo nesporne veljave v

pravu. Toda kadar za določeno kaznivo dejanje ni (dovolj) drugih dokazov, kakor tistih, ki jih je mogoče izluščiti le z metodami digitalne forenzike, je te metode treba uporabiti, čeprav kaznivo dejanje morda ni povzročilo večje škode. Tudi če pustimo ob strani načelno ustavno določbo, da smo pred zakonom vsi enaki, bi bila opustitev dokazovanja manj nevarnih kaznivih dejanj zaradi stroškovnih razlogov dolgoročno slaba rešitev. Taka dejanja bodo sama zase sicer še vedno manj nevarna, a jih bo sčasoma toliko, da bodo pomenila resen družbeni problem.

In tako dalje - vsekakor bi bilo (bo) zanimivo videti, ali bi (bo) znanstveni pristop z uporabo metod ekonomske analize prava ovrgel ali potrdil razmišljanja v tem prispevku.

Literatura / References

Anderson, R. (2001) Why Information Security is Hard – An Economic Perspecitve, dostopno na http://www.acsac.org/2001/abstracts/thu-1530-b-anderson.html (obiskano: 18.11.2008).

Broucek, V., Turner, P. (2006) Winning the battles, losing the war? Rethinking methodology for forensic computer research. Journal in Computer Virology, 2 (2006), 3-12.

Cooter, R., Ulen, T. (2005) Ekonomska analiza prava. Ljubljana, Finance.

Scheetz, M. (2007) Computer Forensics. An Essential Guide for Accountants, Lawyers, and Managers. New Jersey, John Wiley & Sons.

Tyler, M. (2005) The Economics of Digital Foreniscs, dostopno na: http://weis2006.econinfosec.org/docs/14.pdf (obiskano: 17.11.2008).