UDC: **004.738.5:343.97** INFO M: str. 4-8

TOWARDS A METHODOLOGY FOR THE MANAGEMENT OF THE COMPUTER FORENSICS PROCESS
POGLED NA METODOLOGIJU UPRAVLJANJA PROCESOM KOMJUTERSKE FORENZIKE

Hamid Jahankhani, Elli Georgiadou, Amie Taal

ABSTRACT: Computer Forensics is a field that developed from the introduction of new technologies which is readily accessible, affordable and heavily depended upon by both individuals and businesses. The speed in which these technologies have evolved brings both advantages and disadvantages to all. New criminal activity accompanied the development of technologies often referred to a cybercrime or e-crime presenting challenges to law enforcers. In the paper we outline the current context within which e-crimes are committed, the types of e-crimes and their manifestations and the various efforts towards fighting these crimes. We present an emerging methodology for managing the Computer Forensics process based on guidance to assist law enforcement in dealing with computer evidence. We conclude with indications of further work and other emerging issues.
KEY WORDS: Computer Forensics, criminal activity, computer evidence
REZIME: Kompjuterska forenzika je oblast koja se razvila nakon uvođenja dostupnih, pristupačnih i visoko zavisnih novih tehnologija od pojedinaca i poslovnih subjekata. Brzina kojom se ove tehnologije razvijaju je donela svima određene prednosti a i nedostatke. Nove kriminalne aktivnosti, često nazivane cyber kriminal ili e-kriminal, su propratile razvoj tehnologije i postavile nove izazove pred izvršioce zakona. U ovom radu smo predstavili širi kontekst u okviru kog se javlja e-kriminal, pojavne oblike e-kriminala i njegove manifestacije, kao i različite načine borbe protiv ove vrste kriminala. Predstavili smo metodologiju na pomolu za upravljanje procesom kompjuterske forenzike, a vođeni idejom da pomognemo primenu zakona u borbi sa kompjuterskim dokazima. Na kraju rada su dati nagoveštaji budućeg rada i najnovijih problema u ovoj oblasti.
KLJUČNE REČI: Kompjuterska forenzika, kriminalne radnje, kompjuterski dokazi

1. UVOD

U potpuno povezanom i istinski globalizovanom svetu mreža, u kom značajno mesto zauzimaju Internet, mobilne tehnologije, rasprostranjene baze podataka, elektronska trgovina i e-uprava, e-kriminal se manifestuje kroz pranje novca, krađu intelektualne svojine, krađu identiteta, neautorizovan pristup poverljivim informacijama, uništavanje podataka, prikazivanje uvredljivog materijala, *spoofing* i *fishing*, viruse, crve i *cyber* proganjanje, industrijsku špijunažu itd. Ova lista nije konačna jer se novi oblici e-kriminala pojavljuju iz dana u dan [1].

Do skoro se borba protiv e-kriminala vodila pomoću zakonskih odredbi definisanih za stare zločine kao što su zavera za činjenje prevare, krađa, uznemiravanje i krađa identiteta. Situacija se neznatno promenila devedesetih godina prošlog veka kada je donet Zakon o zloupotrebi kompjutera (*Computer Misuse Act*), ali je ovo bilo manje nego dovoljno s obzirom da je zakon uglavnom pokrivao hakerske aktivnosti.

Nisu doneti novi zakoni specifični za kompjuterski kriminal od Zakona o zloupotrebi kompjutera 1990. godine, sve do donošenja Zakona o prevarama (*The Fraud Act*) iz 2006. godine za borbu protiv e-kriminala. Zakoni na koje se on oslanjao su:

- Zakon o krađama (*Theft Act*) iz 1968., 1978 i amandman zakona iz 1996. godine
- Zakon o krivičnim poduhvatima (*Criminal Attempts Act*) iz 1981. godine
- Zakon o telekomunikacijama (*Telecommunications Act*) iz 1984. godine
- Zakon o javnom redu (*Public Order Act*) iz 1986. godine
- Zakon o zaštiti dece (*Protection of Children Act*) iz 1978. godine
- Zakon o prikazivanju uvredljivih sadržaja (*Obscene Publications Act*) iz 1959. i 1964. godine
- Zakon o zaštiti podataka (*Data Protection Act*) iz 1998. godine
- Zakon o ljudskim pravima (*Human Rights Act*) iz 1998. godine
- Zakon o kleveti (*Defamation Act*) iz 1952. i 1996. godine
- Zakon o slobodi informisanja (*Freedom of Information Act*) iz 2000. godine
- Zakon o sprečavanju uznemiravanja (*Protection from Harassment Act*) iz 1997. godine.

Bez obzira na to, sudski procesi i dalje nisu bili adekvatni za suzbijanje e-kriminala usled brzog širenja informacionih tehnologija i informacionih sistema. Godine 2006., dva nova zakona su doneta za brobu protiv e-kriminala, i to: Zakon o prevarama (*The Fraud Act*) koji je stupio na snagu 2007. godine, koji „ima za cilj da zatvori nekoliko rupa u vođenju procesa vezanih za prevare, jer po rečima vlade, stari zakon nije adekvatan za nove oblike prevara“, [1] i Zakon o policiji i sudstvu (*Police and Justice Act*) iz 2006. godine koji (u petom delu) zabranjuje „neautorizovani pristup kompjuterskim materijalima; neautorizovana dela sa namerom činjenja štete na računaru i nabavku alata koji se može koristiti u svrhe hakinga“ [2].

Dokumentovane smernice, praksa i procedure su bile zastarele i u potpunosti neadekvatne za upravljanje elektronskim dokazima u forenzičkom smilsu, sve do juna 2007. godine kada su objavljene revidirane ACPO smernice. One su prihvaćene kao najbolje smernice ikada definisane za upravljanje digitalnim dokazima.

Nedostatak stručnosti organa reda da razumeju zamršenost e-kriminala se javlja zbog diverziteta i kompleksnosti problema koji obuhvata e-spremnost, kultutu, rasu, pol i širok demografski domašaj. Pitanja nadležnosti su iznad svega pružila odličnu priliku za privatni sektor, pružajući utočište i potrebu tržišta za uslugama pojedinaca u oblasti kompjeterske forenzike. Veliki broj privatnih kompanija se pojavio pružajući usluge vađenja podataka i usluge kompjuterske forenzike.

U isto vreme se na tržištu pojavio popriličan broj kompjuterskih alata kao što su: Encase, FTK, Helix, ParabenCell Seizure, MOBILedit, BitPim, besplatni alati, itd. Softverski i hardverski alati su automatizovali obradu kompjuterskih dokaza i nisu zahtevali dublje znanje o kompjuterima da bi se njima upravljalo. Ovakva situacija je olakšala posao svima koji su radili na obradi kompjuterskih dokaza, ali je u isto vreme dala lažan osećaj sigurnosti i uverenje pojedinaca da ih adekvatno korišćenje ovih alata čini ekspertima u oblasti.

Organi reda su postali visoko zavisni od postojećih alata i usluga, a bez odgovarajuće evaluacije su se oslanjali na pojedince i kompanije bez dovoljno kvalifikacija, znanja ili iskustva, gledajući na njih kao na eksperte u oblasti kompjuterske forenzike.

2. OSNOVNE POTEŠKOĆE ISTRAŽITELJA U BORBI PROTIV CYBER KRIMINALA

Očigledno je da *cyber* kriminal nije više u ranoj fazi razvoja. On predstavlja „unosan posao“ za preduzetnika sa potencijalom da zaradi mnogo novca uz minimalan rizik. U isto vreme su identifikovane centralne oblasti kao elementi koji najviše doprinose neuspešnoj primeni zakona u praksi:

– Nedostatak ažurnih smernica
– Nedostatak odgovarajućih trening programa
– Nedostatak finansijskih sredstava.

U skorašnjem izveštaju policije Velike Britanje koji je predstavljen članovima parlamenta u martu 2007. godine je iznet podatak o talasu nacionalnog kriminala. Procenjeno je da godišnji gubici usled prevara iznose 200 milijardi funti što je dovoljna suma da se zaposli 200 000 policajaca, pri čemu najveći procenat zauzimaju internet i telefonske prevare. Procena je da 4 milijarde gubitaka snose poslovni subjekti a 2.75 milijarde pojedinci. Ovi iznosi se odnose samo na prevaru koja je jedan od mnogo pojavnih oblika e-kriminala.

Istražni organi u Velikoj Britaniji ne mogu da istraže sve navodne prestupe, što nameće pitanje, na koji način se donose odluke o tome koji slučajevi će biti istraženi, a koji neće, zbog srazmere i međunarodne prirode ovih zločina. Da li se interes javnosti uzima u razmatranje i da li je ovaj način borbe sa e-kriminalom nezavisan od njegove efikasnosti i uspešnosti?

Borba protiv *cyber* kriminala je težak zadatak sa tačke gledišta istražnih organa. Iako je zločin uvek zločin, bez obzira na njegovu veličinu i značaj, odluka o istraživanju i sudskom gonjenju pojedinačnih slučajeva se donosi u odnosu na interes javnosti. Aprila 2007. godine je doneta odluka da se sve prevare vezane za kreditne kartice prijave bankama umesto direktno policiji. Banke su mogle samostalno da odlučuju koju prevaru će da prijave policiji. Opšte je prihvaćena činjenica da nije uvek moguće da se prikupi dovoljno dokaza za podizanje optužnice, a sa ograničenim resursima ovakav pristup obezbeđuje da se resursi raspoređuju na mesta gde će nejbolje biti iskorišćeni [3]. Ovakav način rada nije naročito prihvatljiv političarima iz razloga što je otežano prikupljanje podataka i formiranje precizne statistike o prisutnosti e-kriminala. To nikada nije ni bilo moguće usled činjenice da se ne prijavljuju sve aktivnosti e-kriminala.

Smatra se da više nije odgovarajuća situacija da vlade zavise od pojedinaca s obzirom da one kontrolišu ogromne baze podataka sa osetljivim informacijama, od privatnih informacija pojedinaca do informacija od značaja za nacionalnu sigurnost.

Razumevanje i upravljanje procesom kompjuterske forenzike je postalo neminovnost u današnje vreme.

Jula 2007. godine je Izborni komitet za nauku i tehnologiju (*Select Committee on Science and Technology*) objavio svoj peti izveštaj, i u sklopu zaključaka i rezultata izneo sledeće:

„Opšta javnost slabo razume koristi, troškove i opasnosti koje vrebaju na internetu. Ovo nije iznenađujuće s obzirom na nedostatak verodostojnih podataka za koji vlada mora da snosi deo odgovornosti. Vlada nije u poziciji da samostalno i direktno prikuplja potrebne podatke, ali ima odgovornost kao lider u prikupljanju dostupnih podataka, njihovoj interpretaciji za javnost i postavljanju istih u odgovarajući kontekst, isticanjem koristi i rizika. Umesto da se time bavi, vlada još uvek nije definisala ključne koncepte, kao što je koncept „e-krimiinala“.

Izveštaj sadrži i određene preporuke:

„Preporučujemo da vlada oformi među odeljensku grupu sastavljenu od stručnjaka iz industrije i nauke, a u cilju razvoja koordiniranog pristupa prikupljanju podataka u budućnosti. Ovde treba uključiti i klasifikacionu šemu svih pojavnih oblika e-kriminala. Takva šema treba da obuhvati ne samo ilegalna dela vezana za internet, poput dela odbijanja usluga (*Denial of Service*), već i tradicionalna krivična dela počinjena elektronskim putem ili uz značajan elektronski aspekt prilikom činjenja ovakvih dela“.

Određena istraživanja [4,5,6] su definisala skup principa i dala predlog metodologije visokog nivoa za ove svrhe. Sve procedure i smernice za prikupljanje i upravljanje kompjuterskim dokazima su zasnovane na smernicama izdatim od strane Asocijacije policijskih inspektora (*Association of Chief Police Officers – ACPO*); mnoge institucije se pridržavaju ovih smernica uključujući i privatni sektor. ACPO je profesionalno i strateški vođeno telo koje upravlja pravcem razvoja policijskih usluga u Engleskoj, Velsu i Severnoj Irskoj.

Ove smernice su definisane kao podrška istražnim organima u borbi sa kompjuterskim dokazima [7]. Postoje četiri osnovna principa:

Princip 1: Nikakva aktivnost od strane istražnih organa i njihovih agenata ne sme da bude usmerena u pravcu izmene

podataka koji se čuvaju na računaru ili nekom drugom skladištu, ako postoji mogućnost da će ti podaci da se koriste tokom sudskog procesa.

Princip 2: U izuzetnim slučajevima, kada pojedinac smatra da je neophodan pristup originalnim podacima na računaru ili nekom drugom skladištu, taj pojedinac mora da bude stručan da to i uradi, kao i da pruži razloge i implikacije ovakvog čina.

Princip 3: Audio trag ili drugi zapis svih realizovanih aktivnosti nad elektronskim dokazima mora de se napravi i sačuva. Nezavisno treće lice treba da bude u mogućnosti da ispita te aktivnosti i ostvari isti rezultat.

Princip 4: Pojedinac zadužen za istragu (istražitelj slučaja) snosi svu odgovornost za sprovođenje zakona i ovih principa.

Verzija (3.0) je objavljena 2003. godine i bila je u upotrebi do juna 2007. godine. Postoji generalni konsenzus da je tehnologija poprilično napredovala od tada.

Usled mnogobrojnih pritisaka sa nekoliko različitih strana, nova verzija principa je objavljena sredinom juna 2007. godine. U ovoj verziji je je definisano da se smernice odnose na istražne organe ali i na privatni sektor, pri čemu se nude smernice istražnim organima o načinima rada sa spoljnim svedocima i forenzičarima, a posebno u slučajevima pedofilije.

Ove smernice su pripremane od 2005. godine i predstavljaju rezultat zajedničkog rada Asocijacije policijskih inspektora, Radne grupe za e-kriminal, Metropolitan policije i privatne kompjuterske forenzičke kompanije 7Safe.

Najnovija verzija pruža detaljnije smernice za područja koja su površno objašnjena u prethodnoj verziji, kao što su: mesta zločina (kućne mreže i *wireless* tehnologija), mrežna forenzika i kratkotrajni podaci (istražno osoblje) i kontrola pedofilnih slika (spoljni svedoci i forenzičari). Nove oblasti koje smernice obuhvataju podrazumevaju: otkrivanje podataka (pronalaženje video i kablovskih dokaza) i smernice za konfiskaciju i ispitivanje mobilnih telefona (prvi kontakt sa žrtvama: spisak pitanja). Smernice su javne i moguć je njihov *download* sa internet sajta [7].

Odlaganje u objavljivanju ovih smernica, posebno zbog toga što se većina stručnjaka u oblasti oslanja na njih, je dovelo do situacije da ljudi samostalno smišljaju pravila, procedure i smernice u hodu da bi se izborili sa novim tehnologijama, naročito po pitanju mobilnih tehnologija i PDA (*Personal Digital Assistance*) uređaja. Problem koji se sada javlja je obuka istražitelja u korišćenju isključivo novih smernica iz razloga što su već neko vreme koristili metode za koje niko nije smatrao da su loše. U okviru istražnih tela postoji verovanje da će se obezbediti dovoljna zaštita u slučajevima oštećenih dokaza ukoliko se smernice primenjuju 100%.

U privatnom sektoru su smernice obično sastavni deo internih procedura jer se većina kompjuterskih forenzičkih kompanija bavi odbranom i građanskim pitanjima na koje se smernice ne odnose u svim situacijama. Samo nekoliko kompanija ima ugovore sa Metropolitan policijom *Scotland Yard*-om i tužilaštvom, i u tim slučajevima oni moraju da ispoštuju definisane smernice.

Iz gore navedenog je jasno da su smernice neophodne ali da njihova primena iziskuje odgovarajući trening i razumevanje. Većina istražitelja se našla u ovoj oblasti protivno svojoj volji usled visokih zahteva za suzbijanjem e-kriminala.

Studija o e-kriminalu je sprovedena 2004. godine od strane Grupe za evropsko informaciono društvo (*The European Information Society Group – EURIM*) i Instituta za istraživanje javnih politika (*Institute of Public Policy Research – IPPR*) u cilju analize potreba istražnih organa i industrije za veštinama istraživanja i vođenja sudskih slučajeva. Nakon tri godine potrebe za tim i dalje postoje [5].

3. POTREBA ZA OBRAZOVANJEM U OBLASTI KOMPJUTERSKE FORENZIKE

U većini slučajeva se trening sastoji od 1-2 nedelje treninga iz povraćaja informacija i njihove analize na Cranfield Univerzitetu u Shriveham-u ili u Nacionalnom centru za specijaliste za sprovođenje prava (*National Specialist Law Enforcement Centre - NSLEC*) u Wyboston-u, što je postao obavezan uslov za bavljenje ovom profesijom. Drugi deo treninga predstavlja jednonedeljni nesertifikovani trening iz odabanog forenzičkog alata.

„Prikupljanje podataka i hapšenja iziskuju iskustvo organa reda, ali prikupljanje dokaza sa računara i drugih elektronskih uređaja zahteva posebne veštine kompjuterske forenzike“. Ova izjava se pojavila na BBC-u u emisiji pod naslovom „Borba protiv net kriminala“ [8].

Slični novinski članci i izjave su se pojavljivali prethodna 3 meseca u nacionalnim i međunarodnim časopisima, što govori o velikom interesovanju za načine korišćenja kompjuterskih dokaza. Ovakva situacija mora da se promeni ukoliko postoji želja da se održi korak sa *cyber* kriminalom i da se ne rešavaju problemi u hodu kako se do sada radilo, a i kako se i dalje radi.

Kompjuterska forenzika nije više novo područje kao što bi pojedinci želeli da veruju, i mnogo toga je potrebno da se uradi na ohrabrivanju novih ljudi u ovoj oblasti, i na ujednačavanju veština i iskustva već anagažovanih na poslu. Vlada, trening kompanije i univerziteti u potpunosti podržavaju inicijativu da je neophodan ne samo tehnički, već i trening iz pravnih aspekata. Većina univerziteta trenutno nudi kurseve specijalno pripremljene za istražitelje, mada se za sada za ovakve kurseve odlučuju uglavnom pripadnici organa reda koji žele da imaju alternativu nakom penzionisanja.

Oni koji pristupaju profesiji moraju da razumeju značaj akademskih kvalifikacija, naročito ukoliko uopšte nemaju iskustva u praksi.

Kompjuterska forenzika nije više profesija za koju je dovoljan trening tokom posla da bi se steklo iskustvo. Za većinu drugih profesija je neophodna diploma pre treninga, kao što je slučaj sa nastavnicima, advokatima, naučnicima forenzičarima, lekarima, itd. Isto treba da važi i za kompjutersku forenziku jer je posao podjednako značajan kao i druge profesije, i bez obzira da li je pozitivan ili negativan, on utiče na ljudske živote.

Veliki broj univerziteta u zemlji i inostranstvu ima u ponudi predmete iz oblasti kompjuterske forenzike i informacione sigurnosti na diplomskim i postdiplomskim studijama, što

pomaže studentima koji slušaju ove predmete pružajući im solidnu osnovu iz kompjuterske nauke, bolje razumevanje teorije kompjuterske forenzike i, najvažnije, pomaže im da postanu inovativni u razmišljanju u susretu sa novim forenzičkim načinima borbe sa e-kriminalom.

Vreme je da vlada počne aktivno da sarađuje sa univerzitetima u ohrabrivanju ljudi da se odluče za ove predmete, a naročito onih koji rade u javnom sektoru.

Diploma je danas preduslov u privatnom sektoru, kao i iskustvo, jer je sve teže održavanje statusa stručnjaka u oblasti kompjuterske forenzike i statusa stručnog svedoka tokom sudskih procesa. Prošlo je vreme kada je „uradi sam" forenzika bila prihvatljiva.

Ovo nas vodi u drugo područje po pitanju kog je dosta stručnjaka u oblasti kompjuterske forenzike rezervisano, a to je ideja o akreditaciji. To je oblast u kojoj je teško donošenje adekvatne odluke. Većina se slaže i prihvata da je potrebno da se osnuje savet, ali se kao problem javlja definisanje institucije koja će biti zadužena za njegov rad. Neki predlažu da savet treba da vode univerziteti, vlada, ili univerziteti, vlada i poslovni subjekti zajedno.

Ukoliko tu ulogu preuzmu univerziteti, postoji briga ljudi koji godinama rade u oblasti bez akademskih kvalifikacija da će morati da steknu dodatne kvalifikacije bez obzira na iskustvo, ne bi li postali priznati i akreditovani u oblasti. Većina njih je protiv toga.

Ukoliko vlada preuzme ulogu lidera, bez definisanih standarda situacija se neće promeniti u odnosu na već postojeću. To bi podrazumevalo da zaposleni u oblasti forenzike daju određene smernice za rad, ali se postavlja pitanje jesu li ti pojedinci stručni da odlučuju o oblicima akreditacije.

Ovo nas dovodi do poslednje alternative – zajedničkog partnerstva između vlade, univerziteta i poslovnih subjekata. Ujedno je to i najizvodljivija opcija ali je potrebno mnogo zajedničkog truda da bi se došlo do verodostojne akreditacije prihvatljive od strane svih uključenih strana.

Marta 2007. godine je u Guardian-u objavljen članak Peter Warren-a što je donelo značajne probleme profesiji. „Prošlog meseca sam gledao propast Gene Morrison-a. Otkriven je prevarant koji se predstavljao kao forenzički stručnjak a učestvovao je u pružanju dokaza za više od 700 policijskih slučajeva, od kojih su mnogi bili vezani za silovanja i vožnju u pijanom stanju. Morrison (48 godina) iz Hyde-a, Timeside, je proglašen krivim za 22 tačke krivokletstva na sudu Minshull Street Crown, i osuđen na 5 godina zatvora. Njegove tvrdnje da je forenzički stručnjak su bile lažne, a diplomu i doktorat je kupio na univerzitetu koji postoji samo na internetu.

Kompjuterski stručnjaci su upozoravali da slična stvar može da se dogodi i u njihovoj oblasti. „Mnogo ljudi se bavi kompjuterskom forenzikom, a bez bilo kakvih kvalifikacija", tvrdi Neil Hare-Brown, izvršni direktor QCC-a, kompanije koja sprovodi forenzičku istragu za policiju. U članku se dalje navodi „Smatram da je između 5% i 10% ljudi u ovoj oblasti nekompetentno a to je donelo probleme prilikom sprovođenja istraga. Nama je dato dosta (kompjuterskih) diskova od stane policije za koje je rečeno da ne sadrže nikakve dokaze, a naknadno je na njima pronađena značajna količina dokaza."

Peter Warren [14] takođe naglašava da je od uvek svima, od istražitelja do advokata i sudija, poznata činjenica da u oblasti kompjuterske forenzike postoje ljudi koji nisu dovoljno kvalifikovani ili iskusni; „Ipak, stručnjaci su izjavljivali da nije korisno uspostavljanje sistema sličnog programu stručnih svedoka Glavnog veća za medicinu." Doktor Andrew Blyth, predavač sa Glamorgan Univerziteta na predmetima informaciona sigurnost i kompjuterski kriminal, koji je često stručni svedok, kaže: „Ono što nam je potrebno je profesionalno telo koje će obavljati registraciju ljudi i proveravati njihove akreditacije. Potreban nam je uredjen sistem koji će nam omogućiti da razlikujemo pojedince koji pokušavaju da nas obmanu i pojedince koji su eksperti u oblasti, a možda nemaju odgovarajuće kvalifikacje".

Jedan od vrhunskih komputerskih naučnika iz Velike Britanije, koji je odbio da se predstavi, smatra da je situacija neodrživa. „Svaki vid kriminala koji dolazi do suda podrazumeva uključenost računara na neki način, tako da moramo da nađemo pravi izlaz iz ove situacije. Mi moramo da sastavimo skup podataka koje eksperti moraju da imaju, treba nam telo koje će da definiše šta su eksperti radili u prošlosti, skup formalnih kvalifikacija koje oni moraju da imaju i kooperativnost sudova.

Sigurno je da će akreditacija primorati vladu, naučnike, istraživače, i ljude u oblasti kompjuterske forenzike da postave prihvatljivije standarde i mehanizme kontrole onih koji rukuju, analizuraju i istražuju kompjuterske dokaze.

4. METODOLOGIJA UPRAVLJANJA KOMPUTERSKOM FORENZIKOM

Metodologija upravljanja kompjuterskom forenzikom se sastoji iz 4 faze: identifikacija, prikupljanje, čuvanje i izveštavanje.

1. **Identifikacija**: izvori digitalnih dokaza
2. **Prikupljanje**: slikanje uređaja na mestu zločina
3. **Čuvanje**: Lanac staranja i očuvanja integriteta podataka u cilju obezbeđenja da se nijedna informacija ne izgubi ili izmeni.
4. **Izveštavanje**: izveštavanje o svim zaključcima i korišćenim procesima

Osobe koje izvršavaju gore navedene aktivnosti moraju da poštuju standardna pravila dokazivanja kao što je Zakon o policijskim i krivičnim dokazima iz 1984. godine. Trenutno se sprovodi revizija ovog zakona, a njegov rezime je objavljen 31.07.2007.godine [14].

Predlažemo da četvrta faza obuhvati detaljnije raščlanjivanje neophodnih metoda za analizu i klasifikaciju podataka koji su dokazni materijal i istorijski zapisi. Još uvek puno treba da bude urađeno u oblasti komjuterske forenzike, kao što je standardizacija procedura. Sama oblast se sastoji od nekoliko grana digitalne forenzike: internet forenzika, mrežna forenzika i mobila forenzika. Pojedinačne smernice za ove grane će omogućiti naučnicima da obezbede kvalitet procesa i prikupljenih podataka.

Takođe predlažemo da se upravljanje kompjuterskom forenzikom proširi i uključi peta fazu revizije i unapređenja, a u svetlu empirijskih podataka koji mogu da se kvalifikuju i organizuju radi maksimizacije i efektivnosti procesa.

5. DALJA RAZRADA

„Napredak ka standardima u internet forenzici“ je članak Beth Rozenberg [11]. Članak je specifičan za mrežnu forenziku ali je uvodni pasus interesantan jer ukazuje na vrednosti onih koji rade u oblasti. „Digitalna forenzika je još mlada nauka. Ta novina, praćena brzim promenama u svetu kompjuterske tehnologije, je rezultirala slabo definisanom i zbunjujućom regulativom digitalne forenzike i za stručnjake iz oblasti kompjuterske bezbednosti i za pravnike“[12]. “Istraživanja bezbednosti informacionih tehnologija u Velikoj Britaniji su kvalitetna, ali malobrojna. Potrebno je dosta više podrške ovakvom vidu istraživanja, iznad svega iz privrede. Neophodan je razvoj jednog ili više multidisciplinarnog istraživačkog centra za privlačenje privatnih izvora finansiranja i povezivanje stučnjaka iz različitih akademskih sredina. Preporučujemo da veća istraživača preuzmu ulogu lidera u započinjanju pregovora sa vladom, univerzitetima i privredom sa ciljem brzog uspostavljanja prvog centra u zemlji”.

“Legitimni istraživači u oblasti bezbednosti su na granici legalnosti zbog skorih dopuna Zakona o zloupotrebi računara iz 1990. godine. Sa oduševljenjem prihvatamo uveravanje ministra da će se smernice pojaviti krajem leta, ali apelujemo da se one objave što je pre moguće, ne bi li se izbeglo podcenjivanje ovih istraživanja u međuvremenu” [13].

Ostaje da se vidi koliko će to doprineti kompjuterskoj forenzici.

LITERATURA

[1] Na svakih 10 sekundi se u Velikoj Britaniji dogodi po jedan zločin prema istraživanjima. (06/09/07) http://www.out-law.com/page-8450 (pristupljeno 07/07/08).

[2] Police and Justice Act 2006, http://www.opsi.gov.uk/acts/acts2006/20060048.htm (pristupljeno 05/07/08).

[3] Metro Newspaper, 2007, Banks now in charge of card crime” (22 June 2007) http://www.metro.co.uk/money/article.html?in_article_id=54164&in_page_id=36 (pristupljeno 14/07/08).

[4] Taal A., 2007, Report examining the weaknesses in the fight against cyber-crime from within, Int. J. Electronic Security and Digital Forensics, Vol.1, No. 2, Inderscience Publishers.

[5] EURIM-IPPR E-Crime study., Supplying the Skills for Justice, 18 May 2004.

[6] Higginson J., “We lose £20bn a year to fraud”, Metro Newspaper, 8 March 2007, pp. 2. Section 3 - Private Security Industry Act 2001.

[7] ACPO Guidelines (2007) http://www.7safe.com/electronic_evidence/index.html (pristupljeno 16/07/08).

[8] BBC, The fight against net crime (13/7/07), http://news.bbc.co.uk/1/hi/programmes/click_online/6897121.stm , (pristupljeno 13/07/08)

[9] The Police and Criminal Act (PACE) 1984 http://police.homeoffice.gov.uk/operational-policing/powers-pace-codes/pace-code-intro/ (pristupljeno 16/8/07).

[10] PACE Review 2007 http://police.homeoffice.gov.uk/operational-policing/powers-pace-codes/PACE-Review (pristupljeno 16/8/07).

[11] A Push to Standards for Net Forensics (23 June 2003), http://www.pcworld.com/article/id,133327-c,researchreports/article.html (pristupljeno 31/8/07).

[12] Computer Weekly Magazine “The enemy at the cyber-gates”, (17 July 2007)

[13] Select Committee on Science and Technology Fifth Report, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16505.htm#a2 (pristupljeno 31/8/07)

[14] Warren P., “The evidence mounts on the need for expert witnesses” Guardian Newspaper, 8 March 2007.

Dr. Hamid Jahankhani, Middlesex University, School of Computing Science, Velika Britanija
Oblasti interesovanja: Information Security and Computer Forensics

Elli Georgiadou, Middlesex University, School of Computing Science, Velika Britanija
Oblast interesovajna: Software Quality, Metamodelling, Methodologies

Amie Taal, Bivši pravni savetnik Odeljenja za pronevere, Metropolitan Police, Velika Britanija

Rad na srpskom priredila: Ana Nikodijević, FON, Oblasti interesovanja: Kompjuterska forenzika, Cyber kriminal