Digitalna forenzika u funkciji forenzičkog računovodstva

Nataša Simeunović
Fakultet za poslovnu ekonomiju
Univerzitet Sinergija
Bijeljina, BiH
nsimeunovic@sinergija.edu.ba

Nenad Ristić
Fakultet za računarstvo i informatiku
Univerzitet Sinergija
Bijeljina, BiH
nristic@sinergija.edu.ba

Sadržaj—**Digitalna forenzika, kao jedna od grana forenzičke nauke, za osnovni cilj ima da legalnim metodama prikupi i obradi dokaze pohranjene na računaru ili nekom drugom nosiocu digitalnih podataka, a vezanih za neku vrstu nelegalne aktivnosti. Sa druge strane, forenzičko računovodstvo ima zadatak da otkrije i istraži sve sumnjive ekonomske transakcije koje se mogu okarakterisati kao kriminalne radnje, odnosno rezultirati sudskim sporom. Sa porastom digitalizacije podataka, i razvijanja računovodstvenih softvera, javila se i potreba za primjenom alata digitalne forenzike u istrazi i obezbjeđivanju dokaza o kriminalnim radnjama u finansijskim izvještajima.**

Ključne riječi - forenzičko računovodstvo; prevare; digitalna forenzika; revizija; digitalni dokaz

Key words – forensic accounting; fraud; digital forensic, audit; digital evidence.

I. UVOD

Savremeno digitalno okruženje ponudilo je nove mogućnosti za počinioce finansijskih prevara, ali i istražitelje. Na mnogo načina, digitalizacija i modernizacija je promijenila način na koji se sprovodi istraga, metode koje interni revizori koriste za planiranje i obavljanje posla, kao i pristupi koje koriste spoljni revizori da procijene rizik i izvrše reviziju. Dok neke metode, kao što su online dokumentacija predstavljaju kompjuterizovane verzije klasičnih dokumenata, druge metode, poput analize rizika zasnovane na neuronskim mrežama unijele su revoluciju u to polje. Mnogi revizori i istraživači konstantno mijenjaju radne lokacije vodeći se računarskim tehnologijama kao glavnim alatom, što uslovljava potrebu za upotrebom digitalne forenzike u otkrivanju mogućih računovodstvenih manipulacija.

II. FORENZIČKO RAČUNOVODSTVO

Korisnici finansijskih izvještaja žele finansijske izvještaje koji na fer način prikazuju finansijski položaj, finansijsku uspješnost i tokove gotovine posmatranog privrednog subjekta, odnosno one finansijske izvještaje koji na pošten (fer) način prikazuju efekte transakcija i ostalih događaja u skladu sa definicijama i kriterijumima za priznavanje sredstava, obaveza, prihoda i rashoda, definisanih Okvirom za pripremanje i prikazivanje finansijskih izvještaja. Investitori i kreditori koriste računovodstvene informacije u cilju procjene kvaliteta ostvarenog rezultata kompanije (dobitka ili gubitka) i budućih novčanih tokova koji su povezani sa njihovim ulaganjima (kamate za imaoce obveznica, kamate za zajmodavce - banke i dividende, kapitalne dobitke za akcionare). Država i njeni organi koriste računovodstvene informacije u cilju utvrđivanja mjera ekonomske politike, donošenja odgovarajućih odluka o podsticanju određenih djelatnosti i privrednih grana i nadziranje sprovođenja mjera ekonomske politike. Upravo iz tih razloga je neophodno obezbijediti realno finansijsko izvještavanje o poslovanju svakog preduzeća kako bi se zaštitili interesi internih i eksternih korisnika finansijskih izvještaja.

Računovodstvena profesija u cjelini, svjesna da ne može potpuno spriječiti da obmanjujući finansijski izvještaji budu sastavljeni i objavljeni, smatra neophodnim da sve nastale prevare u finansijskom izvještavanju otkrije, istraži i sankcioniše. U tom cilju se u računovodstvenoj profesiji javlja nova grana – forenzički računovođa.

U računovodstvenoj literaturi ne postoji jedinstvena definicija forenzičkog računovodstva, no ono u čemu se svi slažu jeste da forenzičko računovodstvo uključuje primjenu računovodstvenih koncepata i tehnika na pravne probleme. Ono je specijalnost koja zahtjeva integraciju istražiteljskih, računovodstvenih i revizorskih vještina. Od brojnih definicija koje se nalaze u literaturi koja se bavi forenzičkim računovodstvom najpotpunijom se čini ona koju je dala ACFE - *Association of Certified Fraud Examiners.* Prema ovom Udruženju ovlašćenih istražitelja prevara forenzičko računovodstvo je korišćenje računovodstvenih vještina u potencijalnim ili stvarnim civilnim ili krivičnim sporovima, uključujući opšteprihvaćene računovodstvene i revizorske principe; utvrđujući gubitke profita, prihoda, imovine, ili štete, procjene internih kontrola, prevare i sve drugo što zahtjeva uključivanje računovodstvenih ekspertiza u pravni sistem [1].

Ključne komponente forenzičkog računovodstva, u skladu sa navedenim, čine računovodstvene vještine, revizorske tehnike i istražiteljske procedure.

Najčešća područja prevara vezanih za računovodstvo su [2]:

- nepoštovanje zakonskih propisa s ciljem prikazivanja željenih rezultata
- krivotvorenje podataka i knjigovodstvenih dokumenata
- prikazivanje fiktivnih događaja
- namjerno iskrivljavanje poslovnih događaja
- prikrivanje krađe novca i ostale imovine.

Nepoštovanje zakonskih propisa s ciljem prikazivanja željenih rezultata predstavlja zanemarivanje zakonskih propisa i prilagođavanje prikaza s namjerom lažiranja u nadi da to neće biti otkriveno. Lažni rezultati se mogu postići manipulacijama računovodstvenih stavki kako bi se proizveo željeni rezultat ili utajio porez. Fiktivni događaji se mogu prikazati pomoću fiktivne dokumentacije i poslovanja s fiktivnim preduzećima ili preduzećima koja su legalno osnovana, a služe za obavljanje fiktivnih poslova. Namjerno iskrivljavanje poslovnih događaja predstavlja tumačenje i knjiženje nekog poslovnog događaja na potpuno drugačiji način od istine kako bi se postigao željeni cilj. Najbolji primjer za to možemo naći u tumačenju štetnih događaja kako bi se naplatila šteta od osiguravajućih društava. Prikrivanje krađe novca i druge imovine je najčešće povezano s krivotvorenjem knjigovodstvenih dokumenata i raznih izvještaja.

Iz svega rečenog, može se zaključiti da forenzičko računovodstvo ne obuhvata samo klasično računovodstvo i klasične prevare. Ono ide mnogo šire, bavi se i kompjuterskim prevarama i kompjuterskim kriminalom. Obzirom da su danas skoro svi dokumenti u elektronskom obliku, stoga se forenzičko računovodstvo širi i na to područje, a digitalna forenzika je jedan od alata čijom primjenom se može utvrditi da li je došlo do prevare.

III. IKT U RAČUNOVODSTVU

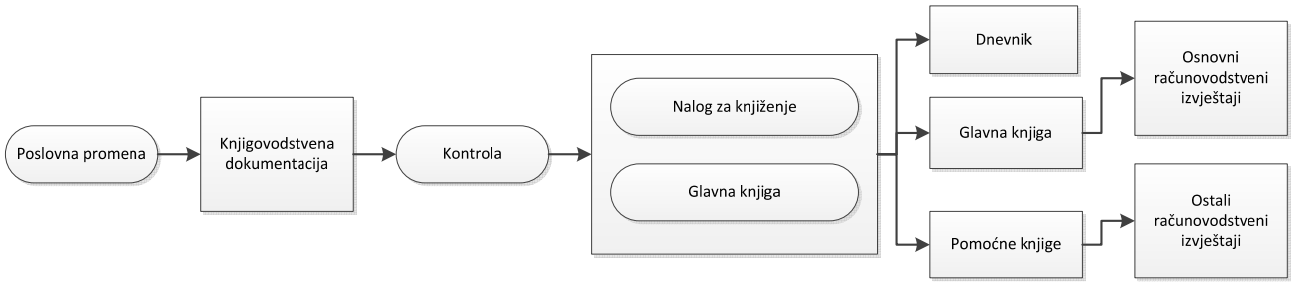
Kao ključne prednosti primjene informaciono-komunikacionih tehnologija u računovodstvenom procesu ističu se:

- povećana brzina obrade podataka, čime se omogućava ažurnost knjigovodstva i blagovremeno informisanje različitih korisnika putem različitih računovodstvenih informacionih sadržaja,
- vrlo jednostavna primjena računovodstvenih funkcija,
- veći nivo kvaliteta obrade, s aspekta potpunosti, preciznosti, preglednosti i tačnosti prezentovanih informacija,
- povećanje ukupne iskazne moći računovodstva, što podrazumijeva sveobuhvatnije informisanje korisnika,
- snižavanje troškova, naročito troškova papira, radne snage, distribucije i slično,
- veći kvalitet organizacionih rješenja,
- olakšavanje rada računovodstvenom osoblju, usljed smanjivanja rutinskih, a povećanja mogućnosti za vršenje kreativnih poslova, i
- lakša povezanost sa drugim organizacionim funkcijama preduzeća,
- kreiranje izvještaja u zahtjevanom trenutku.

Sa druge strane, moramo pomenuti i određene nedostatke primjene istih kao što su:

- gubitak podataka, zbog softverskih ili hardverskih kvarova,
- mogućnost greške, pošto softver ne može da misli, kao što čovjek može, mogu se desiti određene greške u procesu računovodstvene obrade, ili uslijed pogrešnog programiranja,
- veća izloženost prevarama ili malverzacijama, kao i hakerskim upadima u računovodstvene programe određenih kompanija,
- postojanje rizika, koje je uvijek bolje otkloniti osiguranjem, nego zapostavljanjem istih.

Proces knjiženja nastalih poslovnih promjena vrši se na osnovu formiranog naloga za knjiženje, kao jednog aplikativnog elementa, u koji se putem tastature i druge ulazne opreme unose podaci iz odgovarajućih knjigovodstvenih dokumenata. Knjigovođa upisuje u dati obrazac sve neophodne podatke iz knjigovodstvenog dokumenta (datum, šifru, iznos koji duguje ili potražuje i slično), i nakon toga unesene podatke šalje u centralnu jedinicu na dalju obradu. Zatim, centralna jedinica vrši obradu unijetih podataka, tačnije, automatski realizuje kompletnu računovodstvenu proceduru (knjiženje kroz dnevnik, glavnu knjigu, analitičke evidencije, analiza ravnoteže dugovnih i potražnih strana, izrada računovodstvenih izvještaja do datog trenutka, štampanje, ili automatsko slanje datih informacija daljim korisnicima) kao što je prikazano na sl. 1.



Sl. 1 Računovodstvena procedura primjenom IKT

Prevare u finansijskom izvještavanju, kojima se u ovom radu bavimo, mogu nastati u postupku kreiranja dokumentacije i obuhvatanja dokumentacije u knjigama, kao i u postupku izrade finansijskih izvještaja. Jasno je otuda da su brojni događaji i indicije, koje treba da revizora, menadžera ili bilo kog drugog korisnika finansijskih informacija koje prezentira neka kompanija navedu na sumnju da prevara postoji. Ovim indicijama i događajima treba pridodati, zbog gotovo jednakog značaja, i one koje potiču iz okruženja. Prema stepenu izvjesnosti da je uzrok određenih pojava prevara, svi događaji i indicije se mogu podijeliti u dvije grupe. Prvu grupu čine oni događaji čiji nastanak čini postojanje prevare izvjesnim, u literaturi označeni kao potencijalni okidači prevara, dok drugu grupu čine događaji i pojave koje mogu, ali i ne moraju biti indikatori prevara. Iako je broj događaja čiji nastanak indicira postojanje prevare veliki, ipak je moguće prema učestalosti njihovog nastanka i stoga i po značaju izdvojiti sljedeće [3]:

- anonimne optužbe za prevaru dostavljene pismom, elektronskom poštom, ili preko telefona,
- saznanje da je visokorangirani menadžer dao otkaz zbog poznatih ili mogućih nelegalnih poslova,
- kompanija – preduzeće je identifikovano kao predmet istrage koju sprovode sudski organi,
- preduzeće je dobilo poziv od suda ili od regulatorne agencije,
- revizor vjeruje da je namjerno doveden u zabludu verbalnim informacijama dobijenim od strane preduzeća ili da su zahtjevana dokumenta prepravljana ili je pak njihovo dostavljanje uskraćeno,
- otkriće da je klijent predmet prevare, u ma kako malom iznosu ona bila, čak i u onim slučajevima kada osumnjičeni nije više među zaposlenima,
- indikacije da dobavljači mogu biti fiktivni, i
- indikacije koje potiču od netačnog priznavanja prihoda ili rashoda kao što je priznavanje prodaje prije no što je ona konačna, isporuka robe prije konačne prodaje, priznavanje prihoda iako postoji obaveza izvršenja značajnih usluga u vezi sa tom robom u budućnosti, očigledno evidentiranje nepostojećih prihoda, odlaganje rashoda na buduće periode ili priznavanje rashoda budućih kao rashoda tekućeg perioda.

U pronalaženju dokaza koji potvrđuju postojanje prevara indiciranih bilo kojim od gore pomenutih događaja, a koji su počinjeni korišćenjem računara, pomaže nam digitalna forenzika.

IV. DIGITALNA FORENZIKA U RAČUNOVODSTVU

Najveći izazov u upotrebi digitalne forenzike i tehnika zasnovanih na računarskim tehnologijama u reviziji predstavlja širok opseg metoda digitalne analize, prikupljanja elektronskih dokaza, istraživanja podataka (eng. Data mining) kao i tehnika digitalne forenzike. U procesima zvanične istrage tehnikama digitalne forenzike, prikupljanja, analize i prezentacije digitalnih dokaza potrebno je pridržavati se određenih principa koji određuju proces upravljanja digitalnim dokazima. Ti principi treba da [4]:

- budu konzistentni sa svim legalnim sistemima,
- dopuštaju korišćenje s uobičajenim jezikom,
- budu trajni i međunarodno prihvatljivi,
- ulivaju povjerenje i obezbjeđuju integritet digitalnih dokaza,
- budu primjenljivi na sve vrste digitalnih dokaza,
- budu primjenljivi na svim nivoima, od pojedinca, preko zvaničnih agencije, do najvišeg nacionalnog nivoa.

V. ALATI I PROCEDURE U DIGITALNOJ FORENZICI

U digitalnoj forenzici dva vodeća softverska paketa su EnCase, firme Guidance Software i Forensic Toolkit (FTK), firme AccessData. Ovi aplikativni paketi omogućavaju brže savladavanje tehnika digitalne forenzike jer na jednom mjestu imamo obuhvaćeno više zadataka za koje bi inače koristili više alata. U posljednjih nekoliko godina alati bazirani na Linux platformi postali su popularni i često se koriste kao besplatna alternativa. Helix, the Penguin Sleuth i BackTrack su Linux distribucije koje se pokreću direktno sa CD-a pružajući čisto okruženje za istragu, bez potrebe za kloniranjem sistema. Ovi alati pokreću Linux sistem sa CD-a, a hard diskove računara učitavaju u režimu za čitanje zaobilazeći većinu lozinki i bezbjedonosnih zaštita. Glavna mana Linux rješenja je u njihovoj kompleksnosti kao i u slaboj podršci. Takođe, dostupni su specijalizovani alati koji su usmjereni na otključavanje lozinki i vraćanje obrisanih fajlova.

Od forenzičara se očekuje razumijevanje procesa brisanja fajla u NTFS fajl sistemu i razlikovanje tog procesa od korišćenja Recycle bin-a. Postoji više načina na koji korisnik može brisati fajl, a sljedeći metodi šalju izbrisani fajl u Recycle bin [5]:

1) Desni taster miša i selektovanje Delete,
2) Drag&Drop u Recycle bin,
3) Taster Delete, potvrđeni Delete.

Sljedeći metodi brišu fajl iz fajl sistema zaobilazeći Recycle bin:

1) Shift + Delete,
2) Delete u DOS-u.

Brisanje fajla u NTFS fajl sistemu zahtjeva promjene u metadata fajlovima. Kad se izvrše promjene u metadata fajlovima, $Logfile treba da prati te promjene za potrebe oporavka. Tako će brisanje fajla biti ažurirano u $Logfile. Svaki fajl u NTFS ima jedan ulaz u MFT tabeli i zato, ako se fajl briše iz fajl sistema tada se on mora izmijeniti i u $MFT ulazu zaglavlja, da bi odrazilo tekuće stanje ulaza.

U MFT ulazu zaglavlja ažuriraju se bajtovi 22 i 23 [6]. Moguća stanja koja možemo naći na ovim lokacijama su:

00 00 = Izbrisani fajl,

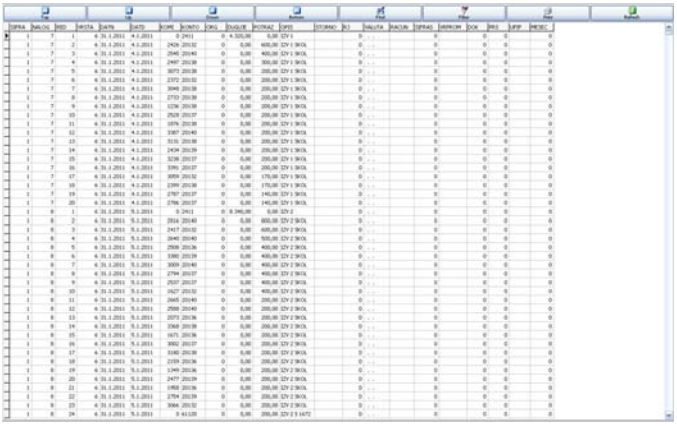
01 00 = Aktivan fajl,

02 00 = Izbrisani direktorijum,

03 00 = Aktivan direktorijum.

Proces obezbjeđenja ili pribavljanja dokaza počinje sa pregledanjem sadržaja hard diska računara ili drugih medija. Za pronalaženje elektronskih podataka, uključujući izbrisane informacije, uređaji za skladištenje moraju biti klonirani ili duplirani bit po bit. Stvarna veličina prostora za skladištenje i brzine prenosa preko mrežnog kabla će diktirati dužinu vremena potrebnog da se disk klonira. Kada je uređaj za skladištenje obezbjeđen, drugi uređaj je potreban kao radna kopija kako bi originalna kopija ostala nepromijenjena. Ovo omogućava da i drugi istraživači imaju pristup nepromijenjenoj kopiji elektronskih podataka.

Na slici 2 se može vidjeti prikaz forenzičke analize jednog od fajlova koji se nalaze u aplikaciji za knjiženje.



Sl. 2 Forenzička analiza tabele sa podacima knjiženja

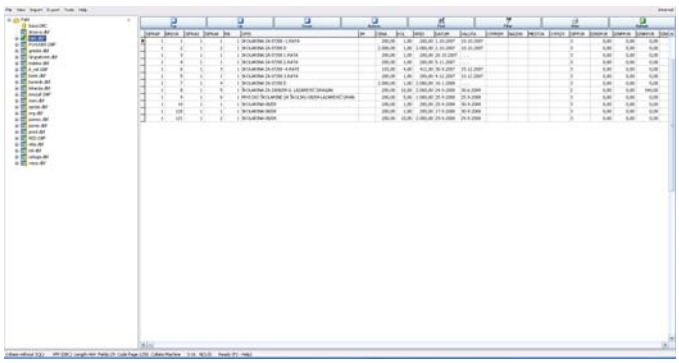
Naredni korak u prikupljanju dokaza je faza pregleda. U ovoj fazi revizor ili istražitelj izvršava jednostavnu provjeru ili pregled dostupnih podataka da bi utvrdio stanje. Ova faza može pružiti korisne informacije o vlasništvu podataka kao i da usmjeri nastavak istrage. Svi podaci se moraju analizirati, uključujući izbrisane ili fajlove koji su djelimično prepisani, podatke skrivene van standardnih lokacija kao i podatke u virtuelnoj memoriji. Najčešći metod koji se koristi za pribavljanje ovih podataka je upotreba uređaja koji blokiraju upisivanje podataka. Ovakav uređaj sprječava da se tokom analize izvrši bilo kakva izmjena nad podacima koji se istražuju. Windows operativni sistem je posebno problematičan u ovakvim situacijama. Najčešće se disk izvadi iz računara koji se istražuje i priključuje se na uređaj za blokiranje upisivanja. Nakon ovog, pristupa se pravljenju ili kloniranju diska koji treba ispitati. Ovaj proces kreira identičnu repliku postojećeg diska procesom kopiranja bit po bit.

Druga metoda pribavljanja podataka podrazumijeva upotrebu neke od „live“ distribucija Linux-a koja omogućava da istražitelj pregleda datoteke na disku uključujući i izbrisane, bez promjene na disku koji se ispituje. Istražitelj zatim može prekopirati datoteke za koje postoji interes da ih prikaže ili detaljnije ispita. Skriveni podaci najčešće sadrže vitalne dokaze koji mogu dokazati ili opovrgnuti slučaj. Koraci koje treba poštovati tokom pribavljanja i analize dokaza su:

- Nikada ne raditi analizu na prvobitno kreiranom klonu diska, uvijek napraviti dodatnu radnu verziju.
- Prije rada na radnoj verziji treba izvršiti hešovanje verzije, zbog potvrde da nije došlo do promjene u toku istrage.
- Praviti bilješke o svim pronalascima.
- Što češće snimati rezultate zbog potencijalnog gubitka električne energije i gubitka podataka [7].

Prije i tokom forenzičke analize, potrebno je da revizori preduzmu dodatne korake da bi obezbijedili dokaze. Prije forenzičkog pregleda, revizor mora fizički obezbijediti sistem koji ispituje, fotografisati prostoriju, prostor oko sistema i sam sistem. Pored toga, revizor mora obezbijediti dokaze na licu mjesta ili u laboratoriji u kojoj se vrši pregled zbog pravilnog rukovanja dokazima. Revizor, takođe, treba da dokumentuje sve detalje u vezi sistema kao i povezanost sistema putem žične ili bežične mreže. Postoje i određene procedure i postupci koje treba maksimalno izbjegavati prije prikupljanja datoteka i kloniranja diska:

- Modifikovanje sistemskog vremena, kao i „time stamp“ vremena
- Pokretanje aplikacija ili neprovjerenih programa na računaru koji se istražuje (npr. tajni podaci.exe aplikacija može biti zamka - program koji će kada se pokrene izbrisati sve dokaze na disku)
- Prekid procesa koji se obavlja na računaru ili gašenje aplikacije u upotrebi (ovo može prouzrokovati brisanje log datoteke ili prekida komunikacije sa udaljenom lokacijom)
- Ažuriranje sistema prije forenzičke istrage
- Propust u evidentiranju komandi koje se izvršavaju
- Instalacija softvera na sistem.



Sl. 3 Analiza baze podataka sa podacima iz aplikacije za knjigovodstvo

Na slici 3 se vidi ostvaren pristup i pregled svih unosa u program za knjiženje. Ovakvim pregledom utvrđeno je da se može izvršiti nesmetan pristup kompletnoj bazi kao i mogućnost da se vrše izmjene ili manipulacije nad svim podacima. Većina preduzeća i organizacija imaju procedure kojima pokušavaju spriječiti prevare i malverzacije. Dobra tehnika forenzičke revizije je pokušavanje i pronalaženje slabosti u tim sigurnosnim procedurama i na taj način pronalaženje slabosti u samom sistemu. Slabosti koje se pronađu u okviru kontrole organizacije najvjerovatnije će odvesti do počinioca.

U slučaju potreba za pronalaženjem sličnih dokumenata i poređenja nekog postojećeg dokumenta metoda koja je dala najbolje rezultate je upotreba segmentnog hešovanja iniciranog sadržajem [8]. Ova metoda nudi mogućnost poređenja postojećih fajlova uz identifikovanje indeksa sličnosti.

A. *Encase*

EnCase je alat za kompjutersku forenziku od proizvođača Guidance Software i koristi se za analizu digitalnih medija (na primjer u kriminalnim istragama). Za upotrebu ovog softvera obično je neophodna specijalna obuka. Podaci otkriveni putem EnCase alata uspješno se koriste na raznim sudovima širom svijeta.

EnCase je trenutno jedan od najboljih paketa za kompjutersku forenziku upravo zbog raznovrsnih komponenti koje posjeduje. Na primjer, korisnici koji žele da istraže neki sumnjivi medijum, ali ne žele tome da posvete vrijeme koje je neophodno kako bi se napravio klon diska, mogu da izvrše samo pregled sumnjivog diska. Za vrijeme ovog pregleda, istražitelji mogu da vode bilo kakve analize koje se preduzimaju i u slučaju da se ispituje klon diska. Kasnije verzije ovog softvera omogućavaju korisnicima da snime stanje forenzičkog istraživanja koje se izvodi metodom pregleda. Prava vrijednost ove osobine dolazi do izražaja u situacijama kada vrijeme, koje je neophodno za pravljenje replike diska ili kloniranje sa više diskova, može dovesti istragu u opasnost. Ukoliko uzmemo za primjer neku istragu koja uključuje 10 računara, gdje je za snimanje svakog pojedinačno neophodno najmanje 30 min, onda se istraživač susreće sa zadatkom koji će trajati više sati. Međutim, otvara se pitanje da li je sigurno da svaki od tih diskova sadrži dokaz. Ukoliko nije sigurno, onda bi prethodni pregled diska mogao da uštedi sate istrage. U takvom slučaju, istraživač bi najprije mogao da izvrši pregled diska, a da nakon toga snimi samo one diskove koji su značajni za slučaj.

Druga važna osobina EnCase softvera je njegova mogućnost da odradi kloniranje diska korišćenjem mrežnog kabla ili serijskog kabla. Iako je za ovakav vid kloniranja diska potrebno više vremena, prednost je da analitičar ne mora da ukloni fizički disk sa kompjutera. EnCase softver omogućava korisnicima da kreiraju butabilan disk koji će zaštititi podatke od toga da budu upisani na neki sumnjivi disk prilikom procesa pokretanja računara. Jednom kada se kompjuter pokrene i krene sa radom, forenzičar može da krene sa kloniranjem diska, bilo pomoću mrežnog ili serijskog kabla. Kada se kreira klon diska, EnCase softver omogućava pretraživanje hard diska na neki od sljedećih načina:

- Istraživanje slika sa hard diska pregledom pomoću galerije
- Istraživanje fajlova korišćenjem heksa pogleda (čitanje heksadecimalnih komponenti fajla)
- Pretraživanje cjelokupnog diska na ključne riječi.

EnCase alat, takođe, posjeduje mogućnost izvještavanja što omogućava istražiteljima da sačuvaju pronađene ključne riječi, slike i da snime lične komentare u formatu koji je lak za izvještavanje. Na taj način, informacije mogu da se štampaju ili proslijede mail-om onima koji su uključeni u slučaj [9].

VI. ZAKLJUČAK

Forenzička nauka, bez obzira na polje svog djelovanja, podrazumijeva primjenu nauke u izvođenju dokaza. Obzirom da su računovodstvene prevare u današnje vrijeme postale veliki problem, a razvojem informacionih tehnologija, njihovo činjenje je i olakšano. Sada nam ostaje da veću pažnju posvetimo otkrivanju već počinjenih zloupotreba putem računara, u čemu nam može pomoći digitalna forenzika, kao i prevenciji od nastajanja budućih zloupotreba dajući naglasak na zaštitu informacionih sistema. Borba protiv kompjuterskog kriminala je sve teža i zahtjeva izuzetna znanja i vještine. Digitalna forenzika, kao efikasno sredstvo u toj borbi, pronalazi svoju široku primjenu te se ubrzano razvija kao posebna grana forenzike.

LITERATURA

[1] Managing the Business Risk of Fraud, A Practical Guide, http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/managing-business-risk.pdf; dostupno januar 2013.

[2] V. Belak, Poslovna forenzika i forenzično računovodstvo, Belak Excellens d.o.o., Zagreb, 2011.

[3] Golden, T., Skalak, S., Clayton, M., A Guide to Forensic Accounting Investigation, John Wiley&Sons, Inc. 2006.

[4] M. Milosavljević, G. Grubor, Istraga kompjuterskog kriminala, Univerzitet Singidunum, Beograd, 2009.

[5] National Policing Improvement Agency, Core Skills in Data Recovery & AnalysisCourse Reference Book V2.01, Bradford, UK, maj 2007.

[6] Data recovery e-book, CHENGDU YIWO Tech Development Co., Ltd 2006.

[7] http://www.theiia.org/intAuditor/itaudit/archives/2006/september/computer-forensics-a-valuable-audit-tool-1/; dostupno januar 2013.

[8] N. Ristić, A. Jevremović, M.Veinović, "Identifikovanje homogenih fajlova upotrebom segmentnog hešovanja iniciranog sadržajem", 20th Telecommunications forum TELFOR 2012, Serbia, Belgrade, November 20-22, 2012, 1665-1668

[9] Advances in Digital Forensics II: IFIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, January 29-February 1, 2006

ABSTRACT

Digital Forensics as a branch of forensic science, deals with legal methods of collecting and processing evidence stored on a computer or other digital data carrier, related to some sort of illegal activity. On the other hand, forensic accounting has the task to identify and investigate any suspicious economic transactions that can be characterized as fraud and result in litigation. With the increasing digitalization of data, and the development of accounting software, there was a need for the application of digital forensics tools in the investigation and obtaining evidence of criminal activity in the financial statements.

DIGITAL FORENSICS IN A FUNCTION OF FORENSIC ACCOUNTING

Nataša Simeunović, Nenad Ristić

nsimeunovic@sinergija.edu.ba, nristic@sinergija.edu.ba