Originalni naučni rad
DOI: 10.47152/Palic2025.3

PRIMENA DIGITALNE FORENZIKE U INFORMACIONO-TEHNIČKIM I FINANSIJSKIM ISTRAGAMA

Marko LAKIĆ*

Iako se često tvrdi da digitalna forenzika postaje sve značajniji alat u savremenim informaciono-tehničkim (IT) i finansijskim istragama, praksa pokazuje da ona nije toliko mlada disciplina kako to predstavlja ustaljeno mišljenje među pravnicima. Ovaj rad istražuje primjenu digitalne forenzike u savremenim sudskim postupcima, sa posebnim fokusom na propuste koji se javljaju prilikom rukovanja digitalnim dokazima. Cilj rada je da ukaže na potencijal digitalne forenzike u predmetima koji uključuju nelegalne finansijske aktivnosti, ali i na ozbiljne posledice koje mogu nastati usled neadekvatnog postupanja s digitalnim tragovima. Metodološki, rad se prvenstveno oslanja na analizu konkretnih slučajeva iz prakse. Rezultati sugerišu da efikasna primena digitalne forenzike zavisi pre svega od tehničke obučenosti kadra, jasnog pravnog okvira i institucionalne spremnosti da se ova znanja i alati u praksi primene. Zaključuje se da digitalna forenzika predstavlja ključnu komponentu savremenih istraga, te da njena pravilna upotreba može značajno unaprediti otkrivanje i procesuiranje učinilaca, dok neadekvatan pristup može dovesti do njihovog izostanka iz krivičnopravnog sistema.

* Sudski veštak informaciono-tehničke struke i oblast telekomunikacija; predsednik Udruženja sudskih veštaka Crne Gore. E-mail: marko@lakic.me.

Ključne reči: digitalna forenzika, informaciono-tehničke istrage, finansijske istage, digitalni dokazi

UVOD

U današnjem digitalnom okruženju granice između informacione bezbednosti, finansijskog nadzora i pravne regulative postaju sve nejasnije. Povećana upotreba informacionih tehnologija u svakodnevnom životu i radu dovela je do porasta različitih oblika digitalnog kriminala, uključujući sajber prevare, nelegalne finansijske transakcije i zloupotrebu podataka. U takvom kontekstu, digitalna forenzika sve češće se prepoznaje kao ključni alat za otkrivanje, dokumentovanje i procesuiranje dokaza u elektronskom formatu.

Ipak, uprkos rastućem značaju ove discipline, praksa pokazuje da i dalje postoje ozbiljne prepreke za njenu efikasnu primenu. Nedovoljna obučenost kadrova, zastareo zakonski okvir i neujednačena praksa u radu sa digitalnim dokazima predstavljaju ključne izazove za institucije koje sprovode IT i finansijske istrage. Dodatno, uočava se i određeni stepen nerazumevanja, pa čak i potcenjivanja značaja digitalnih tragova unutar pravosudnog sistema.

Cilj ovog rada je da ispita načine na koje se digitalna forenzika koristi u okviru navedenih istraga, da ukaže na praktične izazove sa kojima se suočavaju stručnjaci u ovoj oblasti, kao i da predloži mogućnosti za unapređenje postojećeg pristupa kroz bolje povezivanje tehničkih, pravnih i organizacionih aspekata.

Teorijski okvir

Digitalna forenzika je naučna disciplina koja se bavi metodama identifikacije, očuvanja, analize i prezentacije digitalnih dokaza. Njena osnovna funkcija je da pruži preciznu i zakonitu analizu podataka koji se koriste kao dokazi u sudskim i drugim pravnim postupcima. Digitalni dokazi se mogu naći u različitim oblicima, uključujući elektronske poruke, logove aktivnosti na mreži, slike, fajlove i podatke sa mobilnih uređaja (Casey, 2011; Nelson et al., 2018).

Digitalna forenzika je postala ključna u istrazi i procesuiranju sajber kriminala, kao i u analizi finansijskih transakcija. Forenzička analiza omogućava da se otkriju zločini koji se odvijaju u digitalnim sistemima, kao što su prevare, pranje novca i druge nelegalne aktivnosti u vezi sa informacionim tehnologijama.

Informaciono-tehničke istrage

Informaciono-tehničke istrage predstavljaju skup aktivnosti usmerenih na otkrivanje, dokumentovanje i analiziranje podataka u informacionim sistemima, sa ciljem identifikacije izvora propusta, kompromitovanih podataka ili nezakonitih radnji u digitalnom okruženju. Ove istrage se sprovode u različitim kontekstima – od incidenata u korporativnim mrežama, preko sajber napada, do internih zloupotreba informacionih sistema.

Finansijske istrage (klasični model)

Finansijske istrage u klasičnom modelu fokusiraju se na analizu i istraživanje finansijskih transakcija, sa ciljem identifikacije nepravilnosti, prevara, ili drugih oblika zloupotrebe u finansijskim sistemima. Ove istrage često obuhvataju analizu računovodstvenih evidencija, izveštaja, transakcija i postupaka koji mogu ukazivati na nelegalne aktivnosti, kao što su pronevera, prevara ili pranje novca.

Proces klasične finansijske istrage obuhvata sledeće korake:

1. Prikupljanje i analiza finansijskih dokumenata – računovodstvenih izveštaja, faktura, bankovnih izvoda i drugih poslovnih dokumenata koji mogu ukazivati na nepravilnosti.
2. Analiza tokova novca – identifikacija i praćenje tokova novca kako bi se utvrdilo poreklo sredstava i potencijalne ilegalne aktivnosti.
3. Obdukcija knjigovodstvenih praksi – procena validnosti računovodstvenih postupaka i usklađenost sa važećim zakonodavstvom i standardima.
4. Intervjui i istrage sa zaposlenima – razgovori sa ključnim osobama u organizaciji kako bi se utvrdile namere i razjasnile okolnosti.
5. Izveštavanje i preporuke – izrada izveštaja sa zaključcima o utvrđenim nepravilnostima i preporukama za dalje postupanje.

Primena digitalne forenzike u informaciono-tehničkim i finansijskim istragama

Digitalna forenzika se pokazuje kao ključna alatka za uspešno sprovođenje informaciono-tehničkih i finansijskih istraga. Informaciono-tehničke istrage ne odnose se samo na delovanja iz oblasti sajber kriminala, već su od presudne važnosti u detektovanju i analizi nelegalnih radnji u svim vrstama finansijskih istraga. U današnjem

digitalnom okruženju, klasični model finansijskih istraga gotovo da nema smisla bez primene digitalne forenzike, jer se najveći broj dokaza nalazi u digitalnom formatu i u velikom broju slučajeva ne postoji fizički oblik tih podataka.

Finansijske istrage koriste digitalne alate za praćenje tokova novca i povezivanje finansijskih transakcija sa fizičkim dokazima. Uparivanjem podataka do kojih se dolazi kroz analizu telefonskih uređaja, personalnih računara, ličnih rokovnika i drugih izvora, istražitelji mogu da stvore celovitu sliku događaja, povežu ključne aktere i otkriju obim prevara ili drugih nezakonitih aktivnosti.

Za uspešan ishod istrage, izuzetno je važno da se dokazi prikupljaju i dokumentuju na odgovarajući način, kako bi bili prihvaćeni kao validni u sudskom postupku.

Metodologija

Digitalna forenzika u informaciono-tehničkim i finansijskim istragama primenjuje se kroz nekoliko ključnih koraka, koji uključuju identifikaciju, očuvanje, analizu i interpretaciju digitalnih podataka. Ovaj proces zahteva primenu specijalizovanih alata i metoda kako bi se osiguralo da se svi dokazi prikupljeni u toku istrage mogu koristiti u sudskom postupku. U kontekstu informaciono-tehničkih i finansijskih istraga, digitalna forenzika se primenjuje kroz sledeće ključne faze:

1. Prikupljanje podataka
2. Analiza podataka
3. Rekonstrukcija događaja
4. Pravilno čuvanje dokaza i pravna validnost
5. Izveštavanje i preporuke

Kroz ove faze, digitalna forenzika omogućava identifikaciju i analizu podataka koji bi inače ostali neprepoznati. Efikasna primena metodologije digitalne forenzike ne samo da pomaže u razumevanju kriminalnih aktivnosti, već takođe omogućava efikasno rešavanje slučajeva i donošenje zakonskih odluka koje mogu imati dugoročne posledice za organizacije i pojedince (Casey, 2011).

Studija slučaja i primeri iz prakse

Primer 1. Nezakonito preknjižavanje robe u telekomunikacionoj kompaniji

U jednoj telekomunikacionoj kompaniji, u sistemu za automatsku obradu podataka (SAP), pripravnica je uočila nelogične aktivnosti u vezi sa knjiženjem robe. Naime, zaposleni u kompaniji izvršava preknjižavanje robe iz jedne vrste u drugu, čime menja realno stanje robe na zalihama. Preknjižavanje se vrši na način da robu vrednu nekoliko miliona evra, koja je regularno popisana i kontrolisana, preknjižava u robu koja ima vrednost od nekoliko centi, i koja se zbog velike količine ne broji prilikom popisa. Ova roba se obično ne računa zbog niske vrednosti i velike količine, što omogućava prekršiocu da obezbedi nelegalne koristi, dok sama roba ostaje fizički prisutna u magacinu, ali se u sistemu ne vidi zbog pogrešnog knjiženja.

Konkretno, preknjižavanje je vršeno na način da je vrednost jedne dopune prepaid broja (5 €) preknjižena u naljepnice za pakete, čija vrednost nije prelazila 1 cent po komadu. Na taj način, sistem je prikazivao manje količine visokovredne robe, dok je stvarna količina proizvoda u magacinu bila znatno veća. Iako je pretnja bila evidentna, kroz sistem nije bila moguća trenutna detekcija ovih grešaka jer su sistem i interni procesi bili prilagođeni velikim količinama niskovrednih predmeta, kao što su naljepnice za pakete.

U okviru IT dela istrage, detaljno su analizirani podaci o svim preknjižavanjima u SAP sistemu. Ispitani su svi logovi transakcija, uključujući korisničke aktivnosti i podešavanja koja su omogućila ovakve izmene. Analizom je utvrđeno da je prekršilac koristio administrativna prava za obavljanje ovih preknjižavanja, kao i da je sistem dozvoljavao ovakve izmene bez dodatnih provera, što je omogućilo manipulaciju.

Finansijski deo istrage je omogućio dodatnu dubinsku analizu, koja je uključivala praćenje tokova novca povezanih sa preknjižavanjima, kao i analizu podataka sa računara i mobilnog telefona zaposlenog. Detaljno su pregledani komunikacioni zapisi, uključujući e-mailove, SMS poruke, i interne poruke na poslovnoj mreži, kroz koje su zaposlenima bili upućeni podaci za dalje distribucije.

Uz pomoć analize informacija iz rokovnika zaposlenog, pronađeni su tragovi koji su ukazivali na povezana lica, odnosno na osobe koje su direktno ili indirektno učestvovale u distribuciji nelegalno prisvojenih prepaid dopuna. Ove dopune su zatim prodavane na crnom tržištu, što je

generisalo značajan prihod. Ispitani su načini na koje su povezana lica koristila dopune, kao i na koji način je zaposleni trošio novac koji je stekao prodajom tih dopuna, uključujući analizu njegovih bankovnih izveštaja i transakcija na računima, što je dovelo do otkrivanja novih dokaza.

Ovaj slučaj jasno pokazuje kako multidisciplinarni pristup IT i finansijskim istragama omogućava identifikaciju i analizu složenih nelegalnih aktivnosti. Kroz sinergiju forenzičkih alata, finansijskih analiza, kao i pristupa pravnim metodama, uspešno je razotkrivena ozbiljna finansijska prevara, a dalje istrage i sudski postupci omogućili su pokretanje krivičnih prijava prema osumnjičenima.

Primer 2. Trgovina uticajem i značaj poštovanja procedura

U drugom primeru, policija je sprovela operativni rad koji je doveo do osnova sumnje za krivično delo trgovina uticajem. Tokom istrage, svedoci su saslušavani i njihova iskazi su doprinosili razumevanju obima sumnje, koja je postepeno evoluirala u osnovanu sumnju. Ovaj napredak je omogućio izdavanje Naredbe za sprovođenje istrage, kao i Naredbe za veštačenje relevantnih uređaja koji su bili povezani sa osumnjičenim licima.

Međutim, iako su postojale konkretne naredbe za sprovođenje istrage, tokom veštačenja uređaja došlo je do ozbiljnih proceduralnih grešaka. Prvenstveno, nije primenjena odgovarajuća metodologija za sakupljanje digitalnih dokaza, što je uključivalo nepoštovanje propisa o zaštiti integriteta podataka. Umesto da se primene standardizovane forenzičke tehnike i alati za očuvanje nepromenjenosti podataka, kao što je bit-po-bit kopiranje podataka sa uređaja, korišćeni su nespecijalizovani alati, što je dovelo do mogućnosti izmene originalnih podataka. Takođe, nisu poštovani postupci za zaštitu fizičkih uređaja i nisu sprovedene sve potrebne sigurnosne mere prilikom transporta i čuvanja tih uređaja. Ove greške su stvorile osnovu za osporavanje autentičnosti dokaza tokom sudskog postupka.

Dodatno, u toku analize podataka, veštaci koji su obavljali analize nisu bili dovoljno obučeni u specifičnostima digitalnih forenzičkih alata potrebnih za analizu dokaza ove vrste. Nedostatak stručnosti u kombinaciji sa tehničkim propustima doveo je do situacije u kojoj su rezultati analize bili diskutabilni i nedovoljno utemeljeni. U suštini, sve dokaze koji su bili ključni za razumevanje načina na koji je trgovina uticajem vršena, a koji su bili pohranjeni na računarskim uređajima, morali su da budu izuzeti iz spisa predmeta. Sud je prihvatio tvrdnje

odbrane o mogućem falsifikovanju podataka, i samim tim svi digitalni dokazi su izgubili svoju pravnu validnost.

Zbog nedostatka drugih relevantnih dokaza, optužnica je bila odbačena, a osumnjičeni su oslobođeni. Ovaj slučaj pokazuje koliko je bitno poštovanje striktnih procedura prilikom rukovanja digitalnim dokazima. Svaka greška u postupku, bilo da se radi o nepravilnom prikupljanju, analizi, skladištenju, ili čak izveštavanju o rezultatima analize, može ugroziti validnost dokaza. Ovaj slučaj je poslužio kao primer za sve istražitelje i pravosudne organe o značaju tačnog primenjivanja forenzičkih tehnika i pravilnog rukovanja digitalnim podacima kako bi se obezbedio zakonit ishod.

Situacija u praksi pokazuje da često policijski timovi na terenu nemaju adekvatna znanja, resurse ili opremu da pravilno postupaju sa digitalnim dokazima. Zbog toga je vrlo važno da se svi učesnici u istražnim procesima redovno obučavaju i koriste standardizovane metode kako bi se osigurala preciznost i tačnost tokom celokupnog procesa. Bez odgovarajuće obuke i osiguravanja tehničke i proceduralne usklađenosti, istrage mogu naići na ozbiljne prepreke, što može dovesti do nepovratnih grešaka i neuspeha u postupku.

Ovaj primer takođe naglašava da digitalna forenzika nije samo tehnička, već i pravna disciplina koja zahteva sinergiju između tehničkih, pravnih i organizacionih aspekata istrage. Samo koordinisani rad između forenzičara, pravnika i istražitelja može obezbediti da svi dokazi budu pravilno prikupljeni, analizirani i upotrebljeni na sudu.

Diskusija i analiza problema i izazova

Izazovi u prikupljanju i očuvanju dokaza

Problem: Prikupljanje digitalnih dokaza često je teško zbog velikih količina podataka i njihove fragmentacije. Takođe, dokazni materijali često mogu biti lako promenjeni, obrisani ili oštećeni ako se ne preduzmu odgovarajuće mere zaštite.

Izazov: Kako obezbediti da se digitalni dokazi prikupljaju na način koji omogućava njihovu zakonsku prihvatljivost i integritet tokom celog procesa istrage?

Rešenja: Korišćenje naprednih alata za forenzičko prikupljanje podataka koji omogućavaju bit-po-bit kopiranje podataka, kao i usklađivanje sa zakonskim normama za zaštitu dokaza.

Tehnička složenost i stalne promene u tehnologiji

Problem: Tehnološki napredak često stvara nove oblike sajber kriminala i novih metoda napada, dok postojeći alati brzo zastarevaju.

Izazov: Kako se stručnjaci za digitalnu forenziku mogu držati korak sa stalnim promenama u tehnologiji i razvijati alate koji odgovaraju na nove pretnje?

Rešenja: Kontinuirana obuka i sertifikacija stručnjaka, ulaganje u razvoj novih alata i tehnologija koje mogu efikasno analizirati nove oblike malvera, napada i digitalnih tragova.

Ljudski faktor i obuka stručnjaka

Problem: Mnogi profesionalci u oblasti digitalne forenzike ne poseduju odgovarajuće veštine, što može ugroziti tačnost i efikasnost istraga.

Izazov: Kako osigurati da stručnjaci za digitalnu forenziku imaju potrebne veštine i znanje, posebno u IT i finansijskim istragama?

Rešenja: Razvijanje specijalizovanih programa obuke i certificiranja, uključivanje forenzičara u stalne profesionalne organizacije i mreže koje podržavaju razmenu znanja i iskustava.

Pravni okvir i saradnja sa pravosudnim sistemom

Problem: Zakoni koji regulišu digitalne dokaze i sajber kriminal nisu uvek ažurirani, što može otežati korišćenje digitalnih dokaza u sudskim postupcima.

Izazov: Kako obezbediti da digitalni dokazi uvek budu zakonski prihvatljivi i da se procesuiranje kriminalaca ne odlaže zbog pravnih nesigurnosti?

Rešenja: Proširenje zakonodavstva za bolje praćenje novih tehnoloških pretnji, uključujući usklađivanje sa međunarodnim normama i praksama za forenzičko sakupljanje podataka.

Zaštita privatnosti i etička pitanja

Problem: S obzirom na to da digitalna forenzika uključuje analizu ličnih podataka, postoji ozbiljan rizik od kršenja privatnosti ili zloupotrebe podataka.

Izazov: Kako balansirati između efikasne istrage i poštovanja prava pojedinaca na privatnost?

Rešenja: Implementacija etičkih smernica i procedura koje omogućavaju pravilnu selekciju podataka koji se analiziraju, kao i striktna ograničenja u vezi sa pristupom osetljivim informacijama.

Kompleksnost u analizi i interpretaciji dokaza

Problem: Ponekad se podaci iz digitalnih sistema moraju analizirati i interpretirati u kontekstu specifičnih pravnih normi ili poslovnih procesa, što može biti izazovno, pogotovo kada su podaci fragmentirani ili skrivani.

Izazov: Kako izvući tačne zaključke i interpretirati digitalne dokaze u kontekstu zakonodavnih i organizacionih normi?

Rešenja: Saradnja između IT stručnjaka, finansijskih analitičara, pravnika i drugih stručnjaka kako bi se pravilno interpretirali podaci u skladu sa zakonodavstvom i poslovnim praksama.

ZAKLJUČAK I PREPORUKE

Zaključak

Digitalna forenzika je ključna u istražnim postupcima, posebno u IT i finansijskim istragama, jer omogućava otkrivanje složenih kriminalnih aktivnosti koje bi inače prošle nezapaženo. Ipak, praksa pokazuje da se suočavamo sa značajnim izazovima - stalna promena tehnologije, nedostatak edukovanih stručnjaka, neadekvatan pravni okvir i česte greške u postupanju sa digitalnim dokazima.

Studije slučaja, kao što su slučaj u telekomunikacionoj kompaniji i trgovina uticajem, ukazuju na realnost ovih problema i njihovu mogućnost da značajno utiču na uspeh istraga. Multidisciplinarni pristup koji uključuje saradnju IT stručnjaka, finansijskih analitičara i pravnika postaje neophodan za efikasno rešavanje savremenih kriminalnih slučajeva. Nažalost, takav pristup nije uvek prisutan, pa često dolazi do gubitka podataka ili otežanog povezivanja svih podataka u toku istrage. Najbolja opcija bila bi kada bi stručnjaci bili obučeni za oba područja – IT i finansije, ali to je retkost, naročito u državnim institucijama.

Preporuke

Unapređenje zakonodavnog okvira: Potrebno je ažurirati zakonske regulative koje se odnose na digitalne dokaze. Jasne pravne norme omogućile bi veću pravnu sigurnost i tačnost tokom istražnih postupaka.

Povećanje ulaganja u obuku i sertifikaciju stručnjaka: Stručnjaci za digitalnu forenziku moraju biti stalno obučavani i sertifikovani kako bi odgovarali na nove tehnologije. Obuka treba da obuhvati međunarodne standarde i metodologiju kako bi se obezbedila usklađenost sa globalnim normama.

Razvijanje novih forenzičkih alata: S obzirom na brzinu tehnološkog napretka, nužno je ulagati u razvoj alata za analizu novih vrsta digitalnih tragova, omogućavajući efikasnu analizu i zaštitu od manipulacije.

Jačanje saradnje između IT, finansijskih analitičara i pravnih stručnjaka: Multidisciplinarni timovi treba da sarađuju od početka istrage, kako bi se podaci efikasno analizirali, a dokazi prikupili na zakonit način. Timska saradnja smanjuje rizik od grešaka i omogućava bolju interpretaciju podataka.

Značaj poštovanja procedura i metodologije: Ključna preporuka je striktno poštovanje svih procedura prilikom rukovanja digitalnim dokazima. Greške u bilo kojem od ovih koraka mogu ugroziti validnost dokaza i dovesti do neuspešnih optužbi.

Podrška institucionalnim i vladinim inicijativama: Potrebno je ulagati u razvoj institucija koje se bave digitalnom forenzikom i pronaći načine da se kvalifikovan kadar zadrži u tim institucijama. Državne institucije često nemaju modalitete da zadrže iskusne i obučene stručnjake, što je velika prepreka za efikasnu borbu protiv ove vrste kriminala.

LITERATURA

Casey, E. (2011) *Digital Evidence and Computer Crime*. Academic Press.

Mandia, K., Prosise, C., Pepe, M. (2003) *Incident Response & Computer Forensics*. McGraw-Hill/Osborne.

Nelson, B., Phillips, A., Steuart, C. (2018) *Guide to Computer Forensics and Investigations*. Cengage Learning.

Singleton, T. W., Singleton, A. J. (2010) *Fraud Auditing and Forensic Accounting*. Wiley.

Wells, J. T. (2017) *Corporate Fraud Handbook: Prevention and Detection*. Wiley.

Gajić, D. (2017) *Digitalna forenzika i zaštita podataka*. Novi Sad: Fakultet tehničkih nauka.

Milić, M. (2016) *Kriminalistička forenzika u informatičkom okruženju*. Beograd: Akademska misao.

Petrović, M. (2019) *Sajber kriminal i digitalna forenzika: Teorija i praksa*. Beograd: Univerzitet u Beogradu.

Marko LAKIĆ*

APPLICATION OF DIGITAL FORENSICS IN INFORMATION TECHNOLOGY AND FINANCIAL INVESTIGATIONS

Although it is often claimed that digital forensics is becoming an increasingly important tool in modern information technology (IT) and financial investigations, practice shows that it is not as new a discipline as commonly believed among legal professionals. This paper examines the application of digital forensics in modern judicial procedures, with a particular focus on the shortcomings that arise when handling digital evidence. The aim of the paper is to highlight the potential of digital forensics in cases involving illegal financial activities, as well as the serious consequences that can arise from inadequate handling of digital traces. Methodologically, the paper primarily relies on the analysis of specific case studies from practice. The results suggest that the effective application of digital forensics depends primarily on the technical training of personnel, a clear legal framework, and institutional readiness to apply this knowledge and tools in practice. It concludes that digital forensics is a crucial component of modern investigations, and its proper use can significantly improve the detection and prosecution of perpetrators, while inadequate approaches may lead to their exclusion from the criminal justice system.

Keywords: digital forensics, information technology investigations, financial investigations, digital evidence.

* Court Appointed Expert in Information Technology and Telecommunications; President of the Association of Expert Witnesses of Montenegro. E-mail: marko@lakic.me.