УДК: 34:659.2:004]:657
Biblid 1451-3188, 16 (2017)
Год XVI, бр. 60, стр. 198–208
Изворни научни рад

ПРАВНИ АСПЕКТИ ДИГИТАЛНЕ ФОРЕНЗИКЕ У РАЧУНОВОДСТВУ И РЕВИЗИЈИ

Жаклина СПАЛЕВИЋ[1]
Косана ВИЋЕНТИЈЕВИЋ[2]

ABSTRACT

The growth of computer crime and complex forms of digital frauds create increasing pressure on the ability of digital fraud investigators to apply the process of digital forensics and digital investigations in order to obtain timely results. This paper points out the current investigative techniques, particularly in the field of digital forensics, for the purposes of the audit of the financial operations of economic entities. To eliminate such problems there is a need to increase the use of available resources that exceed the capabilities and limitations of forensic tools that are in use. Intelligent techniques that should be used proactively are needed. The application of these techniques for digital investigations should be an answer to the complex domain of digital fraud that takes place in the modern business environment. The aim of this paper is to explain the issues and to present proposals for improving the collection of digital evidence in a legal and lawful manner in the state where a forensic auditor is conducting the investigation.

Key words: digital forensics, financial operations, digital frauds.

1) УВОД

Дигиталну форензику *McKemmish* дефинише као процес идентификације, очувања, анализирања и представљања дигиталних доказа на начин који је законски прихватљив.[3] *US-CERT* даје потпунију дефиницију: дигитална форензика је дисциплина која комбинује елементе права и компјутерских

[1] Факултет за туристички и хотелијерски менаџмент Београд, Универзитет Сингидунум, Е-маил: zspalevic@singidunum.ac.rs

[2] Факултет здравствених, правних и пословних студија Ваљево, Универзитет Сингидунум.

[3] McKemmish, R, What Is Forensic Computing?; Australian Institute of Criminology: Canberra, 1999, pp. 1.

наука за прикупљање и анализу података из компјутерских система, мрежа, система бежичне комуникације и уређаја за складиштење података на начин који је прихватљив као доказ на суду.[4] Одељење за правосуђе САД дефинише дигиталну форензику као употребу научно изведених доказних метода за прикупљање, валидацију, идентификовање, анализе, тумачења докумената и презентацију дигиталних доказа који потичу из дигиталних извора у циљу олакшања или унапређења реконструкције догађаја. Постоје и друге дефиниције али користе исти скуп кључних речи. Можемо рећи да дигитална форензика као дисциплина прикупља, чува и анализира податке на начин који је прихватљив на суду као доказ. Циљ форензичке истраге је, дакле, да се идентификују и сачувају докази, издвоје информације, да се документују процеси, анализирају издвојене информације и да се пронађу одговори у вези са *5Ws* (*Why, When, Where, What and Who*).[5]Дигитална форензика у ревизији спроводи се током истраге преваре, јер резултати могу обезбедити информације о томе: који су кључни учесници у претпостављеној злоупотреби, какве су могућности да се сазна којим документима су имали приступ, које су поступке (активности) предузели и да ли су успели да сакрију своје поступке. С обзиром да су данас све рачуноводствене евиденције у електронском облику, знања и услуге дигиталне форзензике су од изузетног значаја и за рачуновође и за ревизоре. Наиме, током последњих деценија рачуновође су имале посебне користи од напретка у области информационих технологија. Уместо да се ослањају на хард копије, папирне изворе, у пословну праксу је уведена економичност и ефикасност информационих технологија (ИТ), да сачува и анализира информације у рачуноводству. Негативна последица ових предности јесте да сајбер криминалци могу на нове начине да присвоје или преусмере податке привредног субјекта, да преузму вредне информације, а да никада нису у контакту са жртвом којој су направили привредну штету.[6] Веома је важно одговарајућим мерама онемогућити да финансијски систем буде коришћен[7] за злоупотребне и противправне радње. Рачуноводствена и ревизорска професија прати промене у области савремених дигиталних технологија. Данашње рачуновође и ревизори треба да поседују знања и вештине, да критички анализирају проблеме, да се ефикасно супротстављају и бране своје ставове кроз формалне и неформалне комуникације.

---

[4] United States Computer Emergency Readiness Team (US-CERT), Computer Forensics; Produced 2008 by US-CERT, a government organization, 2008, pp.1.

[5] Kruse, W.G., II; Heiser, J.G., Computer Forensics: Incident Response Essentials, 14th ed.; Pearson Education:Indianapolis, IN, USA. 2010, pp. 1-23.

[6] John Brozovsky and Jie Luo, Digital forensics, A New Challenge for Accounting Professionals, Strategic finance, Institute of Management Accountants, USA, 2013, pp. 37-43.

[7] Горан Бејатовић, Сања Максимовић, „Прање новца као деривативан облик криминалитета“, *Култура полиса*, год. XIV, Нови Сад, 2017, стр. 199-210.

2) ПРОФЕСИОНАЛНА РЕГУЛАТИВА ДИГИТАЛНЕ ФОРЕНЗИЧКЕ РЕВИЗИЈЕ

Допринос пружању комплексних рачуноводствених форензичких услуга даје професионална регулатива, национални и међународни закони и прописи. У овом делу рада ћемо изнети који су ИТ сертификати и алати глобално признати у ИТ ревизији и законску регулативу појединих земаља која третира дигиталне преварне радње.

ИТ сертификати и алати у употреби у дигиталној форензичкој ревизији

Управљање и контрола информационих система привредних субјеката баве се спречавањем, одвраћањем и откривањем лоших података у дигиталном окружењу. За успешно управљање и контролу информационих система потребни су: одговарајући стручњаци (дигитални форензичари) – бројни су сертификати којима се потврђује стручност дигиталног форензичара, процедуре (стандарди) поступања дигиталног форензичара и одговарајући алат. *Informtion Systems Audit and Control Association* (ISACA)[8] је глобална организација за управљање информацијама, за контролу, сигурност и ревизију, а њене стандарде ревизије и контроле информационих система следе практичари широм света. ISACA препознаје област дигиталне форензике, даје смернице за обављање ревизије ИТ. *ISACA* препознаје да се стандард *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals* (G28, *Computer Forensics*)[9] примењује током годишњег програма ревизије, као и код појединачних прегледа ИТ ревизије у току године. Међународни сертификати у ревизији информационих система *ISACA* су: *Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT), Certified in Risk and Information Systems Control (CRISC), Cybersecurity Nexus – CSX Certificate* и *CSX-P Certification.* Са више од 140.000 чланова у 187 земаља *ISACA* је водећа у свету у области пружања знања, сертификата, заговарања и образовања о информационим системима у области безбедности, корпоративног управљања, управљања ИТ, ИТ ризицима и усклађености са прописима и стандарднима везаним за ИТ. Огранак *ISACA* у Хрватској основан је 2001. године. Према стању из 2014. године број сертификованих чланова је 175 (*CGEIT*: 18, *CRISC*: 22, *CISA*: 87, *CISM*: 52). Огранак *ISACA* у Србији основан је 2016. године и тренутно има преко 70 домаћих сертификованих професионалаца.

[8] Интернет: https://www.isaca.org/pages/default.aspx

[9] ISACA, (2010): *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals*, USA, pp. 138-143.

Велики број домаћих професионалаца регистрован је код других *ISACA* удружења у свету, тако да ће се у Србији број регистрованих чланова у будућем периоду значајно повећати. *Computer Assisted Audit Techniques* (*CAATS*) као помоћни алати за ревизију који се понекад називају само *CAATS*, постају све популарнији у ревизијској професији. Ови алати користе се као помоћ ревизорима у потрази за неправилностима у датотекама, током претраге велике количине података, који се даље анализирају ради детекције преваре. Заправо, *CAATS* алати се користе да поједноставе и аутоматизују процес анализе података.

Глобална регулатива и сертификати за форензичке рачуновође

Регулатива спровођења ревизије информационих система прилично је ригорозна и односи се на регулативу[10] на међународном нивоу (у зависности од делатности клијента; за финансијске институције то су *Sarbanes-Oxley закон, Basell III, The European 8th Direcive, MiFID*) и националном нивоу (у зависности од делатности клијента). Наиме, због чињенице да екстерни ревизори раде у окружењу на које утиче *SAS No*. 99 – *Разматрање преваре у ревизији финансијских извештаја* и *SOX*, од њих се очекује да имају адекватно знање и вештине како би се осигурало да су финансијски извештаји ослобођени значајне преваре. Ревизори унапређују квалитет ревизије у сарадњи са свим релевантним стручним и професионалним телима која унапређују питања квалитета ревизорског рада.[11] Три заједничке области у пракси дигиталних форензичких рачуновођа у англосаксонским земљама су: да постоји спор, да је потребно вештачење (истрага) и да је потребно истражити превару.[12] *SAS No*. 99 наводи да ревизори морају експлицитно да размотре могућности постојања преваре у финансијским извештајима, да размотре како је превара могла бити учињена од стране и против клијента ревизије и на који начин је могла утицати на финансијске извештаје. Такође се наводе извори које ревизори могу користити да би прибавили информације за идентификовање ризика од преваре. *OLAF* – канцеларија Европске комисије за борбу против превара истражује преваре повезане са буџетом ЕУ, корупцију и прекршаје у оквиру

[10] Mario Spremić, Digitalna transformacija poslovanja, Sveučilište u Zagrebu, Ekonomski fakultet, Zagreb, 2017, str. 211.

[11] Косана Вићентијевић, „Нова форма и садржај извештаја независног ревизора", *Ревизор*, Година XX, бр. 77/2017, Институт за економику и финансије, Београд, 2017, стр. 37-48.

[12] Rezaee, Z., L. Crumbley and R. Elmore, „Forensic accounting education: A survey of academics and practitioners", *Advances in Accounting Education Teaching and Curriculum Innovations,* 2004, no. 6, pp. 193-232.

европских институција, а за Европску комисију планира и формулише политику за борбу против превара. *OLAF* дигиталне доказе за своје истражитеље прикупља уз подршку дигиталне форензике за идентификацију, аквизицију, снимање, прикупљање, анализу и чување дигиталних доказа.[13] Европска комисија је током 2013. године формирала *European Cybercrime Centre* (*EC3*), као центар за спровођење правне регулативе (закони, директиве и подзаконска акта) везане за сајбер криминал у ЕУ. На тај начин она помаже у заштити права грађана ЕУ, привредних субјеката и влада од *on line* криминала. *EC3* има тростран приступ борби против сајбер криминала: форензика, стратегије и оператива.[14] *Certified Fraud Examiner* (*CFE*) сертификат је водећа квалификација за испитиваче превара, форензичке рачуновође и полицију коју могу поседовати. Сертификацију спроводи Асоцијација сертификованих истражитеља превара – *Association of Certified Fraud Examiners* (*ACFE*),[15] која има преко 80.000 чланова који су сертификовани и увежбани у разним аспектима откривања, испитивања и спречавања професионалних превара у финансијским извештајима, као и професионалних злочина. Квалификација *Certification in Financial Forensics* (*CFF*), комбинује посебну стручност у форензичком рачуноводству са основним знањима и вештинама које сврставају *CPA* међу најкредибилније пословне саветнике. *CFF* обухвата фундаменталне и специјализоване вештине форензичког рачуноводства које практичари *CPA* примењују у низу подручја услуга, као што су: стечај и несолвентност, компјутерска форензика, економске штете, породично право, истраге превара, подршке у судским поступцима и друго. МУП Републике Србије уз подршку *OEBSA* и Норвешке владе ишколовао је 10 форензичких стручњака са међународно признатим сертификатом за финансијски криминал. Сертификате су добили 2015. године након обуке и припрема у трајању од две године, са ментором у Србији који има међународни сертификат за форензичког рачуновођу. *Стратегија истрага финансијског криминала у Србији* предвиђа циљеве и мере за јачање финансијских истрага у Србији, кроз повезивање полиције и тужилаштва, увођење финансијских форензичара, континуиране обуке, међународну сарадњу и низ других мера. *ACFE* и *AICPA* су формирале *Institute for Fraud Prevention* (*IFP*),[16] који има за циљ развијање разумевања узрока и последица превара служењем као катализатор за размену идеја међу врхунским противпреварним практичарима, запосленима у владиним институцијама и академицима. То је добровољна организација

[13] Интернет: http://ec.europa.eu/anti-fraud//home_en; датум прегледа:19.3.2017.

[14] Интернет: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3; датум прегледа:19.3.2017.

[15] Интернет: http://www.acfe.com; датум прегледа: 19.3.2016.

[16] Интернет: http://www.theifp.org/

истраживача посвећених превенцији превара, са оријентацијом према истраживању и образовању као бази за развој најбољих пракси против превара. Добар пример примене дигиталне форензике у рачуноводству и ревизији је Канада. Канадски институт овлашћених рачуновођа *Chartered Professional Accountants of Canada* (*CPA Canada*) преузео је иницијативу у правцу издавања смерница у вези са истражним рачуноводством. За своје чланове из области форензике организује освежавање и продубљивање знања и вештина у форензичком рачуноводству, кроз обуке које воде искусни дигитални форензичари из рачуноводства, организују и учествују на међународним конференцијама, обезбеђују стручну литературу из форензичког рачуноводства.[17] *The Southern African Fraud Prevention Service* (*SAFPS*) – Сервис за превенцију превара у Јужноафричкој Републици посвећен је борби против превара у области финансијских услуга, обезбеђивањем базе података привредних субјеката који су њихови чланови, као и заштити физичких лица од крађе идентитета.[18] При решавању спорова у оквиру привредног друштва или између привредних друштава у случају стечаја дигитални форензички рачуновођа идентификује финансијске, правне и ИТ чињенице и околности које су довеле до спора, односно преварне радње. У случају сумњивих неправилности, као што су конфликт интереса, преваре или корупције дигиталне форензичке рачуновође у Холандији за откривање истине решење проналазе у ИТ окружењу. У Холандији се форензичко рачуноводство препоручује у случају сукоба привредног субјекта са пореским органима – као специјализовано истраживање, истичу проналажење неправилности у финансијским извештајима. Холандски институт за форензику (*The Netherlands Forensic Institute – NFI*[19]) развио је иновативне програме са циљем како да се дигитални докази детектују и најбоље обезбеде. Програм сајбер форензика и *Big Data* примењују методе за анализу материјала за сајбер криминал на форензички одговоран начин. Ове програме *NFI* ће даље развијати, тако да ће платформа омогућавати аутоматско отпремање и категоризацију велике количине података, што ће омогућити клијентима да траже материјалне доказе. У оквиру ових програма *NFI* такође развија интелигентне алате који се могу користити за дигиталне форензичке истраге, да се открију сложени токови података од стране форензичких стручњака.[20] Норвешка безбедносна информациона лабораторија (*Norwegian Information Security laboratory* –

[17] Интернет: https://www.cpacanada.ca/; датум прегледа: 19.3.2017.

[18] Интернет: https://www.safps.org.za/index.aspx?ReturnUrl=/; датум прегледа: 19.3.2017.

[19] Интернет: https://www.forensicinstitute.nl/; датум прегледа: 19.3.2017.

[20] Интернет: https://www.forensicinstitute.nl/research_and_innovation/Researchprogrammes/Cyber%20Forensics%20Big% 20Data%20and%20Digitalising%20Investigation.aspx; датум прегледа: 26.3.2017.

NISlab) је део одељења за безбедност информација и комуникација на норвешком универзитету за науку и технологију (*Norwegian University of Science and Technology – NTNU*).[21] Са око 60 повезаних лица из више од 28 земаља, *NISlab* представља једну од највећих база академских информација и сајбер безбедности група у Европи, има приступ *end-to-end* информацијама и сајбер безбедности. Лабораторија има посебан фокус на биометрије, форензику, заштиту критичне инфраструктуре и управљање информацијама за безбедност мреже.[22] Ирска се суочава са све већим бројем случајева где се електронски докази користе у грађанским и кривичним предметима. У Ирској је евидентан пораст превара и крађа интелектуалне својине.[23] *Institute of Fraud Auditors* (*IFA*)[24] је национална професионална организација форензичких ревизора у Белгији, основана 2001. године као непрофитна асоцијација, која води регистар професионалаца који поседују сертификат као *Registered Fraud Auditor*. *IFA* развија најбоље праксе за професионалце који су активни у области превара у јавном и приватном сектору. У Хрватској дигиталном форензиком се бави посебан тим у оквиру *Одјела за кибернетички криминал* при Министарству унутрашњих послова, а послује и неколико информатичко безбедносних фирми које су специјализоване за дигитална вештачења. У циљу спречавања нежељених догађаја земље морају да сарађују,[25] сарадња се одвија и са ИТ компанијама исте делатности из иностранства. Информативно безбедносне фирме у Хрватској баве се и системом безбедности ИТ система код заинтересованих привредних субјеката.

3) ПРАВНА РЕГУЛАТИВА ДИГИТАЛНИХ ПРЕВАРА

У теорији кривичног права област дигиталног (високотехнолошког) криминала обухвата различите облике противправног недозвољеног понашања као што су: компјутерске преваре, финансијске крађе и злоупотребе, фалсификовање података и докумената, компјутерска шпијунажа и други. У овом делу рада наводимо законодавне оквире неких земаља из области дигиталних превара и начин исправног формирања *ланца дигиталног доказа*.

---

[21] Интернет: http://www.ntnu.edu/iik; датум прегледа: 26.3.2017.

[22] Интернет: https://www.nislab.no; датум прегледа: 26.3.2017.

[23] Leonard McAuliffe & Andrew Browne, "Forensic Accounting and Computer Forensics", *In practice*, CPA Ireland, 2009, pp. 36-37.

[24] Интернет: https://www.ifabelgium.be/; датум прегледа: 26.3.2017.

[25] Жаклина Спалевић, Жељко Спалевић, „Стање сервиса електронске управе базираних на рачунарству у облаку", *Култура полиса*, год. XIV, Нови Сад, 2017, стр. 171-183.

Законодавни оквири дигиталних превара

Када је домаће законодавство у питању, Кривични законик Републике Србије – Службени гласник РС, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014) садржи посебну Главу 27, о кривичним делима против безбедности рачунарских података у Члановима 298–304. У Немачкој је 1978. године донет Кривични законик који не познаје компјутерска кривична дела, али то не значи да ова правно недопуштена понашања нису инкриминисана.[26] У Немачкој је 1986. године донет Кривични закон за сузбијање привредног криминалитета који предвиђа низ компјутерских кривичних дела (Члан 202а – компјутерска шпијунажа, Члан 263а – компјутерска превара, Члан 269 – фалсификовање података, Члан 270 – обмана у правном промету при обради података, Члан 302а – промена података, Члан 303а – компјутерска саботажа). У Члану 126а Аустријског кривичног законика оштећење података категорисано је као кривично дело.[27]

У Великој Британије је 1990. године донет Закон о злоупотреби компјутера. Овај закон предвиђа низ кривичних дела везаних за злоупотебу компјутера и других информационих система за које су прописане веома строге казне.[28] Кривични законик у Македонији (Службен весник на Република Македонија, Скопје, број 37/1996) Чланом 251 одређује кривично дело под називом упад у компјутерски ситем. У Словенији Кривични законик из 1999. године познаје следећа кривична дела: у Члану 225 – противзаконити улаз у заштићену рачунарску базу података, у Члану 242 – упад у рачунарски систем.[29] Кривични закон Републике Хрватске (Narodne novine RH, Zagreb, br. 110/1996) препознаје у Члану 223 кривично дело под називом оштећење и употреба туђих података (а односи се на аутоматски обрађене податке и компјутерске програме). У Русији Кривични законик познаје више компјутерских кривичних дела у посебној Глави 23 под називом: Кривична дела у сфери компјутерске информације.[30] Овде су препозната следећа кривична дела: Члан 272 – противправни приступ компјутерској информацији, Члан 273 – прављење, коришћење и ширење штетних компјутерских програма, Члан 274 – повреда прописа о експлоатацији компјутера, компјутерских система и њихових мрежа. У јануару 2016. године у Републици Србији усвојен је Закон о информационој безбедности ("Сл. гласник РС", бр. 6/2016). Овим законом (и подзаконским

[26] Schonke-Schroder, *Strafgesetzubuch* , Kommentar, Munchen, 1978.

[27] Foregger, E., Serini, E, Strafgesetzbuch. Wien: Manz, 1989.

[28] Martin Wasik, *The computer misuse act*, The Criminal Review, 1990, p. 767.

[29] B. Penko, K. Strolig, *Kazenski zakonik z uvodnimi pojasnili*, Ljubljana, 1999.

[30] J. I. Skuratov, V. M. Lebedov, „Kommentarii k Ugolovnomu kodeksu Rossijskoj federaciji", *Norma*, Moskv, 1996.

актима који су усвојени крајем новембра 2016 ("Сл. гласник РС", бр. 94/2016) уређују се мере заштите од безбедоносних ризика у информационо-комуникационим (ИКТ) системима од посебног значаја, одговорности правних лица приликом управљања и коришћења, као и надлежни органи за спровођење мера, координацију и праћење правилне примене.

Дигитални докази у форензичком рачуноводству и ревизији

Судска пракса прихвата софтверски генерисане податке (датотеке, симулације и апликације) као генерисане и меморисане дигиталне доказе под адекватним условима који доказују њихову непорецивост. Процес трансформације дигиталних података, који представљају дугачке кодоване битске секвенце у судски доказ, за правосудни систем је ипак апстрактан процес, који неретко судске органе наводи на сумњу у интегритет софтверски генерисаног доказа. Стога је основни задатак националних правосудних система да се законским решењима и подзаконским актима дефинишу посебне процедуре коришћења дигиталних доказа. То би пре свега биле: процедура руковања и чувања дигиталних доказа и процедура за форензичку аквизицију и анализу дигиталних доказа у доказном поступку. Форензичка анализа дигиталних доказа у области рачуноводстава и ревизије треба да обезбеди податке за формирање чврстог и необоривог дигиталног доказа преваре или злоупотребе положаја без пукотина недоречености. Рачунарски дигитални доказ у рачунару или мобилном телефону може се сматрати аутентичним уколико се може непорециво доказати да није измењен у односу на тренутак посматрања. Постојећи Закон о кривичном постуку Републике Србије (ЗКП) није дао појмовно одређење ни елементарног појма доказа, а ни појма дигиталног (електронског) доказа. Ова неодређеност је посебно значајна у преткривичном поступку и судским процесима који процесуирају извршена кривична дела у области високотехнолошког криминалитета. Став Судске праксе у Републици Србији је да дигитални доказ има исту вредност као материјални и да за њега важе потпуно иста процесна правила као и за материјалне. Препорука Савета Европе о дефинисању процесних правила у вези са информатичким технологијама (*Recommendation COE on Criminal Procedural Law Connected with Information Technology,* 1995) представља основни акт кога морају узети у обзир национална законодавства при дефинисању дигиталног доказа. Ова препорука утврђује осамнаест принципа који утврђују основне услове за претрагу и заплену предмета, технички надзор, обавезу сарадње истражних органа, дигиталне доказе, процес употребе енкрипције, процес истраживања меморијског простора, документовање података и међународну сарадњу у циљу размене дигиталног доказног материјала и формирања јединственог судског предмета. Међутим, судови узимају у обзир

и чињеницу да су у електронском књиговодству докази веома осетљиви и да се лако могу изменити или обрисати. Имајући у виду да преваре у електронском рачуноводству и ревизији унутар сајбер простора као специфичног медијума могу бити генерисане на више локација које се могу налазити чак и на различитим континентима, поставља се питање националне и месне правосудне надлежности. Питање вишеструке надлежности судова у овој области није дефинисано ни међународним споразумима, а ни нашим Законом о кривичном постуку и Кривичним закоником. У циљу доказивања кривичних дела у области рачуноводства и ревизије, потребно је обезбедити аутентичну документацију, тј. фактуре, отпремнице и изводе на текућем рачуну правног субјекта код пословне банке. Међутим, савремено пословање привредних субјеката подразумева вођење компјутерског књиговодства, које омогућава: тренутно и аутентично формирање књиговодствених докумената, велику брзину операција у процесу књижења и брзо и ефикасно претраживање пословне документације. Такође, овакав вид пословања омогућава стварање услова за формирање лажне документације која, с једне стране, представља интелектуални фалсификат а, с друге стране, омогућава стицање противправне имовинске користи. За откривање и проналажење дигиталних доказа кривотворења у процесу комјутерског књиговодства и ревизије потребно је познавање процедура и делокруга рада компјутерског књиговодства, карактеристика специјализованих софтвера за проналажење података, поновно генерисање брисаних података, утврђивање свих измена података у меморији уређаја или унутар датотека и аутентичне информације са сервера провајдера које доказују непорецивост комуникација финансијских трансакција кроз мрежу. При томе, најосетљивија карика у формирању квалитетног дигиталног доказа је *време контакта* са истим, чиме обезбеђује непорецивост праћења ланца доказа. Исправно формиран ланац дигиталног доказа мора садржати време настанка дигиталног доказа, време приступа дигиталном доказу без модификације, време модификације дигиталног доказа, време похране дигиталног доказа, време брисања, време исписа дигиталног доказа, време анализе дигиталног доказа, документацију са материјалним доказима и изометријским потписом овлашћене особе о исправности поступка прикупљања података, транспорта, чувања, руковања, копирања и поступка анализе. На тај начин обезбеђује се непорецивост дигитаних доказа у судским процесима коју је потребно да потврде ИТ вештаци. Основна дилема у судској пракси је да ли у поступку обезбеђивања дигиталних доказа треба приступити привременом одузимању хард дискова и дигиталних уређаја унутар којих су похрањени релевантни подаци или се доказом могу сматрати копије тих података које су начињене на лицу места према унапред одређеној законски дефинисаној процедури. Привремено одузимање хард дискова и дигиталних уређаја има јасно оправдање, јер се унутар истих могу налазити и други релевантни подаци или путање ка истим

у мрежи, које нас доводе до црног књиговодства или брисаних података који указују на стварно пословање привредног субјекта.

4) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Дигитална форензика у рачуноводству и ревизији, својим изазовима и могућностима, стандардизацијом и приступима, може бити од значаја за садашње и будуће кретање рачуноводства и ревизије у информационо-комуникационим технологијама Републике Србије. Интернет је олакшао чињење криминалних радњи, тако што криминалци могу да учине противзаконито дело и да остану релативно анонимни. Повећана сложеност глобалних комуникација, мрежна инфраструктура и уређаји чине истрагу форензичким ревизорима за дигиталне преваре тешком. Трагови нелегалних активности често су невидљиви у великим количинама података, које је потребно претражити у циљу откривања преваре и прикупљања доказа. Област дигиталне форензике је отуд постала веома важна за спровођење закона, очување националне безбедности и сигурности информација у Републици Србији. Дигитална форензика је истрага која је мултидисциплинарна у областима које обухватају право, компјутерске науке, финансије, телекомуникације, аналитику података, полицију и друго. Сертификовани форензички ревизори често раде у тимовима у следећим областима: *Big Data* и дигитална форензика*, Business Applications* и дигитална форензика, *Cloud* форензика, дигитална форензика и алати за тестирање, дигитална форензика и закони, *Network* форензика, и многе друге области које се отварају са развојем информационо-комуникационих технологија.