Оригинални научни рад 343.98:004
doi:10.5937/zrpfns46-1971

Др Татјана Лукић, ванредни професор
Правног факултета у Новом Саду

ДИГИТАЛНИ ДОКАЗИ[1]

Сажетак: *Иако су компјутери учинили људске активности бржим и једноставнијим, а истовремено иновативним у смислу стварања нових облика рада и других активности, они су исто тако утицали и на криминалне активности. Развој информационих и информатичких технологија директно утиче на развој компјутерске форензике, без које се не може ни замислити откривање и доказивање кривичних дела помоћу компјутера и хватање њихових учинилаца. Борба против савремених облика криминалитета код којих се рачунари често појављују као средство, или као предмет извршења кривичног дела, нужно захтева познавање дигиталног доказа, као и посебна правила и процедуре њиховог откривања, фиксирања и прикупљања од стране стручњака информационе технологије. У овом раду, аутор се бави проблематиком дигиталног доказа, форензичке (компјутерске) истраге и коришћења ове врсте доказа у кривичном поступку.*

Кључне речи: *дигитални доказ**,** компјутерска форензика, информациона технологија, кривични поступак.*

1. Уводна разматрања

Савремно друштво се данас не може ни замислити без компјутера који су значајно изменили њихов начин живота и рада. Људске делатности су постале брже и једноставније, а створени су и нови облици рада и других врста активности. Међутим, предности које су донели компјутери нису, на жалост, искоришћени само у позитивном смислу, него су и криминалне делат-

[1] Овај рад је настао као резултат научно-истраживачког рада на Пројекту „Теоријски и практични проблеми стварања и примене права (ЕУ и Србија)“ чији носилац је Правни факултет у Новом Саду.

ности "иновиране" овим савременим средством које пружа до сада невиђене могућности. Овако нешто је било и за очекивати, с обзиром на то да је опште позната чињеница да информациони и информатички развој има одраза на све активности људи, па самим тим и криминалне. У намери да се избори са новим начинима и средствима вршења кривичних дела, друштво је развило нову врсту криминалистичке технике, тзв. компјутерске форензике која је омогућила откривање и доказивање извршених кривичних дела помоћу компјутера и идентификовање њихових учинилаца.

Кривично дело има за последицу неку промену у спољном свету, независно од тога да ли је извршено чињењем или нечињењем. Ове промене настају самим припремањем, извршењем или прикривањем кривичног дела. Свака промена у спољном свету садржи у себи неке информације које могу да се односе на саму радњу извршења (начин, средство) или на учиниоца. Те промене су, уствари, знакови који су носиоци криминалистичких информација и они могу бити материјалне и психичке (личне) природе. Ови знакови су смернице оперативног рада полиције и правосудних органа. Материјални носиоци криминалистичких информација су предмети и трагови кривичног дела, а психички носилац криминалистичких информација је сећање лица која су у прошлости чулно опазила неке чињенице релевантне за учиниоца или за кривично дело. Иако знакови настају као последица кривичног дела, они су самостални и као такви егзистирају у спољном свету, а информације које садрже се не виде голим оком, већ су оне латентне и прикривене. Осим што су самостални, знакови су у процесу перманентног мењања под утицајем бројних спољашњих фактора, али и унутрашњих фактора (психички знакови). На материјалне знакове - носиоце информација директно утичу, тј. они зависе од временских услова, протека времена, лица која покушавају да их уклоне (униште или измене), као и бројних других чинилаца са којима долазе у додир. За разлику од њих, психички знакови - носиоци информација су највише изложени утицају времена услед кога, по правилу, бледе и модификују се. Због тога је хитно поступање по сазнању за извршено кривично дело први и главни услов за остваривање ефикасних резултата рада надлежних органа у откривању и доказивању кривичног дела. Наравно, ово поступање мора да буде у складу са свим правилима криминалистике.

2. Лични и материјални докази

Докази представљају податке чињеничне природе, који произлазе из кривичнопроцесних радњи које су предузели субјекти кривичног поступка, а пре свега суд, који је примарно одговоран за извођење доказа у кривичном поступку, иако и странке учествују у извођењу доказа, на сонову

којих се утврђује чињенично стање, а на темељу кога се изводе кривичноправно релевантни закључци у погледу битних елемената кривичног дела и кривичне одговорности, те избора, односно мере конкретне кривичне санкције када су за то испуњени потребни материјални и процесни услови, или се на темељу тих података извлаче одређени кривичнопроцесни закључци, при чему се такви закључци суда у процесном смислу уобличавају у оквиру одлуке којом се на законски регулисан начин решава предмет кривичног поступка.[2] Доказ није ништа друго него чињеница, односно информација и они се могу поделити на разне начине, према различитим критеријумима. За доказе компјутерског криминалитета, значајна је подела на личне и материјалне доказе, а критеријум за поделу је сама њихова природа. Лични докази представљају чулним опажањем сазнате чињенице које пружају одређени запис о догађају, а материјални докази су физички докази и трагови. И једни и други су равноправни у кривичном поступку и релевантни за доношење судске одлуке, под условом да садрже релевантне чињенице које се односе на извршено кривично дело, окривљеног, оштећеног и, уопште, да су значајни за утврђивање чињеничног стања, односно за доношење одлуке. Што се тиче међусобног односа материјалних и личних доказа, потребно је нагласити, да данас, и поред развијене криминалистичке технике, у кривичном поступку се одлуке у највећем делу ослањају на личне доказе, а материјалним доказима се најчешће само поткрепљују лични докази, и отклања или потврђује сумња, да је одређено лице извршило кривично дело. Разлог за ово је чињеница да у највећем броју случајева нема или има врло мало материјалних доказа, јер се окривљени труде на све начине да осујете кривични поступак уништавајући или сакривајући материјалне доказе, али исто тако и утичући на сведоке и вештаке, најчешће застрашивањем. У ситуацији оскудице материјалних доказа, судови прибегавају личним доказима.

Материјални докази у вези са извршењем кривичног дела настају у процесу међусобног деловања извршиоца и оштећеног, при чему долази до узајамног преноса криминалистички релевантних информација. Под материјалним доказима се подразумевају разне физичке ствари које могу послужити као доказ, с тим да оне нису никаква посебна врста доказа, него припадају другим доказима (исправама) или су предмет увиђаја или вештачења.[3] Због тога суд, најчешће приликом извођења и оцене материјалних доказа, ангажује стручњака неке друге, неправне струке, који се у поступку појављује као вештак и који даје свој налаз и мишљење на основу

[2] Шкулић М., Кривично процесно право, Београд 2011., стр.185-186.

[3] V.Bayer, Jugoslovensko krivično procesno pravo, knjiga druga, Pravo o činjenicama i njihovom utvrđivanju u krivičnom postupku, Zagreb 1972. стр.17.

правила и достигнућа своје струке. У налазу, вештак констатује постојање или непостојање чињеница које су предмет доказивања, а у мишљењу износи свој суд (лични став, закључак) о констатованим чињеницама.

3. Откривање и доказивање кривичног дела компјутерског криминала

Савремени облици криминалитета, високософистицирани у погледу начина и средстава извршења, као и стручности извршилаца су наметнули као правило да се за њихово откривање и доказивање све чешће користе наука и логика. Ово је отворило пут форензици у смислу да се она наметнула као водећа наука у процесу расветљења кривичних дела, и идентификовања њихових извршилаца. Форензичко знање морају да поседују инспектори, криминалистички техничари, тужиоци и судије, односно њихово стручно знање се не може ни замислити без форензике. Ово из разлога што се без одређеног, да тако кажемо предзнања из форензике, не би могли ни позивати вештаци у кривични поступак, нити би се могао оценити њихов налаз и мишљење о чињеницама које су предмет доказивања. Такође, знање из форензике омогућава и правилно прибављање, као и вредновање доказа. Због тога је оно неопходно свим учесницима у поступку, а у кривичном поступку адверзијалног типа, оно је посебно потребно браниоцу окривљеног.

4. Компјутерска форензика и дигитална форензика

Форензичке науке - форензика (које се понекад називају и судске науке) представљају скуп научних грана које су потребне за утврђивање чињеница у поступку (судском или управном). Постоје различите гране форензичке науке у које спада и компјутерска форензика. Не постоји јединствена дефиниција компјутерске форензике, али имајући у виду чиме се она бави, може се рећи да је то једна врста технолошке контрола компјутерског система, као и његовог садржаја ради прикупљања и обезбеђења доказа у вези са извршеним кривичним делом, или неким другим преступом, где је компјутер искоришћен у незаконите сврхе. У науци није јединствено одређено место, односно статус компјутерске форензике. Док једни тврде да је термин компјутерска форензика само замењен термином дигитална форензика, други тврде да је компјутерска форензика део дигиталне форензике. Без обзира на то, око предмета ове гране форензике постоји општа усаглашеност, да је то компјутер у најширем смислу, па то онда подразумева и садржај дискова (хард дискова, CD/DVD дискова), садржај оперативне меморије, мрежни саобраћај и све радње реализоване уз помоћ рачунара, као што су електронска кореспонденијца, штампање, Skype кому-

никације и друго. Данас се поред рачунара, појављују и друга средства извршења кривичног дела, као што су дигитални фото апарати и камере, мобилни телефони, паметни телефони, персонални дигитални асистенти и слично, а сви они могу бити предмет обраде у поступку, применом правила компјутерске форензике. Компјутерска (дигитална) форензика је наука која се бави идентификовањем, прикупљањем, чувањем, документовањем и анализом података који се ускладиштени, обрађивани или преношени у дигиталној форми. Она се бави рачунарима, мобилним и фиксним телефонима, PDA уређајима, меморијским картицама, као и другим медијима на којима се налазе потребни подаци. Стручњаци из ове области у свом раду наилазе на бројне проблеме, а то се покушава превазићи специјализацијом стручњака за уже области, као што су рачунарска форензика, форензика мобилних уређаја, мрежна форензика и форензика базе података, форензика оперативних система (Windows, Linux i Mac OS). Од када је призната од стране ASCLD-LAB-а[4] (2003) као самостална форензичка дисциплина, за компјутерску форензику је порасло интересовање у смислу едукације и стручног усваршавања из ове области.

Иако је широко употребљива, компјутерску (дигиталну) форензику у кривичном поступку треба користи само у оним ситуацијама, када је евидентно да се на неком компјутеру налазе могући релевантни докази. У таквим ситуацијама се, по правилу, веома тешко долази до тих доказа па је потребно да технике компјутерске форензике примењује стручњак из те области, како не би дошло до оштећења доказа и смањења њихове употребљивости у судском поступку. Активности које чине компјутерску форензику се битно разликују од оних активности које се спроведе у неким традиционалним форензичким дисциплинама. Материјали које обрађује, као и алати и технике које користи компјутерска форензика нису природног порекла. Осим тога, разлика компјутерске (дигиталне) форензике у односу на традиционалне форензичке дисциплине је и томе што она врши испитивање и анализе на свакој локацији, а не само у контролисаним (лабораторијским) условима. Наравно, основни, али не и довољан услов за примену компјутерске форензике је дигитални доказ у односу на кога се примењују научне методе ради идентификације, прикупљања и анализирања података који почивају унутар компјутерског система, као и за опоравак обрисаних, криптованих или оштећених података, уз очување интегритета оригиналног доказа.

Компјутерска (дигитална) форензика има изузетно широк спектар примене, па тако, иако су за њу првенствено заинтересовани органи јавне

[4] Више видети: The American Society of Crime Laboratory Directors/Laboratory Accreditation Board http://www.ascld-lab.org/

безбедности, државне безбедности и правосудни органи, све више је приватних компанија и банака које користе компјутерску форензику за вршење унутрашње контроле. Осим тога, у надлежност и делокруг рада приватног обезбеђења и самозаштитне делатности у фирмама, компанијама и свим другим установама и институцијама, спада и вршење почетних истрага компјутерског инцидента, па је за очекивати, да тек пошто спроведу сопствену истрагу, обавесте надлежне органе полиције или тужилаштво. Овим, тзв. претходним истраживањем, они утврђују природу инцидента, па уколико се покаже да се ради о кривичном делу, даљи рад на томе морају да препусте надлежним државним органима. Претходно истраживање може много да помогне полицијским органима у даљем раду, али исто тако може да буде чак и штетно за даље поступање полиције, уколико је оно извршено од стране нестручних људи и без одговарајуће опреме за компјутерску анализу. На овом месту је важно напоменути и да су овлашћења органа тзв. претходног истраживања веома ограничена. Добро решење је ангажовање стручног консултанта за иницијалну истрагу, аквизицију и форензичку анализу дигиталних доказа, властитим снагама, најмање до тренутка утврђивања природе инцидента и доношења одлуке о (не) укључивању званичних истражних органа, што се најчешће чини.[5]

5. Дигитални докази

Дигитални доказ је врста доказа који се од осталих материјалних доказа разликује по форми у којој су инкорпорисане информације, а то је дигитална форма, која подразумева неки електронски или магнетни уређај (подаци у оперативној меморији, на хард диску, флеш картицама, али и подаци који се налазе у трансмисији). Дигитални доказ се манифестује као низ јединица и нула које се помоћу електронског уређаја преводи у нама разумљив облик. Ови докази су по својој вредности изједначени са материјалним доказима до којих се долази на већ традиционалан начин, док је за прикупљање дигиталних доказа потребна специјална опрема. Сваки оригинални доказ треба да буде сачуван у изворном облику, па то исто важи и за дигиталне доказе. Свако даље вештачење се не сме вршити на оригиналном доказу, већ на његовој копији, јер су у питању код истраживања дигиталних доказа најчешће у питању инвазивне методе којима се ови докази могу уништити. Копија дигиталног доказа мора бити верна оригиналу у сваком погледу и треба да буде смештена на тзв. "чистом" медију, односно оном на коме није било података раније.

[5] М. Ђорђевић, Ресурси за истрагу компјутерског криминала, стр.2 http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-04.pdf

Дигиталним доказима се бави компјутерска форензика која се базира на принципу *законитости* – под којим се подразумева могућност прикупљања дигиталних доказа само на основу одлуке суда; *ланца истраге* – према коме један дигитални доказ не сме да искључи други; *очувања дигиталног доказа*; *идентифентификације потенцијалног доказног материјала* и *интегритета доказног материјала.*

Компјутерска форензика се бави обрадом и анализом законито прикупљених дигиталних доказа који су пронађени у самом рачунару или медијима за чување података (FDD, HDD, USB, CD/DVD ROM и др.). Поступак који се примењује је стандардизован и он се, као и сваки процес налази у стању динамичног кретања под којим се подразумева низ унапред утврђених радњи и мера, а то су: препознавање, сакупљање, чување, документовање, класификација, упоређивање, индивидуализација и реконструкција доказа.

Локардов „принцип размене" је заснован на тврдњи да приликом сваког контакта две ствари долази до размене.[6] Овај принцип се примењује од 1940. године, али се поставља питање да ли се он може примењивати и у компјутерским истрагама. У случајевима кривичних дела компјутерског криминалитета обично у контакт долазе два или више рачунара од којих један припада оштећеном, а други извршиоцу. Када ови рачунари дођу у контакт, они свакако врше размену података или информација, што се може доказати на нивоу оперативног система рачунара. Уколико се на једном рачунару у CMD укуца нека мрежна команда која се односи на други рачунар, може се доћи до IP адресе и других података другог рачунара.

У вези са дигиталним доказима потребно је указати и на њихове карактеристике као и саму природу[7]. На првом месту то је ***велики број осумњичених лица***, јер су корисници Интернета најчешће анонимни, па је самим тим велик број потенцијално осумњичених лица. ***Идентификација преступа*** се код компјутерског криминалитета често врши временски много касније у односу на извршено кривично дело, а најбољи пример за то је крађа поверљивих информација или крађа идентитета. ***Велики број потенцијалних доказа*** се на самом почетку истраге елиминише, а да би се могла поставити почетна хипотеза истражитеља, што се врши у зависности од саме природе преступа***. Подложност контаминацији*** је такође карактеристика дигиталних доказа и она подразумева њихову велику осетљивост на промену стања,

[6] Едмонд Локарт (1877-1966) био је први директор Криминалистичке лабораторије у Лиону (Француска)- Локардова теорија или Локардов закон – више видети: Chisum, W.J., & Turvey, B. "Evidence Dynamics: Locard's Exchange Principle & Crime Reconstruction, *Journal of Behavioral Profiling*, January, 2000, Vol. 1, No. 1.

[7] Видети: G.Mohay & A.Anderson & B.Collie & D. Vel Rodney & R.McKemmish, - *Computer and Intrusion Forensics*, Boston 2003 str.44.

много већи него код других доказа. Због тога је потребно правовремено предузети све мере којима се може очувати затечено стање, а то се постиже само строгом процедуром активности. ***Лакоћа губитка доказа*** је присутна онда када је човек сам фактор тога, у смислу да је лице које поступа нестручно, али и онда када није знао да је доказ присутан.

6. Компјутерска истрага[8]

Докази који могу бити релевантни у истрази која се води поводом компјутерског криминалитета су компјутер, лаптоп, штампач, фотокопир апарати, мобилни телефон, лична дигитална средства (PDA), CD, флопи диск, USB меморија, дигитална камере, зип дискови, hard drive и све друге направе које имају могућност складиштења података. Ови докази високе технологије захтевају другачију врсту истраге у односу на класичну, као и лица посебне стручности. Када форензичари предузму све неопходне мере да би осигурали интегритет доказног материјала, он је прихватљив у судском поступку, као и код класичне истраге, и даљи правац истраге је директно одређен оперативним сазнањима и доказима који су прикупљени на лицу места. Иако у највећем броју случајева криминалистичка истрага почиње на самом лицу места, код компјутерских истрага је нешто другачије. Лице места је место извршења кривичног дела (где је предузета радња или наступила последица или је према умишљају извршиоца требала да наступи), као и свако друго место на коме се налазе докази и трагови у вези са извршеним кривичним делом. Истраге компјутерског криминалитета почињу идентификовањем доказа, онда следи документовање доказа и на крају њихово прикупљање.[9] Приликом истраживања лица места потребно је поштовати правила и процедуре јер се само на тај начин обезбеђује комплетно документовање лица места, обрада свих релевантних доказа у смислу правилног руковања и паковања доказа и њиховог слања на вештачење. У супротном, непоштовање правила може да прикупљене доказе у судском поступку учини незаконитим и неприхватљивим за поступак. Идентификовање доказа, односно препознавање доказа се врши прегледом лица места, а начин претраге лица места зависи од природе и величине области коју треба претражити, као и врсте доказа (посебно латентних доказа). Преглед лица места почиње визуелним посматрањем, а користе се и разна техничка средства. По идентификацији доказа се прелази на њихово документовање, односно фиксирање које се врши снимањем и фотографисањем.

[8] Видети: I.Marcella & A.Greenfield, *Computer crimes−Investigation−Handbooks,* Boston 2002.

[9] Видети: J. Vacca , Computer Forensics: Computer Crime Scene Investigation, 3rd Edition, London 2005.

Прикупљање доказа током вршења увиђаја обухвата примену метода, техника и процедура које се користе за изузимање доказа са лица места. Овај поступак захтева време, пажљиво и стрпљиво поступање стручних лица, а тимски рад током обраде лица места је од пресудног значаја. Потребно је приликом вршења увиђаја узети све трагове отисака прстију са површине апарата, CRT екрана и компјутерског миша. Уколико, на основу мисаоне реконструкције догађаја, као и сазнатих чињеница, постоји сумња да је компјутер коришћен за складиштење доказа, обавезно се одузимају сви медији за складиштење података. За истрагу могу бити значајни и пронађени програми који прикупљају и анализирају информације, као и било каква упутства за употребу тих програма.

Компјутер који је затечен на лицу места, уколико је укључен, не сме се искључити, јер би то могло изазвати губитак вредних доказа, па форензичар мора прво да тестира поступак гашења да би отклонио ризик од евентуалних деструктивних програма који би се несмотреним гашењем могли активирати и обрисати доказе. Уколико постоји потреба у конкретном сличају да се компјутер склони са лица места јер постоји сумња у постојање замке која би могла да активира злоћудне програме, у таквим ситуацијама је посебно важно пажљиво расклопити рачунарску опрему и тада се најчешће прво каблови правилно обележавају, а да би се касније могли повезати. Наравно све ово се ради у динамичкој фази увиђаја. Све електронске компоненте се чувају у статичким кесама, а користи се и уређај за статичко уземљење да не би дошло до статичког пражњења којим би се уништили докази. Све мере и радње које се предузимају на лицу места захтевају време, па тако, ако је потребно спасити слике са хард драјва, потребан је изузетно дуг технички процес обраде. Претрага медија се такође може извршити на лицу места, а истражна екипа сама одређује време које јој је потребно за преузимање доказа. Наравно, стручност и адекватна опрема су предуслови ефикасне обраде лица места. Поступак увиђаја код компјутерског криминала је исти као и код других традиционалних облика криминала. Ова доказна радња почиње обезбеђењем лица места, а затим следи: визуелни преглед лица места (уз мисаону реконструкцију догађаја), фиксирање лица места (фотографисањем), израда скице лица места, детаљна претрага лица места, снимање и сакупљање материјалних докза и на крају, врши се још једном визуелни преглед лица места. Разлика у односу на увиђаје за друга кривична дела је у томе, што је овде увиђај више техничке природе. С обзиром на то да је предмет увиђаја компјутер или неки електронски уређај, користе се редовне форензичке технике. Приликом обраде лица места потребно је заштити и обезбедити компјутерски систем, а такође је важно да лица која

раде са компјутерима буду удаљена из простора лица места који је обезбеђен. Том приликом се мора установити која лица су била у додиру са лицем места и са њима се одмах по доласку увиђајне екипе, обавља информативни разговор. Управо због тога што оштећена лица прво сама покушавају да отклоне насталу штету, сама или ангажујући стручна лица, често се уништавају непосредни докази који могу да укажу на извршиоца. Због тога је јако важно да по сазнању за извршено кривично дело, оштећена лица одмах обавесте надлежне органе.

Код кривичних дела високотехнолошког криминала, лице места може бити чак и удаљено неко место или возило, што је последица мрежних способности. Радње које су специфичне за вршење увиђаја код тзв. компјутерског лица места се односе на одређивање свих локалитета које је потребно претражити и проналажење специфичности хардвера или софтвера који су предмет увиђаја. Приликом ове доказне радње морају се идентификовати све мрежне могућности, као и везе са местом где се компјутер налази у том тренутку, а ако постоји и Интернет конекција, истрага поприма, поправилу, међународну димензију, и у њу су онда укључени разни Интернет провајдери и други надлежни органи.

Развијање фотографског профила је још једна каратеристика увиђаја за дела компјутерског криминала. Под овим се подразумева фотографисање лица места из свих углова, одмах пошто је оно обезбеђено у затеченом стању. Фотографије изблиза су битне за све конекторе на кабловима и уређајима, који се потом правилно обележавају. Фото албум се прилаже на крају уз записник о увиђају. Развијање фотографског профила захтева хитно поступање и ту се разликује три типа фотографија: фотографије целокупног изгледа лица места - тзв. широк поглед кроз објектив (даљи изглед лица места), фотографије средњег ранга - показују везу између предмета и фотографије доказа изблиза – показују детаље као што су серијски бројеви, ознаке и универзални кодови производа. Ово све се врши у статичкој фази, а у динамичкој - фази претраге, врши се физички преглед лица места и сакупљају се електронски докази. У овој фази је важно да форензичар има претпоставку о врстама доказа који су присутни на лицу места на основу мисаоне реконструкције догађаја. Разлике у истрагама компјутерског криминала се огледају у величини компјутерског система и количини података на диску, која се обезбеђује и снима. С обзиром на то да хард дискови који се могу тренутно наћи на тржишту могу да складиште чак више од 200 ГБ података, прво је потребно одредити капацитет диска који треба да се копира или сними за касније форензичке анализе, јер је код великих датотека то немогуће, па се у тим случајевима форензичка истрага врши на лицу места. Прикупљени докази на лицу места чине тзв. „ланац диги-

талних доказа," а то се постиже применом сложених форензичких метода и строго прописане процедуре.

О привремено одузетим електронским уређајима се саставља посебан записник и они се фотографишу, а лицу од кога је он одузет се издаје потврда. Мобилни телефони су мали и чувају се у Фарадејевим кесама, а дискови се пакују у анти-статичке кесе, пошто су претходно обележени.

За прикупљање и очување дигиталних и мултимедијалних доказа, као и за њихов пренос, неопходно је да постоји успостављен систем квалитета. Овај систем морају имати све установе које се баве форензиком. У том смислу је потребно да се пропишу стандардне процедуре који нису ништа друго, него документоване смернице, односно индикатори контроле квалитета.[10] Сва правила и процедуре у вези са дигиталним доказима морају бити прецизно наведене у документацији форензичке установе стандардних процедура. Употреба стандардних процедура је од фундаменталног значаја како за поступајуће надлежне органе, тако и за саму форензичку науку. Смернице које су у складу са струком су услов за прихватање резултата и закључака од стране судова у кривичном поступку. Имајући у виду чињеницу да су интензивне технолошке промене основна карактеристика дигиталних доказа, врсте, облици и начини прикупљања и испитивања дигиталних доказа се морају правовремено ажурирати, и најчешће се то ради на годишњем нивоу. Стандарди и критеријуми за оцену процедура које се примењују у вези са дигиталним доказима треба да буду флексибилни, а валидност поступка се установљава према егзактношћу и поузданошћу појединих техника. У овом контексту, потребно је користити прикладне хардвере и софтвере (тестиране) који су ефикасни у прикупљању и испитивању дигиталних доказа. Такође треба напоменути да све активности које се односе на одузимање, чување, испитивање или пренос дигиталног доказа, морају бити забележене и у писаној форми. Захтев за поузданошћу доказа подразумева одговарајући непрекинути ланац свих елемената доказа, уз који је потребно обезбедити одговарајућу документацију. Документација која се прилаже уз налаз и мишљење вештака служи за поткрепљење његових закључака.

Међународна организација за компјутерске доказе (International Organization on Computer Evidence (IOCE)) која је основана 1995. године, имала је за циљ да обезбеди размену информација које се односе на кривична дела компјутерског криминалитета, али је ова организација дала и посебан

[10] Стандарде и критеријуме у вези са дигиталним доказима - видети: Digital Evidence: Standards and Principles, Scientific Working Group on Digital Evidence (SWGDE) International Organization on Digital Evidence (IOCE)
http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm#Proposed

допринос у смислу установљавања међународних стандарда за размену електронских података. Међународни стандарди, презентовани и прихваћени на Међународној конференцији високотехнолошког криминала и форензике 1999. године су следећи:[11]

- Ни једна активност која се предузима у вези са дигиталним доказима не сме да утиче на њихову измену.
- Само стручна и компетентна лица могу да имају приступ дигиталном доказу.
- Све активности које се односе на одузимање, складиштење или пренос дигиталног доказа морају бити у потпуности документоване.
- Лице у чијем поседу су дигитални докази је одговорно за све активности које предузме у вези са њима.
- Сваки државни орган (агенција) која је одговорна за одузимање, приступ, складиштење или пренос дигиталних доказа, мора да поступа у складу са опште прихваћем стандардима.

Остале препоруке Међународне организације за компјутерске доказе се односе на форензичку компетенцију и потребу за међународном акредитацијом алатки, техника и обуке, као и размену информација које се односе на високотехнолошки криминал и форензичко рачунарство.

После извршеног увиђаја је важно како се архивирају дигитални и мултимедијални докази из разлога што је потребно да се то изврши на начин којим ће се омогућити приступ тим доказима, када се за тим укаже потреба. Архивирање је поступак складиштења података у дужем временском периоду, на начин који их чини доступним. У случајевима где је потребно да се изврши архивирање, потребно је да оно буде планирано од самог почетка генерисања, обраде, па до одузимања доказа.[12]

7. Истраге у сајбер простору

Једна од карактеристика кривичних дела високотехнолошког криминала је специфично место извршења дела. Наиме, место извршења ових кривичних дела не може се везати за рачунар и сто на коме се рачунар налазио у тренутку извршења, јер је сајбер простор виртуелни део стварности који не познаје државне границе као ни суверену власт државе. Ова специфичност је последица појаве Интернета и глобализације мрежа које

[11]Digital Evidence: Standards and Principles, Scientific Working Group on Digital Evidence (SWGDE)International Organization on Digital Evidence (IOCE)
http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm#Proposed

[12] SWGIT Guidelines for the Forensic Imaging Practitioner / Section 15 Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal Justice System
http://www.theiai.org/guidelines/swgit/guidelines/section_15_v1-1.pdf

данас постоје. Експанизија Интернета и глобализација локалних мрежа, као и нагли развој информационе компјутерске технологије условиле су нови начин рада стручњака информационе технологије. Наиме, пошто су се класичне лабораторије показале као неадекватне у овим случајевима, форензичари су од сајбер простора направили нове лабораторије. Сајбер форензика је омогућила да се докази проналазе у рачунарским мрежама и на Интернету. Имајући у виду да се све одиграва *on-line*, на мрежи у реалном времену, потребно је да се прате тзв. *упади*, преглед забрањеног садржаја на Интернету, евентуалне злоупотребе и друге сумњиве активности. Као логична и нужна последица наведеног, поставило се најдискутабилније питање за сајбер форензичаре, а то је законитост њихових активности у смислу поштовања приватности, односно границе задирања у ову зону. Ово је највећи проблем данас са којим се сусрећу сајбер форензичари. Ипак, ефикасна борба против овог вида криминалитета показује активност форензичара усмерену на спречавање, откривање и доказивање преступа у сајбер простору као претежнији интерес, а законодавац је тај који треба да успостави потребну равнотежу између два, на први поглед супротстављена интереса, право на ефикасно кривично законодавство и право на заштиту основних права и слобода грађана.

Приликом истраге на Интернету постоје одређена опште прихваћена правила у поступању, односно стандардизација које се треба придржавати. [13] Истраживање форензичара у сајбер простору почиње утврђивањем идентитета корисника, а то се врши помоћу IP адресе рачунара. Ова адреса је почетна степеница у истрази. IP адреса је јединствени број рачунара, изражен у бројевима који омогућава међусобни саобраћај корисника путем Интернета, а у складу са правилима Интернет протокола. Тај међусобни саобраћај подразумева примање и спровођење информација у име пошиљаоца. Применом посебних метода, када се утврди *web hosting service*, од сервисера правосудни органи траже податке о идентитету лица које је осумњичени у конкретном случају. *Web hosting service* је врста сервиса домаћина на Интернету који омогућава физичким и правним лицима да своје веб сајтове учине доступним у оквиру целе мреже. Уколико се утврди да су подаци о кориснику неистинити, онда се тражи листа корисника који су креатори Интернет странице, јер се на основу тога може утврдити IP адреса код провајдера, где се појављује осумњичено лице. Ту се прво врши индивидуализација лица, утврђује се да ли је осумњичено лице правно или физичко лице, а тек онда се установљава његов идентитет. Обавеза задр-

[13] Видети: Ј.Крстић, Стандарди у поступању тужилаца у борби против компјутерског криминала, CD Зборник *ZITEH,* 2004., стр. 10.
http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-12.pdf

жавања телекомуникационих података за провајдере која је прописана законом у државама чланицама ЕУ (а који су усклађени са Директивом ЕУ о задржавању података), омогућава долажење до података о времену и месту деловања корисника на Интернету, односно осумњиченог лица.

Дигитална форензика своју примену није нашла само у оквиру рада служби јавне безбедности, државне безбедности и правосудних органа, већ и у организацијама и предузећима, где је потребно уз помоћ форензичких научних метода утврдити одређене чињенице и доказати их.

8. Закључна разматрања

Компјутерска форензика је данас *condicio sine qua non* за откривање дигиталних доказа, поступање са њима и њихово презентовање у кривичном поступку. Да би се ова грана форензике могла на ефикасан начин употребити, односно применити у судском поступку, потребно је да постоји одговарајућа законска регулатива. У том смислу, треба истаћи да су Сједињене Америчке Државе и земље западне Европе регулисале својим позитивним законодавством компјутерску форензику тако што су усвојиле опште процедуре и стандарде који се односе на дигиталне доказе. У Републици Србији у Кривичном законику, глави 27. - кривична дела против против безбедности рачунарских података[14] и у Закону и организацији и надлежности државних органа за борбу против високотехнолошког криминала[15] је дефинисана улога компјутера код ових кривичних дела, и на овај начин су дигитални докази ушли у судске поступке и постали незаобилазни део откривања и доказивања. С обзиром да је веома комплексан задатак извођење дигиталних доказа у поступку, потребно је да се форензичари информационе технологије строго придржавају основних правила и процедура у поступању са дигиталним доказима. Развој информационе технологије и дигиталне форензике је показао да, иако трагови могу бити у дигиталном облику, готово невидљиви у сајбер простору, могуће их је повезати траг са појединцем, односно извршиоцем кривичног дела. Ипак, с обзиром на то да се информациона технологија брзо развија, неопходно је да позитивноправни прописи, као и знање учесника у кривичном поступку прате овај развој јер само на тај начин ће се остваривати циљеви кривичног права. Позитивно законодавство које се односи на ову проблематику треба да буде засновано на релевантним међународним стандардима, а стандардизација поступања са дигиталним

[14] Кривични законик, Службени гласник РС број 85/2005, 88/05 - исправка, 107/05-исправка и 72/09.

[15] Слижбени гласник РС број 61/2005.

доказима је неопходна за размену информација у вези са кривичним делима високотехнолошког криминала на националном и на међународном плану. На крају, треба истаћи да су полиција, тужилаштво и Интернет провајдери основни носиоци откривања и доказивања кривичних дела високотехнолошког криминала, али је исто тако неопходно да држава својим прописима омогући надзор од стране ових органа над саобраћајем који се одвија на Интернету, уз заштиту свих права која припадају корисницима рачунара, односно Интернета.

Tatjana Lukić, Ph.D., Associate Professor
Faculty of Law Novi Sad

Digital Evidence

Abstract:

Although computer makes human activities faster and easier, innovating and creating new forms of work and other kinds of activities, it also influenced the criminal activity. The development of information technology directly affects the development of computer forensics without which, it can not even imagine the discovering and proving the computer offences and apprehending the perpetrator. Information technology and computer forensic allows us to detect and prove the crimes committed by computer and capture the perpetrators. Computer forensics is a type of forensics which can be defined as a process of collecting, preserving, analyzing and presenting digital evidence in court proceedings. Bearing in mind, that combat against crime, in which computers appear as an asset or object of the offense, requires knowledge of digital evidence as well as specific rules and procedures, the author in this article specifically addresses the issues of digital evidence, forensic (computer) investigation, specific rules and procedures for detecting, fixing and collecting digital evidence and use of this type of evidence in criminal proceedings. The author also delas with international standards regarding digital evidence and cyber-space investigation.

Key words: digital evidence, computer forensic, information technology, criminal procedure.