Др Видоје Спасић,*
Ванредни професор Правног факултета,
Универзитет у Нишу

Бранко Стевановић,*
дипл. инг. електронике, администратор мреже Правног факултета,
Универзитет у Нишу

СТРУЧНИ ЧЛАНАК

UDK: 347.78:004.738.5

Рад примљен: 03.04.2015.
Рад прихваћен: 11.06.2015.

*ДОКАЗИВАЊЕ ДИГИТАЛНИХ ПОВРЕДА ПРАВА ИНТЕЛЕКТУАЛНЕ СВОЈИНЕ - ОСВРТ НА АНГЛОСАКСОНСКИ ПРАВНИ СИСТЕМ***

Апстракт**:** *Развој дигиталне технологије довео је до драматичног пораста сајбер криминала у разним областима, а нарочито на пољу интелектуалне својине. Корисници све више користе рачунаре и друге електронске уређаје за вршење повреда интелектуалне својине. Притом, многи починиоци оваквих дела верују да се могу изгубити у мору личних и мрежних рачунара и да могу избећи одговорност за учињене радње. Ипак, ствари не стоје тако. Уколико је извршена злоупотреба рачунара, он се може претражити и анализирати, па је тако могуће утврдити одговорност починиоца дела. Ово се врши утврђивањем дигиталних доказа, који се од осталих материјалних доказа разликују по форми у којој су инкорпорисане информације, а то је дигитална форма која подразумева неки електронски или магнетни уређај.*

Поступак утврђивања дигиталних доказа спроводе сертификовани рачунарски форензичари, употребом различитих техника и алата, поштујући одговарајуће процедуре, јер се подаци током прикупљања могу изгубити или оштетити.

У раду су обрађени најважнији аспекти доказивања дигиталних повреда интелектуалне својине, као и проблеми који се појављују у вези са тим, са посебним освртом на англосаксонско право.

Кључне речи**:** *дигитални доказ*, *компјутерска форензика, дигитална технологија, интелектуална својина.*

* vidza@prafak.ni.ac.rs

* bane@prafak.ni.ac.rs

** Чланак је резултат рада на пројекту „Усклађивање права Србије са правом Европске уније“, који финансира Правни факултет Универзитета у Нишу.

1. Увод

У данашње време чак 90% свих постојећих информација налази се у дигиталном формату.[1] Развој дигиталне технологије, поред многих погодности, донео је и одређене нежељене, па и штетне последице. Пре свега, настао је нови облик криминала – тзв. сајбер криминал у различитим сферама. Поред тога, приватност појединца озбиљно је доведена у питање. Најзад, информатичка технологија ставила је права интелектуалне својине пред велике изазове и искушења, тиме што је знатно олакшала њихово кршење. При свему томе, нова технологија је отежала доказивање дигиталних повреда, чиме је, на неки начин, ставила починиоце повреда у релативно комфорнији и заштићенији положај у односу на легалне носиоце права.

Починоци дигиталних повреда права интелектуалне својине обично мисле да неће бити откривени и да се лако могу изгубити и сакрити у мору личних и мрежних рачунара. Међутим, ствари не стоје баш тако. Технички, постоји само пар метода за брисање, а много начина за скривање података. Захваљујући дигиталној или мрежној форензици могуће је откривање и презентовања веродостојних доказа о дигиталним повредама интелектуалне својине. Овакве доказе могуће је открити чак и када је починилац обрисао податке с рачунара. То чине рачунарски форензичари различитим алатима за обнову података, уз поштовање строге процедуре како би докази били веродостојни.

Компјутерска (рачунарска) форензика представља примену компјутерске истраге и техника анализе у циљу утврђивања релевантних дигиталних доказа. Основни циљ рачунарске форензике је објаснити тренутно стање дигиталног артефакта. Појам дигитални артефакт укључује рачунарски систем, медијум за смештај података, као што су чврсти диск или ДВД медијум, електронски документ (порука електронске поште, дигитална фотографија) или низ мрежних пакета. При спровођењу форензичке истраге неопходно је предузети посебне мере да би докази били валидни и прихватљиви на суду. Једна од најважнијих мера је осигуравање да је доказ прикупљен на исправан начин и да се поштује ланац поседа доказа од места повреде до лабораторија и, коначно, до суда.

1 ТВ који нас шпијунира, смарт апарати за домаћинство који се активарају путем СМС порука, 3Д штампачи људских органа, козметичких производа, аутомобилских делова и грађевинских елемената – само су неки од производа нове технологије.

2. Интернет пиратерија

Под дигиталном пиратеријом, у најширем смислу, подразумева се израда нелегалних копија дигиталних производа и информација заштићених правом интелектуалне својине. Прецизније, под пиратеријом дигиталног садржаја на Интернету подразумева се незаконито коришћење или дистрибуција ауторизованог дигиталног садржаја који се дистрибуира преко Интернета.

Интернет пиратерија представља незакониту репродукцију и/или дистрибуцију заштићеног дигиталног материјала путем рачунарске мреже. Генерално, у области информационо-комуникационих технологија два најзначајнија облика и предмета потенцијалних повреда интелектуалне својине су софтвер и мултимедијални садржаји у дигиталном облику.

Под дигиталним садржајем најчешће се подразумевају: аудио садржаји (компакт дискови музичких кућа), телевизијске серије, играни и документарни филмови, комерцијални софтвер, електронске и аудио књиге, комерцијални мултимедијални туторијали и други садржаји који се масовно дистрибуирају преко Интернета, а заштићени су ауторским правима.

Електронски садржаји различите врсте и природе могу се преносити путем мрежа за размену фајлова, пиратских сервера, veb-сајтова или хакованих рачунара.

Дељење датотека (енгл. *file sharing*) се дефинише као процес слања датотека на Интернет тако да се оне касније могу преузети и репродуковати. Софтвери који се за то користе нису нелегални per se, али је њихова употреба за прибављање датотека заштићених ауторским правима противзаконита. Посебни дистрибуциони канали за дељење датотека су P2P (енгл. *peer-to-peer*) сервиси који омогућавају рачунарима директно повезивање са другима у циљу размене и копирања датотека путем децентрализованих мрежа. У овим мрежама рачунари су међусобно директно повезани без посредовања централног сервера.

Први популарни сервис за дистрибуцију музике који је корисницима омогућио приступ великој мрежи музичких датотека био је Napster, који се појавио крајем 20. века.[2] Након Napster-а, појавили су се нови програми који су по функцији били слични њему, као нпр. Kazaa, Grokster, Morpheus,

2 Софтвер је омогућавао корисницима да претражују музичке датотеке на чврстим дисковима других корисника и преузму их бесплатно. Иако Napster није чувао пиратске садржаје на сопственим серверима, убрзо је наишао на оптужбе да дељење фајлова између корисника представља пиратерију. Организација за заштиту права музичких издавача у Сједињеним Америчким Државама – RIAA тужила је Napster због повреде ауторских права. Судском одлуком из 2002. године наложено је гашење сервиса и

eDonkey и сл., који су развили модификоване сервисе који нису могли бити директно одговорни за дистрибуцију пиратског садржаја, већ су ту одговорност пребацивали на појединце, тј. кориснике. И ови сервиси су доживели исту судбину, па су неки убрзо били угашени, док су други наставили да функционишу по легалним принципима.[3]

Софтверска пиратерија односи се на израду и употребу нелегалних копија рачунарског програма. Корисник куповином софтвера купује само лиценцу, односно право коришћења софтвера, али не и право његове даље дистрибуције.[4] Приликом куповине и инсталације софтвера, корисник „потписује уговор" са произвођачем, којим се обавезује на поштовање свих обавеза у вези са употребом софтвера. Овај уговор познат је под називом уговор крајњег корисника о коришћењу лиценце (EULA – End User Licence Agreement).

Иако ниједан од постојећих метода не гарантује потпуну заштиту, данас се у свету најчешће примењују следеће методе борбе против софтверске пиратерије: заштита по основу ауторских права, заштита од копирања и лиценцирање по месту употребе.

Технике заштите од копирања састоје се у примени хардверских и софтверских карактеристика које спречавају покушаје копирања или копирани софтвер чине непоузданим. Иако су до сада коришћене многе технике заштите (нпр. ДВД дискови се заштићују дигиталним „омотачима" – wrappers), показало се да ниједна од њих не даје потпуну сигурност. Због тога већина произвођача одустаје од ове методе и више се ослања на преостале две.

За потребе компанија и институција са великим бројем корисника, а у циљу сузбијања пиратерије, неки произвођачи софтвера нуде могућност мрежног лиценцирања (site licencing).[5] Осим тога, неке софтверске компаније, у циљу свог пропагирања, често своје производе уступају

исплаћивање милионских одштета музичким стваралоцима и власницима ауторских и сродних права.

3 Због свега изнетог, пирати су креирали нови протокол који ће онемогућити кривично гоњење лица које учествује у размени датотека – BitTorrent.

4 Према неким проценама, данас око 40% свих персоналних рачунара у свету ради помоћу илегалног софтвера (у САД око 25%, у Европи око 35%). Као земље са највећим процентом илегалног софтвера истичу се Вијетнам, Кина, Индонезија, Украјина и Русија, у којима више од 85% софтвера представљају нелегалне копије.

5 У овом случају, корисник на основу уговора са произвођачем, добија један примерак инсталационог диска и пратеће документације, а добија дозволу за инсталацију софтвера на онолико рачунара за колико је лиценца плаћена.

потпуно бесплатно за некомерцијалне сврхе (нпр. универзитетима или факултетима). У том смислу, последњих година у успону је и тзв. концепт отвореног кôда (Open Source), по коме произвођачи софтвера уступају бесплатно на коришћење своје производе.[6] Проблем пиратерије се повећао са развојем нових технологија које омогућавају лакше и ефикасније неовлашћено копирање музике (и других садржаја) и њене дистрибуције.[7]

Генерално, постоје четири доминантна вида пиратизације дигиталних производа, што се може остварити:

- куповином легалне копије филма, музике, видео-игрице, књиге или софтвера након чега следи креирање илегалних копија;
- директно од извора, од стране инсајдера, из сфере филмске и музичке индустрије које најновија остварења редовно деле са светом путем торената;
- снимањем садржаја који се емитује на телевизији на својим рачунарима;
- неке врсте ТВ емисија, као што су преноси спортских утакмица захтевају тренутну доступност садржаја, па нема говора о снимању и накнадном аплоудовању. Уместо тога, корисници који имају плаћене канале на којима се поменути садржај емитује помоћу брзе мреже успостављају канал за стрим и World Series – који иначе можда не би могли да гледају.

Други значајан сегмент у процесу пиратерије представља дистрибуција креираног дигиталног садржаја. Технички, она се може реализовати на више начина.

2.1. BitTorent

Корисник који је сачинио нелегалну копију садржаја заштићеног ауторским правом, помоћу свима доступног софтвера креира torrent фајл који затим аплоудује на један (или на све) од veb-сајтова (PirateBay, Kickass.to, некада Demonoid, MiniNova…), који служе као базе за њихово складиштење. Пират је обично регистрован под препознатљивим надимком, па они који од њега "скидају" могу да буду уверени у квалитет његовог рипа.

6 Примери за овај концепт су оперативни систем Linux, софтверски пакет OpenOffice.org, veb server Apache, итд.

7 Према једном истраживању, годишња штета у Сједињеним Америчким Државама проузрокована музичком пиратеријом процењује се на близу 15 милијарди долара, више од 70.000 изгубљених радних места и укупним губитком плата од 2 милијарде долара.

За разлику од претходних варијанти P2P технологије, торент сам по себи није нелегалан садржај већ обичан фајл који садржи извесну групу информација о већем фајлу, који не мора сам по себи да буде заштићен ауторским правом.[8] Заинтересовани корисник са било ког места у свету са сајта "скида" торент фајл, покреће га путем једног од бројних BitTorent програма и преузима филм који се налази на пиратовом рачунару. Већ током "скидања" филма, корисник постаје и сам пират пошто до тог тренутка преузете информације већ дели са трећом, четвртом, н-том особом. На крају, филм је преузео толики број људи да пират од кога је све почело може без проблема да престане са дељењем: филм је у суштини свуда и нигде (у виртуелном простору) и његова дистрибуција више не може бити заустављена. Мрежа базирана на овом протоколу је децентрализована, а претрага за датотекама се своди на претрагу .torrent датотека у којима се налази списак рачунара са жељеним датотекама.

2.2. Директно преузимање са сервера

Релативна спорост "скидања" путем торената, узрокована и зависношћу од других корисника, довела је до директног преузимања са сајтова који служе за складиштење података.[9] Систем функционише тако што се пиратизовани филм "пакује" обично у .rar формат, а потом дели на више једнаких делова и подиже на сервере тих сајтова. Пирати то обично раде сакривајући своје IP адресе коришћењем прокси сервера, након чега добијене линкове остављају на специјализованим форумима, како би свако заинтересовано лице могло да дође до пиратизованог садржаја.[10]

2.3. Онлајн гледање или слушање садржаја

За кориснике који не желе да чекају "скидање" садржаја, а имају довољно брзе интернет конекције, најбоље решење јесте онлајн приступ садржају. На Интернету постоје бројни сајтови на којима се филмови, серије и друге емисије могу гледати без претходног даунлоуда. Код нас је овај начин мање популаран, јер већина оваквих сајтова не омогућава учитавање титлова, док је у свету равноправни канал са осталима. У питању су сајтови који су

8 Суд америчке државе Ајова одбио је 2014. године масовну тужбу против корисника BitTorrent програма као неосновану, јер не доказује сарадњу између интернет пирата. http://torrentfreak.com/judge-understands-bittorrent-kills-mass-piracy-lawsuits-140130/

9 Најпопуларнији је био MegaUpload.com (сада на адреси Mega.co.nz).

10 Преузимање фајлова од стране крајњег корисника може бити једноставно обављено путем browser-a (сваки фајл скида се посебно, за сваки се мора укуцати код, на сваки мора да се чека одбројавање), али постоји и много програма који све то раде аутоматски.

обично регистровани у државама у којима борба против пиратерије није узела маха, па се кршење интелектуалне својине толерише.[11]

2.4. "Скидање" у клауду

Последњи и најновији тренд у дистрибуцији пиратизованог садржаја до крајњих корисника представљају тзв. клауд сервиси. Сервиси као што су Wuala, uTorrent и Tribler омогућавају "скидање" садржаја и држање у клауду, и да се њему може приступити на жељеном месту, нпр. путем телефона током вожње или на било ком другом месту. Ова технологија се популарно назива "рачунарство у облаку" (енгл. "Cloud computing"), а обезбеђује флексибилан, од локације независан приступ рачунарским ресурсима који се брзо и неприметно алоцирају и деалоцирају према потражњи.

Важно је истаћи да сајтови на којима се могу "скидати" торенти немају на својим серверима филмове или музику: такви садржаји "скидају" се од других корисника са њихових рачунара, а торент само служи за повезивање са њима. Теоретски, торент у имену може да тврди да садржи филм, а да садржи нешто потпуно друго. Због тога је било јако тешко судски доказати да се путем ових сајтова крше закони, мада пресуде у том смислу ипак постоје.

3. Дигитална (рачунарска) форензика

Термин компјутерска или дигитална форензика означава примену научних метода у циљу идентификације, прикупљања и анализирања података уз очување интегритета оригиналног доказа, као и ланца надлежности. Другим речима, компјутерска форензика се бави прикупљањем, опоравком обрисаних, криптованих или оштећених података и њиховим презентовањем пред надлежним државним органима. Сви дигитални уређаји остављају делиће информација. Ови делићи представљају веома значајан доказ у различитим врстама истрага. Притом, алати и технике које ова дисциплина захтева су релативно лако доступни свакоме ко жели да спроведе форензичку анализу.

Циљ методологије и технологије рачунарске форензичке анализе јесте обезбедити поуздано чување дигиталних података, опоравак избрисаних података, реконструкцију рачунарских догађаја, одвраћање нападача, генерисање добрих форензичких алата и процедура (Тривић, 2011: 300-311).

11 Један он тренутно најпознатијих је мексички спортски сајт: www.rojadirecta.me

Дигиталним доказима се бави компјутерска форензика. Она се базира на следећим принципима: *законитости; ланца истраге; очувања диги-талног доказа; идентификације потенцијалног доказног материјала и интегритета доказног материјала.*

У Кривичном праву постоји тзв. Локаров „принцип размене", који је заснован на постулату да при сваком контакту две ствари долази до размене.[12] Таква је ситуација и приликом контакта два електронска уређаја.

Рачунарска форензика дели се на четири основне гране:

- форензика заштитног зида (енг. *firewall forensics*);
- мрежна форензика (енг. *network forensics*);
- форензика база података (енг. *database forensics*) и
- форензика мобилних уређаја (енг. *mobile device forensics*).

Форензика заштитног зида се бави механизмима заштите од неовлашћеног приступа блокирањем приступа потенцијално штетним програмима или информацијама (Спасић, 2010: 91).

Мрежна форензика се бави употребом научно доказаних техника за прикупљање дигиталних доказа и поступање са њима, а све у циљу откривања чињеница везаних за инкриминисане рање. Базира се на праћењу мрежног промета и откривању аномалија, односно инцидената на њему. Рачунарски сигурносни инцидент представља сваки догађај који угрожава било који аспект рачунарске сигурности, односно који за последицу има губитак поверљивости, интегритета и расположивости података, злоупотребу или оштећење информација или информацијског система, као и сваку незакониту радњу чији се докази могу сместити на рачунарски медијум. Форензички специјалисти увидом у прикупљене доказе могу одговорити на сигурносни инцидент. Системи мрежне форензике могу бити различити.[13]

12 Edmond Lokart (1877–1966) био је први директор Криминалистичке лабораторије у Лиону (Француска) – Локарова терорија или Локаров 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.

13 Системи мрежне форензике могу бити тзв.: „улови-то-на-било који-начин" системи (енг. *„Catch-it-as-you-can" systems*) – сви пакети информација који пролазе кроз одређену прометну тачку се пресрећу и спремају за даљњу анализу; „стани, погледај и послушај" системи (енг. *„Stop, look and listen" systems*) – сваки пакет се анализира на рудиментаран начин у меморији и само се одређени подаци чувају за будућу анализу.

Форензика база података се бави претрагом и анализом база података или посебних трансакција и релација (енг. *Tables transactions end relations*) извучених из базе, не дирајући у интегритет података у циљу реконструкције података или чињеница који су се догодили у систему.

Форензика мобилних уређаја укључује скуп метода претраживања доказа с мобилних уређаја. Ови мултифункционални уређаји користе другачије типове меморије и интерфејса од личних рачунара, па су и технике стварања форензичке слике медија другачије. На овим апаратима се налазе бројни подаци као што су контакти (бројеви телефона, адресе), фотографије, календари, белешке и сл., па они имају све већу улогу у истражном процесу. Најновије генерације мобилних уређаја имају фантастичне перформансе, па стога они могу послужити као драгоцено средство за утврђивање доказа и починилаца различитих незаконитости, па тако и повреда права интелектуалне својине.

4. Дигитални докази

4.1. Појам

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) (Лукић, 2012: 182). Докази дигиталних повреда интелектуалне својине деле се на личне и материјалне, 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. 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 одрђено дело. (Лукић, 2012: 179).

Дигитални докази могу бити тројаки. Оригинални дигитални доказ (енг. evidence media) чине физички предмет и/или подаци садржани у том предмету у време аквизиције (откривања, препознавања, извлачења) или заплене предмета које треба истражити. То могу бити подаци снимљени на рачунару који је физички привремено одузет док истрага траје са циљем достављања тог доказа суду, по иницирању судског поступка.

Дупликат дигиталног доказа (енг. target media) је прецизна дигитална репродукција свих објеката података садржаних у оригиналном физичком предмету (HD, CD ROM, FD, итд.).

Копија дигиталног доказа је прецизна репродукција информација које су садржане на оригиналном физичком предмету, независно од оригиналног физичког предмета.

Веома значајан датум за дигиталну форензику као младу научну дисциплину представља 1991. година. Наиме, те године је у Портланду (држава Орегон) одржано заседање Међународне асоцијације рачунарских научника IACIS (International Association of Computer Specialist), којом прилико је констатовано и одлучено да су „дигитални докази" равноправни са доказима прикупљеним на традиционалан начин, односно физичким предметима.

Америчко удружење директора лабораторије за злочине (American Society of Crime Laboratory Directors / Laboratory Accreditation Board (ASCLD/LAB) је 2003. године, потврдило је горе изнети став. Упоредо са прихватањем компјутерске форензике као легитимног поступка анализе доказа долази и до повећаног интересовања за обучавање и едукацију на овом пољу. [14]

Према *National Institue of Justice SAD* од 2008. године, дигитални доказ је дефинисан као информација или податак од значаја за истрагу који је ускладиштен, примљен или послат преко електронског уређаја. Према другој дефиницији предложеној од стране *Scientific Working Group on Digital Evidence* од 2009. године, дигитални доказ је свака информација која има доказујућу вредност, а која је ускладиштена или се преноси у дигиталном облику. Дигитални доказ је било која информација генерисана, обрађена, ускладиштена, или пренесена у дигиталном облику на коју се суд може ослонити као валидну.[15] То је свака бинарна информација ускладиштена или пренесена у дигиталној форми која има доказујућу вредност и на коју се суд може ослонити, у контексту форензичке аквизиције, анализе и презентације (Petrović, 2004).

Дигитални докази морају бити чврсти и кохерентни и не смеју имати такозване пукотине за доношење неспорних закључака. За разлику од

14 Више видети: The American Society of Crime Laboratory Directors/Laboratory Accreditation Board http://www.ascld-lab.org/. Тренутно постоји више од тридесет колеџа и универзитета само у Америци који обављају едукацију на овом пољу.

15 То је свака бинарна информација, састављена од дигиталних 1 и 0, ускладиштена или пренесена у дигиталном формату. Обухвата компјутерски ускладиштене и генерисана доказе, дигитални аудио и видео сигнак, запис са мобилног телефона, запис са дигиталне факс машине или других уређаја.

физичких доказа који су робустни, дигитални докази су крхке природе и лако могу бити модификовани, уништени или изгубљени.

Валидни дигитални доказ треба да поткрепи чињенице изнете на суду. Он мора бити поуздан и доприносити истрази. Да би се неки форензички алат користио у истрази, потребно је да буде сертификован и признат од државних органа, како би дигитални докази били валидни у одређеном поступку. Ово утолико пре јер се интегритет и егзактност дигиталних доказа лако могу компромитовати и њихова валидност довести у питање.

У компјутерском инциденту постоје три основне категорије дигиталних података који могу чинити дигитални доказ:

- променљиви подаци или информације које се губе након искључивања рачунара, као нпр. подаци о радној меморији (RAM), резидентни меморијски програми и сл.;
- осетљиви подаци или подаци ускладиштени на чврстом диску (HD), који се лако могу изменити, као што је нпр. последње време приступа лог датотеци итд.;
- привремено доступни подаци или подаци ускладиштени на HD којима се може приступити само у одређено време (нпр. шифровани подаци).

Компромитовани рачунар подразумева нападнути рачунар (жртву), али за потребе рачунарско форензичке анализе (РФА), зависно од конкретног контекста, може обухватити и осумњичени изворни или посредни рачунар (нпр. онај преко чијег налога је нападач ушао у систем). Појавом смарт мобилних телефона и уређаја са оперативним системима Android и Apple iOs, све више се појављује као компромитовани рачунар и оваква врста уређаја па ће се, следствено томе, овакви уређаји све више бити предмет РФА.

4.2. Карактеристике дигиталног доказа

Утврђивање дигиталних доказа карактерише, пре свега, велики број осумњичених лица, јер су корисници Интернета најчешће анонимни, па је круг потенцијалнх починилаца велики. Идентификација преступа се код дигиталних повреда интелектуалне својине често врши временски много касније у односу на извршено дело. Велики број потенцијалних доказа се на самом почетку истраге елиминише да би се могла поставити почетна хипотеза истражитеља, што се врши у зависности од саме природе преступа. Подложност контаминацији подразумева њихову велику осетљивост на промену стања, па се морају предузети све мере за очување

затеченог стања и то 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 знало да је доказ присутан (Лукић, 2012: 184).

Поред наведеног, дигитални доказ карактеришу и: технолошка напредност; флексибилност; могућност умножавања и модификовања; невидљивост; транснационални карактер.

Пошто компјутерски криминалитет тангира земље са различитим суверенитетом, Међународна организација за компјутерске доказе (International Organization of Computer Evidence – IOCE) је, марта 1998. године, формулисала међународне принципе за поступке којима би се гарантовало коришћење дигиталних доказа прикупљених од стране једне државе у суду друге државе (Вукоман, 2010). Да би се дигитални докази што ефикасније размењивали, морају бити задовољени основни принципи (Грубор, 2004):

- конзистентност са правосудним системима у свакој држави;
- употреба уобичајеног и разумљивог језика;
- поседовање трајне вредности;
- међународна прихватљивост и признавање;
- уливање поверења и заштита интегритета дигиталних доказа;
- применљивост на све дигиталне доказе;
- применљивост на појединца, званичне агенције и највиши национални ниво.

Henry Lee, професор Форензичке науке на универзитету New Have и директор "Forensic Research and Training Center" истиче да паралелно са истражним фазама, дигитални докази пролазе кроз своје фазе (Lee's, 2001: 272-276).

Прва фаза је фаза препознавања (енг. recognition) односно изједначавање места проналажења доказа са местом извршења радње. Наведено препознавање врши се током извођења истражних радњи прикупљања доказа (фаза истраживања и претраживања).

Друга фаза је идентификација (енг. identification) у којој се прегледају и упоређују класне карактеристике доказа са познатим узорцима да би се утврдила класа конкретног доказа.

Следећа фаза је индивидуализација (енг. individualization), у којој се прегледају индивидуалне карактеристике предметног доказа да би се

одредило да ли је предметни доказ јединствен у односу на друге доказе у оквиру класе или да утврди да ли предметни доказ потиче из предметног извора извршења дела као и остали докази. Када су рачунари у питању, тешко је извршити индивидуализацију дигиталног доказа у истој мери као што се то може урадити са физичким доказом, зато што су дигитални објекти генерисани инструкцијама код којих се може јавити и елемент случајности. Најзад, последња фаза је реконструкција (енг. reconstruction), која представља круну свих претходних фаза.

Иако је IOCE прописала опште принципе и процедуре у вези дигиталних доказа, још увек нигде у свету не постоји верификација званичних истражних органа, форензичких аналитичара и правосудних органа, подједнако квалификованих у својим областима, да објективно и тачно воде истрагу, форензичку аквизицију, анализу, доказни поступак и презентацију дигиталних доказа на суду.[16]

4.3. Прихватање доказа

Одређени докази, као што су ДНК анализа или отисци прстију, општеприхваћени су у свету. За неке друге доказе није тако. У дугом периоду прихватања и оспоравања одређених метода као судских доказа издваја се тзв. Даубертово правило (Daubert rule or rule 702), које је суд у Дауберту предложио 1973. године. По овом правилу да би метод прикупљања доказа био валидан потребно је следеће:

а. да је метод који су научници (форензичари) користили тестиран у теоријском и техничком смислу;

б. да је теорија која стоји иза метода била презентована научној јавности на преиспитивање;

в. да је теорија и техника прихваћена у научној јавности;

г. да су позната статистичка одступања при примени ове методе, и

д. да су приликом извођења доказа примењени стандарди које метода налаже.

Приликом прикупљања дигиталних доказа настао је велики проблем у примени овог правила. Пре свега, тешкоће се огледају у томе што не постоје општеприхваћене научне теорије за одређене појаве у дигиталном свету. Ово због саме природе дигиталних информација. У зависности од начина на који су бинарне цифре распоређене у фајлу, рачунарски

16 Seminar "Specifičnosti veštačenja u oblasti zloupotrebe IT", Udruženje IT veštak, 15.11.2011. Преузето 20. 01. 2015. http://www.itvestak.org.rs/ skupovi/Seminar_saopstenje.htm

програми интерпретирају фајл као текст, слику, аудио, или видео снимак, програм или слично. Постоји огроман број врста фајлова, од којих су неки формати фајлова познати само произвођачима софтвера за те фајлове, неки су општепознати, неки подложни константној промени, а неки, иако формално стандардизовани, због недовољно чврстих стандарда различито интерпретирани од различитих програма.[17] Поред тога, и код познатих врста фајлова постоје тзв. резервисани бајтови који су остављени за даљу надградњу формата фајла, који су разне програмерске куће користиле свака на свој начин. Притом, и у истој програмерској кући постоје одређени проблеми.[18] У таквом хаосу није могуће говорити о опште прихваћеној теорији или стандарду.

Да би се дигитални докази како-тако прихватили, дошло је до проширења Даубертовог правила поводом једног судског спора.[19] Врховни суд САД (United States Supreme Court) је у том случају успоставио принцип да се докази могу прихватити ако су део сведочења експерата без обзира да ли су засновани на научном, инжењерском или другом специјализованом знању. Иако је овај принцип дао решење за конкретан случај, он је, с друге стране, отворио многа друга питања.

Још један проблем који се јавља у признавању доказа огледа се у томе што је већина дигиталних информација у суштини подложна променама. Дигиталне информације се морају у поступку прибављања доказа очитати преко одређених уређаја који могу изменити те информације.[20] Да би се избегли ови и слични проблеми на Међународној конференцији о високотехнолошком криминалу (International HighTech Crime Conference) 1999. године, усвојени су следећи принципи:

- активности у прикупљању дигиталних доказа не смеју мењати те доказе;

17 Типичан пример за то је html фајл формат, тако да исти фајл може да буде различито приказан у зависности који претраживач се користи (internet explorer, google chrome, mozila firefox или неки други).

18 Познато је признање програмера запослених у Microsoft-u који су наследили посао од раније запослених програмера да за одређене делове програма уопште нису знали чему служе, али су их оставили у финалном производу из страха да нешто не поремете.

19 KUMHO TIRE CO. V. CARMICHAEL (97-1709) 526 U.S. 137 (1999)

20 Тако, на пример, ако истражитељ прикључи заплењени хард диск за који се сумња да садржи одређене доказе на рачунар на коме је инсталиран Windows оперативни систем и затим укључи рачунар, садржај хард диска ће бити промењен – неће бити у потпуности идентичан оригиналу који је заплењен. Самим тим се и валидност тако изведених доказа доводи у питање иако обично те промене нису битне и не утичу на доказе.

- свака особа која приступа дигиталним доказима мора бити форензички компетентна;
- свако прикупљане, приступ, чување или трансфер дигиталних доказа мора бити документовано, објашњено и подложно провери;
- појединац у чијем су поседу дигитални докази одговоран је за њихово чување све време поседовања;
- свака агенција или појединац који се бави прибављањем, приступом, чувањем или трансфером дигиталних доказа мора се понашати у складу са овим правилима.

5. Процес рачунарске форензике

Процес рачунарске форензике спроводи се у више фаза. Сагласно томе, постоје четири основна корака на подручју рачунарске форензике: а) прикупљање; б) претраживање; в) анализа и г) презентација.

5.1. Прикупљање

Прикупљање (документовање) чињеница (података) представља почетну фазу РФА. Она почиње када се информација и/или физички објект прикупе или ускладиште у очекивању испитивања. Ова фаза треба да започне што пре по извршењу инкриминисане радње. Чим форензички стручњак дође на место извршења, мора одмах започети с документовањем, тј. фотографисањем затеченог стања, снимањем, записивањем релевантних одредница и сл. Битно је констатовати да ли је средство извршења (рачунар) укључен и, уколико јесте, обавезно га треба оставити у том стању. Искључивање би за последицу имало измену више стотина датотека на које делује оперативни систем при гашењу. Важно је уочити и под којим оперативним системом рачунар ради и којим хард диском је опремљен.

Најчешћи извори прикупљања дигиталних доказа су: а) лични рачунари; б) мобилни телефони; в) дигиталне камере; г) хард дискови; д) оптички медији; ђ) USB меморијски уређаји и друго.

Поред наведеног, докази се могу прикупити и из поставки дигиталних термометара, црних кутија аутомобила (ако их има), veb-страница и слично. Технологија RFID (скраћеница од radio-frequency identification) представља пренос података путем радио таласа са електронске ознаке преко RFID читача до рачунара или другог уређаја који је у стању да прими и обради те податке.

У прикупљању дигиталних доказа поред начела хитности важно је примењивати и начело повећане пажње, пошто је већина дигиталних података веома подложна изменама. Једном промењени, они тешко да могу бити враћени у изворно стање. Због тога се креира форензичка копија диска (енг. *bit-stream image, forensic image*). Она није обична логичка копија зато што не садржи само податке видљиве кориснику и који се тренутно налазе на диску, него и податке који су били избрисани. Након стварања форензичке копије диска, проверава се аутентичност копије уз помоћ криптографског сажетка, у циљу потврде исправности копије, као и интегритета података, односно доказног материјала.

Осим наведеног, у прикупљању података примењују се методе руковања дигиталним доказима које укључују:

- стварање слика (енг. *image*) рачунарског медија употребом алата који спречава измену или брисање са уређаја података који су прикупљени као доказни материјал;
- успостављање и одржавање ланца поседа доказа;
- документовање поступања са доказним материјалом и
- употребу алата и метода које су проверене и чију је тачност могуће изразити у процентима.

У овој фази неке од најдрагоценијих података могуће је добити од корисника рачунара. У разговору с њим могу се сазнати вредни подаци о поставкама система, програмским пакетима, коришћеној енкрипцији и слично. У истрази у којој власник дигиталног уређаја, који је уведен као доказни материјал, није пристао на сарадњу форензички истражитељ мора имати налог за копирање и претраживање података.

5.2. Претраживање

Претраживање дигиталних записа представља другу фазу РФА, која следи након прикупљања доказа. Ова фаза мора се спроводити ефикасно и целисходно. Почетна радња је издвајање релевантних података и елиминисање небитних. Издвајање података може започети анализом криптографског сажетка.[21]

21 Примера ради, нека је диск који се прегледава један од дискова из велике компаније у којој се догодило цурење података. Власници сумњају да је запосленик одао неке важне информације конкурентској фирми. Она форензичком тиму даје све критичне податке за које се сумња да су могли бити прослеђени па их они помоћу алгоритма криптографских сажетака упоређују с подацима на диску. Уколико алгоритам пронађе подударне датотеке, исписаће их на екрану рачунара.

Следећи корак укључује проверу заглавља датотеке (енг. *file signature*). Потпис датотеке се користи за идентификацију формата или проверу садржаја датотеке.[22] Овај метод је врло користан када се проверава да ли је корисник рачунара променио име или екстензију датотеке како би прикрио њен прави садржај. Форензички стручњак ће датотеку провести кроз посебан алат, и, уколико се покаже да тренутна екстензија не одговара њеном стварном формату, прећи ће се на детаљнију анализу датотеке.

Надаље, претрага се може наставити према кључној речи (енг. *keyword analysis*).[23] Датотека се може издвојити и по: типу, величини и датуму настанка.

Након издвајања, односно селекције свих доступних датотека прелази се на прегледавање обрисаних података, датотеке за размену (енг. *swap file*) и неискоришћених сектора на диску.

Следеће место које је потребно прегледати је *recycle bin* (простор на диску, посебна датотека, у коју се спремају датотеке пре коначног брисања с диска).[24]

Релевантни докази се могу открити и у привременим датотекама (енг. *temporary Internet files*). Различите апликације их стварају током свога рада и по завршетку их бришу.[25] То значи да ће форензички стручњак видети када и како се мењао документ и сазнати како је настала одређена датотека.

Следећи извор података може представљати in-box. Прегледом његовог садржаја, може се сазнати с киме је и када особа комуницирала и какве су податке размењивали. Такође, ту је могуће пронаћи и бројне податке о свим активностима на Интернету.[26]

---

22 Свака датотека има свој потпис који се састоји од магичног броја (кратког низа бајтова, обично 2-4 смештених на почетак датотеке) и он говори у којем је програмском алату настала.

23 Ствара се текстуална датотека у коју се уписују кључне речи. Помоћу посебних алата могу се пронаћи сва појављивања речи из текстуалне датотеке и на тај начин издвојити датотеке према садржају.

24 Починилац је можда у страху покушао брзо прикрити доказе и одлучио их избрисати. Међутим, обрисани подаци нису у потпуности уклоњени из система, чак и када су избрисани из *recycle bin-a*. Ако корисник није избрисао датотеке из *recycle bin-a* те је датотеке врло лако вратити, јер ће оне још неко време бити на диску. Уз то, могуће је прочитати и њихове метаподатке (податке о подацима) који садрже име, време настајања, време измене, име аутора и слично.

25 Microsoft Word, на пример, ствара привремену датотеку сваки пут када се снимају измене на документу с којим корисник ради.

26 Понекад се корисници служе *webmail* услугом, па се приликом преузимања порука електронске поште с интернета оне спремају у привремене датотеке (енг. *Temporary*

Подаци везани за активности на Интернету налазе се и у *cookies* (тзв. "колачићи") датотекама. Помоћу њих могуће је пратити које странице корисник посећује. Изузетно важне су и дневничке датотеке које се налазе на серверу. Оне могу садржавати информације о системским средствима, процесима и активностима корисника. Све описане методе односе се на претраживање диска којег је било могуће искључити с мреже, понети у лабораторију и тамо спровести даље кораке истраге.

5.3. Анализа

Анализа представља процес тумачења доказа прикупљених претраживањем. Путем анализе истражитељ супсумира све расположиве чињенице и долази до крајњих резултата истраге. Постоји неколико врста анализа:

- временска анализа – стварање слике о хронолошком настајању података, односно развоју инкриминисаних радњи корак по корак (step by step). Ова анализа се спроводи прегледом временских метаподатака (време настанка, последња измена, последњи приступ и сл.) или дневничке датотеке (када се корисник пријавио на систем или одјавио са њега);
- анализа скривених података – значајна је у реконструкцији скривених података и може указивати на власништво, вештину или намеру. Дохват криптованих, компримираних података и података заштићених лозинкама упућује на скривање података од стране злонамерних корисника. Такође, наилажење на податке или фајлове који имају измењену екстензију индицира на намерно скривање или преиначење података;
- анализа датотека и апликација – извођење закључака о систему и вештини корисника. Постигнути резултати указују на нужност предузимања следећих мера у циљу успешног окончања ове фазе. То могу бити: прегледавање садржаја датотека; идентификовање броја и врста оперативних система; утврђивање повезаности датотека и прегледавање корисничких поставки.

Крајњи корак анализе је њен закључак. У њему се сви до тада прикупљени и анализирани подаци повезују у једну логичку и кохерентну целину, материјализовани у форми извештаја.

Internet files).

5.4. Презентација резултата истраге

Стварање извештаја је најважнија фаза рачунарске форензике. Извештај представља круну целокупног истражног поступка. Он повезује закључке анализе, детаљан опис резултата, све релевантне доказе и документацију која све то поткрепљује. Извештај треба да садржи детаљну документацију алата, процеса и методологије. Сложеност извештаја, његов конкретан облик и садржај зависе од његове намене. Када је истрага закључена, резултати истраге се презентирају правосудним органима. Форензички стручњак мора бити у стању на једноставан и аргументован начин образложити резултате рачунарско форензичке анализе како би исти били веродостојни и као такви прихваћени у судском процесу.

6. Форензички алати

Успешно спровођење РФА незамисливо је без употребе форензичких алата. Избор адекватног алата који ће бити коришћен за дигиталну форензичку истрагу у великој мери утиче на исход судског поступка. Иако је циљ јасан – добијање валидних дигиталних доказа прихватљивих на суду, у пракси се показује да до тога није нимало лако доћи. Постоји више врста форензичких алата и они се генерално деле на алате за анализу програма, односно програмских компоненти и алате за анализу физичких компоненти. Притом, неки од њих су бесплатни док су други комерцијалне природе.

6.1. Алати за анализу програма

Постоје бројни технички алати који стручњацима помажу у прегледавању, претраживању и анализи доказа. Најпознатији и најпримењиванији су следећи програмски алати за управљање подацима на чврстом диску:

- *DriveSpy* – алат базиран на оперативном систему ДОС са интерфејсом сличним истом, који омогућује стварање форензичке копије диска, обнављање обрисаних података и неискоришћених делова сектора и анализу употребом криптографског сажетка;
- *SnapBack Exact* – алат фирме SnapBack који служи за форензичко копирање диска; *-MediaMerge* – алат фирме Computer Conversions намењен обнављању података с оптичких медија и тврдих дискова.[27]

27 Постоје и многи други алати: Forensic Replicator, PDBlock, FTK Imager, GetFree, Ontrack, AcoDisk, DiskSig и др.

Поред наведеног, постоји и неколико прегледника бинарних датотека, као и вишенаменских програмских пакета.[28]

6.2. Алати за анализу диска

На хард диску се обично налази оперативни систем који садржи различите програмске пакете. Већина форензичких алата може се покренути с једног таквог система. Међутим, ако је потребно засебно анализирати делове рачунара, као што су хард дискови, оптички медији, USB меморијске картице, мобилни уређаји и слично, потребна је посебна опрема.[29] Докази прикупљени форензичким методама могу се користити у разним врстама истрага и у различите сврхе.

7. Закључни осврт на проблеме у доказивању дигиталних повреда интелектуалне својине

Интелектуална својина је и у тзв. аналогном окружењу изложена озбиљним насртајима и искушењима. Са тог разлога, питање њене заштите одувек је било актуелно и суштинско. Што би рекао Džek Valenti "Ако не можете да заштитите оно што поседујете, онда ништа не поседујете." (Ganc, Dž. Roče-ster, B. Dž, 2007: 13). Дакле, интелектуална својина је предмет различитих повреда и у аналогном окружењу и тешко ју је заштитити.

У информатичком друштву, односно у дигиталном окружењу проблеми у вези са интелектуалном својином су још израженији и далеко озбиљнији. Нове технологије, с једне стране, омогућавају много лакше, брже и јефтиније искоришћавање, а тиме и повређивање интелектуалне својине, а са друге стране, отежавају утврђивање и доказивање таквих повреда. Из изнетих разлога, питање доказивања дигиталних повреда постаје све актуелније и појављује се као озбиљан проблем који треба у што већој мери решити.

Фантастичан и перманентан развитак науке и технике извршио је значајан утицај и на облике и методе сузбијања криминалитета, док је експанзија развоја информационих технологија и телекомуникација омогућила коришћење доказа у електронској форми.

У сагледавању и решавању наведеног проблема најдаље се отишло у англосаксонском правном систему, посебно у САД-у. Тамо је доста

28 Прегледници бинарних датотека: *010 Hex editor, Hex Workshop.* Такође и вишенаменски програмски пакети: EnCase, Maresware, *Access Data*.

29 Постоји неколико произвођача таквих форензичких уређаја за анализу доказног материјала (делова рачунара за смештај података) и најважнији међу њима су Digital Intelligence и Vogon International.

учињено на доношењу бројних правних правила и установљавању бројних техничких стандарда у прибављању, чувању и примени дигаталних доказа.

Ипак, упркос свим напорима и настојањима, проблем доказивања дигиталних повреда још увек није адекватно и свеобухватно решен. На путу ка решењу наведеног проблема појављују се многе препреке. Све се оне, генерално, могу свести на две најважније категорије: правне и техничке. Пре свега, легислатива (национална и међународна) у овој области није задовољавајућа, односно перманентно заостаје за развојем информатичке технологије. Такође, постоје и разлике у законодавствима, чак и у појединим државама САД. Кад се томе дода чињеница да повреде интелектуалне својине скоро увек садрже елемент иностраности, односно тангирају различите суверенитете, онда проблем постаје још сложенији.

Иако је Међународна организација за компјутерске доказе (IOCE) прописала опште принципе и процедуре за усаглашавање метода и практичних решења у вези дигиталних доказа, још увек нигде у свету не постоји верификација званичних истражних органа, форензичких аналитичара и правосудних органа, подједнако квалификованих у својим областима да објективно и тачно воде истрагу, форензичку аквизицију, анализу, доказни поступак и презентацију дигиталних доказа пред надлежним органом.

Осим правних присутни су и технички проблеми. Упркос постојању различитих форензичких метода и техничких алата, некада је веома тешко доћи до дигиталних доказа о повреди права интелектуалне својине, због саме природе мрежног окружења. Најзад, не постоји стандардизована и унификована технологија у овој области која би омогућавала јединствено поступање и квалификовање дигиталних повреда интелектуалне својине.

На основу свега реченог, можемо изнети закључак да интелектуални ствараоци имају разлога да буду забринути за будућност својих права, али и реалну наду да ће друштво наћи начине и механизме да из ове ситуације изађе као победник и повреде права интелектуалне својине сведе на разумну и прихватљиву меру.

Литература

Athanasopoulos, E. et. Al. (2008). Antisocial Networks: Turning a Social Network into a Botnet, 11th international conference on Information Security, Springer-Verlag Berlin, Heidelberg, pp. 146–160.

Britz, M.T. (2004). Computer forensis and cyber crime: An introduction, Pearson Education, New Jersey

Casey, E. (2004). Handbook of computer crime investigation: forensic tools and technology, Elsevier Academic Press, London, San Diego

Ђокић, З. Живановић, С. (2004). „Проблеми прибављања, обезбеђивања и коришћења доказа у електронској форми, од значаја за кривични поступак“, Тешки облици криминала (зборник), ИКСИ; ВШУП, Будва, стр. 305–318

Ganc, Dž. Ročester, B. Dž. (2007). Pirati digitalnog doba, Clio, Beograd, стр 13

Grubor, G. (2004). "Funkcionalni model istrage kompjuterskog događaja", savetovanje Ziteh`04, приступ 20. 01. 2015. са: http://www.singipedia.com/content/971-Funkcionalni-model-istrage-kompjuterskog-kriminala

Јерковић, Р. (2009). „Високотехнолошки криминал – актери и жртве“, Ревија за безбедност, бр. 3/2009, стр. 27–34

Комлен Николић, Л. и др. (2010). Сузбијање високотехнолошког криминала, Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд

Крстић, Ј. (2004). "Стандарди у поступању тужилаца у борби против компјутерског криминала", : ЗИТЕХ (зборник), Удружење ИТ вештак,Тара.

Lee's, H. Palmbach, T. and Miller, M. (2001). Henry Lee's Crime Scene Handbook, San Diego: Academic Press

Лукић, Т. (2012). Дигитални докази, Зборник радова Правног факултета у Новом Саду, бр. 2/12, стр. 177–192

Petrović, L. (2004). "Digitalni dokazi", savetovanje Ziteh`04, приступ 15. 01. 2015. са: http://www.singipedia.com/content/986-Digitalni-dokazi

Радуловић, С. (2008). „Претње високотехнолошког криминала и домаћа законска регулатива“, Ревија за безбедност, бр. 8/2008, стр. 18–24

Спасић, В. (2010). Онлајн безбедност, Зборник радова Правног факултета у Нишу, бр. 56, 2010, стр. 77–102

Спасић, В. (2011). Дигитални докази, Зборник радова Правног факултета у Косовској Митровици, са међународне научне конференције, св. 1, стр. 283–298

Stephenson, P. (2000). Investigating Computer-Realted Crime, CRC Press, Boca Raton (etc.)

Timofeeva, Y. (2002). Hate speech online: restricted or protected? Comparison of regulations in the United States and Germany, J.Transnational law & policy. p.256

Тривић, С. (2011). Виртуелни злочин и његово санкционисање, Страни правни живот, бр 3/2011, стр. 300-311

Vetsbi, DŽ. R. i dr. (2004). Međunarodni vodič za borbu protiv kompjuterskog kriminala, Produktivnost AD, Beograd

Vukoman, M. (2010). "Digitalni dokazi i mesto zločina", Univerzitet u Beogradu, Fakultet organizacionih nauka, Beograd, приступ 20. 02. 2015. са: http://www.scribd.com/doc/40239735/Digitalni-Dokazi-i-Mesto-Zlocina

Vidoje Spasić, LL.D.
Associate Professor,
Faculty of Law, University of Niš

Branko Stevanović,
B.Sci (Electronics)
System Administrator,
Faculty of Law, University of Niš

PROVING THE INFRINGEMENT OF DIGITAL INTELLECTUAL PROPERTY RIGHTS: OVERVIEW OF THE ANGLO-SAXON LEGAL SYSTEM

Summary

The multifaceted process of identifying and proving the infringement of intellectual property rights is further complicated and aggravated in the so-called analogue environment. The development of Information Technologies has given rise to a new set of problems. The digital technology has facilitated the infringement of intellectual property rights and additionally aggravated the process of proving these infringements. Hence, it is the duty of digital forensics to identify relevant (valid) evidence and present it in the court of law, which is not an easy task. In that course, the problems are twofold: legal and technical. First of all, the legislation in many countries is not adjusted to resolving the issues constantly emerging in the digital environment and there are apparent differences in the manner of regulating these issues. On the other hand, there is no standardized and unified technology which would provide for a uniform qualification and comprehensive treatment of these issues. Moreover, the place of commission of these criminal offences as a rule does not coincide with the place of occurring legal consequences. Yet, in spite of all these difficulties, there are technological methods and tools which facilitate the detection of cybercrime and provide evidence for securing relevant punishment. In the time to come, the developments in this area are expected to be aimed at strengthening the protection of legitimate interests of holders of intellectual property rights.

Key words: *digital evidence, digital forensics, digital technology, intellectual property.*