КОМПЈУТЕРСКИ КРИМИНАЛ И ДИГИТАЛНА ФОРЕНЗИКА

БУДУЋНОСТ ПРЕД ВРАТИМА

У судским процесима и процесима истраге захтеви за дигиталном форензиком јављају се код грађанских парница, парница везаних за породично или материјално право, злоупотреба података о личности, крађе идентитета, проневере, злоупотребе службе, преваре у осигурањима, крађе новца на банкоматима или са рачуна грађана и правних лица, педофилије, узнемиравања и других појавних облика криминала и злоупотреба, од којих се велики део односи на друштвене мреже

ОДБРАНА

Специјални прилог 159

Пише: Милорад МАРКАГИЋ

У времену масовних аналогних комуникација, а нарочито садашњих дигитализованих, као основни облик интересовања јавља се информација. Најчешћи облици испољавања информација остају глас и писмо. Но, пренос информација превазилази конвенционалне начине и скоро у потпуности се прилагођава савременом виду обраде и преноса. Највећу заслугу за то имају рачунари.

Дигитална форензика је научна област криминалистике која се примарно бави прикупљањем, анализом и презентацијом дигиталних података, који се налазе на електронским уређајима који привремено или трајно чувају информације унете у њих.

Такође, бави се рачунарима, мобилним и фиксним телефонима, ПДА уређајима, меморијским картицама и осталим статичким или преносним медијима на којима су забележени подаци потребни за безбедносну анализу или криминалистичку истрагу.

Саставни део дигиталне форензике је и компјутерска форензика, а предмет њене обраде је рачунар у општем смислу, односно дискови (хард-дискови, ЦД/ДВД), садржај оперативне меморије, мрежни саобраћај, коришћени протоколи, права и задужења оператера на рачунару, те све радње које су урађене помоћу рачунара (штампање, нарезивање дискова, комуникација: и-мејлови, друштвене мреже, блогови...).

У почетку компјутерска форензика била је област којом су се бавиле само безбедносне службе (полиција, тужилаштво, обавештајне и контраобавештајне службе, војска...), али у последње време јављају се и нови заинтересовани субјекти за ту врсту истраге: корпорације које сумњају или желе да буду сигурне да њихови запослени крше интерна правила која се односе на безбедност података, државне и приватне установе, па чак и појединци који желе заштити своје податке и трансакције. Форензика је скуп мера, метода и поступака којима се испитује откривање, прикупљање и чување података на рачунарима, рачунарским системима и мрежама и преносивим медијима.

Најчешћи захтеви индивидуалних корисника су да се након физичких оштећења, неправилног и нестручног руковања или након пада система на рачунарима због утицаја малициозних програма, врате макар неки подаци. У судским процесима и процесима истраге захтеви за дигиталном форензиком јављају се код грађанских парница, парница везаних за породично или материјално право, злоупотреба података о личности, крађе идентитета, проневере, злоупотребе службе, преваре у осигурањима, крађе новца на банкоматима или са рачуна грађана и правних лица, педофилије, узнемиравања и још низ других појавних облика криминала и злоупотреба, од којих се велики део односи на друштвене мреже.

Једним именом, све што се прикупи у процесу форензичке истраге назива се дигитални доказ.

Сви дигитални уређаји у себи имају велики број информација, произвођачких и корисничких, било да се ради о оперативном систему, програму меморије, подацима о врсти и карактеристикама уређаја или медија, инсталираним апликацијама, раду са уређајима, подацима који су обрађивани и мењани, брисани или криптовани.Дигитални докази применљиви су и код приватних лица, али и у судским процесима, а интересантни су и обавештајно-безбедносним службама.

У свету, па и код нас, дигитални доказ признат је као равноправан са свим осталим форензичким доказима, те свака земља, поред стручних служби у одређеним државним институцијама, има и посебно регистроване и овлашћене вештаке за дигиталну форензику.

Порастом корисника дигиталних медија и наглим развојем интернета повећава се и број захтева за обављањем радњи дигиталне форензике, а самим тим и потреба за оспособљавањем корисника за правилну употребу медија, школовањем кадрова за ту област, те производњу хардвера и софтверских алата за процес форензичке истраге.У Србији кадар се обучава на неколико универзитета, а и у свету се тој материји придаје

све већи значај. Ипак велики проблем и даље представља недовољно познавање те области, која није у потребној мери заступљена у свакодневном животу и није препозната као велика помоћ институцијама и појединцима.

Томе доприноси и сазнање да се дигитална форензика знатно разликује од традиционалних форензичких метода, није видљива на око и докази се налазе у нематеријалном облику, па се сакупљају и на физичким локацијама, али и кроз мреже и спојне путеве.

Масовна употреба рачунара, рачунарске технологије и микропроцесора и све бржи развој тих технологија доприноси да се велики део послова лакше, брже, елегантније и јефтиније обави. Развој у области телекомуникација и информатике човеку несумњиво олакшава обављање свакодневних активности, омогућава лакшу, ефикаснију и бржу комуникацију, али паралелно са тим доприноси и развоју могућности за велики број злоупотреба и бујање криминалних радњи специфичне високо софистициране технолошке врсте. Све је чешће извршење кривичних дела, пре свега у виртуелном свету, али и у институцијама где је масовно заступљена употреба ових технологија у процесима за обраду и чување података.

Компјутерски криминал велика је претња по појединца, компаније и институције, али и за друштво у целини, па се посебна пажња треба посветити пре свега познавању могућности информационо-комуникационих технологија, њиховој правилној употреби и познавању компјутерског криминала.

Елементи дигиталне форензике су:

- проналажење (добијање) места истраживања,
- прикупљање дигиталних података,
- аквизиција,
- анализа,
- складиштење и
- презентација доказа

Случајни и намерни упади у рачунаре

Од процеса набавке и почетка коришћења рачунара, обуке у познавању уређаја, средстава и система, па све до познавања метода заштите, генерално се прескачу многи кориснички процеси, па системи постају и остају рањиви на велики број (непознатих) уплива и напада, како намерних, које изводе обавештајно-безбедносне службе и друге државне институције и злонамерни нападачи, тако и ненамерних, до којих долази случајно или грешком корисника, па подаци постану доступни трећем лицу без намере.

Тој претњи углавном се веома мало поклања пажња, иако је она заступљена у свим сферама живота појединца, али и државе у етичком, војно-политичком, економском и психосоцијалном аспекту. Када ипак дође до злоупотребе технологија, појаве кривичног дела и његове касније истраге, на сцену ступају истражитељи из области дигиталне форензике, који помажу органима власти и судским органима у доказивању учињеног дела.

Иако релативно млада, дигитална форензика се из научне подобласти веома брзо развила у мултидисциплинарну научну област, која у стопу прати прогресивни развој технологија и њихове злоупотребе.

Без обзира на то што се у литератури, као и на интернет страницама, резултати рада у тој области веома мало публикују, делом због очувања тајности, делом због непознавања и незаинтересованости шире популације, чему доприноси и податак да је велики број форензичких алата изузетно скуп и слабо доступан широј популацији, сазнања су довољна за ефикасну

борбу против технолошког криминала. Охрабрује чињеница да је за масовну, пре свега личну, али и формалну употребу, све доступнији велики број бесплатних, некомерцијалних програма који, уз познавање принципа и метода дигиталне форензике, могу у великој мери да олакшају кориснички део, како у смислу откривања нежељених и/или криминалних радњи, тако и у познавању метода и принципа заштите уређаја, система и мрежа у целини.

Дигитална форензика се мења и прати развој дигиталне технологије, хардверских и софтверских иновација и решења.

СВЕ РАЊИВИЈИ ХАРДВЕР

Од почетка увођења микропроцесора у машине, уређаје и системе, са најширом применом на пољу рачунарских технологија, хардверска структура претрпела је низ измена и иновација, па се данас с правом може рећи да већина апарата за кућну употребу, скоро сва средства из области телекомуникација и сва средства из области рачунарске технологије, постају савременија, компатибилна једна са другим, јефтинија и да достижу неслућене могућности у примени апликативних софтверских решења.

Ако се вратимо у блиску прошлост, када рачунари полако преузимају примат од других масовних средстава за обраду и чување података, а касније и за пренос података и информација, видећемо да се од гломазних, спорих и компликованих за употребу, дошло до габаритно веома малих, брзих и за употребу једноставних уређаја.

Осим рачунара, данас се масовно употребљава и велики број других хардвера, као што су преносиви медији, дигитални фото-апарати, мобилни телефони и слично. Они су масовно присутни у свакодневној корисничкој, али и комерцијалној употреби. Највидљивији је напредак на пољу екстерних меморија, које су од флопи-дискете, преко ЦД и ДВД дискова, достигли ниво УСБ меморија, смарт-картица и екстерних хард-дискова са веома великом могућношћу чувања информација и података.

У свету постоји више стотина типова и врста различитих екстерних меморија, које су прилагодљиве за рад на скоро свим рачунарима и употребљеним оперативним системима, како рачунара, тако и сопствених инсталираних у самом уређају.

Хард-диск

Диск рачунара намењен је за инсталацију оперативног система, али и свих других програма за рад са подацима, инсталацију пакета и чување садржаја. Најчешће се код корисника дели на више делова (партиција), од којих је један програмски, док се на другим складиште подаци. Основна ствар коју код истраге у дигиталној форензици истражитељи испитују јесте партиција на којој је оперативни систем и на којој су инсталирани програми и апликације, јер се преко ње врше обрада, трансфер и измена по-

датака. Нешто је лакши посао када се проверавају партиције које служе само за чување података, мада учиниоци кривичних дела имају начина да и њих прикрију и заштите.

Много је начина на које злонамерни корисници скривају рад на рачунарима, а који се тичу података на хард-диску, почевши од двоструког диска, где је један видљив, а други није, његовог форматирања, брисања слободног простора, закључавања, маскирања, криптовања, измене бројева партиције итд.

Тежиште дигиталне форензике је управо на оним радњама којим се, применом инсталираних алата самог оперативног система, али и коришћењем наменских алата, долази до тражених садржаја.

Меморија рачунара

Као витални орган рачунара јавља се и меморија, која има више функција. У случају истраге кривичног дела или злоупотребе, из ње се може одређеним методама и поступцима прикупити знатан број рањивих и скривених података, нарочито у фази директног рада на рачунару или истраживањем док још није искључен.

Флеш-меморије су уређаји који чувају податке, али и омогућавају њихову директну измену прикључењем на рачунар, као и пренос са једне локације на другу. Засновани су на технологији смарт-картица, али су репрограмирани у блоковима са вишеструким локацијама. Користе се и за инсталацију апликација или за непосредан утицај на оперативне системе, за такозвано живо дизање система, а да се при том на рачунару ништа не мења нити се чак примети нечији боравак.

Иако су лично власништво појединца или институције, због малих димензија и често несавесне употребе, лако се могу изгубити, заборавити на нежељеној локацији или бити предмет крађе и тако постати доступни злонамерним корисницима. На пољу дигиталних доказа то представља могућност крађе података, идентитета или објављивања тајних података. Када се УСБ меморије користе за скидање података са рачунара, помоћу форензичких алата треба открити време спајања на рачунар, број УСБ меморије и подаци који су копирани, мењани или брисани.

Фото-апарати и камере

Савремени фото-апарати и камере, поред личне и комерцијалне употребе, представљају и погодне медије за извршење кривичних дела. Садашњи ниво развоја омогућује све већи и бољи квалитет слика или видео-записа, али и тражи све већи простор за чување података. За то се користе меморије самих уређаја, али неретко и придодате меморијске картице. Тиме је, нарочито када се ради о извршењу кривичних дела, знатно отежан рад истражитељима, јер се меморијским картицама лако манипулише, брзо се могу извадити и уништити. Такође, велики проблем представља и начин смештања података у самом уређају јер сваки произвођач има своју методологију израде.

Мобилни телефони

Савремени мобилни телефони полако, али сигурно, преузимају примат од класичних рачунара, јер осим првобитне намене, данас представљају мини преносиве рачунаре на којима је могуће реализовати све радње и операције као и на десктоп или лаптоп рачунарима. Осим именика и осталих телефонски апликација, у њима су инсталирани оперативни систем и низ апликација, мултимедијалних са-

држаја, а скоро сви су повезани на јавну мрежу. Преко њих се такође може презентовати садржај или вршити администрација мрежа бежичним путем.

Рањивост софтвера

Када се говори о софтверу, већина корисника веже се само за оперативни систем и евентуално програмске офис пакете, заборављајући да свака инсталирана апликација, додатак или чак и игрица, има свој софтвер односно програм. Део њих не изискује велику повезаност са хард-диском, а део је и те како завистан од оперативног система.

Гледајући данашње рачунаре, али и остале електронске уређаје који користе дигитални начин рада са подацима, тешко је на први поглед направити разлику који су програми лиценцирани и на неки начин валидни, а који су дело пиратства, приручне израде или нелегални. Ови други, осим могућности коришћења у сврху недозвољених радњи, често због непотпуне претходне провере пре пуштања у оптицај знатно утичу на рад уређаја, обарају систем или су носиоци злонамерних програма.

У трци за лаком и брзом зарадом, са једне стране, и трци за осавремењивањем софтвера или набавком и инсталацијом нових апликација и програма, са друге, поред ангажованих учесника неретко се нађе и трећа страна. То су појединци или институције које користећи рупе у начину набавке, инсталирању, крековању и употреби софтвера, спроводе криминалне радње. Те радње огледају се у великом броју праћења и прислушкивања комуникација, скидања електронске поште, крађи личних података, крађи бројева рачуна, финансијским малверзацијама, дечјој порнографији, крађи података са рачунара или њиховом уништавању, утицајем на енкрипцију података, па изискивањем новчаних средстава за њихов повраћај, уништење оперативних система, обарање сајтова или чак и целих мрежа.

Данас је у употреби више оперативних система, али највећи и најчешће коришћени на класичним рачунарима, али и на преносним дигиталним уређајима, јесу две групе – MS Windows и Unix оперативни системи.

MC Windows група оперативних система настала је као графичка надоградња старог оперативног система (MS-DOS) прве генерације рачунара. Данашње верзије базирају се на напреднијој варијанти која није више само графичко окружење већ потпуни оперативни систем. Windows ради на рачунарима заснованим на процесорима фирме „Интел" и њима сличним. Ознака за такве процесоре је ×86 компатибилни, а најпознатији су: АМД, DEC Alpha, MIPS и PowerPC. Такође, постоје варијанте процесора са 32 и 64 бита.

Данас је Windows најпопуларнији ОС, заступљен код више од 80 одсто корисника. Знатно је распрострањен и у сегменту малих и средњих сервера, у применама као што су мрежни сервери или сервери база података.

Породица Unix система је група оперативних система која укључује и System V, BSD, и GNU/Linux. Unix системи покрећу рачунаре разних унутрашњих архитектура. Најраспрострањенија примена је међу серверима у корпоративном сектору, али и међу радним станицама у инжењерском и академском сектору.

Бесплатне и лако доступне варијанте Unix-а, као што су Linux и BSD, у последње време улазе у ширу примену и све су популарнији. Направљен је пробој и на тржишту стоних рачунара, нарочито код Linux дистрибуција, као што је Убунту GNU/Linux.

Одређене варијанте Unix-а, као што су HP-UX и IBM AIX, направљене су тако да раде само на рачунарима и са опремом оригиналног произвођача. Други, попут Соларис, могу радити на оригиналним рачунарима али и на другим који одговарају захтевима произвођача. Еплов Mac OS X је BSD варијанта настала из NeXTSTEP и FreeBSD је замена за ранији Mac OS у уском сегменту тржишта, али с временом постаје најпопуларнији власнички Unix систем.

У последње време слободни Unix системи умногоме су потиснули првобитне. На пример, научничко моделовање и рачунарска анимација некад су били својина Силикон Графикса и његовог ИРИКС оперативног система. Данас су они под влашћу рачунарских система GNU/Linux.

Важно је напоменути и то да апликације које немају могућност привременог чувања података препуштају оперативном систему да их меморише, користећи свап датотеке или виртуалну меморију. Када апликацији затреба привремено сачувани податак, оперативни систем га шаље аплика-

цији и брише са хард-диска, али ту лежи опасност јер иако су избрисане свап датотеке, до података је могуће доћи јер још постоје на хард-диску.

РАЊИВОСТ РАЧУНАРСКИХ МРЕЖА И КОМУНИКАЦИЈА

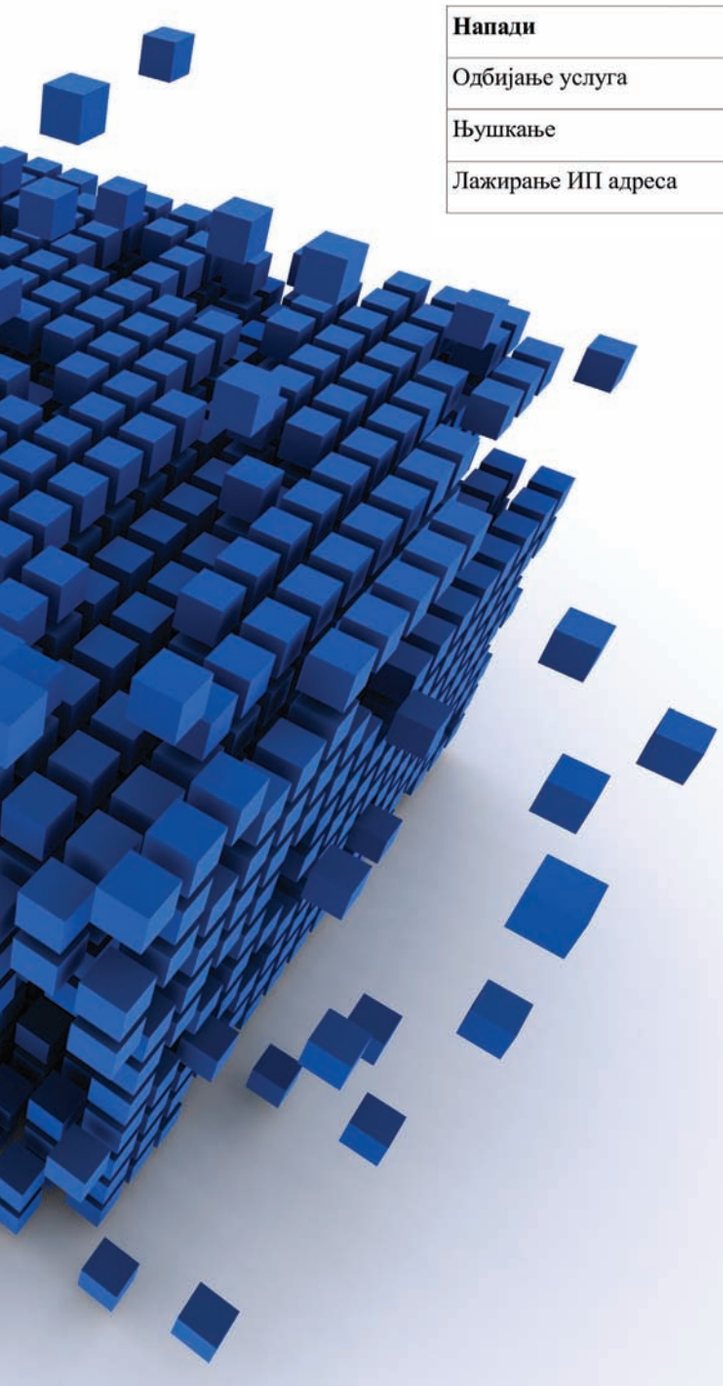
На рачунарске мреже свакодневно се изведе више милиона напада, како на саму мрежу или на одређени сајт, тако и на појединца. Део напада изврши се са тачно утврђеним циљем и усмерен је на конкретну државу, институцију или корисника, али је највећи део напада базиран на случајном одабиру жртве. Прекраћујући досаду нападачи се једноставно, методом случајног избора, накаче на неку мрежу, порт или кроз неки од сајтова улете код жртве. Било да је реч о прелиставању страна, четовању, дискусијама на форумима, посећивању друштвених мрежа, размени електронске поште или раду на рачунару, све док је жртва конектована на јавну мрежу, може се приступити њеном рачунару.

Позната је подела на две врсте напада или претњи на рачунарске мреже – пасивни и активни напади.

Пасивни напади су они који индиректно могу утицати или уопште не утичу на понашање оперативног система или функционисање мреже. То су најчешће праћење, прислушкивање, откривање садржаја и анализа карактеристика рада и рачунара и корисника.

Насупрот њима, активни напади битно утичу на функционисање система и мрежа и на садржај, изглед и пренос података. У ове нападе спадају маскирање, репродуковање, лажно представљање, понављање саобраћаја, измена садржаја и блокирање саобраћаја.

Напади	Програмске претње	Системске претње
Одбијање услуга	Клопке	Вируси
Њушкање	Тројански коњи	Црви
Лажирање ИП адреса	Преливање бафера	.....



Рањивост се може дефинисати као слабост или пропуст неке вредности, неке целине или радње која може бити злоупотребљена. Слабости су узроковане са више фактора као што су неадекватна пројекција мрежа, лоша имплементација, слаба заштита, нестручно руковање и недозвољени приступ.

Електронска пошта

Као посебно значајан сегмент у мрежама, поготово друштвеним, јавља се електронска пошта, најраспрострањенији вид персоналне и комерцијалне комуникације. У случају рачунарског инцидента она представља значајан извор дигиталних доказа.

Свака порука у електронској пошти има заглавље и тело. У заглављу су видљиве адресе примаоца и пошиљаоца, а у телу текст, односно садржај поруке. Елементи који се из електронске поште истражују и користе јесу: анализа електронске поште, екстензија докумената, интернет сервери, привремени документи и инстант поруке.

Рачунар прикупља информације о кориснику рачунара и складишти их у датотекама скривеним на хард-диску.

Фајлови као што су кеш, историја претраживача и други привремени интернет фајлови могу се користити како би се реконструисале online навике корисника. Те датотеке складиште информације као што су корисничка имена и лозинке, имена, адресе, бројеви кредитних картица..... Хакер може преузети те информације тако што их покупи док се шаљу преко неке незаштићене мреже, или може да инсталира злонамерни софтвер на туђем рачунару (нпр. spyware), који ће прикупљати све што му је потребно и аутоматски му то слати назад.

Интернет преваре у различитим појавним облицима, осим путем разних сајтова, погодно тле налазе управо у електронској размени порука.

Преваре на интернету могу се обавити на много начина, од којих су најчешћи: електронска пошта или ћаскање (phishing), злонамерни програми (*тројански коњ*, spyware…)

Phishing је слање електронске поруке кориснику у којој се налазе лажни подаци о компанији у покушају да преваре примаоца поруке, да им преда своје личне, приватне информације које ће касније бити коришћене за крађу идентитета. Електронска пошта усмерава корисника да посети неки сајт на коме се тражи да унесе личне податке, лозинке, бројеве картица, бројеве рачуна, а које легитимна организација већ има. То су све лажни веб-сајтови и подешени су искључиво за крађу информација од корисника.

Коришћењем злонамерних софтвера помоћу електронске поште као што су тројански коњи, који служе да са рачунара жртве покупе лозинке, корисничка имена и бројеве кредитних картица које користе на рачунару и пошаљу их назад до хакера, може се доћи до мноштва података корисника.

ФОРЕНЗИКА И ФОРЕНЗИЧКИ АЛАТИ

Имајући у виду да је начин обраде и чувања података у електронском (дигиталном) облику постао доминантан, као и поменуту рањивост хардвера и софтвера и веома велики број напада на уређаје, системе и мреже, долазимо до закључка да се осим њихове заштите, веома често јавља потреба и за неколико радњи и поступака, као што су повраћај података или доказивање кривичног дела учињеног овим путем. Осим извођења дигиталних доказа, неретко се у пракси дешава да и физичке радње на медијима и уређајима умногоме могу допринети сазнањима о извршеном делу.

У процесу истраге сваки вид физичког оштећења или мењања оригиналних података може довести до обарања доказа на суду, те се поставља приоритетни задатак да се оригинал никако не сме мењати, а копија мора бити верна

истом, те се мора урадити још једна копија за архиву и презентацију, уколико у току истраге дође до непредвиђених околности на медију.

Да би резултати форензичке истраге били валидни и признати пред заинтересованом страном која је наручила истрагу, као и што је најчешћи случај пред надлежним судовима, форензика мора да испуни одређене услове и стандарде који су прописани најпре судском праксом, а касније те услове прихватају и остали наручиоци истраге.

Примарни захтев је да форензичка истрага буде технички необорива. Када се испитује хард-диск, тражећи фајлове, документе као целине или само одређене садржаје, електронске поште или само приступања мрежи преко датог компјутера, обавезно је да се његов целокупни садржај прекопира на посебан уређај, који не дозвољава даље уписивање, па се на њему даље врши претрага.

Копија диска мора да буде таква да се ископира целокупни садржај са све непопуњеним простором на коме могу да се налазе фајлови који су обрисани, а који могу бити интересантни у поступку истраге. На тај начин копира се, преписује, бит по бит, са целокупном структуром фајл система, задржавајући простор у коме се налазе фрагменти прегажених фајлова. Тиме се обезбеђује валидности истраживаног материјала, односно то је доказ да ништа од садржаја није мењано на диску који се истражује. Тако у току доказног поступка нико не може да тврди да су докази који су пронађени подметнути, мењани на штету било које стране у поступку истраге, оштећени или изгубљени.

Други захтев који форензичка истрага мора да испуни јесте да добијене резултате, помоћу истих алата и процедура, могу проверити други стручњаци, ако то тражи једна од страна. Тај услов испуњава се применом прихваћених протокола, методологије и процедура.

Процедуре и методологија истраживања нису исте у свету, па чак различити правни системи у свету на различите начине прописују начин на који се долази до форензичких доказа који могу бити прихватљиви на суду. У светској судској пракси не постоје општеприхваћена процедура и правила понашања, те се све више јављају заговорници стандардизације ове области.

Да би поступак истраге био применљив у даљем судском процесу мора бити документован. Документовањем процеса истраге и прибављања доказа истражитељ обезбеђује кредибилност целокупног поступка и своје улоге у њему, и исто тако омогућава проверу независног тела, било струковног или судског. Документовање истраге врло је важно и за унапређење струке. И многи озбиљни експерти спремни су да случајеве на којима су радили поделе са колегама, на семинарима, у оквиру предавања, као чланке у стручним часописима или форумима који окупљају професионалце али и аматере.

Најчешћи проблеми са којима се компјутерски форензичари у свом раду суочавају јесу:

– немогућност да објекат који обрађују физички пренесу у лабораторију или другу погодну просторију за истрагу;
– немогућност изузимања сервера, јер морају да остану на својој локацији због даљег функционисања мреже – тада се подаци морају прикупити на лицу места, коришћењем лаптопова и друге хардверске опреме, али и фактор ограниченог времена је још једна отежавајућа околност која може да утиче на резултате истраге; како је систем активан у тренутку прикупљања података, у сваком тренутку може доћи и до промене садржаја хард-диска, па истражитељ има задатак да учини све да те промене битно не наруше структуру и садржај диска;
– физички оштећени медији који се анализирају траже додатно време, специјалну опрему и велико искуство и знање читавих тимова истражитеља, изузетно пажљиво и документовано спровођење истраге.

Знатан проблем у истрази могу представљати меморијске картице, јер се веома лако и брзо могу преносити и постављати у различите врсте и типове уређаја (мобилни телефони, таблет рачунари, фото-апарати). Ипак важно је знати да се код сваког уређаја и медија врши увезивање и да трагови коришћења свакако остају на њима.

У зависности од типа хардверске компоненте, подаци се могу повратити и након неколико брисања и преправки, а време њиховог чувања мери се десетинама година. Ипак, за процес форензичке истраге у пракси се користе подаци старости до једне године.

Постоји више дефинисаних метода и поступака за дигиталну форензику који би помогли у случајевима губитака података са рачунара или екстерних меморија, али и за прикупљање доказа с циљем спровођења истраге.

Треба имати у виду да је део података који се обрађују и складиште на стандардним дисковима рачунара и осталих уређаја релативно стабилан и доступан, али да су подаци у локалним меморијама и меморијским екстерним уређајима веома рањиви, како због њихове структуре, тако и због временског ограничења ресурса, начина употребе, условима чувања, транспорта и слично.

Стога, осим познавања структуре, начина функционисања и рада уређаја, компоненти и софтверских решења, треба добро знати који су поступци у повраћају или истрази података и који се алати том приликом користе. Свака импровизација или непотпуно спровођење метода, мера и поступака доводи до трајног губљења података и неретко до онемогућавања даљег коришћења хардверских компоненти.

Приоритетне радње у повраћају података јесу свакако да се што већи број њих врати у претходно стање, употребљиво за даљу експлоатацију или дораду, а код извођења доказа важна је и њихова аквизиција.

Дигитална, често називана компјутерска, односно рачунарска форензика јесте, у ствари, поступак којим се подаци враћају или откривају на тај начин да се сачува њихова оригиналност, онемогући уништење, сачувају трагови на рачунарском систему о радњама и догађајима који су спровођени, као и њихова реконструкција када не постоји јасан и на први поглед видљив траг.

Познавање хардверских и софтверских решења, њихових могућности и употребљености на истраживаном уређају помаже нам да урадимо процену расподеле и распореда информација, начина на који је дошло до губитка, оштећења или уништења података, начина поновног долажења до њих и очувања интегритета, ради даљег поступка анализе и извођења доказа.

Не постоји чаробни штапић нити јединствен и универзални метод спровођења дигиталне форензике. Сваки уређај, сваки документ, сваки податак и свака радња су јединствени, те се сходно датој ситуацији примењују различити алати, методе и поступци.

Шта је потребно знати пре предузимања радњи дигиталне форензике?

Да би се успешно спровео процес реконструкције догађаја и повраћаја података у било којој ситуацији неопходно је да се испуне неки предуслови и имају чврста сазнања о месту где се догађај десио, свим хардверским и софтверским компонентама уређаја или медија, повезаности уређаја или медија са осталим елементима рачунарских система или мрежа, физичкој и софтверској заштићености уређаја, медија, компоненти или појединих фолдера и фајлова, као и о томе да ли је вршена енкрипција података, да ли је нешто мењано или допуњавано на оперативном систему, да ли су изворни директоријуми модификовани, да ли постоји резервна копија података, да ли је био покушај намерног, или је дошло до ненамерног мењања и брисања података. Такође је потребно знати који форензички алат треба употребити, уверити се у оправданост и економичност рада и задовољити етичку и законску претпоставку оправданости обављања радњи и поступака дигиталне форензике.

Ако се има у виду податак да се више од 90 процената података обрађује, складишти и дистрибуира у електронском облику, веома је битно да се нађе могућност провере да ли су подаци још на неки начин доступни, ако јесу где се и код кога налазе, ко рукује њима и да ли је дошло до умножавања и даље дистрибуције.

Неопходно је и да се сви делови хардвера и софтверска решења рада са подацима посматрају и кроз кориснички и кроз форензички аспект.

Имајући у виду статистичке податке да се за обраду, чување и дистрибуцију података у највећој мери користе хард-дисови, УСБ меморије, меморијске картице и екстерни хард-дискови, највећи број истрага спроводи се управо на овим медијима.

Стандардни хард-дискови су незаменљиви у свакодневном процесу рада, али поменути екстерни уређаји све више симулирају рад хард-дискова и користе се за пренос или чување података трајне или привремене употребне вредности.

Форензика дигиталних медија није само израз времена у коме живимо и вид забаве и разбибриге, већ реалност и насушна потреба, јер се иновације уређаја, а нарочито програма дешавају вртоглавом брзином. Све је више нових оперативних система, алата за заштиту уређаја и података, као и програма за енкрипцију података, злонамерних малициозних софтвера, којима се утиче на рад уређаја и компоненти, краду подаци и врше друга кривична дела. Зато је и потреба за израдом добрих форензичких алата и њиховом употребом све актуелнија.

Велики броја алата који су ван оперативних система представља у ствари алат хакера за покушај доласка до података или су незванични и често у свету и судској пракси непризнати. Зато је неопходно да се изузетно добро познају како истраживани медији, тако и форензички алати којима се врши аквизиција доказа како би се омогућила анализа, повратак обрисаних, скривених и привремених података који су на први поглед неуочљиви. Тиме се и избегава могућност оборивости доказа.

Шта је потребно знати о уређају на коме се врши форензика?

Искусни технолошки форензичари полазе од сазнања да су хард-дискови стабилни, да се преносне меморије лако скривају и бришу, те се подаци некада могу и трајно изгубити, да су принципи рада преносивих меморија различити, зависно од типа, врсте и произвођачких спецификација, да су упис и читање података различити на различитим медијима, да је и чување података различито на сваком медију, да постоји велики број програма за енкрипцију података на медијима и да је развој форензичких алата спорији у односу на програме за рад на рачунарима и осталим медијима.

Прикупљање података ван легалног процеса истраге

Поред легалног и легитимног начина прикупљања података, корисници са просечним знањем из области информатике, коришћењем неког од комерцијалних програма, могу упадом у систем преко рачунарске мреже или физичким пристб+упом, најчешће убацивањем флеш-меморије на рачунар жртве, а да претходно направе autorun фајл, покупе све податке са рачунара (лог шифре, поруке, логовање на мрежу, копирати фајлове). Нажалост, овај вид форензичке истраге не може се применити у процесу презентовања дигиталних доказа јер се не сматра валидним, тако да само злонамерници имају користи од њега.

Истрага ширења злонамерних софтвера

Злонамерни софтвери могу да се шире на више начина, а о врстама и начину њиховог деловања може се испричати посебна прича. Овде ћемо се осврнути само на три врсте интересантне за процес форензичке истраге. Први и најраспрострањенији је начин преко рачунарски јавних мрежа, као и упадом у приватне мреже. Други је преко електронске поште, најчешће слањем корумпираних фајлова, датотека или лажних сајтова. Трећи је преко преносивих медија, од којих су најчешће коришћени (намерно или не) УСБ и меморијске картице.

За проналажење намерног убацивања злонамерних програма путем мрежа потребно је велико искуство, али неретко и дозвола судских органа и сарадња са провајдерима – пружаоцима услуга, ради приступа мрежама, портовима, лог фајловима и слично.

Код електронске поште је нешто једноставније, јер на рачунару примаоца остају трагови, мада починиоци тих дела често прибегавају триковима гашења сајтова, њиховом маскирању или у великом броју случајева нису из исте државе са корисником – примаоцем поште.

Честа промена локације УСБ медија и меморијских картица, коришћење на више различитих уређаја, од којих неки немају или имају слабу антивирусну заштиту или су пак ан-

тивирусни програми различити, доводи до ширења ових програма, те је мукотрпан процес наћи тачан извор, пронаћи број уређаја и медија и слично. Еклатантан је пример ширења злоћудног програма у Америци 2008. године, када су астронаути НАСА-е крајњом непажњом, али и из незнања, пренели црв на свемирску станицу преко УСБ меморије.

Процес дигиталне форензике

Свака истрага, па самим тим и истрага дигиталних доказа састоји се из неколико фаза, како би се процес заокружио у једну целину и био ваљан судски доказ или био користан наручиоцу повраћаја података. Дигитална истрага, како ћемо је звати без обзира на сврху и намену, састоји се такође из неколико корака, од којих је идентификација медија први.

На почетку мора се утврдити врста, тип, модел и стање медија на коме се спроводи истрага. По својим карактеристикама сваки уређај или медиј је прича за себе. Ово се може обавити физичким очитавањем и прегледом уређаја и медија, али да би се избегле замке маскирања и мењања података, пожељно је и извршити дигитални преглед.

Опис будућег посла, прављењем слике уређаја или медија, евентуалне енкрипције, посебне ознаке, врсте фајл система, врсте датотека и слично, означићемо као фазу утврђивања чињеница.

Процена успешности

Поступак којим се утврђује да ли је могућ повраћај података, копија и извлачење оригинала или је у међувремену дошло до извршења радњи које би успешност довеле у питање, било да се ради о намерном или ненамерном брисању и измени података. Иако велики број чак и стручних лица сматра да се до података не може доћи ако је рађена корекција, ипак је у највећој мери то могуће, сем у случају великог и трајног физичког оштећења.

У зависности од типа уређаја или медија, алгоритми за упис и читање података су различити, па се њихова копија мора урадити валидно за конкретан тип и врсту. Потребно је извршити пробијање алгоритма јер су они патентирани од сваког произвођача посебно и представљају тајну (нису јавно доступни). Такође је важна чињеница да није исто смештање података на хард-диску или некој екстерној меморији, па копија података мора одражавати оригинал медија.

Затим следи прикупљање доказа о почињеном неделу. Овај део истраге користи се да се дигитални докази са једне или више локација преместе на другу, тако да не претрпе оштећења, структуралне измене или брисање у току експлоатације. Зависно од тога на ком се уређају или медију спроводи истрага, прави се и копија која подржава оригинал. Овде треба посебну пажњу обратити на врсту меморије, избор алата, безбедно копирање података – доказа, аутентификацију података, израду копије копије (дупликата копије) и реконструкцију догађаја.

Иако се у литератури и пракси поступак откривања софтверске заштите често разматра под израдом копије медија, потребно је нагласити и издвојити га као посебну целину, јер корисници постављају замке у виду енкрипције

података, закључавања фајлова, стеганографије и низ других метода. Из тог разлога такви подаци често се сматрају оштећеним, а применом неодговарајућих алата или неправилним поступањима могу да буду и трајно изгубљени.

Откривање хардверске заштите

Готово најбезбеднији начин који учиниоци дела користе за заштиту података јесте енкрипција података заснована на хардверу. Овај тип заштите пружају сами произвођачи компоненти, те је приступ истражитељима умногоме отежан. Често се покретањем погрешних процеса долази до трајног уништења података на хардверу, а самим тим и процес истраге престаје.

Савременији хардвери заштићени су и функцијама пребрисавања локација, тако да се уклоњени подаци сматрају трајно оштећеним. За пробијање такве заштите потребни су огромни временски и материјални ресурси, са неизвесним крајем и резултатом.

Алати за аквизицију

Када се ради о ненамерним губицима података, који могу бити узроковани незнањем, неадекватном употребом и коришћењем хардвера или софтвера, истеком временских ресурса, физичким уништењем медија, упадом малициозних програма у уређај и слично, повраћај података је нешто једноставнији, јер су трагови рада на неки начин сачувани, иако обичном кориснику невидљиви. У великом броју случајева, једноставним софтверским решењима самих оперативних система или коришћењем комерцијалних програма подаци се могу повратити, односно спасити.

Ако је реч о крађи података односно извршењу неког кривичног дела, у дигиталној форензици користе се специјализовани алати. Када се ради тим алатима, неопходно је њихово врхунско познавање, разумевање сврхе и намене и ефикасности употребе. Неретко се дешава да брзи развој програма за комерцијалну употребу, али и злонамерних програма за нападе на дигиталне медије, није у довољној мери испраћен развојем алата за дигиталну форензику.

Ако се поштује премиса да алат за дигиталну форензику мора бити исте генерације као и алат извршиоца кривичних дела, често се долази у пат позицију – да се за поједине апликације или делове неких оперативних система не може употребити адекватан алат и метод истраге због застарелости. Када је реч о преносивим медијима ситуација је много критичнија.

Брзи развој, ниске цене коштања, лако руковање и компатибилност преносивих меморија условљавају и доминантне светске произвођаче софтвера да најчешће у оквиру оперативних система угради програме за хардверску и софтверску заштиту. Опасност лежи управо у томе да постоји много начина да криминогене структуре злоупотребе те додатке програмима за извршење неког дела.

Сваки алат за дигиталну форензику који није саставни део оперативног система или није већ инсталиран на рачунару налази се на неком медију. У последње време примат за смештај форензичких алата од ЦД или ДВД дискова преузимају УСБ меморије. Зашто? Једноставно, мањи су по габариту, лакши за руковање, транспорт, прикључење на рачунар, а у потпуности

служе сврси подизања оперативног система тако да се не угрожавају подаци на хард-диску, као и прављења копије података са места извршења дела.

Меморијске картице такође могу бити коришћене за смештај програма и алата форензичке истраге јер велики део рачунара и осталих дигиталних уређаја већ има уграђен читач картице, а и ако га нема, веома лако се може прикључити преко екстерног читача, што се посебно односи на рачунаре, таблете, дигиталне камере и фото-апарате и мобилне телефоне новије генерације.

Откривање података заштићених софтверским путем

Велики део заштите података софтверским путем ради се или алатима и програмима самог оперативног система или једноставним јавним програмима који су бесплатно доступни. Откривање података пробојем алгоритама за заштиту је овде једноставно и не изискује нарочито велико знање, време или ресурсе.

У ову категорију спада најпре DriveCrypt – алат за заштиту целог диска, са јавно доступним алгоритмом, који ради на свим оперативним системима, мале величине за инсталацију, бесплатан је и обезбеђује минималне губитке података у случају оштећења дискова или преносних медија и меморија.

Форензика података заштићена тим програмом веома је тешка, скоро немогућа и заснива се углавном на бруталном нападу.

Ту је и BitLocker – веома моћан начин заштите свих меморија, уграђен у новије оперативне МС системе, а користи AEC алгоритам за енкрипцију. Није компатибилан са неким верзијама МС оперативних система. Овај алат пружа често слику да подаци на појединим медијима не постоје. Уназад неколико година развијено је неколико алата за разбијање енкрипције BitLocker-a.

Поред најраспрострањенијих начина софтверске заштите које смо споменули постоји још стотинак других софтвера за заштиту података.

Најкоришћенији и најпознатији алати

На оперативним системима Linux, у склопу самог подизања оперативног система познате су дистрибуције Helix, Caine, Deft, FBIFC..., док је за Windows оперативни систем најпознатији Windows FD.

EnCase – програмски алат један је од најнапреднијих и најсигурнијих, који се користи за истрагу високотехнолошких дела. Има изузетан графички интерфејс, којим се прегледају обрисани и неалоцирани подаци. Не дозвољава да се у процесу истраге мењају подаци, што га чини валидним за судско вештачење. Успешно заобилази заштите све до оних уграђених у Windows-7, као и све старије видове заштите.

FTK (Forensic Toolkit) – веома популаран, један од најранијих алата, који у себи има и такозвани FTK Imager, који копира бит по бит, веома функционалан, а јавно и бесплатно доступан. Предност му је и та што може да обједини све формате који су направљени осталим форензичкима алатима.

DriveSpy – намењен за форензику ДОС оперативног система, без графичког интерфејса, малог капацитета. Проширује основне MS-DOS функције, креира хеш финк-

цију за копирани диск, партицију или датотеку за брисање диска. Модерније верзије имају додатак који омогућава и форензику преносивих медија.

Helix – до скоро бесплатан, а у последње време надограђен и комерцијалан програм заснован на Ubuntu Linux-у. Ради директно са ЦД медија, никада не користи свап партицију и може да анализира све Windows и Linux оперативне системе. Препознаје скоро све фајл системе. Покреће се као самостална апликација.

Остали алати

Без задирања у опис и суштину, а да читаоци примете колико је ова област развијена, набројаћемо и друге комерцијалне и некомерцијалне алате за дигиталну форензику. Ту спадају Passware Kit Forensic, TestDisk, Recuva, GetDataBack, Forensic Replicator, Norton Ghost, Caine дистрибуција, Deft форензичка дистрибуција, DD је стандардан Unix/Linux алат, VMware , SafeBack – DOS алат, SMART, Linux алат, WinHex алат, ProDiscover, FTK Imager Mdd, Win32dd...

Ово је попис малог дела алата који су у употреби било као самостални или као делови или допуне осталим форензичким алатима, а раде на свим врстама оперативних система.

Поред њих постоји и низ ненаменских или званично непризнатих алата, а који се користе у процесу форензичке истраге. Нажалост део њих је продукт рада злонамерних корисника, који их користе у криминалне сврхе, али су понекад једини могући алати за проналажење података и откривање догађаја. У свету постоји још неколико компанија (као што су ElcomSoft, Passware...) које се баве производњом форензичког алата, који још нису ушли у процес легализације и комерцијализације.

Често спомињани алати, а да им форензика није основна намена, јесу они извесног програмера Нира Софера и његов програм NirSoft, мада још није утврђено ко стоји иза сајта који се тако публикује.

Материја и проблем дигиталне форензике, ако се сагледавају са аспекта заштите медија и комуникација, али и са аспекта могућности и врста напада, толико су обимни и комплексни и изискују перманентно праћење иновација, како у развоју информационих технологија, тако и на заштити од напада и пробијања, па самим тим и на изради алата и њиховој примени у аквизицији.

Етика

Као посебна целина форензичке истраге јесу и законска регулатива и етички кодекс. Непознавање ове материје може да компромитује истрагу. Основни захтеви које треба испунити да би истрага била прихваћена јесу:

- истрагу реализује искључиво лице овлашћено од надлежног судског, полицијског или корпоративног тела, са прецизним задацима, обавезама и смерницама у раду;
- истрага се реализује само ако постоји основана сумња да су закон или правило институције прекршени, и спроводи се само у границама доказивања или одбацивања те основане сумње;
- истрага с циљем проналажења сумњивих активности спада у шпијунску и недозвољену активност;
- мора да постоји јасна дефиниција захтева, који је

циљ, предмет и задатак истраге, и може да се креће само у оквирима наведеног захтева;
- неопходно је документовање захтева, процедура, алата и места и времена истраге са валидним и проверљивим доказима;
- заштита од нестручног рада и задирања у приватност корисника рачунара;
- документовање налаза мора бити у складу са правилима струке, али и јасно схватљивим терминима осталим учесницима у поступку и
- закључак налаза мора бити прецизан и конкретан и не сме оставити сумњу, недоумицу или изазивати и показивати двосмисленост.

Очекивани правци развоја

Као област која још није покривена општеприхваћеним стандардима, како због чињенице да је то релативно ново поље, тако и због различитог приступа појединих законских аката овој материји, дигитална форензика ће своје место сигурно задржати у садашњим институционалним оквирима,

Све бржи развој технологије, већа едукација корисника рачунарских услуга, већи број стручног особља за одржавање хардверских и софтверских елемената, доприносе да ова област налази све ширу примену. Такође је и немали значај доношења законских и подзаконских регулативних аката, као и све боља стручност тужилаца, судија и адвоката за ову област.

Уз ова сазнања, наравно, нужно је напоменути да је људски фактор у свим сегментима, без обзира на развијеност технологије, и даље доминантан. Човек је најслабија, али и најјача карика сваког безбедносног система. ■