АНТИФОРЕНЗИКА

Потпуковник *Дејан Станивуковић**

Слично извршиоцима класичних облика криминала и извршиоци кривичних дела високотехнолошког криминала настоје да уклоне трагове кривичног дела и на тај начин спрече његово откривање и документовање. У том смислу, заједно са развојем дигиталне форензике, развијен је и читав низ антифорензичких метода и посебних техника, које имају за циљ да отежају или спрече проналажење дигиталних доказа неопходних за вођење судског поступка.

Истовремено, на интернету је доступан велики број софтвера који применом научних метода врше прикривање или брисање дигиталних података ради заштите личне приватности или интегритета приватних предузећа и државних институција. Неки од ових софтвера, када се користе ради спречавања или отежавања доказивања кривичних дела високотехнолошког криминала, постају моћни алати антифорензике.

У раду су тестиране могућности једног од таквих софтвера – Eraser, у спречавању доказивања кривичног дела високотехнолошког криминала алатима дигиталне форензике EnCase и FTK, који представља стандард у истрагама ове врсте криминала и судској пракси САД и земљама ЕУ.

* Аутор ради у Криминалистичко-истражној групи Управе Војне полиције ГШ ВС

У научно-стручним круговима уочено је да постоје различита гледишта о садржају појма антифорензика. Аутори антифорензику, као нову област проучавања, различито дефинишу, а карактеристична су следећа одређења појма антифорензике: према једнима, антифорензика представља алате и методе који се користе за спречавање стручних служби система кривичног правосуђа у извођењу форензичке истраге и примене науке у доказивању и извођењу валидних дигиталних доказа; према другима, антифорензика представља технике хакера и кибернетичких криминалаца намењене за

борбу против форензичке истраге – отежавања или онемогућавања те истраге; За треће, антифорензика подразумева последњу фазу хакерисања у којој извршилац, пре напуштања система у који је извршио упад, настоји да, применом различитих програма али и уређаја, уништи, измени, прикрије, фалсификује или оштети трагове које је за собом оставио.

Наведене дефиниције указују на то да појам антифорензика језички и логички није у довољној мери прецизан. Закључено је да синтагма дигитална антифорензика (ДАФ) непосредно одређује појам и појаву која се дефинише за разлику од антифорензике која се, као непосредно виши појам, подједнако односи како на дигиталне тако и на биолошке и друге доказе чије се прикупљање спречава или отежава. Анализом наведених одређења садржаја појма антифорензика уочено је да постоје одређене сличности: (1) антифорензиком се спречава или отежава доказивање кривичних дела високотехнолошког криминала, (2) спречавање или отежавање доказивања ових дела врши посебна врста криминалаца – кибернетички криминалци, (3) ради спречавања или отежавања доказивања ових дела кибернетички криминалци користе различите алате (програме и уређаје) и методе (технике) и (4) антифорензика има негативан контекст.

Полазећи од тога да циљ и начин на који се циљ остварује одређују сврху, може се закључити да је циљ антифорензике уништење дигиталних података, применом научних метода као начина остварења циља, ради спречавања доказивања кривичних дела, при чему се под сврхом не подразумева само уништење дигиталних података већ и изналажење најбољег начина на који се то остварује.

Дигиталну антифорензику није могуће посматрати одвојено од дигиталне форензике. Без јасне идентификације њихових заједничких особина и разлика није могуће у потпуности сагледати садржај појмова који их одређују. Заједничка особина дигиталне антифорензике и дигиталне форензике је начин на који остварују циљ, односно примена научних метода и посебних техника у остварењу циља. Основне разлике између дигиталне антифорензике и дигиталне форензике је у њиховим циљевима и сврхама. С једне стране, циљ дигиталне антифорензике је прикривање или брисање дигиталних података, а са друге стране циљ дигиталне форензике је идентификовање и анализирање дигиталних података. Сврха дигиталне антифорензике је отежавање или онемогућавање доказивања кривичних дела високотехнолошког криминала, а насупрот томе сврха дигиталне форензике је обезбеђивање и презентовање дигиталних доказа ради ефикасног вођења кривичног поступка (слика 1).

Слика 1. *Однос дигиталне антифорензике и дигиталне форензике*

Полазећи од наведених заједничких особина и разлика, дигитал-

ну антифорензику можемо дефинисати као процес прикривања и брисања дигиталних података, применом научних метода и посебних техника, ради отежавања или спречавања вођења судског поступка за кривична дела високотехнолошког криминала.

Имајући у виду да су отежавање или спречавање доказивања кривичних дела високотехнолошког криминала сврха дигиталне антифорензике, може се закључити да третирање дигиталних података значајних за вођење кривичног поступка на такав начин истовремено представља и облик кривичног дела „Спречавање и ометање доказивања" из члана 336. Кривичног законика Републике Србије, односно да дигитална антифорензика има негативан контекст. Предмет доказивања кривичног дела „Спречавање и ометање доказивања" јесу све чињенице које су значајне за доношење судске одлуке, а које се доказују помоћу доказних средстава (сведока, вештака, исправа и сл.).

Радња извршења облика наведеног дела састоји се у скривању, уништењу, оштећењу или чињењу неупотребљивом (делимично или потпуно) туђе исправе или других предмета који служе за доказивање. Код потпуног или делимичног чињења неупотребљивим туђе исправе или другог предмета мора се имати у виду функција коју треба да обави исправа, односно предмет, тј. довољно је да су они постали неупотребљиви за доказивање. Дело је довршено самим предузимањем радње.

Објекат радње јесте исправа или предмет који може да служи за доказивање. Исправа и предмети морају бити туђи, тј. у својини неког другог лица. С тим у вези, поставља се питање – шта је са рачунарским подацима који су подобни или одређени да служе као доказ у поступку, а сакрило их је, уништило или оштетило лице осумњичено за кривично дело високотехнолошког криминала, које је уједно и власник тих података. И исправа и други предмет морају бити подобни да се помоћу њих доказује нека чињеница. У противном, постојао би неподобан покушај који код овог кривичног дела није кажњив. Овај облик може се учинити само са умишљајем, с тим што мора постојати и намера да се предузимањем радње извршења спречи или отежа доказивање. Уколико се ово дело учини у кривичном поступку, постојаће тежи облик дела. Полазећи од примене научних метода и посебних техника као начина остварења циља, а тиме и сврхе дигиталне антифорензике, закључено је да се под антифорен- зичким третирањем дигиталних података не може сматрати и њихово уништење употребом физичке силе, хемијских средстава или на друге „ненаучне" начине.

Када је у питању извршилац овог дела, Кривични законик Републике Србије у одређењу наведеног дела користи термин „ко" тј. било које лице. Са једне стране, у стручној и научној литератури за означавање ових лица користи се термин „кибернетички криминалци". Законска одредба да извршилац овог дела може бити било ко веома је „широко" дефинисана, имајући у виду да се прикривање, уништење и оштећење рачунарских података врши применом научних метода и посебних техника, које су познате само мањем делу популације. Са друге стране, одређење да су „кибернетички криминалци" извршиоци овог дела било би веома „сужено" имајући у виду да су научне методе и посебне технике прикривања, уништења и оштећења рачунарских података познате значајном делу популације која се не би могла сврстати у „кибернетичке криминалце", а чији припадници, под одређеним условима, могу бити извршиоци овог кривичног дела. Очити пример су ауторска права.

Имајући у виду наведено, извршилац кривичног дела „Спречавање и ометање доказивања" (антифорензичким третирањем дигиталних података) може бити свако лице којем су познате научне методе и посебне технике прикривања, уништења и оштећења дигиталних података, које у моменту њихове примене има свест да предузимањем тих радње може доћи до спречавања или отежавања доказивања и које има вољу да до тог спречавања или отежавања дође.

У литератури постоје различите категоризације антифорензичких метода, а у научно-стручним круговима најчешће цитирана је *Rogers*-ова класификација: (1) скривање података (*data hiding*); (2) уништавање корисничких објеката (*artifact wiping*), (3) прикривање трага, односно путање (*trail obfuscation*) и (4) деловање против дигиталних форензичких процеса/алата (*attacks against the CF process/tools*).

Постоје различите врсте антифорензичких метода, а као најчешће наводе се методе одређене у дискусионом материјалу Савета Европе: (1) Измена атрибута датотека (нпр. датума и времена последњег приступања) у оквиру којих можемо разликовати атрибуте који се односе на различите оперативне системе (*DOS*, *Windows*, *Linux*, *Solaris* и др.); (2) Записивање нових података преко постојећих, ради њихове измене и стварања информација које погрешно усмеравају онога ко анализира систем; (3) Брисање или физичко одстрањивање датотека – преписивање датотека са неупотребљивим подацима преко створених датотека; (4) Брисање датотека (писање преко указивача на садржај);

(5) „Капсулирање" података – сакривање убацивањем у друге датотеке; (6) Отмица рачуна – фингирање приказивањем другог лица као извршиоца, преузимањем његових идентификационих елемената (лого- вањем под његовим генералијама) и коришћењем његовог рачунара вршење кривичних дела и (7) Архивске/имиџ бомбе – прављење трагова ради компромитовања анализе имиџа (фотографије).

На интернету је доступан велики број софтвера који применом научних метода врше прикривање или брисање дигиталних података ради заштите личне приватности или интегритета приватних предузећа и државних институција. Када се користе у сврху спречавања или отежавања доказивања ови софтвери постају моћни алати дигиталне антифорензике. Неки од таквих софтвера су: *BCWipe*, *Active@ Kill Disk*, *Eraser* и *Folder Lock*.

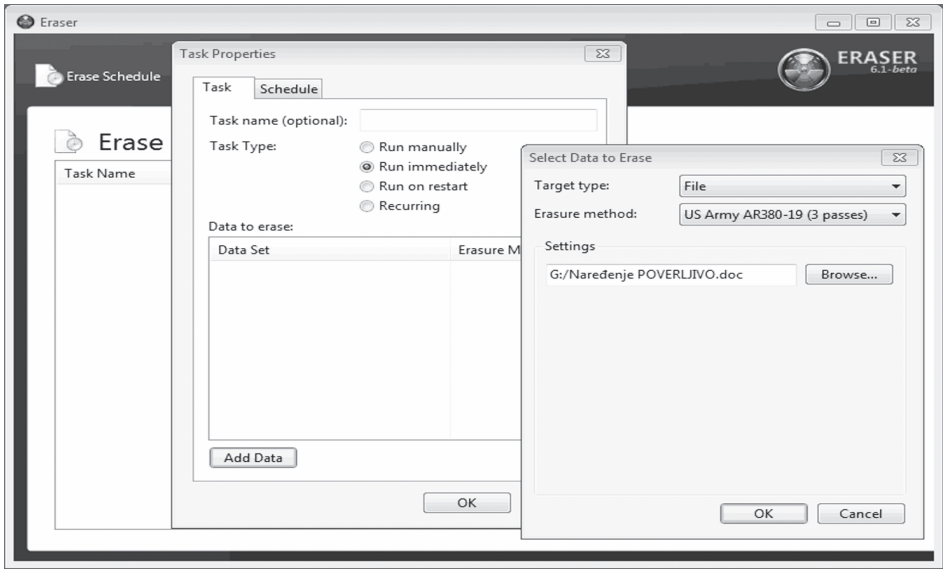
BCWipe је апликација која је у стању да трајно уклони или обрише дигиталне податке који се покрећу различитим оперативним системима (*Windows*, *Mac OS X* и *UNIX*). Користи се у комерцијалне сврахе, као и за војне потребе, и има одобрење Министарства одбране САД. Користи је велики број страних влада и/или војних организација.

Active@ Kill Disk је бесплатан услужни програм за безбедно брисање хард дискова, који је подржало Министарство одбране САД као стандард *DoD 5220.22M* за уклањање података са хард диска. Значајна карактеристика програма јесте да када брише чврсти диск генерише сертификат који је могуће одштампати као доказ да је диск безбедно обрисан.

Eraser је бесплатан програм за безбедно брисање података са хард диска. Карактеристика програма јесте да има разне методе за преписивање података, на основу више различитих стандарда, као и дефинисање властите методе преписивања. Безбедно брише датотеке, директоријуме, неискоришћен простор на диску и корпу за отпатке, непосредним или унапред одређеним покретањем.

Folder Lock је програм који омогућава: закључавање, сакривање и обезбеђење заштите одабраних података уношењем централне шифре (*Master Password*) једноставном „*drag and drop*" (превуци и отпусти) методом; енкрипцију важних датотека и чување података на било ком преносном уређају. *Folder Lock* користи централну лозинку за приступ свим наведеним и другим карактеристикама.

Начин функционисања и могућности ових софтвера приказани су на примеру датотека: *Наређење POVERLJIVO.doc* и *Karta POVERLJIVO.JPG*, третираних најпре методом дигиталне антифорензике – брисање са преписивањем, помоћу софтвера *Eraser 6.1-beta*, а затим методом дигиталне форензике – опоравак избрисаних дигиталних података, помоћу стандардних софтвера дигиталне форензике *EnCase Enterprise v4* и *FTK v1.81.6*.

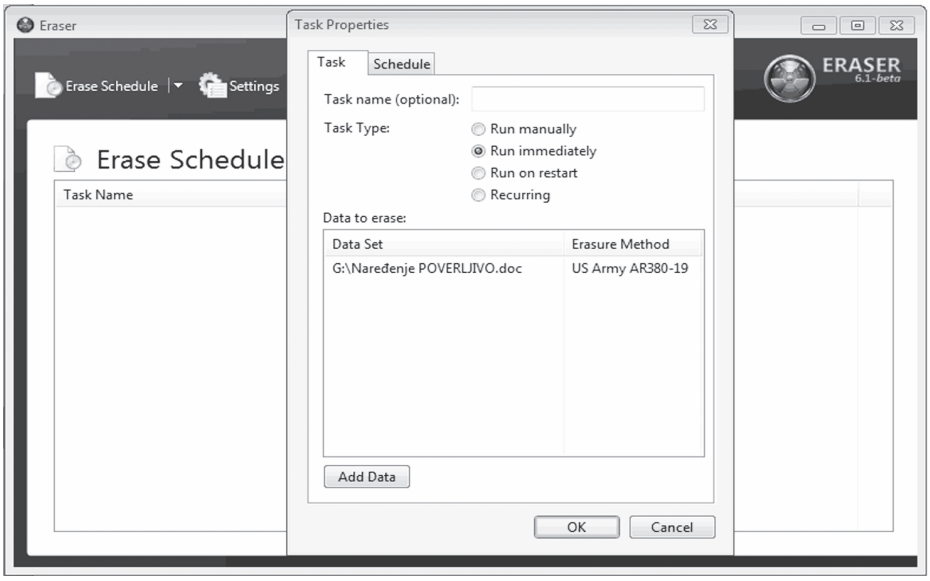


Слика 2. *Селектовање опција у потпрозорима Task Properties и Select Data to Erase*

Након покретања апликације *Eraser 6.1-beta*, десним кликом на празан простор *Task Name* активира се понуђена опција *New Task* која отвара потпрозор *Task Properties* у којем се селектује перманентно брисање као тип задатка који треба да се изврши – *Run Immediately*, а затим се активира контролно дугме *Add Data*.

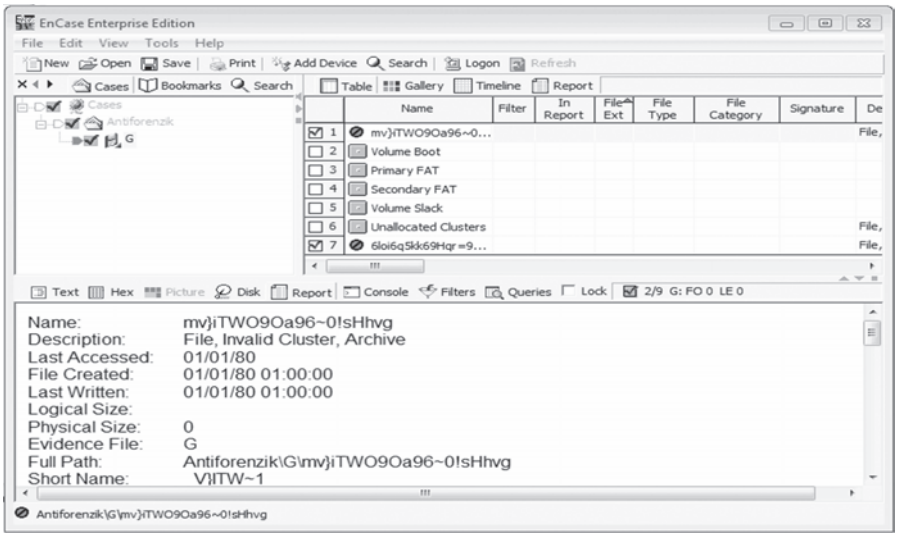
У отвореном прозору *Select Data to Erase* врши се селектовање опција: тип података који се брише – *File*; метод брисања са преписивањем – *US Army AR380-19* (*3 passes*) и локација датотеке која је предмет брисања – G:/ *Наређење POVERLJIVO.doc*. Активирањем контролног дугмета *ОК* потпрозора *Select Data to Erase* потврђују се селектоване опције (слика 2).

Активирањем контролног дугмета *ОК* потпрозора *Task Properties* потврђује се задатак у целости и започиње процес брисања са преписивањем (слика 3). Овај процес, у зависности од селектованог модела брисања са преписивањем и количине података која се брише, има различито трајање. Начелно, за исту количину података процес брисања најдуже траје код модела *Gutmann*, са 35 преписивања, а најкраће код модела *British HMG IS5 (Baseline)*, са једним преписивањем. На исти начин како је то учињено са датотеком *Наређење POVERLJIVO.doc* извршено је и брисање датотеке *Karta POVERLJIVO.JPG*.



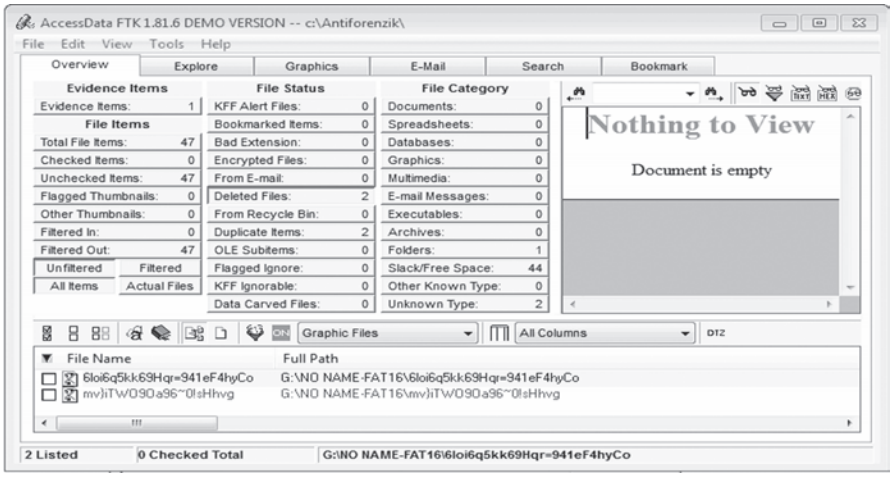
Слика 3. *Потпрозор Task Properties са контролним дугметом ОК за потврђивање задатка у целости и започињање процеса брисања са преписивањем*

У покушају опоравка наведених датотека обрисаних софтвером дигиталне антифорензике *Eraser,* применом софтвера дигиталне форензике *EnCase* идентификоване су две датотеке непознатог назива које није било могуће опоравити: *mv}iTWO9Oa96~0!sHhvg* и *6loi6q5kk69Hgr=941eF4hyCo* (слика 4).



Слика 4. *Опоравак података обрисаних софтвером дигиталне антифорензике Eraser применом софтвера дигиталне форензике EnCase*

У покушају опоравка наведених датотека, применом софтвера дигиталне форензике *FTK,* такође су идентификоване две датотеке непознатог назива које није било могуће опоравити: *mv}iTWO9Oa96~0!sHhvg* и *6loi6q5kk69Hgr=941eF4hyCo* (слика 5).



Слика 5. *Опоравак података обрисаних софтвером дигиталне антифорензике Eraser помоћу софтвера дигиталне форензике FTK*

ЗАКЉУЧАК

Имајући у виду доступност и ефикасност софтвера који применом научних метода врше прикривање или брисање дигиталних података ради заштите личне приватности или интегритета приватних предузећа и државних институција, потврђену наведеним тестирањем, као и могућност њихове употребе у антифорензичке сврхе, може се закључити да се пред произвођаче софтвера дигиталне форензике поставља изузетно тежак задатак изналажења целисходног решења за опоравак вишеструко преписаних дигиталних података.

Ипак, треба имати у виду да нису сви алати за брисање података савршени и да је често могуће опоравити мање или веће делове датотека. У том случају, за дигиталне форензичаре и вештаке информационих технологија представљаће изазов доказати да ти делови датотека заиста припадају и потичу од одређене датотеке као целине.

Литература

1. Ранђеловић, Д.: *Поређење комерцијалних и некомерцијалних алата дигиталне форензике и њихова употреба,* Војнотехнички институт, Београд, 2011.
2. Милосављевић, М.; Грубор, Г.: Дигитална форензика рачунарског система, Универзитет Сингидунум, Београд, 2009.
3. Ивановић, З.; Жарковић, М.; Лајић, О.: *Криминалистичка разматрања дигиталних доказа: Тематски зборник радова, Криминалистичко-форензичка обрада места кривичног догађаја,* Криминалистичко-полицијска академија, Београд, 2013.
4. Стојановић, З.: *Коментар Кривичног законика,* Јавно предузеће „Службени гласник", Београд, 2007.
5. http://cyberforensics.purdue.edu/documents/AntiForensics_LockheedMartin09152005pdf [16.03.2014]
6. http://www.eraser.heidi.ie/ [16.03.2014]
7. http://www.killdisk.com/eraser.htm [16.03.2014]
8. http://www.newsoftwares.net/folderlock/ [16.03.2014]
9. http://www.qwhatis.com/what-is-bcwipe/ [16.03.2014]