РАШКОВСКА Вероника[1]
РАШКОВСКИ Драги[2]

УДК: 343.14:004
343.98:004

ПОТВРДУВАЊЕ НА ВЕРОДОСТОЈНОСТА НА ДИГИТАЛНИТЕ ДОКАЗИ

Апстракт: „Помодерните“ судски власти се чини дека стануваат се повеќе свесни за потребата од разгледување на автентичноста на дигиталните податоци, без разлика дали се утврдува дека се гласини/рекла-кажала или не, во корист на поопшта и флексибилна грижа за веродостојноста. Основата за одредување на веродостојноста на компјутерски генерираните информации во голема мера се разликува од онаа на физичките докази. Иако потеклото на доказите секако мора да се утврди, барањата во однос на дигиталните податоци не се исти како и за физичките докази. Дигиталните податоци се речиси целосно зависни од поткрепено сведочење кое има мала, или воопшто нема, врска со автентичноста на содржината за која се бара да се допушти. Критериумите за утврдување на допуштеноста на компјутерски генерираните информации мора да побаруваат прикажување зголемена веродостојност.

Дигиталната форензика несомнено е висока техничка област заснована на наука: компјутерски науки, математика, физика итн. Тоа е и област која бара познавање од инженерство, особено електроинженерство, машинско инженерство и системско инженерство. Процесот на примена на науката и инженерските дисциплини е сложен и бара стручно размислување кое понекогаш помалку наликува на наука, а повеќе на уметност. Токму заради тоа, потврдувањето на веродостојноста на дигиталните докази не е само правен предизвик, а можеби е и помалку правен, отколку технолошки предизвик, поради што, веродостојноста во најчест случај ќе се бара да биде потврдена од ИТ експерти.

Клучни зборови: *дигитални докази, компјутерска форензика, веродостојност, автентичност.*

RASHKOVSKA Veronika[3]
RASHKOVSKI Dragi[4]

VALIDATING THE RELIABILITY OF DIGITAL EVIDENCE

Abstract: “More modern” judicial authorities seem to be becoming more aware of the need to consider the authenticity of digital data, regardless of whether it is established to be hearsay or not, in favour of a more general and flexible concern with reliability. The starting point for establishing the reliability of computer-generated information differs greatly from the one of physical evidence. While the provenance of the evidence must of course be established, the requirements for digital data are not the same as for physical evidence. Digital data is almost entirely dependent on supported testimony that bears little or no relation to the authenticity of the content required to be admitted. The criteria for establishing the admissibility of computer-generated information must require a reflection of increased reliability. Digital forensics is undoubtedly a highly technical field based on science: computer science, mathematics, physics, etc. It is also an area that requires knowledge of engineering, particularly electrical engineering, mechanical engineering and systems engineering. The process of applying science and engineering disciplines is complex and requires expert reasoning that sometimes follows less science and more art. Consequently, verifying the reliability of digital evidence is not only a legal challenge, and it may be less of a legal than a technological challenge, which is why, in most cases, the reliability shall in most cases be required to be verified by IT experts.

Key words: *digital evidence, computer forensics, reliability, authenticity.*

1) Доцент на Факултет за правни науки, меѓународни односи и дипломатија - МИТ Универзитет Скопје, veronika-nachevska@hotmail.com
2) Вонреден професор на Правен факултет „Јустинијан Први” при УКИМ во Скопје, d_rashkovski@yahoo.com
3) Assistant Professor at The Faculty of legal sciences international relations and diplomacy - MIT University, Skopje, veronika-nachevska@hotmail.com
4) Associate Professor at the Iustinianus Primus Faculty of Law at the Sts. Cyril and Methodius University in Skopje, d_rashkovski@yahoo.com

1. Вовед

Дигиталната форензика[5], образование за дигитална форензика[6] и општа дигитална форензика[7] се делови од општата форензика кои користат опаѓачки пристап за развивање хиерархиски распоред на теми за истражување кои би помогнале во идентификување на потребите за истражување во оваа област полна со предизвици во нивната примена, во она кое е еден од најголемите импаративи на денешницата – правото и правдата. Дигиталната форензика изискува висока прецизност во своето практицирање со оглед на својата природа, која ја прави доста ранлива од надворешни влијанија, како технички така и човечки, па затоа правните аспекти на дигиталната форензика се далеку посложени од многуте други аспекти кои се тесно поврзани поради строгите барања за нивна прифатеност како научни и технички докази кога се употребуваат во правни постапки, особено при нивното користење во кривичната постапка каде најчесто на удар е слободата и физичкиот интегритет на странките во постапката. Токму затоа дигиталните докази потребно е да бидат соодветни, материјално поткрепени и веродостојни за да може да се квалификуваат како прифатливи и со тоа да можат да влезат во судница.

Судницата е место каде што треба да се спроведува правда, а, од друга страна, улогата на дигиталните истражители во таа насока е да претстават издржани факти и веројатности за време на судскиот процес. Тоа значи дека судовите се зависни од доверливоста на дигиталните истражители, како и нивната способност за претставување технички докази на соодветен точен начин. Приложувањето на доказите на јасен, фактички и објективен начин е нивна должност. Тие мора да ги тргнат на страна влијанијата од околината и мислењата на луѓето околу нив и да не донесуваат брзи заклучоци. Независно дали станува збор за сведочење или експертски извештај, во професионалното работење на дигиталните истражители нема простор за посредништво или расудувачки тврдења.

Компаративно, искуствено, правото и правната пракса во САД е многу поприсутва во научните истражувања, за сметка на европско-континенталната, што во никој случај не треба да значи и забрана или непроодност од правни влијанија, затоа што техниката не познава територијални граници и нејзиниот принцип на функционирање е унифициран независно од политичкото или општественото уредување. „*Алфа и омега*" во создавање на основите на примената на дигиталните докази во судница претставуваат случаите во САД: Дуаберт против Мерел-Дау Фармацеутикалс[8], Џенерал Електрик Ко. против Џојнер[9] и Кумхо Тајер Ко. против Кармичел[10] и примената на Правилото за докази 702. Без почитување на основните принципи, дигиталните докази би останале само записи на кои судот не би требало да поклони верба. Тие се како меур од сапуница, кој доколку не се пренесува во контролирани услови за миг може да се претвори само во ситни капки од истата.

2. Прифатливост на дигиталните докази

Дигиталните докази треба да поминат неколку пречки за потврдување на нивната соодветност во однос на начинот на собирање, чување, обработка и претставување како доказ. Компјутерите во денешно време содржат огромна меморија (капацитет) за чување на податоци или истата може да се надгради. Со оглед на брзиот развој на технологијата, постоењето на меморија на хард диск од 1 терабајт е речиси стандардна и почетна капацитетност на истиот. Ако се земе во предвид и можноста за поврзување во ланец на неколку хард дискови, тогаш таа капацитетност е уште податна за складирање на податоци, меѓу кои може да се најдат и дигитални докази. Нивното преземање и чување не може веќе да биде така едноставно како што беше порано зачувувањето на ЦД или на флеш меморија. Неможноста да се замрзнат доказите пред отворање на датотеките, заедно со фактот дека самото отворање на датотеките може да доведе до нивна промена, може и ги поништува клучните докази, да ги измени или да ги енкриптира. Како резултат на тоа, се јавува проблем со лоцирање на соодветните докази во склоп на голема количина на податоци, а пребарувањето на информации во таков случај е макотрпно, што само по себе процесот го прави адекватен на барање игла во огромна бала сено.

5) Pollitt, M., K. Nance, B. Hay, et al (2008) *Virtualization and Digital Forensics: A Research and Education Agenda*. Journal of Digital Forensic Practice, 2 (2), 62-73.

6) Nance, K., H. Armstrong, and C. Armstrong. (2010) *Developing a Research Agenda to Improve Digital Forensics Education*. Digital Forensics Minitrack of 43rd Hawaii International Conference on Systems Sciences.

7) Nance, K., B. Hay, M. Bishop. (2009) *Digital Forensics: Defining a Research Agenda*. 42nd Hawaii International Conference on System Sciences. Digital Forensics Research Track.

8) 509 U.S. 579 (1993).

9) 522 U.S. 136 (1997).

10) 526 U.S. 137 (1999).

Присуството на технологијата „во облаците" дава дополнителен предизвик и затоа е потребно да се разгледаат работите и подалеку од еден компјутер. Во модерната компјутерска архитектура, дигиталните докази може да постојат на многу различни сервери и клиенти во рамките на ИТ структурата на една организација. Поврзувањето на дигиталните записи преку логички алгоритми кои се распространети на сервери на различни континенти, при што секое парче од мозаикот е на различен континент го усложнува процесот на прибирање на докази и постапката станува потешко кога ИТ инфраструктурата е поврзана на интернет затоа што во таков случај, дигиталните докази може да се распространат на широки географски растојанија и во неколку судски надлежности.

Дигиталните докази треба да имаат соодветна основа за нивно претставување, но судовите не наложуваат тие да исполнуваат построги основи од оние пропишани за другите видови докази[11]. Претставувањето на дигиталните докази (или компјутерски исписи за дигитални докази затоа што истите се бескорисни во дигитална форма за оние кои ги споредуваат фактите) е дозволено под услов „страната која ги дава компјутерските информации да постави претставување кои како такво го гарантира наодот дека таа информација е доверлива и спротивната страна ја има истата можност да ја провери точноста на компјутерот и внатрешните постапки како што треба да ја провери и точноста на пишаните деловни записи"[12]. Судот не ги прифаќа така лесно тврдењата дека дигиталните докази се наследно недоверливи затоа што лесно и незабележително може да се менуваат[13]. Тоа значи дека страната од постапката која фрла сомнеж кон веродостојноста на приложените дигитални докази мора да даде соодветно научно и технолошко објаснување зошто истото го предлага, кое во најмала рака може да биде поткрепено со незапазување на соодветната процедура за нивно прибирање, чување и презентирање, па движејќи се кон стручноста на кадарот кој учествувал во овој процес, неконтаминираноста и форензички чистата околина... и ред други процесни претпоставки, без чие исполнување, тежината на докажување на нивната веродостојност ќе премине на страната која ги предлага.

Дигиталните докази најчесто се јавуваат во пишана форма или во форма која може да соодветствува на пишаната, па затоа истите мора да поминат низ постапка на проверка на автентичноста и исполнување на барањата.

На пример, во САД за истото постои Правилникот за најдобри практики.[14] Правилникот се однесува на информации зачувани на компјутер. Факт е дека диск или друг запишувач на податоци не се корисни за оние кои ги проверуваат фактите, па според правилото 1001(3), „доколку податоците се зачувани на компјутер или сличен уред, секој испис што може да се прочита со око, а кој ги прикажува податоците точно, се смета за оригинал". Според правилото 1003, дупликат се смета за прифатлив освен доколку станува збор за неговата точност или доколку, заради која било причина, неправедно е да се приложи дупликат како замена за оригиналот. Правилното управување со и земање и чување на доказите од страна на стручно лице за компјутерска форензика ги поништува сите прашања и дилеми во однос на точноста. Заштитникот на доказите не треба да приложи сведочење од програмер, туку од сведок кој би опишал како информациите се обработуваат во компјутерот и како организацијата ги користи тие информации.

Кога станува збор за гласините (рекла-казала), голем дел од судовите во САД имале случаи на приговор кон претставување на компјутерски записи според исклучокот за деловни записи[15]. Овој пристап може да биде функционален за ревизорски записи доколку се во согласност со правилото, а што не мора да важи за компјутерски записи собрани како дел од истрага туку како резултат на повторлив периодичен процес. Во државата Хјустон (САД), судот ги смета за прифатливи записите кои се создадени посебно како поддршка на судски спор затоа што основните податоци се внесени во компјутерот како резултат на легитимни деловни цели и навремено.

Подолу се дадени насоки усвоени на Меѓународната конференција за високо-технички кривични дела во 1999 година во одбрана на прифатливоста на дигиталните докази.

- По земање на дигитален доказ, делувањето не треба да го менува тој доказ.
- Кога е неопходно некое лице да пристапи кон оригиналниот дигитален доказ, тоа лице мора да има компетенции од областа на форензика.
- Сите активности поврзани со земање, пристап, чување или пренос на дигитални докази мора целосно да бидат документирани, зачувани и достапни за преглед.

11) На пример, *U. S. v. Tank*, 200 F.3d 627 (9 th Cir. 2000); *Perfect 10 v. Cybernet Ventures*, No. CV012595LGB(SHX)2002 ILRWeb (P&F) 1411, 2002 WL 731721(U. S. D. C., C. D. CA, April 22, 2002); *U. S. v. Catabra,n* 836 F.2d 453,457 (9 th Cir. 1988); *U. S. v. Miller*, 771 F.2 nd 1219, 1237 (5 th Cir. 1985); *U. S. v. Yong Brothers, Inc*., 728 F.2d 682 (5 th Cir. 1984).

12) U. S. v. Liebert, 519 F.2d 542, 547 (3d Cir. 1975) cert. denied 423 U. S. 985 (1975).

13) U. S. v. Bonallo, 858 F.2nd 1427,1436 (9th Cir.1988).

14) Fed. R. Evid. 1002.

15) Fed. R. Evid. 803(6).

- Секој поединец е одговорен за сите дејствија кои ги презема во однос на дигиталните докази кога истите се во негово владеење.
- Секо орган одговорен за земање, пристап, чување или пренос на дигитални докази има одговорност за почитување на овие принципи.[16]

3. Проверка на автентичноста на дигиталните докази

Вообичаена постапка на судовите при утврдување на прифатливоста на доказите е да испитаат дали обновените докази се исти со оригинално одземените. Потребно е да се докаже нивната автентичност, а тоа значи дека треба да се докаже пред судот дека доказите се земени од одреден компјутер и/или локација, дека е земен комплетен и вистински примерок од дигиталниот доказ и дека истиот е непроменет од времето на негово земање. Понекогаш е потребно да се покаже дека одредени информации се вистинити и точни, на пример датуми кои се однесуваат на одредена датотека важна за одреден предмет. Тоа значи дека клучна улога во процесот на докажување автентичност игра доследноста на дигиталните докази.

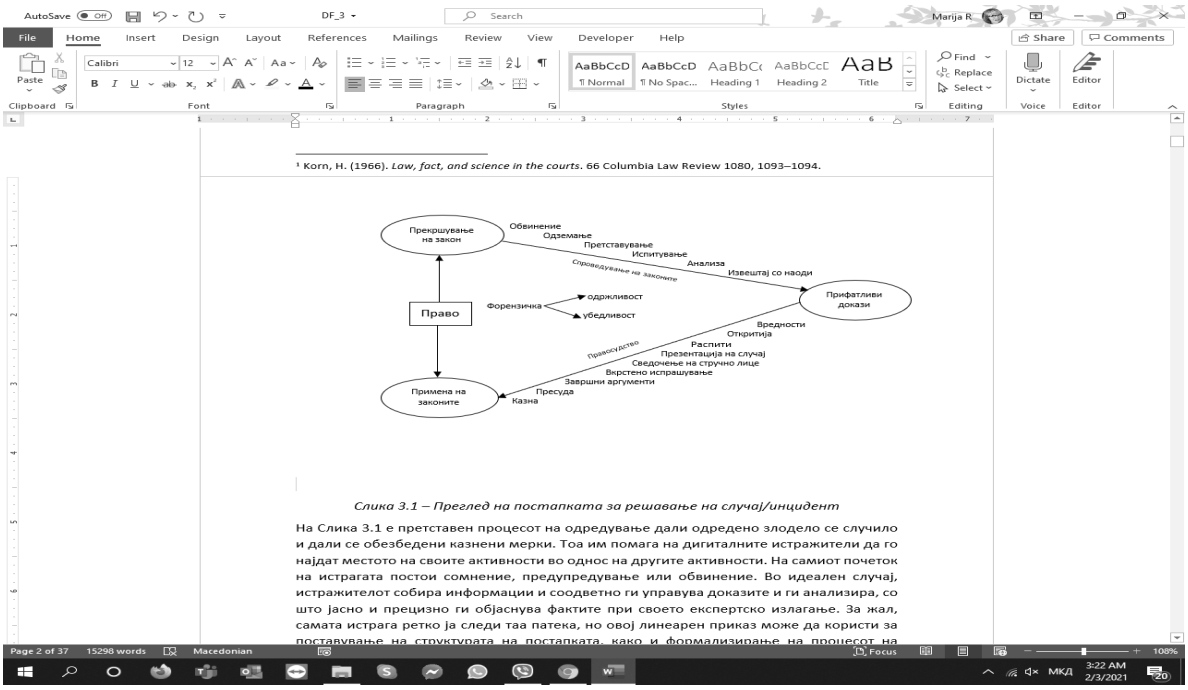
Документацијата на синџирот за чување и на интегритет на податоци е важен елемент за докажување на автентичноста на дигиталните докази. Соодветноста на истите укажува на тоа дека дигиталните докази се земени од одреден систем и/или локација и дека истите постојано се контролираат после земањето. Тоа значи дека соодветната документација овозможува поврзување на дигиталните докази од страна на судот во однос на кривичното дело, додека нецелосната документација може да доведе до неусогласеност во однос на изворот на добивање на доказите и со тоа се создаваат сомнежи за нивната веродостојност.

Интегритетот помага во докажување на фактот дека дигиталните докази не претрпеле никаква промена после нивното земање. Доколку се јави ситуација во која хеш вредностите на дигиталните докази се различни од оригиналните, може да се изолираат изменетите делови и да се потврдува само интегритетот на останатото. Пример за тоа може да биде ситуација во која лоши сектори од еден тврд диск влијаат на промената на пресметаната хеш вредност за дискот секогаш кога таа се калкулира. Со документирање на локацијата на лошите сектори, дигиталниот истражител може да одреди дали истите се наоѓаат во датотеки кои се од важност за предметот. Хеш вредностите на поединечни датотеки кои се од важност за предметот може да се споредуваат со оние кои се наоѓаат на оригиналниот тврд диск за да се обезбеди сигурност дека одредени датотеки не се засегнати со лош сектор.

За пионер во докажувањето на автентичноста на дигиталните докази може да го сметаме случајот САД против Тенк (United States v. Tank)[17] затоа што станува збор за еден од првите случаи во кој се работи за докажување автентичност на записи за разговор. И покрај тоа, сè уште се поставуваат прашања за автентичноста и доследноста на записите за разговорите на интернет. IRC (Internet Relay Chat), дополнително на прозорецот за разговор, дава и други важни информации како што се прозорец за статус и приватен разговор или прозорец за fserve. Еден истражител не може истовремено да ги отвори сите прозорци, па затоа дигиталните истражители се потпираат на записите во однос на тоа што се случило. Може да се случи истражителите да надоместат за недостатокот на документација преку сведочење дека приложените докази се автентични и доследни. Но, секако, најдобро би било кога тие би имале цврсто поткрепена документација.

Компаративно гледано, секоја од државите има пропишани правила во кои би можело да се вклопи и процесот со дигиталните докази. Вреднувањето на доказите се прави со соодветни норми за докази како што се Правилата за докази во САД, Законот за полиција и кривични докази и Законот за граѓански докази во Обединетото Кралство и слични такви нормативи во други земји. На пример, пред потврдување на доказите, судот најчесто проверува дали истите се релевантни и прави евалуација за одредување на соодветноста во однос на тужбата, дали станува збор за гласини (кажувања од други лица), погрешно пређудицирање и дали е потребен оригиналниот доказ или примерок од истиот е доволен за приказ. Неможноста да се обезбеди сето тоа може да придонесе кон отфрлање на доказите, а тоа би значело и можно губење на предметот/случајот.

16) Louis Strydom, *Computer Evidence*, 2nd World Conference on the Investigation of Crime, ICC Durban, Dec. 2001.
17) United States v. Tank. (1998). Appeals Court, 9th Circuit. Case Number 98-10001.



Слика 3.1 – Преглед на постапката за решавање на случај/инцидент

На Слика 3.1 е претставен процесот на одредување дали одредено злодело се случило и дали се обезбедени казнени мерки. Тоа им помага на дигиталните истражители да го најдат местото на своите активности во однос на другите активности. На самиот почеток на истрагата постои сомнение, предупредување или обвинение. Во идеален случај, истражителот собира информации и соодветно ги управува доказите и ги анализира, со што јасно и прецизно ги објаснува фактите при своето експертско излагање. За жал, самата истрага ретко ја следи таа патека, но овој линеарен приказ може да користи за поставување на структурата на постапката, како и формализирање на процесот на управување со случајот/предметот. Во реалноста/праксата, истрагата следи нелинеарен тек кој вклучува изведување основна анализа во фазата на собирање информации или враќање кон чекорот на собирање информации во случај кога анализата наведува на дополнителни докази.

Кога станува збор за фазата на собирање информации како дел од дигиталната истрага, многу е важно во тимот да има член кој лесно може да управува со дигитални докази, а со тоа се намалува и бројот на такви луѓе, на тој начин насочувајќи го претставувањето на случајот и намалувајќи ја можноста на одбраната да го оспорува интегритетот на доказите. Стандардните оперативни постапки, обуките и јасните процедури дополнително придонесуваат кон постојаноста на доказите и нивна заштита од контаминација. Јасно е дека дигиталните докази лесно може да се менуваат, па затоа постапката на нивно собирање е важна и не смее да се занемари фактот дека истите мора да се користат исклучиво од страна на соодветно обучен персонал кој би управувал и би ги прегледувал доказите.

Постојат многу сложени моменти кои се поврзани со приложувањето на доказите. Постапката на подготвување случај за на суд е временски исполнителна, но и скапа и можеби и нема да ги даде очекуваните задоволувачки резултати, особено во случај кога има недостиг на докази или кога доказите не се соодветно управувани. Организациите кои се дел од процеси со дигитални докази мора да размислат дали е неопходно да откриваат чувствителни информации за своите системи (на пример, мрежна типологија, системски конфигурации и извор на код за следење), како и други детали за своето работење кои не би сакале да бидат јавни.

Дополнително, доказите за постоењето на дигитални податоци (и што се случило со нив во текот на нивниот животен циклус) може да се најдат во табелата на главната датотека или друга операција за евидентирање што се одвива без знаење на корисникот. Дополнително, едноставното бришење или отстранување вообичаено не ги брише податоците, туку само го отстранува „покажувачот“ на податоците, а самите податоци остануваат достапни освен ако и додека не бидат презапишани (целосно или делумно) од новогенерирани податоци. Во мрежен систем, корисникот може да мисли дека ги брише податоците на работната станица, за подоцна да открие дека мрежниот сервер автоматски ги копира, архивира или прави резервна копија на сите

податоци генерирани од работната станица. Сепак, разликата помеѓу бришењето на податоците и ефемерната/преодната природа на податоците може најдобро да се објасни со претпоставката дека ефемерните дигитални податоци се однесуваат на пречката да се докаже постојаниот интегритет на податоците (некои технолози може да го опишат ова како докажување на „припадност"), наместо дали нивното постоење или непостоење. Оваа карактеристика треба да се земе предвид при одредување на веродостојноста

Дигиталните податоци се речиси целосно зависни од поткрепено сведочење кое има мала, или воопшто нема, врска со автентичноста на содржината за која се бара да се допушти. Критериумите за утврдување на допуштеноста на компјутерски генерираните информации мора, се предлага, да побаруваат прикажување зголемена веродостојност. Дополнително, тоа мора да се направи на начин што не ги отсликува само техниките за оценување физички докази.

Обврска и одговорност на експертите е да прикажат објективна непристрасна вистина за предметот пред судот. Тие никако не смеат да застапуваат која било од двете страни затоа што тој товар, таа обврска ја носат адвокатите. Подолу се дадени тврдења според Правилата за кривична постапка во Обединетото Кралство, а со кои се дефинираат обврските на експертите, и тоа:

1. Експертот треба да му помогне на судот да ја оствари најважната цел преку давање објективно непристрасно мислење за проблематиката во рамките на својата стручност.
2. Оваа обврска е над секоја обврска кон личноста од која се добиени информациите или личноста од која експертот е платен.
3. Оваа обврска вклучува и одговорност за информирање на сите засегнати страни и на судот во случај на промена на експертското мислење од она наведено во извештајот што служи како доказ или од она дадено како изјава.

Обврските на експертите може да се пренасочат под влијание на различни фактори, без разлика на нивните добри намери. Човечки е да се јават емоционални реакции, заштитнички предрасуди и други слични влијанија. Токму затоа ефективноста на дигиталниот иследник и експертскиот сведок треба да биде насочена кон самосвест и отпорност на влијанија како заземање страна, чувства и алчност. Подолу ќе ги разгледаме сите овие фактори кои може да влијаат врз ефикасноста на експертското работење.

4. Заклучок

Од дигиталните истражители се бара искреност и директност, а судовите се насочени кон обезбедување автентичност на приложените дигитални докази. Дополнително на релевантноста, доказите мора да исполнуваат и одредени стандарди, а со тоа треба да се запознаени лицата кои ги обработуваат доказите. Едноставно е да кажеме дека во домот на осомничениот е најдена крвава ракавица, но тоа треба да се докаже. Кога треба да се донесе одлука помеѓу вината или невиноста, потврдувањето на автентичноста на доказите е од исклучителна важност.

Дигиталната форензика е научна дисциплина која наоѓа своја примена при собирање на дигиталните докази кај бројни меѓународни организации, владини и невладини, за чија примена истите имаат усвоено бројни правни документи со цел да им дадат писмени процедура на своите вработени по кои треба да ја практицираат оваа научна дисциплина. Ние како држава сме формално членка на некои од нив, некои се организации чија политика треба да ја следиме согласно нашите стратешки определби, а некои се организации кои се наши оперативни партнери во многу правни дејанија. Во секој случај, насоките по кои овие правни субјекти ја дефинираат и практицираат дигиталната форензика се целосно, делумно или морално обврзувачки за нашето правосудство. Ако дојдеме до крајниот заклучок, а тоа е дека сите овие организации речиси на идентичен начин ја дефинираат и практицираат дигиталната форензика, тогаш јасно е дека ваквите правила се повеќе од било што плод на научна поткрепа. Самиот факт што, организација како ОЛАФ врши дигитална форензика за Европското јавно обвинителство,[18] фактот што сме земја членка на НАТО, фактот што сме во фаза на потпишување на договор за стратешко партнерство со САД, фактот што нашата иднина секако ја гледаме во рамките не Европската Унија и негувањето на европските вредности, безусловно треба да значи и можност за повикување на ваквите процедури, но и обврска за нашите правосудни органи да се водат од истите при нивното праворазадавање.

Наспроти сите овие споменати организации и правни акти, кај нас речиси и да не постои (а и реално не постои) правен акт, законски или подзаконски, со кој е уредена дигиталната форензика. Ова особено е погубно за правниот систем, затоа што немањето на процедури, дава огромна можност за самоволие од страна на т.н. дигитални форензичари, кои може и самите не се тоа, но

18) Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Anti - Fraud Office on CBIS Identity and Access Management System, Brussels, 30 June 2008 (Case 2008-223), достапно на https://edps.europa.eu/sites/default/files/publication/08-06-30_olaf_identity_access_system_en.pdf.

себеси така се нарекуваат, што особено негативно се одразува врз самиот процес во кривичната постапка, правејќи го незаконски.

Ние како држава, особено доколку би воделе правни предмети против странски државјани кои се граѓани на земји кои се членки на ЕУ или граѓани на САД, би дошле во ситуација однапред ја осудиме на пропаст ваквата правна неуреденост на дигиталната форензика и дигиталните докази, колку и да се или не се издржани во материјална смисла, од самиот старт ќе бидат незаконски прибавени.

Затоа не треба да измислуваме многу процеси кои веќе некој ги дефинирал до совршенство, како од содржински, така и од процесен аспект, само треба соодветно да се систематизираат и во вид на подзаконски акт да бидат донесени од соодветна институција.

Библиографија:

1. Louis Strydom, Computer Evidence, 2nd World Conference on the Investigation of Crime, ICC Durban, Dec. 2001.
2.Nance, K., B. Hay, M. Bishop. (2009) Digital Forensics: Defining a Research Agenda. 42nd Hawaii International Conference on System Sciences. Digital Forensics Research Track.
3. Nance, K., H. Armstrong, and C. Armstrong. (2010) Developing a Research Agenda to Improve Digital Forensics Education. Digital Forensics Minitrack of 43rd Hawaii International Conference on Systems Sciences.
4. Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Anti - Fraud Office on CBIS Identity and Access Management System, Brussels, 30 June 2008 (Case 2008-223), достапно на https://edps.europa.eu/sites/default/files/publication/08-06-30_olaf_identity_access_system_en.pdf.
5. Pollitt, M., K. Nance, B. Hay, et al (2008) Virtualization and Digital Forensics: A Research and Education Agenda. Journal of Digital Forensic Practice, 2 (2).