# ПРИМЈЕНА ДИГИТАЛНЕ ФОРЕНЗИКЕ У ОТКРИВАЊУ CYBER КРИМИНАЛА

Проф. др Душко Вејновић[1]
*Редовни професор Универзитета у Бањој Луци*
Славен Кнежевић, МА[2]
*Факултет политичких наука Универзитета у Бањој Луци*
*Економски факултет Универзитета у Бањој Луци*
*Правни факултет Универзитета у Бањој Луци*

**Апстракт**: *У раду се истражује кључна улога дигиталне форензике у идентификацији, анализи и превенцији сајбер криминала, који постаје све присутнија пријетња у савременом друштву. Дигитална форензика обухвата низ софистицираних метода и алата који омогућавају прикупљање, очување, анализу и представљање дигиталних доказа, неопходних за идентификацију починилаца и њихових метода. Рад анализира главне технике које се користе у дигиталној форензици, укључујући анализу мрежних протокола, прикупљање података са различитих дигиталних уређаја, као и дешифровање информација заштићених сложеним енкрипцијама. Посебна пажња посвећена је улози дигиталне форензике у откривању сајбер напада као што су ransomware, phishing и DDoS напади, који представљају озбиљне пријетње за појединце, компаније и државне институције. Поред техничких аспеката, рад разматра и изазове са којима се стручњаци за дигиталну форензику суочавају, укључујући брзе технолошке промијене, комплексност дигиталних трагова, али и правне препреке и етичке дилеме у погледу приватности и заштите података. Анализом конкретних случајева сајбер криминала и студија из праксе, рад настоји приказати како дигитална форензика може допринијети бржем и ефикаснијем откривању починилаца, као и како унапријеђење технолошких и методолошких капацитета у овој области може помоћи у превенцији будућих пријетњи. Рад нуди иновативна рјешења у овој области. Закључци истраживања указују на неопходност јачања дигиталне форензичке инфраструктуре и едукације стручњака, као и на потребу за међународном сарадњом како би се постигао ефикасан одговор на све комплекснији и глобалнији феномен сајбер криминала, што чини дигиталну форензику незамјењивим дијелом савремених безбједносних стратегија.*

**Кључне ријечи**: *дигитална форензика, cyber криминал, когнитивна форензика, квантна форензика, AI.*

## *ДИНАМИКА СИМБОЛИЧКОГ ОДНОСА ИЗМЕЂУ САЈБЕР КРИМИНАЛА И ДИГИТАЛНЕ ФОРЕНЗИКЕ: ЦИКЛУС АДАПТАЦИЈЕ И ИНОВАЦИЈЕ*

У савременом дигиталном добу, гдје су границе између стварног и виртуелног свијета све тање, појава сајбер криминала постала је свеприсутна пријетња, али и катализатор за развој дигиталне форензике. Умјесто да посматрамо дигиталну форензику искључиво као одговор на криминалне активности, неопходно је разумјети динамику симбиотског односа који се развио између ова два поља; овај однос се не своди на једноставан ланац акција и реакција, већ представља сложен и непрекидан циклус адаптације и иновације, гдје свака страна, сајбер криминалци и дигитални форензичари, подстиче другу на усавршавање и проналажење нових метода и техника. Сајбер криминалци, увијек у потрази за новим начинима да заобиђу постојеће безбједносне мјере и стекну незаконити корист, непрестано развијају нове и софистицираније технике напада. Овај стални притисак на безбједносне системе и инфраструктуру ствара потребу за брзом и

[1] Проф. др Душко Вејновић је редован професор на Шумарском факултету, Факултету политичких наука, Факултету физичког васпитања и спорта и Факултету безбједносних наука Универзитета у Бањој Луци. Е-маил: dusko.vejnović@sf.unibl.org

[2] Славен Кнежевић, МА је докторант Факултета политичких наука Универзитета у Бањој Луци, мастер студент Економског факултета Универзитета у Бањој Луци и мастер студент Правног факултета Универзитета у Бањој Луци. Е-маил: slaven.knezevic998@gmail.com

ефикасном реакцијом, што је и суштина дигиталне форензике. Суштински, кључно је да „сајбер криминал и дигитална форензика постоје у симбиотском односу, дијалектичком процесу гдје развој једног директно обликује развој другог. Ова константна интеракција између напада и одбране подстиче континуирано напредовање у оба домена." (Maras, 2016:33)

Дигитална форензика, са своје стране, не може остати статична - она мора константно да се развија и усавршава како би била у стању да открије, анализира и ефикасно одговори на све сложеније и лукавије методе које користе сајбер криминалци. Динамичка интеракција ствара један континуирани циклус иновација, у којем се свака страна труди да надмаши другу, стварајући тако стални притисак за напредак на оба поља. Динамична природа сајбер свијета „значи да сајбер криминалци непрестано унапријеђују своје технике како би избјегли откривање, што заузврат приморава форензичке стручњаке да иновирају свој приступ. Предочена динамика адаптације чини основу континуираног циклуса иновација." (Hsu & Lin, 2015:103) Почевши од самих почетака, када је сајбер криминал био релативно једноставан и лак за откривање, дигитална форензика је еволуирала, уводећи све сложеније технике за прикупљање, анализу и презентацију дигиталних доказа. Ипак, са сваким новим достигнућем у форензици, сајбер криминалци су брзо прилагођавали своје методе, развијајући технике које су теже за откривање и анализу. Стална игра мачке и миша довела је до непрекидног раста сложености и једног и другог поља. Сада, сајбер криминал више није једноставно нарушавање система или крађа података; он је постао комплетно оркестриран екосистем са мноштвом различитих метода и стратегија. Ту спадају *ransomware* напади, који паралишу комплетне организације и траже откуп за повратак података, *phishin* напади који манипулишу људима да открију осјетљиве информације, *DDoS* напади који циљају да оборе сервере и веб странице, као и бројни други приступи који циљају на различите рањивости у дигиталном простору. Са друге стране, дигитална форензика је прихватила ове изазове и одговорила им развојем напредних метода и техника. Анализа мрежних протокола, прикупљање података са различитих уређаја, дешифровање енкрипције и виртуелизација оперативних система, све су то алати које користе форензичари у борби против сајбер криминала. Штавише, форензичари све више користе вјештачку интелигенцију и машинско учење како би побољшали своју ефикасност у анализи огромних количина података и откривању суптилних образаца који би могли указивати на криминалну активност. Занимљиво је посматрати како се форензичке технике у процесу развоја „оружавају". То значи да се оне не користе само за откривање и рјешавање кривичних дјела, већ се све чешће користе за превенцију и предвиђање будућих напада. На примјер, анализом велике количине података о претходним нападима, форензички алати могу да идентификују потенцијалне рањивости и да упозоре организације на могуће пријетње. Превентивна улога дигиталне форензике постаје све важнија у свијету у којем су сајбер напади све чешћи и све софистицираниji.

Међутим, сајбер криминалци нису само нијеми посматрачи - они такође активно прате развој форензичких техника и уче из њих. На тај начин они покушавају да развију методе које ће бити теже за откривање или које ће им омогућити да се сакрију у дигиталној позадини. На примјер, користе се напредне технике енкрипције, програми за брисање података и анонимне мреже како би се замаскирали и прикрили своје трагове. Штавише, сајбер криминалци користе стечено знање о форензичким алатима како би подметнули лажне доказе или дезинформисали истражитеље. Овакав аспект симбиотског односа је често занемарен, али је кључан за разумијевање циклуса адаптације и иновације. На примјер, у раним данима дигиталне форензике, форензичари су се углавном ослањали на анализу лог датотека и тражили уобичајене обрасце напада. Како су сајбер криминалци постали свјесни ових техника, почели су да бришу лог датотеке или да мијењају њихов садржај, што је за форензичаре стварало нове изазове. Сада форензичари морају да се ослањају на напредније технике, као што су анализа меморије, експлоатација рањивости и коришћење вјештачке интелигенције како би открили и најсуптилније трагове криминалне активности. Указани примјер је један од многих, и он показује како се циклус адаптације и иновације одвија у континуитету. Оно што је некада било рјешење постаје касније проблем, а онда се опет проналази рјешење за тај нови проблем. Кључ разумијевања динамике овог односа лежи у препознавању да се овај циклус не завршава. Умјесто да једноставно реагују на сајбер криминал, форензичари морају бити проактивни и предвиђати будуће трендове. То значи да морају бити у току са најновијим технолошким достигнућима, али и да разумију

мотивације и стратегије сајбер криминалаца. Са друге стране, сајбер криминалци морају бити свјесни ризика од откривања и да се стално прилагођавају новим форензичким техникама. Ова непрекидна ”трка у наоружању” је оно што покреће развој оба поља, што ствара стални притисак за иновацијама. Константна еволуција технологије је „мотор који покреће и сајбер криминал и дигиталну форензику. Како криминалци развијају нове методе, форензичка наука мора да се прилагоди и иновира како би држала корак. Ово је континуирана игра мачке и миша без краја на видику.” (Casey, 2011:78) Један од највећих изазова за дигиталну форензику је растућа количина података и сложеност дигиталних трагова. Како се технологија развија, ствара се све више дигиталних података, који су често раштркани на различитим уређајима и платформама. Интеракција између нападача и бранилаца у сајберпростору „ствара стални циклус акције и реакције, захтијевајући константну иновацију и адаптацију на обје стране. Нападачи увијек траже нове рањивости, док браниоци морају континуирано да развијају своју одбрану како би се супротставили тим пријетњама.” (Skoudis & Liston, 2002:118)

Форензичари морају бити у стању да прикупе, анализирају и разумију ове податке у разумном временском року, што је све тежи задатак како се обим података повећава. Штавише, сајбер криминалци користе све софистицираније технике за скривање и манипулацију дигиталним траговима, што додатно отежава форензичке истраге. Други изазов је брзина технолошких промјена. Нове технологије, као што су вјештачка интелигенција, блокчејн и интернет ствари, стварају нове могућности за сајбер криминал, али и нове изазове за дигиталну форензику. Форензичари морају бити спремни да се адаптирају на ове промјене и да развију нове технике за откривање и анализу ових нових облика криминала. Поред техничких изазова, постоје и правне и етичке дилеме у вези са дигиталном форензиком. Прикупљање и анализа дигиталних доказа често укључују питања о приватности и заштити података, а форензичари морају бити свјесни ових питања и да раде у складу са законом и етичким принципима - ово је посебно важно у свијету у коме се све више ослањамо на дигиталне технологије у свакодневном животу. Да би се ефикасно супротставили сајбер криминалу, форензичари морају бити не само технички стручни, већ и свјесни правних и етичких импликација свог рада. Управо из ових разлога, међународна сарадња је од кључног значаја.

Сајбер криминал не познаје границе и захтијева заједничке напоре да се са њим суочи. Размјена информација и ресурса, заједничко спровођење истрага и усаглашавање правних оквира, све су то важни кораци у борби против сајбер криминала. Штавише, улагање у образовање и обуку стручњака за дигиталну форензику је од пресудног значаја. Све више људи мора да буде оспособљено за рад на овом пољу како би се ефикасно борило против сајбер криминала. Пејзаж дигиталне форензике се брзо мијења „због ширења технологије и све веће софистицираности сајбер злочина. То захтијева континуирани циклус учења, адаптације и иновација како би се одржала способност спровођења ефикасних истрага.” (Yadav & Singh, 2016:145) Динамика симбиотског односа између сајбер криминала и дигиталне форензике представља један комплексан и континуиран циклус адаптације и иновације. Не само да је сајбер криминал катализатор за развој дигиталне форензике, већ и дигитална форензика подстиче сајбер криминалце на усавршавање својих метода и приступа. Представљена непрекидна интеракција и трка у наоружању захтијева од оба поља константно усавршавање и прилагођавање.

У будућности, очекује се да ће се овај циклус само убрзавати, чиме ће дигитална форензика играти све значајнију улогу у заштити дигиталног свијета. Да би се ефикасно супротставили сајбер криминалу, неопходно је не само разумјети динамику овог односа, већ и активно радити на унапријеђењу форензичких техника, јачању међународне сарадње и улагању у образовање и обуку стручњака. У супротном, сајбер криминал ће наставити да представља све већу пријетњу за све нас. Важно је нагласити да дигитална форензика није само алатка за откривање и рјешавање кривичних дјела, већ и за превенцију и предвиђање будућих напада. Користећи напредне технике анализе података и вјештачку интелигенцију, дигитална форензика може да помогне организацијама да пронађу потенцијалне рањивости и да се припреме за могуће пријетње. Проактивна улога дигиталне форензике постаје све важнија у свијету у коме су сајбер напади све чешћи и све софистицираниј. Управо зато, континуирано улагање у развој дигиталне форензике и њено

усавршавање је неопходност за одржавање безбједности и интегритета дигиталног свијета. Сајбер криминал и дигитална форензика, иако су супротстављени, у ствари су нераздвојни партнери у овом динамичном и све сложенијем дигиталном окружењу. Њихова симбиоза ће наставити да обликује и покреће развој оба поља у годинама које долазе. Дигитална форензика је „истраживачко подручје гдје се технологија развија великом брзином. Ово захтијева да област буде у току са свим новим техникама које користе криминалци и да буде у стању да прилагоди технике за нове технологије." (Palmer, 2001:28) Област дигиталне форензике је „константно изазвана новим технологијама и новим методама извршавања компјутерских злочина, што захтијева флексибилан, скалабилан и прилагодљив оквир за ефективне истраге." (Bebbe & Clark, 2005:155)

## *КОГНИТИВНА ФОРЕНЗИКА*

У савременом дигиталном добу, гдје се све више ослањамо на технологију у готово сваком аспекту живота, дигитална форензика је постала незаобилазан елемент у борби против сајбер криминала и других кривичних дјела. Међутим, иако се дигитална форензика често доживљава као строго техничка дисциплина, не сме се занемарити кључна улога људског фактора у процесу анализе дигиталних доказа. Форензика „по мишљењу правника и лингвисте Питера Тирзме (*Piter Tiersma*), не могу се ограничити смао на решавање кривичних дјела, зато што форензичку експертизу може користити и одбрана у кривичним случајевима." (Николић-Новаковић, 2017:26) Управо је то мјесто гдје на сцену ступа „когнитивна форензика", као нова, али све значајнија перспектива у овом пољу. Поље когнитивне форензике „мора да се суочи са бројним критичним изазовима: недостатком стандардног протокола, недостатком свијести међу форензичким практичарима и проблемима у обуци. Стога, будућа истраживања треба да теже прецизнијем разумијевању како когнитивни фактори утичу на доношење одлука, уз активно превођење научног знања у практичне, оперативне стратегије, као што су структурирано извјештавање и алати за подршку стручњацима у одлучивању." (Itiel & Tauber, 2019:982) Когнитивна форензика, која је још увијек релативно мало истражено подручје, скреће пажњу на утицај људског ума на процес анализе дигиталних доказа. Истражује како когнитивне пристрасности, стрес, умор и други психолошки фактори могу утицати на начин на који дигитални форензичари тумаче доказе и доносе закључке. Умјесто да се фокусира искључиво на техничке аспекте дигиталне форензике, когнитивна форензика наглашава важност разумијевања људске психе и њених могућих пропуста у процесу одлучивања. Залаже се за развој оквира који укључује технике за ублажавање негативних ефеката когнитивних пристрасности и других психолошких фактора, како би се осигурала већа тачност и објективност у анализи дигиталних доказа. Когнитивне пристрасности представљају један од највећих изазова у дигиталној форензици. Људски ум је склон да обрађује информације на начин који је под утицајем претходних искустава, увјерења и очекивања. Да би се „побољшала валидност и поузданост форензичке науке, мора се примјенити когнитивна психологија. Ово укључује дизајнирање робуснијих и стандардизованих процедура, развијање програма обуке који се фокусирају на стратегије за ублажавање когнитивних пристрасности и наглашавање холистичког приступа форензичким анализама, а не приступа који је искључиво усмјерен на техничке аспекте." (Lynch & Cooper, 2020:1540)

Пристрасности могу довести до нетачних тумачења доказа и до погрешних закључака, чак и када су сами докази објективни. На примјер, потврда пристрасности, односно тенденција да се обрати више пажње на доказе који подржавају претходно створене хипотезе, може навести форензичара да занемари или подцијени доказе који су у супротности са његовим или њеним унапред створеним увјерењима. Пристрасност може посебно бити опасна у ситуацијама када су улози велики, јер форензичари могу несвјесно да искривљују чињенице како би се уклопиле у њихова очекивања. Друга когнитивна пристрасност која може утицати на дигиталну форензику је доступност пристрасности, што представља тенденцију да се обрати више пажње на информације које су лакше доступне или се лакше памте - ова пристрасност може навести форензичаре да превише ослањају на недавне случајеве или на доказе који су им лакше доступни,

док занемарују важне информације које су теже доступне или које су мање уобичајене. На примјер, форензичар који је недавно радио на случају *ransomware* напада може бити склон да тражи трагове истог типа напада у новом случају, чак и ако су докази указују на другу врсту криминалне активности. Трећа когнитивна пристрасност која је важна у форензици је „ефекат усидрења", што је тенденција да се превише ослањамо на прве информације које добијемо. Таква пристрасност може навести форензичаре да се фиксирају на почетну хипотезу или траг, занемарујући алтернативне могућности и друге релевантне информације. На примјер, ако форензичар добије почетни извјештај који указује на конкретног осумњиченог, он или она могу бити склони да превиде доказе који би могли указивати на другог кривца. Поред когнитивних пристрасности, стрес и умор такође могу значајно утицати на рад дигиталних форензичара. Рад у дигиталној форензици често је под великим притиском, са роковима и високим улозима, што доводи до значајног стреса и изгарања. Стрес може нарушити пажњу, концентрацију и способност доношења исправних одлука, што доводи до грешака у анализи дигиталних доказа. Умор, који често прати стрес, такође може значајно смањити когнитивне способности форензичара. Уморни форензичари могу бити склони пропуштању важних детаља, лошим интерпретацијама доказа и доношењу погрешних закључака. Штавише, умор може повећати вјероватноћу да форензичари подлегну когнитивним пристрасностима. Експертиза „не имунизује од когнитивних пристрасности, а разне пристрасности могу утицати на форензичко доношење одлука. Оне се крећу од потврдне пристрасности, гдје очекивања утичу на закључке, до контекстуалних утицаја, гдје наизглед небитне информације изобличују интерпретације. Боље разумијевање људске подложности грешкама је кључно у било ком форензичком процесу." (Dror, 2020:312)

Један од кључних аспеката когнитивне форензике је развој оквира који ће омогућити ублажавање негативних ефеката когнитивних пристрасности, стреса и умора; овај оквир треба да укључује технике и стратегије које ће форензичарима помоћи да доносе објективније и тачније одлуке. Једна од важних техника је подизање свијести о когнитивним пристрасностима. Обучавајући форензичаре о различитим типовима пристрасности и њиховом утицају на доношење одлука, може се смањити вјероватноћа да форензичари подлегну овим пристрасностима. Обука треба да буде редовна и континуирана како би форензичари остали свјесни својих потенцијалних пропуста. Поред свијести о пристрасностима, форензичари треба да користе структуриране методе анализе. Структурирани методологије, као што су аналитички протоколи и контролне листе, могу помоћи у смањењу утицаја субјективних фактора на процес анализе; ови методи обезбјеђују стандардизован приступ анализи дигиталних доказа, осигуравајући да се сви релевантни докази узимају у обзир и да се смањује вјероватноћа да ће се форензичари ослањати на пречице или претпоставке. Друга важна техника је коришћење рецензија и консултација. Прегледом рада других форензичара може се идентификовати и исправити грешке или пристрасности; овај процес међусобне провјере може помоћи у повећању тачности и објективности форензичких истрага. Консултације са другим стручњацима, укључујући психологе и когнитивне научнике, такође могу бити веома корисне у идентификовању потенцијалних пропуста у процесу анализе. Поред ових техника, важно је створити радно окружење које смањује стрес и умор. Форензичари треба да имају довољно времена за одмор и одмор, као и да имају приступ ресурсима за управљање стресом. Организације треба да буду свјесне важности добробити својих запослених и да обезбиједе услове који подржавају здравље и продуктивност.

Такође је важно обратити пажњу на дизајн софтвера и алата које форензичари користе јер ови алати треба да буду кориснички прилагођени и да олакшавају процес анализе, а не да га отежавају. На примјер, алати треба да буду дизајнирани на такав начин да смањују вјероватноћу грешака и пропуста, и да пружају јасне визуелне представе података. Когнитивна форензика, дакле, представља значајан корак напред у разумијевању сложености дигиталне форензике. Признавањем утицаја људског фактора на процес анализе, когнитивна форензика може помоћи у повећању тачности и објективности форензичких истрага. Развојем оквира за ублажавање негативних ефеката когнитивних пристрасности, стреса и умора, можемо осигурати да дигитална форензика игра све ефикаснију улогу у борби против криминала и у проналажењу правде. Поред практичних техника за ублажавање когнитивних пристрасности, истраживање у области когнитивне форензике треба да укључи дубље разумијевање когнитивних процеса који су укључени у анализу

дигиталних доказа, а то укључује истраживање о томе како форензичари обрађују информације, како доносе одлуке, и како се њихове перцепције формирају. Са дубљим разумијевањем ових процеса, може се развити ефикаснија обука и методи за унапријеђење форензичке праксе. Занимљив аспект когнитивне форензике је и утицај културе и социоекономског статуса на анализу дигиталних доказа. Људи различито перципирају информације и имају различите когнитивне моделе и склоности, што може утицати на њихову интерпретацију доказа. Истраживање о овим разликама може помоћи у стварању инклузивније и праведније дигиталне форензике. Поред тога, у когнитивној форензици треба размотрити и питање етике. Дигитални форензичари имају велику одговорност, јер њихов рад може директно утицати на животе људи. Због тога, неопходно је да форензичари буду свјесни етичких импликација свог рада и да се придржавају највиших стандарда интегритета и професионализма. Познати свјетски стручњаци закључују „наши налази сугеришу да емоционално стање форензичких практичара (тј. осјећај више или мање убеђености у кривицу осумњиченог) може имати значајан утицај на њихово доношење одлука и може довести до различитих интерпретација истих доказа." (Ask & Granhag, 2007:28) Такође, тврде и да „мета-анализа показује да контекстуалне информације могу значајно промјенити одлуке форензичких испитивача, што сугерише да су процедуралне заштите неопходне за минимизирање пристрасности." (Cooper & Brewer, 2013:803)

Когнитивна форензика није само академска дисциплина, већ и практично поље са великим потенцијалом за побољшање правосудног система. Разумијевањем когнитивних изазова у форензици, можемо осигурати да форензичари доносе тачније и објективније одлуке, што ће помоћи у проналажењу правде и заштити невиних. Зато је неопходно да се когнитивна форензика развија и усавршава, и да се њене методе и принципи укључе у форензичку праксу. Коначно, треба нагласити да когнитивна форензика није замјена за техничку стручност у дигиталној форензици: оба аспекта су кључна за успјешан рад у овом пољу. Когнитивна форензика се надовезује на техничку стручност и обезбјеђује неопходни људски контекст у анализи дигиталних доказа; она скреће пажњу на важност разумијевања људских пропуста и помагање форензичарима да доносе боље одлуке. Управо та комбинација техничке стручности и когнитивне свијести представља будућност дигиталне форензике. У закључку, когнитивна форензика је ново, али веома значајно поље истраживања које пружа дубље разумијевање утицаја људског фактора на анализу дигиталних доказа. Когнитивне пристрасности, стрес, умор, и други психолошки фактори значајно утичу на доношење одлука форензичара.[3]

Развој оквира за ублажавање ових негативних ефеката, кроз технике као што су подизање свијести о пристрасностима, коришћење структурираних метода анализе, рецензије и консултације, као и стварање радног окружења које смањује стрес и умор, представљају неопходне кораке ка унапријеђењу дигиталне форензике. Когнитивна форензика нас подсјећа да је форензика ипак и људска дјелатност, те да улагање у разумијевање когнитивних процеса, људских склоности и ограничења може побољшати процес доказивања и да допринесе проналажењу правде. Развојем овог поља, може се осигурати већа тачност и објективност у дигиталној форензици, чиме се повећава њена улога у борби против криминала и у заштити друштва. Имплементација когнитивне форензике „није лака, она захтијева вишеслојан приступ, као и спремност форензичких научника, правних стручњака и научне заједнице да промјене своју перспективу и укључе ове нове методе у стандардну праксу. Не постоји брзо рјешење, и захтијева вријеме, обуку и посвећеност." (Stoel *at al.*, 2019:218) Когнитивна форензика је, стога, не само теоријска, већ и практична дисциплина са великим потенцијалом за позитивну промјену; она је неопходна како би се осигурало да правосудни систем буде праведан и да се пресуде доносе на основу поузданих доказа и објективних процјена. Управо је то будућност дигиталне форензике и у њу треба улагати сву пажњу.

[3] За више информација видјети: Miller, L. S. (2016). *Stress management in law enforcement*. Charles C Thomas Publisher. Van Dongen, H. P. A., Maislin, G., & Dinges, D. F. (2003). *Individual differences in sleep, alertness, and cognitive performance following sleep deprivation*. Journal of Sleep Research, *12*(3), 185–196.

У савремено доба, гдје се технологија развија брзином која превазилази наша очекивања, дигитална форензика, као кључни стуб борбе против сајбер криминала и других злоупотреба, налази се пред новим изазовима и етичким дилемама, па тако „примјена вјештачке интелигенције у дигиталној форензици захтијева пажљиво разматрање њеног потенцијалног утицаја на основна права као што су приватност и слобода изражавања." (Floridi et al., 2018:696) Увођење вјештачке интелигенције (AI) и машинског учења (ML) у дигиталну форензику доноси револуционарне промјене, нудећи нове могућности за бржу и ефикаснију анализу дигиталних доказа, али истовремено отварајући врата за нове облике злоупотреба и етичких проблема. Вјештачка интелигенција и машинско учење доносе значајне промјене у дигиталну форензику, пружајући нове могућности за аутоматизацију процеса анализе, обраду огромних количина података и откривање сложених образаца и аномалија који би промакли људском оку.

На примјер, AI алгоритми се користе за аутоматско претраживање и индексирање дигиталних доказа, брзо и ефикасно идентификујући релевантне информације у великим количинама података. Исто тако „AI алгоритми који се користе у дигиталној форензици склони су пристрасностима ако подаци за тренирање одражавају постојеће друштвене пристрасности. Ово може довести до неправедних или нетачних исхода у истрагама." (Barocas & Selbst, 2016:698) ML алгоритми, са друге стране, могу се користити за откривање суптилних обраца и аномалија који би могли указивати на криминалну активност, као што су необични саобраћај на мрежи, сумњиве трансакције или скривене датотеке. Предочено омогућава форензичарима да се фокусирају на сложеније задатке, а AI и ML преузимају рутинске и временски захтјевне процесе. Један од кључних позитивних аспеката AI у форензици је његова способност да брзо анализира огромне количине података. У савременом дигиталном свијету, форензичари се често суочавају са терабајтима и петабајтима података, што је практично немогуће обрадити ручно. AI и ML алгоритми могу ефикасно претраживати ове податке, идентификовати релевантне информације и приказивати их форензичарима на јасан и прегледан начин и управо то омогућава форензичарима да брже дођу до кључних доказа и да ефикасније ријеше сложене случајеве. Други позитиван аспект је способност AI и ML да откривају суптилне обрасце и аномалије које би промакле људском оку. ML алгоритми могу се обучити да препознају специфичне обрасце криминалне активности, као што су специфични типови малвера, сумњиви саобраћај на мрежи или необичне трансакције што директно помаже форензичарима да брже идентификују криминалну активност и да је спријече у будућности. Међутим, иако AI и ML нуде значајне предности у дигиталној форензици, они такође доносе нове етичке импликације и проблеме који захтијевају пажљиво разматрање.

Један од највећих етичких проблема је потенцијална пристрасност AI система. AI и ML алгоритми се обучавају на великим скуповима података, а ако су ти подаци пристрасни, то ће се одразити и на рад AI система. На примјер, ако је AI систем обучен на подацима који показују да одређена етничка група чешће врши одређене врсте кривичних дјела, он може бити пристрасан при анализи доказа и може погрешно повезати људе из те групе са криминалним активностима. Таква врста пристрасности може имати озбиљне посљедице, посебно у кривичним поступцима, гдје може довести до погрешних осуда. Други етички проблем је могућност манипулације доказима помоћу AI и ML. AI алгоритми се могу користити за стварање лажних дигиталних доказа, укључујући лажне слике, видео записе и аудио записе. Технологија "***deep fake***", која користи AI за стварање реалистичних, али лажних медијских садржаја, представља посебан изазов за дигиталну форензику, а ови "***deep fake***" докази могу се користити за подметање лажних информација, стварање конфузије и манипулацију јавним мњењем, што може имати озбиљне посљедице у кривичним истрагама, политичким процесима и другим областима. Трећи етички проблем је злоупотреба AI алата од стране криминалаца. Криминалци могу користити AI и ML за развијање нових и софистицираних облика сајбер напада, за прикривање својих трагова и за манипулисање форензичким истрагама. На примјер, AI се може користити за аутоматизацију фишинга, за креирање малвера који је теже открити или за маскирање дигиталних трагова, а то представља велики изазов за дигиталну форензику, која мора бити у стању да одговори на ове нове и еволуирајуће пријетње. Четврти етички проблем је питање одговорности и

транспарентности. Ако AI систем направи грешку у анализи дигиталних доказа, ко је одговоран? Да ли је одговорност на програмерима AI система, на форензичарима који користе тај систем или на организацији која је одговорна за његово одржавање? Колико су AI системи транспарентни и разумљиви? Да ли форензичари разумију како AI системи доносе одлуке и да ли могу да верификују њихове резултате? Ова питања су кључна за стварање одговорне и транспарентне дигиталне форензике. Пети етички проблем је питање приватности. AI системи често прикупљају и обрађују велике количине личних података, укључујући осјетљиве информације. Како се осигурава приватност ових података и како се спријечава њихова злоупотреба? Које су границе прикупљања и обраде личних података у дигиталној форензици? Ова питања су посебно важна у свјетлу растуће забринутости око приватности и заштите личних података. Поред ових етичких проблема, постоје и правне импликације које се односе на употребу AI у дигиталној форензици. Како ће судови третирати AI доказе? Како ће се процјенити поузданост и тачност AI система? Да ли ће AI докази имати исту тежину као традиционални дигитални докази? Предочена питања захтијевају пажљиво разматрање и усаглашавање правних оквира са технолошким развојем. Да би се суочили са овим изазовима, неопходно је развити етички оквир за употребу AI у дигиталној форензици - овај оквир треба да укључује скуп принципа и смјерница које ће форензичари слиједити приликом примјене AI и ML технологија.

Један од кључних принципа треба да буде принцип транспарентности. AI системи треба да буду разумљиви и објашњиви, како би форензичари могли да верификују њихове резултате и да разумију како они доносе одлуке. Принцип одговорности је такође важан. Треба јасно дефинисати ко је одговоран за рад AI система и за посљедице његових одлука. Принцип правичности је неопходан. AI системи не смију бити пристрасни и треба да се примјењују на правичан начин, без дискриминације. Принцип заштите приватности је кључан. Лични подаци треба да се прикупљају и обрађују у складу са законом и са поштовањем приватности. Принцип професионализма такође треба да буде укључен, како би се осигурало да се AI и ML користе на етички и одговоран начин. Поред етичког оквира, неопходно је развити и техничке и методолошке стратегије за ублажавање етичких проблема. На примјер, развијање техника за откривање пристрасности у AI алгоритмима и за побољшање њихове транспарентности, стварање алата за детекцију „*deep fake*" доказа, развијање метода за одбрану од криминалне злоупотребе AI, и на крају, развијање стандарда и протокола за верификацију AI доказа, представљају кључне кораке у осигуравању етичне и поуздане дигиталне форензике у ери AI. Неопходно је нагласити да одговорност за етичку употребу AI у дигиталној форензици не лежи само на форензичарима, већ и на програмерима AI система, на истраживачким институцијама, на законодавцима и на цјелокупном друштву. Сви морамо бити свјесни етичких импликација AI и ML и активно радити на стварању система који су поуздани, правични и одговорни. Поред тога, етичка употреба AI у дигиталној форензици захтијева континуирану едукацију и обуку форензичара; они треба да буду оспособљени за рад са AI системима, да разумију њихове предности и ограничења, као и да буду свјесни етичких дилема које се могу појавити. Едукација треба да буде усмјерена не само на техничке аспекте AI, већ и на етичке и правне импликације. Такође је важно развити међународне стандарде и протоколе за употребу AI у дигиталној форензици. Употреба вјештачке интелигенције у „аутоматизованом доношењу одлука у дигиталној форензици покреће питања одговорности и задужења. Кључно је успоставити јасне линије одговорности када алгоритми доносе критичне одлуке у вези са кривичним истрагама." (Mittelstadt *et al*., 2016:952)

Сајбер криминал не познаје границе, па је међународна сарадња кључна за борбу против њега. Усаглашавање стандарда и протокола може помоћи у осигурању да се AI користи на етички и одговоран начин у свим земљама. Увођење AI и ML у дигиталну форензику доноси револуционарне промјене, нудећи нове могућности за ефикаснију анализу дигиталних доказа, али истовремено отварајући врата за нове етичке изазове и проблеме. Потенцијална пристрасност AI система, могућност манипулације доказима, злоупотреба AI алата од стране криминалаца, питања одговорности и транспарентности, као и питање приватности, представљају кључне етичке проблеме које морамо пажљиво размотрити. Развој етичког оквира, техничких и методолошких стратегија, континуирана едукација и међународна сарадња су неопходни кораци ка стварању етичне, поуздане и праведне дигиталне форензике у ери AI. Управо је то будућност коју морамо заједно стварати.

## *РЕЗУЛТАТИ ИСТРАЖИВАЊА*

На основу претходних истраживања о динамици симбиотског односа између сајбер криминала и дигиталне форензике, когнитивној форензици и етици дигиталне форензике у ери AI, могу се извести иновативни и несвакидашњи резултати истраживања који би могли значајно унаприједити ову област, а ови резултати, научно комплексни и популарни, савјетодавни и примјењиви у пракси, имају за циљ да пруже нове перспективе и рјешења у борби против сајбер криминала и обезбјеђивању праведности у дигиталном свијету.

Први иновативни резултат истраживања се односи на развој концепта „адаптивне форензике". Умјесто да се ослањамо на статичне и претходно дефинисане методе, адаптивна форензика користи AI и ML да аутоматски прилагођава своје приступе и технике на основу динамике криминалних активности. Овај приступ подразумијева континуирано праћење развоја сајбер криминала и промјену форензичких стратегија у реалном времену. На примјер, ако се идентификује нови тип малвера, адаптивна форензика аутоматски генерише нове алгоритме за детекцију и анализу тог малвера, умјесто да чека развој нових метода од стране људи - овај концепт подразумијева и коришћење AI за предвиђање будућих трендова у сајбер криминалу, што омогућава форензичким тимовима да се проактивно припремају за предстојеће изазове. Адаптивна форензика, дакле, не само да реагује на криминалне активности, већ их и предвиђа и спријечава, што је значајан корак напред у односу на тренутне форензичке праксе.

Други иновативни резултат истраживања се фокусира на развој „когнитивно-интелигентних форензичких алата"; ови алати, на основу принципа когнитивне форензике, не само да аутоматизују процес анализе, већ и активно помажу форензичарима у ублажавању когнитивних пристрасности. На примјер, алат може аутоматски генерисати више хипотеза о могућим криминалним сценаријима, представљајући их форензичарима на објективан начин, без утицаја потврде пристрасности. Такође, алат ће идентификовати и сигнализирати могуће когнитивне пристрасности на основу форензичаревог начина размишљања и тумачења доказа. Штавише, когнитивно-интелигентни алати могу користити машинско учење да анализирају претходне форензичке случајеве, идентификују уобичајене пропусте и грешке, и пруже форензичарима персонализоване препоруке за унапријеђење њиховог рада; ови алати не само да побољшавају тачност и објективност форензичких истрага, већ и смањују утицај стреса и умора на рад форензичара.

Трећи иновативни резултат истраживања се односи на развој „етички провјерених AI форензичких система". Односни системи, на основу принципа етике дигиталне форензике у ери AI, користе напредне методе за провјеру своје сопствене пристрасности и транспарентности. Системи се обучавају на пажљиво одабраним скуповима података, који су провјерени на могућу пристрасност, и редовно се тестирају како би се осигурала њихова правичност. Штавише, системи користе алгоритме који су објашњиви и разумљиви, што омогућава форензичарима да прате њихов процес одлучивања и да провјере њихове резултате; ови системи, такође, посједују механизме за заштиту приватности, како би се осигурало да се лични подаци прикупљају и обрађују у складу са законом и етичким принципима. Етички провјерени AI форензички системи, дакле, не само да су ефикасни у анализи дигиталних доказа, већ су и поуздани, правични и одговорни, што је од кључног значаја за одржавање повјерења у правосудни систем.

Четврти иновативни резултат истраживања је концепт „виртуелне форензичке лабораторије". Таква лабораторија је виртуелно окружење које симулира различите форензичке сценарије, укључујући различите типове сајбер напада и дигиталне уређаје. Форензичари могу да користе ову лабораторију да тренирају и тестирају нове форензичке технике у контролисаном окружењу, без ризика од угрожавања правих система. Штавише, лабораторија омогућава форензичарима да испитају различите хипотезе и сценарије, без ограничења у реалном свијету. У виртуелној лабораторији се такође може тестирати ефикасност AI форензичких система, откривати и исправати потенцијалне пропусте, што доприноси унапријеђењу њихове поузданости и тачности. Виртуелна форензичка лабораторија је, дакле, не само алатка за обуку и тестирање, већ и за истраживање и иновације у области дигиталне форензике.

Пети иновативни резултат истраживања се односи на развој „глобалне платформе за размјену форензичких информација" - ова платформа омогућава форензичарима из цијелог свијета да размјењују информације, искуства и најбоље праксе, што помаже у борби против сајбер криминала који не познаје границе. Платформа користи AI и ML за аутоматску анализу форензичких извјештаја, идентификовање нових трендова и пријетњи, и проактивно упозоравање на потенцијалне ризике. Платформа такође обезбјеђује безбједну комуникацију и сарадњу између форензичара, што омогућава ефикасније истраге и брже рјешавање кривичних случајева. Глобална платформа за размјену форензичких информација је, дакле, не само алатка за сарадњу, већ и за унапријеђење форензичке праксе на глобалном нивоу.

Шести иновативни резултат истраживања је концепт „квантне форензике". Увођење квантних рачунара и квантних технологија доноси нове изазове и могућности у дигиталној форензици. Квантни рачунари, због своје огромне рачунарске моћи, могу пробити све постојеће енкрипције, што захтијева развој нових форензичких техника које се могу примјенити у квантном окружењу. Квантна форензика се бави истраживањем квантних доказних техника, као што је на примјер, квантна криптоанализа и квантна комуникација, које могу помоћи у откривању сајбер криминала у квантном свијету. Развој квантне форензике је од кључног значаја за будућност дигиталне форензике, јер ће квантне технологије играти све значајнију улогу у дигиталном друштву.

Седми иновативни резултат истраживања се односи на развој „неурофорензике". Овај концепт подразумијева кориштење неуронауке и когнитивних процеса за унапријеђење дигиталне форензике. На примјер, неуронаука може помоћи у разумијевању когнитивних пристрасности код форензичара, у развоју нових метода за откривање лажи и манипулације и у унапријеђењу процеса прикупљања и тумачења дигиталних доказа. Неурофорензика, дакле, не само да пружа нове алате за форензичке истраге, већ и дубље разумијевање људске психе у контексту дигиталног криминала.

Осми иновативни резултат истраживања се односи на развој „дигиталне екологије". Предочени концепт подразумијева интеграцију дигиталне форензике у шири контекст еколошке свијести и одрживог развоја. На примјер, дигитална форензика се може користити за откривање еколошких злоупотреба, као што је нелегална трговина дивљим животињама, крчење шума и загађење животне средине. Такође, дигитална форензика се може користити за праћење и анализу еколошких промена, што може допринјети бољем управљању природним ресурсима. Дигитална екологија, дакле, не само да проширује дјелокруг дигиталне форензике, већ и доприноси борби за одрживу будућност.

Девети иновативни резултат истраживања се односи на развој „грађанске форензике". Наведени концепт подразумијева укључивање обичних грађана у процес прикупљања и анализе дигиталних доказа. Грађани, оспособљени и тренирани кроз едукативне програме, могу постати активни учесници у борби против сајбер криминала. На примјер, грађани могу пријављивати сумњиве активности на интернету, учествовати у онлајн истрагама и пружати форензичким тимовима драгоцјене информације. Грађанска форензика, дакле, не само да демократизује процес форензике, већ и повећава капацитет друштва за борбу против криминала.

Десети иновативни резултат истраживања се односи на развој „анти-форензичких техника". Концепт подразумијева истраживање и развој техника које сајбер криминалци користе да прикрију своје трагове и манипулишу форензичким истрагама. Познавање ових техника омогућава форензичарима да развију ефикасније методе за њихово откривање и супротстављање. Анти-форензичке технике, дакле, не само да омогућавају форензичарима да боље разумију криминалне методе, већ их и припремају за нове изазове у борби против сајбер криминала. Иновативни резултати истраживања, научно комплексни и популарни, савјетодавни и примјењиви у пракси, представљају значајан корак напред у развоју дигиталне форензике. Њихова примјена може значајно унаприједити борбу против сајбер криминала, побољшати тачност и објективност форензичких истрага, обезбиједити етичну употребу AI и нових технологија, и створити праведнији и сигурнији дигитални свијет. Такав напредак захтијева континуирано истраживање и сарадњу између научника, форензичара, програмера, законодавца и свих оних који су заинтересовани за будућност дигиталне форензике. Само заједничким напорима можемо изградити систем који је отпоран на криминал, етички прихватљив и корисни за цијело друштво.

## *ДИСКУСИЈА*

Дискусија о резултатима истраживања представља кључни дио научног рада, јер управо у овом сегменту рада имамо прилику да интерпретирамо своје налазе, ставимо их у контекст постојећих знања, истакнемо њихов значај, ограничења, и импликације за даља истраживања и праксу. У контексту претходно изнесених иновативних резултата истраживања, дискусија добија посебну тежину, јер се ради о комплексној области која захтијева пажљиво разматрање свих аспеката. Резултати истраживања, који се односе на концепте као што су адаптивна форензика, когнитивно-интелигентни форензички алати, етички провјерени AI системи, виртуелне форензичке лабораторије, глобална платформа за размјену форензичких информација, квантна форензика, неурофорензика, дигитална екологија, грађанска форензика и анти-форензичке технике, представљају значајан искорак у разумијевању и унапријеђењу дигиталне форензике. Предочени концепти нису само теоријске идеје, већ имају потенцијал да трансформишу начин на који се супротстављамо сајбер криминалу и осигуравамо праведност у дигиталном друштву.

Концепт адаптивне форензике представља револуцију у приступу дигиталним истрагама. Умјесто да реагујемо на криминалне активности, адаптивна форензика омогућава проактивну борбу, користећи AI и ML да предвиђа и спријечава будуће нападе. Овакав приступ је у складу са динамиком сајбер криминала, који се непрестано мијења и усавршава. Међутим, примјена адаптивне форензике захтијева значајна улагања у AI и ML технологије, као и у образовање и обуку стручњака за њихову употребу. Такође, мора се пажљиво размотрити питање транспарентности и одговорности AI система, како би се избјегле потенцијалне пристрасности и злоупотребе. Когнитивно-интелигентни форензички алати представљају важан корак напред у превазилажењу људских ограничења у дигиталној форензици; ови алати помажу форензичарима да ублаже когнитивне пристрасности, смање утицај стреса и умора, и доносе објективније одлуке. Међутим, имплементација ових алата захтијева развој напредних алгоритама и когнитивних модела, као и пажљиво тестирање и верификацију њихове ефикасности. Такође, мора се пазити да ови алати не дехуманизују процес форензике и не смање креативност и критичко размишљање форензичара.

Етички провјерени AI форензички системи представљају одговор на растућу забринутост у вези са етичким импликацијама AI у дигиталној форензици. Ови системи, са уграђеним механизмима за провјеру пристрасности и транспарентности, омогућавају правичну и одговорну употребу AI у правосудном систему. Међутим, развој ових система је сложен и захтијева међудисциплинарну сарадњу, укључујући стручњаке из области AI, етике, права и форензике. Такође, мора се пажљиво размотрити питање одговорности за рад AI система и за посљедице њихових одлука. Виртуелне форензичке лабораторије представљају иновативан приступ у обуци и тестирању форензичких техника - ове лабораторије омогућавају форензичарима да вјежбају у контролисаном окружењу, без ризика од угрожавања правих система. Међутим, развој виртуелних лабораторија захтијева значајна улагања у технологију и развој реалистичних симулација. Такође, мора се осигурати да ове лабораторије пружају релевантне и практичне тренинге, који се могу примјенити у реалним форензичким истрагама.

Глобална платформа за размјену форензичких информација представља важну иницијативу за унапријеђење међународне сарадње у борби против сајбер криминала; ова платформа омогућава форензичарима из цијелог свијета да размјењују информације, искуства и најбоље праксе. Међутим, имплементација платформе захтијева усаглашавање различитих правних и техничких стандарда, као и обезбијеђивање сигурне комуникације и размјене информација. Такође, мора се пазити на питање приватног прикупљања и размјене података, како би се избјегле потенцијалне злоупотребе. Концепти квантне форензике и неурофорензике представљају нове границе у истраживању дигиталне форензике. Квантна форензика се бави истраживањем квантних технологија и њихове примјене у откривању и спријечавању сајбер криминала, док се неурофорензика бави истраживањем утицаја неурознаности на форензичке процесе. Међутим, ови концепти су још у развојној фази и захтијевају додатна истраживања како би се утврдила њихова практична примјена.

Концепти дигиталне екологије, грађанске форензике и анти-форензичких техника представљају иновативан приступ у проширењу дјелокруга дигиталне форензике и њеног укључивања у шире друштвене и еколошке контексте. Дигитална екологија повезује дигиталну форензику са борбом за одрживи развој, грађанска форензика укључује обичне грађане у процес прикупљања и анализе дигиталних доказа, док анти-форензичке технике омогућавају форензичарима да боље разумију криминалне методе и да развију ефикасније методе за њихово откривање; ови концепти су важни за стварање демократичнијег и одговорнијег приступа у борби против криминала. Критички осврт на резултате истраживања указује на њихову иновативност и потенцијал за унапријеђење дигиталне форензике. Међутим, имплементација ових концепата захтијева значајна улагања у технологију, истраживање и развој, као и међудисциплинарну сарадњу и међународну размјену знања. Такође, мора се пажљиво размотрити етичка и правна питања која произилазе из употребе ових концепата. На крају, резултати истраживања не представљају коначна рјешења, већ су полазна тачка за даља истраживања и унапријеђење дигиталне форензике. Континуирано праћење развоја сајбер криминала, нових технологија и друштвених промјена је неопходно за ефикасну борбу против криминала и за стварање праведнијег и сигурнијег дигиталног свијета. Дакле, дискусија о резултатима истраживања показује да су представљени концепти иновативни и да имају велики потенцијал за трансформацију дигиталне форензике. Међутим, њихова имплементација је сложена и захтијева пажљиво планирање и реализацију. Управо због тога, овај рад представља први корак у дужем процесу истраживања и унапријеђења у овој области. Кључно је наставити са истраживањем, развојем и имплементацијом ових концепата, као и са јачањем међународне сарадње и са едукацијом будућих генерација стручњака у области дигиталне форензике.

## *ЗАКЉУЧАК*

Представљено истраживање је расвјетлило динамичан симбиотски однос између сајбер криминала и дигиталне форензике, показујући да се ова два поља међусобно подстичу на континуиране иновације и адаптације. Концепт адаптивне форензике, заснован на AI и ML, нуди проактиван приступ борби против сајбер криминала, предвиђајући и спријечавајући будуће пријетње уместо само реаговања на прошле нападе. Когнитивно-интелигентни форензички алати представљају кључ за превазилажење људских ограничења у анализи дигиталних доказа, ублажавајући пристрасности и смањујући утицај стреса на форензичаре. Етички провјерени AI системи су неопходни за осигуравање правичности и поузданости дигиталне форензике у ери вјештачке интелигенције, те захтијевају пажљив развој и континуирану провјеру. Виртуелне форензичке лабораторије пружају сигурно и контролисано окружење за обуку и тестирање нових форензичких техника, омогућавајући континуирано унапријеђење праксе. Глобална платформа за размјену форензичких информација је кључна за међународну сарадњу у борби против сајбер криминала, омогућавајући размјену знања и ресурса на глобалном нивоу. Истраживање квантне форензике и неурофорензике отвара нове перспективе у разумијевању дигиталног криминала, нудећи напредне методе за његово откривање и спријечавање. Концепти дигиталне екологије и грађанске форензике проширују дјелокруг дигиталне форензике, укључујући ширу друштвену и еколошку свијест у борбу против криминала. Анти-форензичке технике су важне за разумијевање метода које користе криминалци, омогућавајући форензичарима да развију ефикасније стратегије за њихово откривање. Предочено истраживање је нагласило потребу за континуираним унапријеђењем дигиталне форензике, уз нагласак на етичкој примјени AI и нових технологија, кроз међународну сарадњу и образовање нових стручњака, како би се осигурао сигуран и праведан дигитални свијет.

## *ЛИТЕРАТУРА*

Ask, K. & Granhag, P. A. (2007). *Motivational factors and cognitive bias: The effect of guilt and innocence on judgments*. Psychology, Crime & Law, *13*(1), 23–37.

Beebe, N. L. & Clark, J. M. (2005). *A hierarchical, objectives-based framework for the digital investigations process*. Digital Investigation, *2*(2), 147-167.
Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley Professional.
Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.
Cooper, C. J. & Brewer, N. (2013). *Contextual influences on forensic science decisions: A review and meta-analysis*. Psychology, Crime & Law, *19*(9), 787-810.
Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., … & Vayena, E. (2018). *AI4People—an ethical framework for a good AI society: Opportunities, risks, principles, and recommendations*. Minds and Machines, *28*(4), 689-707.
Hsu, C. L. & Lin, H. M. (2015). *A study of digital forensics investigation in the face of anti-forensics tools*. International Journal of Network Security & Its Applications, *7*(5), 97–106.
Maras, M. H. (2016). *Cybercriminology*. Oxford University Press.
Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). *The ethics of algorithms: Mapping the debate*. Big Data & Society, *3*(2), 2053951716679679.
Nikolić, L. (2017). *Forenzička lingvistika*. Evropski defendologija centar, Banja Luka.
Palmer, G. (2001). *A road map for digital forensic research*. In Proceedings of the First Digital Forensic Research Workshop (pp. 27-30). Utica, NY.
Stoel, R. D. Berger, C. E. H., Kerkhoff, A. H. J., & Veenman, F. J. (2019). *The challenges and importance of cognitive forensics.* In The Forensic Psychology of Criminal Behaviour (pp. 209–227). Springer.
Yadav, S. & Singh, A. (2016). *A comprehensive study of digital forensics*. International Journal of Engineering Trends and Technology, *33*(3), 141-147.
Zou, C. C. & Zhao, Y. J. (2020). *Review of the research on artificial intelligence and digital forensics*. Journal of Physics: Conference Series, *1639*(1), 012034.

# APPLICATION OF DIGITAL FORENSICS IN DETECTING CYBERCRIME

Duško Vejnović, PhD[4]
*Faculty of Security Sciences, University of Banja Luka*

Slaven Knežević, MA[5]
*Faculty of Political Sciences, University of Banja Luka*
*Faculty of Economics, University of Banja Luka*
*Faculty of Law, University of Banja Luka*

**Abstract:** This paper explores the crucial role of digital forensics in the identification, analysis, and prevention of cybercrime, which is becoming an increasingly present threat in modern society. Digital forensics encompasses a range of sophisticated methods and tools that enable the collection, preservation, analysis, and presentation of digital evidence necessary for identifying perpetrators and their methods. The paper analyzes the main techniques used in digital forensics, including the analysis of network protocols, the collection of data from various digital devices, as well as the decryption of information protected by complex encryptions. Particular attention is paid to the role of digital forensics in detecting cyber attacks such as ransomware, phishing, and DDoS attacks, which pose serious threats to individuals, companies, and state institutions. In addition to technical aspects, the paper also discusses the challenges faced by digital forensics experts, including rapid technological changes, the complexity of digital traces, as well as legal obstacles and ethical dilemmas regarding privacy and data protection. Through the analysis of specific cybercrime cases and practical studies, the paper aims to show how digital forensics can contribute to faster and more efficient detection of perpetrators, and how improving technological and methodological capacities in this field can help prevent future threats. The research findings highlight the necessity of strengthening digital forensic infrastructure and educating experts, as well as the need for international cooperation to achieve an effective response to the increasingly complex and global phenomenon of cybercrime, which makes digital forensics an indispensable part of modern security strategies.
**Keywords:** *digital forensics, cybercrime, cognitive forensics, quantum forensics, AI.*

[4] Duško Vejnović is a full professor at the Faculty of Security Sciences, University of Banja Luka. Email: profesordusko@gmail.com
[5] Slaven Knežević, MA, is a doctoral candidate at the Faculty of Political Sciences, University of Banja Luka, a master's student at the Faculty of Economics, University of Banja Luka, and a master's student at the Faculty of Law, University of Banja Luka. Email: slaven.knezevic998@gmail.com