Технически университет - София
Факултет по ПРИЛОЖНА МАТЕМАТИКА И ИНФОРМАТИКА
Катедра „Информатика”

МЕТОДОЛОГИЯ ЗА ОБРАБОТКА, АНАЛИЗ И ВЕРИФИКАЦИЯ НА КОМПЮТЪРНИ ЕКСПЕРТИЗИ В ЦИФРОВАТА КРИМИНАЛИСТИКА

АВТОРЕФЕРАТ

на дисертационен труд за придобиване на образователна и научна степен „доктор”
по научна специалност „Информатика“
направление 4.6. „Информатика и компютърни науки“

маг. инж. Светлин Георгиев Стефанов

Научен ръководител
доц. д-р инж. Малинка Спасова Иванова

СОФИЯ | 2025

Дисертационният труд е обсъден и насочен за защита от разширен научен съвет на катедра Информатика на ТУ-София на редовно заседание, проведено на 03.02.2025г.

Публичната защита на дисертационния труд ще се състои на 03.06.2025г. от 13 часа в Конферентната зала на БИЦ на Технически университет-София на открито заседание на научното жури, определено със заповед № ОЖ-4.6-05 от 05.02.2025г., № ОЖ-4.6-11 от 11.02.2025г. на Ректора на ТУ-София в състав:

1. Доц. д-р Десислава Антонова Иванова
2. Доц. д-р Златко Василев Захариев
3. Проф. д-р Мария Михайлова Нишева-Павлова
4. Проф. д-р Евгения Петрова Ковачева
5. Проф. д-р Галина Тодорова Богданова

Рецензенти:
1. Доц. д-р Десислава Антонова Иванова
2. Проф. д-р Галина Тодорова Богданова

Материалите по защитата са на разположение на интересуващите се в канцеларията на Факултет по Приложна математика и информатика на ТУ-София, блок № 2, кабинет № 2228.

Дисертантът е задочен докторант към катедра Информатика на Факултет по Приложна математика и информатика. Изследванията по дисертационната разработка са направени от автора със съдействието и подкрепата на научния ръководител.

Автор: маг. инж. Светлин Стефанов
Заглавие: Методология за обработка, анализ и верификация на компютърни експертизи в цифровата криминалистика

Тираж: 30 броя
Отпечатано в ИПК на Технически университет – София

Увод

В днешния онлайн свят на киберпрестъпления, цифровата криминалистика се превръща в ключ към ефективното разследване на местопрестъплението и идентифициране на нарушителя. За да бъде проведено разследване по оптимален начин, трябва да се следват подходящи техники и методи за откриване на цифрови доказателства, както и за намиране на данни в цифрови устройства. Подходите за извличане на данни следва да се прилагат и използват и за извличане на доказателства, като трябва да се прилагат техники за сигурно съхранение за запазване целостта на получените доказателства. Когато не е възможно да се изследват цифрови доказателства на местопрестъплението, експертите-криминалисти използват методи за сигурно транспортиране и след това ги анализират в лабораторни условия. Обикновено, криминалистите следват установена методология в своята практика или набор от процедури за откриване на всички цифрови доказателства, както и техните взаимовръзки, когато съществуват.

Съвременната цифрова криминалистика трябва да се справя с редица предизвикателства, които са свързани с непрекъснато разработване на нови технологии и усъвършенствани инструменти за укриване на следи от нарушители. Това от своя страна означава, че криминалистите трябва непрекъснато да изучават нови технологични решения и възникващи теоретични модели, най-добри практики и научни постижения, за да създадат и използват подходящи инструменти за разследване. Затова, напоследък се извършват интензивни изследвания относно приложението и потенциала на техники от машинното обучение и изкуствения интелект за бързо обработване и анализиране на събрани или извлечени данни в цифрово криминалистично разследване, за точно реконструиране на местопрестъпление и времева линия, за откриване и свързване на доказателства, за предсказване на насилствено и противозаконно поведение, за осигуряване на верига за управление на доказателства, за подпомагане подготовката на документация, както и за подобряване на

някои параметри на самия процес по разследване в цифровата криминалистика.

Разработването на методология, подпомагаща дейности на криминалистите и последващото й интегриране в софтуерна система значително би подобрило и автоматизирало тяхната работа, свързана с управление на комуникационни потоци, документооборот, подготвяне на цифрови експертизи, обогатяване на знанията и информираността им.

Дисертационният труд разглежда важен за обществото ни проблем, свързан с осигуряване на точност, бързодействие и гъвкавост на криминалистичните разследвания, което е от изключителна важност на фона на нарасналите и усъвършенствани киберпрестъпления. Автоматизирането на дейности в цифрово криминалистично разследване дава гаранция за:

- Подобряване ефективността на криминалистите;
- По-бързо достигане до качествен резултат и подготовка на компютърната експертиза;
- Повишаване точността при идентифициране и анализ на цифрови доказателства.

Цел и задачи

Въз основа на съвременни научни изследвания, теоретични постановки и най-добри практики да се разработи методология за обработка, анализ и верификация на компютърни експертизи в цифровата криминалистика и да се имплементира в софтуерно решение за подпомагане и автоматизиране на дейности в цифрово криминалистично разследване.

За постигане на поставената цел са дефинирани следните задачи за изпълнение:

1. Извършване на обзор на съвременни модели, техники и методологии, използващи се в цифрово криминалистично разследване и разработване на концептуален модел въз основа на резултатите от проучването;

2. Разработване на методология за обработка, анализ и верификация на компютърни експертизи в цифровата криминалистика;
3. Проучване на съвременни изследвания относно приложението на техники от машинно обучение и изкуствен интелект в цифровата криминалистика и обобщаване на резултата в теоретична рамка;
4. Проектиране и разработване на софтуерна система въз основа на създадената методология за обработка, анализ и верификация на компютърни експертизи в цифровата криминалистика и извършване на последваща оценка.

Дисертационният труд включва оригинални научни изследвания, основани на съвременни теоретични постановки и изследвания на практически проблеми за постигане на нови знания, модели и решения в областта на цифровата криминалистика.

Структура и обем на дисертационния труд

Дисертационният труд е с обем 136 страници и е структуриран по следния начин: увод, пет глави и заключение, приноси. Дисертацията съдържа 53 фигури и 4 таблици. Цитирани са 117 литературни източника. Номерата на фигурите и таблиците в автореферата съответстват на тези в дисертационния труд.

Първа глава е насочена към проучване, анализиране и обобщаване на съвременни научни постижения по отношение на съвременни модели за цифрово криминалистично разследване и очертаване на някои предизвикателства и тенденции в контекста на изследваната тематика. Също така, е показан създаден концептуален модел, обобщаващ текущото състояние в цифровата криминалистика и при извършване на криминалистични разследвания.

Втора глава представя методология, която пълно и точно отразява съвременен процес на разследване в цифровата криминалистика и показва спецификата на нейното практическо приложение. Разработеното решение е наречено *Методология за разследване в*

цифровата криминалистика от практическа гледна точка (*Digital Forensic Investigation from Practical Point of View - DFIP*), за да се подчертае неговата приложимост към настоящата практика и да се разграничи от съществуващите чисто теоретични методологии и рамки.

Трета глава включва разработена функционална архитектура на софтуерна система и архитектурен модел на софтуерен прототип за подпомагане на разследвания в цифровата криминалистика и изготвяне на компютърни експертизи, следвайки методологията за разследване в цифровата криминалистика от практическа гледна точка DFIP, разгледана във втора глава. За тази цел е извършен анализ на потребностите въз основа на създаден анкетен инструмент, предоставен на експерти-криминалисти.

Четвърта глава е посветена на използването на техники от машинно обучение и изкуствен интелект в цифровата криминалистика, в цифрово криминалистично разследване и за подготовка на компютърни експертизи. Създадена е рамка, която обобщава основните проблеми и изследователски насоки за приложение на изкуствения интелект в цифровата криминалистика. Показани са и резултатите от изследване относно прилагане на техники от машинно обучение и изкуствен интелект при класифициране на цифрови доказателства, при анализ на съдържанието и текстово обобщение на pdf документи за улесняване и автоматизиране работата на експерти-криминалисти.

Пета глава представя разработен прототип на софтуерна система за целите на цифровата криминалистика съобразно създадената методология за разследване в цифровата криминалистика от практическа гледна точка DFIP и е извършена оценка относно имплементираната функционалност.

Публикации

Научните публикации във връзка с дисертационния труд са осем, като четири от тях са представени на международни конференции в страната, а останалите четири на международни конференции в чужбина. Три от тях са индексирани в научната база Scopus, като

едната е с SJR: 0.17, Q4. Останалите са под печат. Забелязани са две цитирания на една от публикациите.

ПЪРВА ГЛАВА. ИЗСЛЕДВАНЕ И АНАЛИЗ НА СЪВРЕМЕННИ МОДЕЛИ, МЕТОДИ И ТЕХНИКИ ЗА ИЗГОТВЯНЕ НА ЕКСПЕРТИЗИ В ЦИФРОВАТА КРИМИНАЛИСТИКА

Настоящата глава има за цел да проучи, анализира и обобщи съвременни научни постижения по отношение на модели за цифрово криминалистично разследване (Digital Forensic Investigation - DFI) в наскоро публикувани научни статии, като очертае някои предизвикателства и тенденции в контекста на изследваната тематика. Също така, да обобщи резултатите в концептуален модел, показващ текущото състояние в цифровата криминалистика (Digital Forensics - DF) и при извършване на криминалистични разследвания.

С непрекъснатото развитие на технологиите, заплахите и атаките срещу информационни ресурси, компютърни системи и мрежи стават все по-комплексни с потенциал за причиняване на значителни вреди на физически и юридически лица. Редица изследователи дискутират предизвикателни въпроси, свързани с използвания технически инструментариум, правни рамки, разнообразие от устройства и твърдят, че сложността на тази област и развиващите се технологични решения трябва да доведат до създаване на нови модели и методи в криминалистиката.

За очертаване на настоящото състояние на научните изследвания е извършен библиометричен анализ, като са разгледани най-новите публикации в тази област в научната база данни Scopus.

Извършено е и детайлно проучване на съдържанието на литературни източници, индексирани в Scopus, при същата заявка digital forensics, за да се види по-конкретно какви са получените научни резултати и постижения на изследователите, които могат да бъдат описани по следния начин:

- *По отношение на областта на приложение* - Развитието на технологиите води до появата на нови устройства, софтуерни

решения, интелигентни системи, които също изискват нови методи за събиране, изследване, съхранение и документиране на доказателствен материал. Сред новопоявилите се области са криминалистиката на IoT и криминалистиката на облачните изчисления. Заедно с тях в процес на развитие са и по-старите;

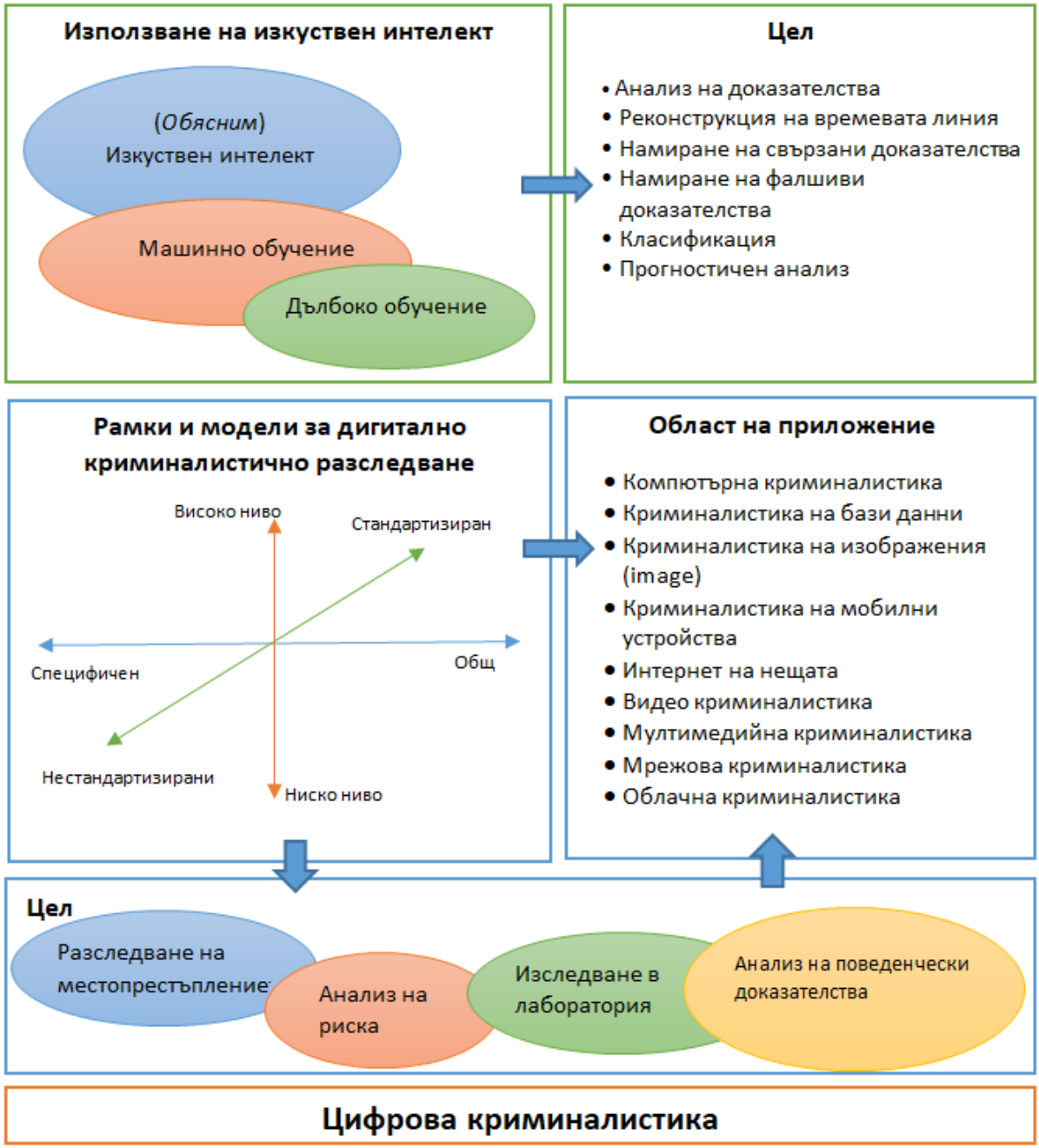
- *По отношение на рамки и модели в DF и DFI* - Целта им е да се усъвършенстват съществуващите модели, за да съответстват на технологичното развитие и нововъзникващите атаки, но също така да се разработят нови модели за решаване на конкретни задачи. Някои от предложените модели присъстват на високо и по-абстрактно ниво, други търсят по-стандартизиран подход, трети са специфично ориентирани;
- *По отношение на използването на изкуствен интелект в DF и DFI* - Изглежда, че прилагането на алгоритми и техники на изкуствен интелект, машинно и дълбоко обучение може да се използва за увеличаване на скоростта на разследването, за намаляване на усилията на експерта и за намаляване на необходимото време за изпълнение на отделни дейности в DFI.

Тенденциите в изследванията могат да бъдат категоризирани в две основни групи: (1) подобряване на съществуващи рамки и модели в DF и DFI и създаване на нови, и (2) прилагане на изкуствен интелект за подобряване на параметрите на процес на DFI.

Разработен концептуален модел в областта на DF

Целта на създадения концептуален модел е да обобщи резултатите, получени чрез извършения библиометричен подход и по-подробен литературен преглед (Фигура 4). Също така, той очертава и концептуализира проведените изследвания през последните години, като изследователите виждат предимствата на изкуствения интелект за автоматизиране на някои повтарящи се ръчно изпълнявани задачи, за намиране на връзки между доказателства в сложна област, за извършване на реконструкция на времева линия, за подпомагане на анализа на доказателства, за решаване на задачи за класификация и прогнозиране. Целта на моделите е да улеснят процеса на разследване

на местопрестъплението или в лабораторията, а напоследък и проучването на поведенчески дейности на нарушителя и жертвата също се считат за подпомагане извършването на прецизна реконструкция на времевата линия. Анализът на риска също е във фокуса на изследванията, които могат да доведат до избягване на някои грешки по време на цифрово криминалистично разследване



Фиг. 4. Създаден концептуален модел

Областите на приложение на DF са добре очертани по време на библиометричния анализ и е важно да се спомене, че заедно с по-старите области на DF (компютърна криминалистика, мрежова криминалистика и т.н.) също се изследват нови криминалистични области като IoT и облачна криминалистика. Това изключително зависи от непрекъснатото развитие на технологиите и появата на нови технологични решения.

ВТОРА ГЛАВА. МЕТОДОЛОГИЯ ЗА ИНФОРМАЦИОННА ОБРАБОТКА, АНАЛИЗ И ВЕРИФИКАЦИЯ В ЦИФРОВАТА КРИМИНАЛИСТИКА

Целта на втора глава е да представи методология, която пълно и точно да отразява съвременен процес на разследване в цифровата криминалистика и да покаже спецификата на нейното практическо приложение. Разработеното решение е наречено *Методология за разследване в цифровата криминалистика от практическа гледна точка* (**D**igital **F**orensic **I**nvestigation from **P**ractical Point of View - DFIP), за да се подчертае неговата приложимост към настоящата практика и да се разграничи от съществуващите чисто теоретични методологии и рамки.

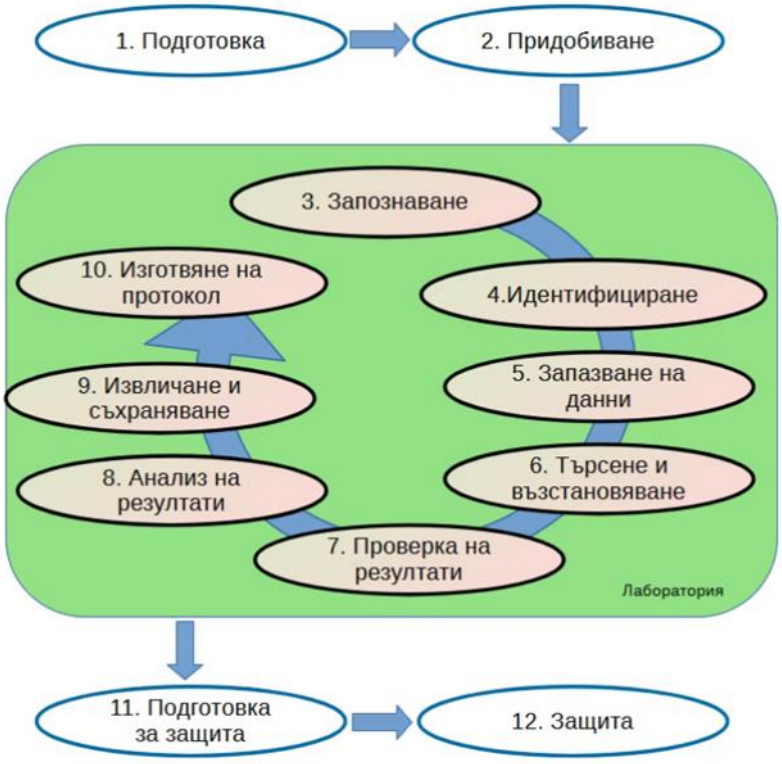
За да могат данните да бъдат правилно извлечени от цифрови носители, съхранени за последващ анализ и използвани в разследване, е необходима стриктна методология, която да се следва от разследващите. Такава методология включва конкретни стъпки и типични дейности за тях. Оказва се, че тази тема в момента се обсъжда и изследва интензивно, като се търсят подходи, които по-пълно и всеобхватно да описват случващото се по време на оглед на местопрестъплението, както и при анализ на доказателства и подготвяне на компютърни експертизи.

Методология за разследване в цифровата криминалистика от практическа гледна точка

Предложената методология за разследване в цифровата криминалистика е в съответствие с настоящата практика при разследване на местопрестъпление и изследване на цифрови

доказателства в страната ни и има за цел да систематизира и улесни извършването на рутинни дейности от криминалистите. Може да подобри комуникацията между експерти-криминалисти и да улесни потока на необходимите документи. Също така, това е възможност необходимите знания в областта на DF и DFI да бъдат събрани на едно място, когато методологията се реализира под формата на софтуерна система.

Разработената методология за разследване в цифровата криминалистика от практическа гледна точка е представена през дванадесет фази и е показана на Фигура 5.



Фиг. 5 Методология за разследване в цифровата криминалистика от практическа гледна точка - DFIP

Подобрен модел за придобиване на цифрови доказателства

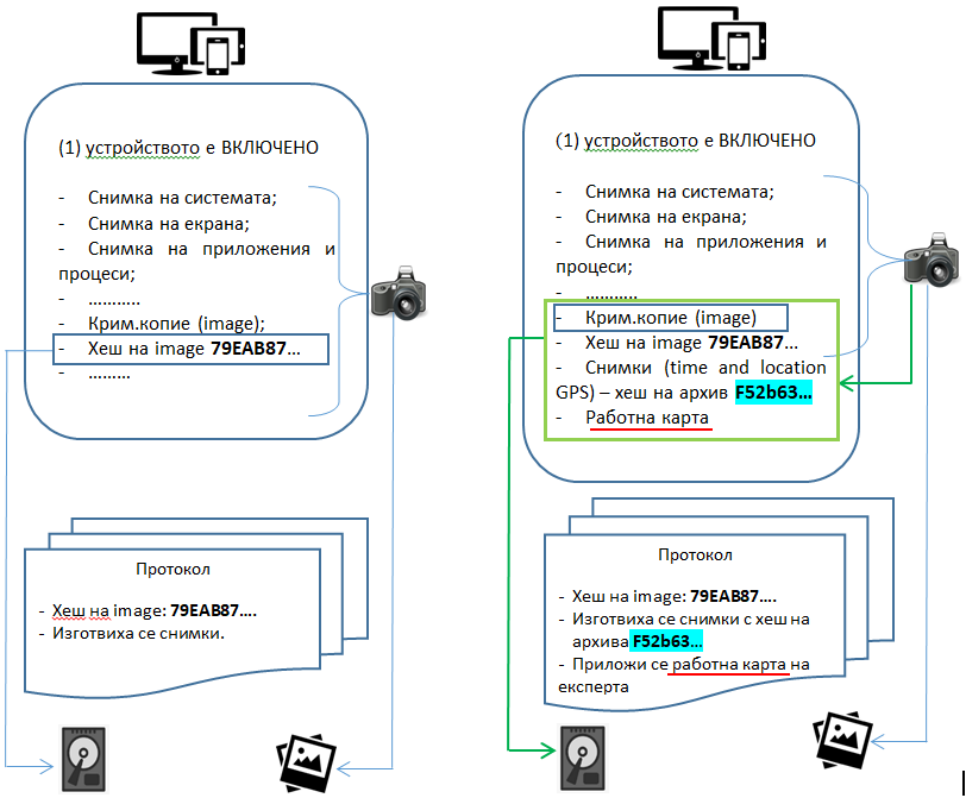
Предложеният модел за извличане на данни е свързан с Фаза 2 на методологията DFIP (Фигура 5) и има за цел да улесни нейното прилагане от разследващите експерти. За да се демонстрира предложеното подобрение в извличането на данни, е сравнен с използваният стар модел.

Предлагат се два момента:

1) Използването на криминалистична техника за заснемане на всяко действие с фотоапарат, настроен с верифицирано време, регионални настройки и включени GPS координати, ще вгражда допълнителна информация във всяко изображение. Тази информация от метаданните на всяка снимка, допълнително ще повиши пълнотата и надеждността на извършваните действия при придобиването на цифрови доказателства;

2) допълнително да се изготви и от експерта/специалист-технически помощник/ вид работна карта (доклад), с описаните процеси и резултатите от извършените действията по DF.

Фигура 8 показва сравнение между стария и подобрения модел за придобиване на цифрови доказателства. В предложения нов подход се извършва архивиране на направените изображенията и изчисляване на тяхната хеш сума и заедно с работната карта на експерта, се прилагат към официалния протокол.



а). б).

Фиг. 8 Модел за придобиване на цифрови доказателства: а). стар модел; б). подобрен модел

Трета глава. Проектиране на интелигентна информационна система с интегрирана методология за подпомагане на разследвания в цифровата криминалистика и изготвяне на компютърни експертизи

Целта на тази глава е да представи разработената функционална архитектура на софтуерна система и архитектурен модел на софтуерен прототип за подпомагане на DFI и изготвяне на компютърни експертизи, следвайки методология за разследване в цифровата криминалистика от практическа гледна точка DFIP, разгледана във втора глава. Затова, е извършен анализ на потребностите въз основа на създаден анкетен инструмент, предоставен на експерти-криминалисти в DI.

Всяка методология е разработена, за да изпълнява набор от изисквания, да е приложима в определен контекст и да е с конкретен фокус. Въпреки че се търси унифицирано решение, това в момента е трудно осъществимо, поради различия в законодателството, възприетите концепции и практически специфики. Затова, е разработена *методологията за разследване в цифровата криминалистика от практическа гледна точка DFIP*, която се основава на съвременни теоретични познания и показва подход за решаване на съществуващи практически проблеми. Методологията включва 12 фази, отразяващи различни типични дейности за всяка фаза и подготовка на компютърна експертиза като краен резултат. Необходимо е проучване как методологията *DFIP* може да бъде интегрирана в софтуерно решение и различни дейности от 12-те фази да бъдат подпомогнати и автоматизирани. Затова, е извършен анализ на потребностите и последващо проектиране, чрез което да се очертаят функциите, които трябва да включва една такава софтуерна система.

За проучване мнението и изискванията на експерти в DF към функциите на софтуерна система, която да автоматизира и подпомага техни дейности в DFI, съобразно разработената методология DFIP, са изпълнени следните три процедури:

- Подготвен е инструмент за онлайн анкета с въпроси с отворен и затворен отговор. Отворените отговори са под формата на кратък и дълъг текст. Чрез въпросите искаме да разберем какви основни функционалности трябва да поддържа едно софтуерно приложение при подготовка на компютърни експертизи в цифрово криминалистично разследване и каква функционалност по време на коя фаза от методологията DFIP да бъде реализирана;
- След приключване на анкетата, отговорите са обобщени и анализирани, за да се разбере какви са очакванията на криминалистите от една такава софтуерна система и по какъв начин техните следствени дейности могат да бъдат улеснени и автоматизирани. Проучването завършва с подготвен анализ на потребностите, който се използва за разработване на функционалната архитектура на софтуерното приложение. Анализът на потребностите е решаваща и много важна стъпка в процеса на разработка на софтуер. Изясняването на изискванията към софтуерната система в началото на проекта е гаранция за успешното му завършване, следвайки инженерен процес за разработка на софтуер, независимо че някои промени могат да възникнат на по-късен етап;
- Следвайки клаузите в анализа на потребностите, е разработена функционална архитектура на софтуерното приложение, показваща няколко работни пространства и важни функционални характеристики за криминалистите. Това е началната фаза в процеса на разработка на софтуер, която след анализ на потребностите включва проектиране, разработване, внедряване, тестване и внедряване на софтуера.

Анализ на мнението на експерти в областта на цифровата криминалистика

Анкетираните вещи лица-експерти са 11, като двама от тях притежават богат опит в DF и изготвянето на компютърни експертизи с повече от 20 години професионален опит, петима са криминалисти с опит над 10 години, а четирима от тях упражняват тази професия за по-малко от 6 години. 73% са мъже и 27% са жени.

Всички респонденти са съгласни, че една софтуерна система за подпомагане на DFI и изготвяне на компютърни експертизи трябва да съдържа инструменти за вътрешна комуникация между експертите, осигуряващи бързи и надеждни комуникационни канали за лични и екипни съобщения. Експертите потвърждават колко важна за тях е синхронната и асинхронна комуникация и практическата необходимост от различни видове комуникационни канали. Предложенията са насочени към възможността в комуникационния канал да се изпращат и получават файлове, да се получават известия и новини по телефона, да се разполага със спомагателна информация за полезни специализирани програми и скриптове.

Установи се, че комуникационните инструменти са най-необходими във фазата *Търсене и възстановяване на цифрови доказателства*, като вотът на експертите е 100%. Отиваме по-нататък и анализираме на кой етап от DFI и подготовката на компютърни експертизи кой комуникационен инструмент(и) би бил полезен. Според мнението на експертите е ясно, че най-необходимият и полезен инструмент за комуникация е чатът.

Всички анкетирани отговарят, че според тях е полезна функцията за търсене на експерти, която може да помогне за бързо сформиране на екип от експерти, който да проведе разследването.

Всички участници са съгласни, че функцията за качване на файлове трябва да бъде включена (100%). Други важни функции при работа с документи са: изпращане на файлове, прикачване на архивирани папки, редактиране и изтриване на файлове.

Всички респонденти смятат, че документите, които са приложени в системата, трябва да имат високо ниво на конфиденциалност.

81,8% от анкетираните смятат, че софтуерната система за подпомагане на DFI и подготовка на компютърни експертизи трябва да има зона за обучение с връзки към отворени курсове, учебни материали и изпитни тестове, възможност за сертифициране.

Относно използването на изкуствен интелект в софтуерната система за подпомагане на DFI и изготвянето на компютърни експертизи и с цел подпомагане на вземането на решения, когато трябва да се обърне внимание върху определен проблем, експертите-криминалисти отговарят, че не са съгласни решенията в DF и DFI да се основават изцяло на изкуствен интелект.

На въпроса "*Смятате ли, че компютърната експертиза трябва да бъде изготвена според предварително подготвен интерактивен шаблон, предлаган от софтуерната система?*", 81,8% от анкетираните отговарят утвърдително. Те искат работата им да бъде подпомогната чрез използване на предварително създадени шаблони на документи или шаблони, които да бъдат динамично генерирани в реално време.

Експертите бяха помолени да опишат какви други характеристики смятат, че трябва да притежава софтуерната система, за да улеснява и автоматизира дейностите по DFI, и техните отговори са както следва: интерактивен съветник, търсене по ключови думи за стари протоколи и заключения, представяне на статистически данни и метаданни на документи, различни модели и алгоритми на действие, възможност за работа в екип, достъп до законови разпоредби относно изготвянето на компютърна експертиза, достъп до публикации, свързани с изготвяне на компютърна експертиза, достъп до разработени образци, схеми и алгоритми.

Функционална архитектура

Извършеният анализ на потребностите по отношение на функционалността на софтуерната система, която е в състояние да поддържа дейности в DFI и изготвяне на компютърни експертизи, се основава на вота на експерти чрез анкетно проучване. Подобно изследване е изключително важно в жизнения цикъл на разработка на софтуер и успеха на проекта като цяло, тъй като очертава основните функционални характеристики, които трябва да притежава софтуерът.

Разработената функционална архитектура е представена на Фигура 13 и основните характеристики са групирани, както следва:

(1) комуникационни функции с възможност за синхронен и асинхронен трансфер на съобщения;

(2) работа в екип с функция за създаване на групи от експерти-криминалисти и тяхното управление;

(3) управление на работния процес на документи – прикачване на файлове, редактиране, изтриване, изпращане и прикачване на папки и достъп до тях;

(4) функция за търсене за намиране на експерти-криминалисти за конкретно DFI и за намиране на документи, протоколи, заключения;

(5) съветник и възможен шаблон в подкрепа на подготовката на компютърни експертизи;

(6) функции за разглеждане и получаване на съвременна и актуална информация относно законодателни норми, новини и събития;

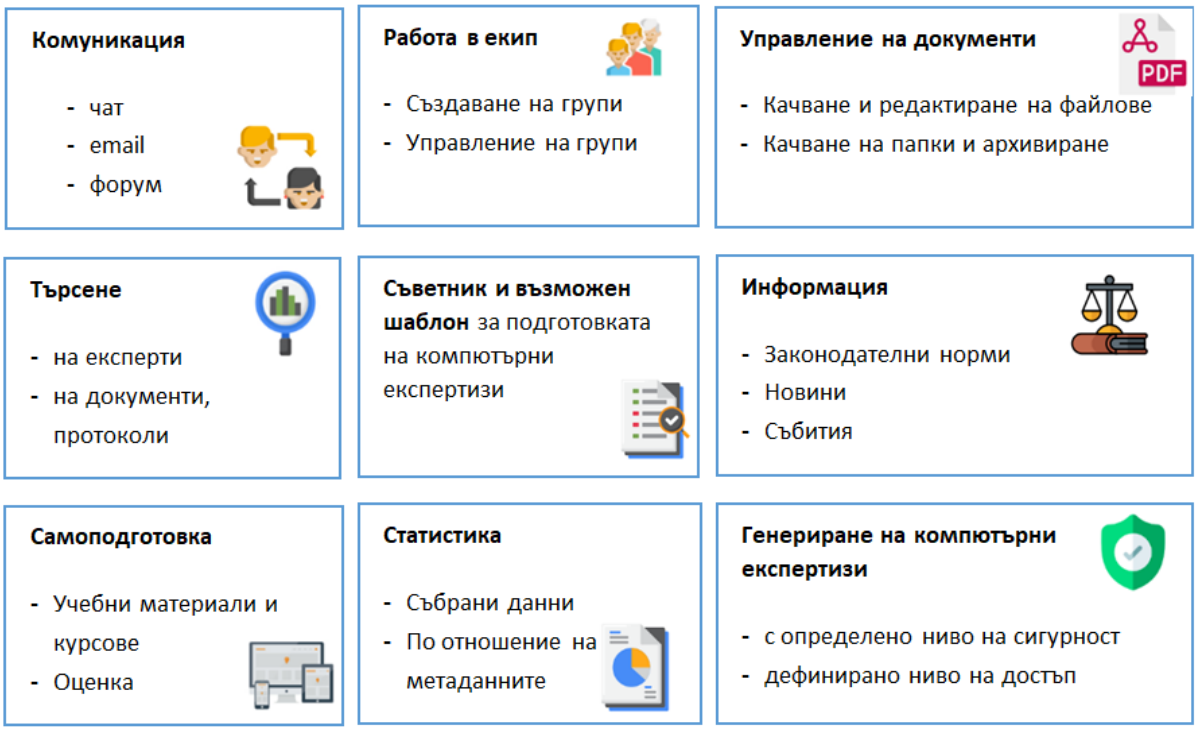
(7) зона за самоподготовка с методически разработени учебни материали и оценка;

(8) функции за предоставяне на статистическо значение по отношение на събраните данни и метаданни;

(9) функции за генериране на компютърни експертизи с определено ниво на сигурност и с подходящо ниво на поверителност.

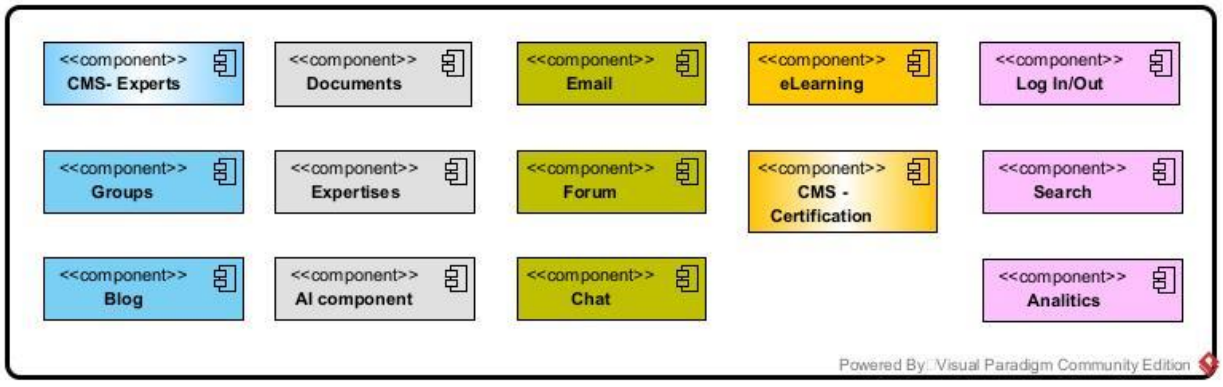
След този анализ на потребностите, проектираната функционалност на софтуерния прототип е показана на Фигура 14 под формата на компоненти. Синхронната и асинхронната комуникация е представена чрез три компонента: Email, Forum и Chat, които дават възможност на експертите да обменят идеи, опит, съобщения, както и да прикачват голямо разнообразие от документи. Функцията за работа в екип е много важна в почти всички фази на методологията DFIP и за тази цел е планиран компонент Groups, тъй като е във връзка с компонента на системата за управление на съдържанието (CMS) и с компонента експерти (CMS-Experts). Функционалността за управление на документи е проектирана чрез компонент Documents, а подготовката

на цифрова експертиза се поддържа чрез компонент Expertise и AI component.



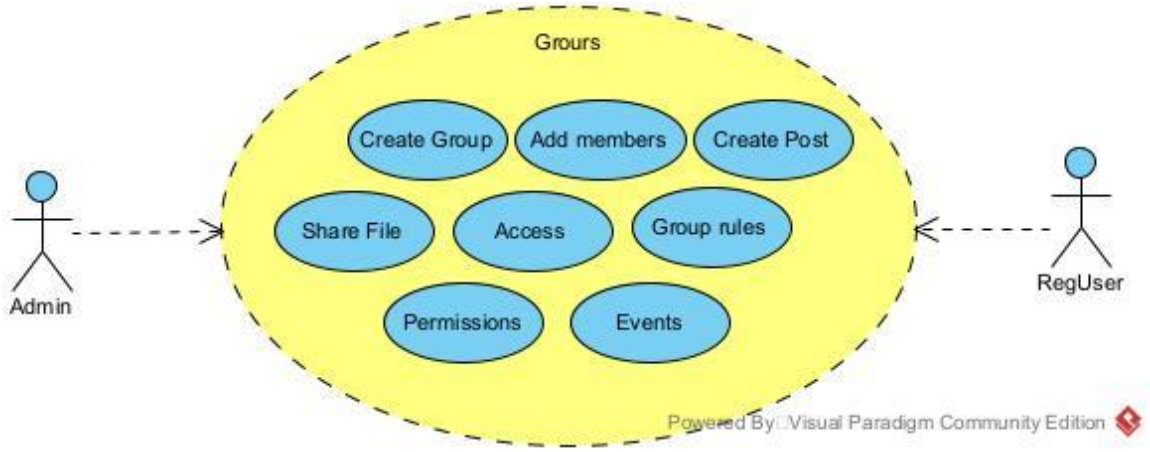
Фиг. 13 Функционална архитектура на софтуерна система, подпомагаща подготовката на компютърна експертиза

Информационната област е представена чрез функционалността на компонента Blog, докато зоната за обучение е свързана с компонента за електронно обучение и компонента за CMS-сертификация (eLearning component и CMS-Certification). Също така, са включени функции за бързо търсене сред експерти, документи и други елементи (компонент Search) и подходящ визуален анализ на факти и информация (компонент Analytics).



Фиг. 14 Функционална архитектура на софтуерния прототип

Компонентът *CMS-Experts* е свързан с компонента *Groups*, тъй като последният позволява на експертите да бъдат организирани в групи, за да формират екипи според случаите на цифрова криминалистика (Фигура 16). За тази цел всеки член, както и администраторът, могат да създадат група и да добавят членове към тази работна група. Предвижда се новосъздадените групи да бъдат частни и този, който ги създаде, да може да отправя покани и да управлява други членове. Целта на тези затворени групи е да улеснят онлайн синхронната и асинхронната комуникация само между експерти, избрани за този случай на цифрова криминалистика, и да подкрепят споделянето на идеи, документи и резултати.



Фиг. 11 Функционалност на компонента Groups

ЧЕТВЪРТА ГЛАВА. МАШИННО ОБУЧЕНИЕ И ИЗКУСТВЕН ИНТЕЛЕКТ В ЦИФРОВАТА КРИМИНАЛИСТИКА

Целта на тази глава е да представи изследване на възможностите за прилагане на ML и AI в цифровата криминалистика, цифрово криминалистично разследване и за подготовка на компютърни експертизи. Показани са и резултатите от изследване относно прилагане на техники за ML и AI при класифициране на цифрови доказателства, при анализ на съдържанието и извършване на текстово обобщение на pdf документи за улесняване и автоматизиране работата на експерти-криминалисти.

Настоящото изследване допринася за по-доброто разбиране на съвременни технологии, кога и какви ML и AI алгоритми да се използват за подобряване на процеса на DFI. Какви са предимствата и недостатъците на тези нови технологии. Констатациите са обобщени чрез рамка, която представя използването на AI и ML в DFI.

За очертаване на състоянието на научните изследвания е извършен библиометричен анализ, като са разгледани най-новите публикации в тази област в научната база данни Scopus.

След очертаване на общата картина е направено и по-детайлно изследване на литературни източници, индексирани в Scopus при същата заявките “digital forensic investigation and machine learning” и “digital forensic investigation and artificial intelligence”, за да се види по-конкретно какви са получените научни резултати и постижения на изследователите, които могат да бъдат описани по следния начин:

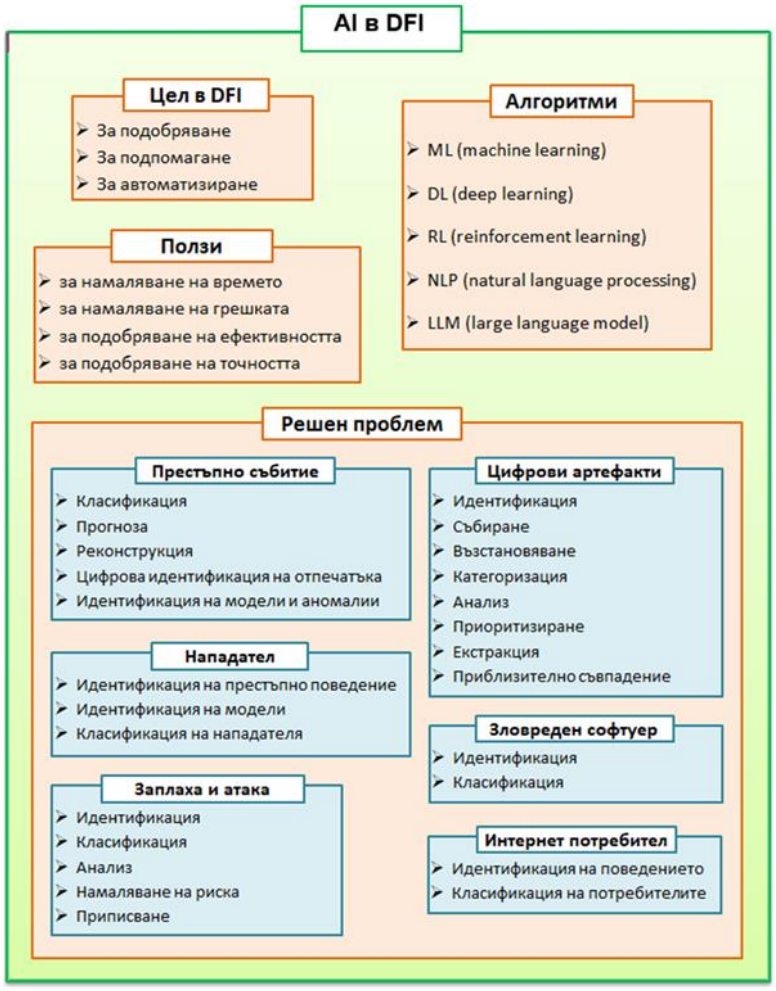
- Повечето от изследователите виждат потенциала на тези технологии за DFI и препоръчват ускоряване на разработването на инструменти, които да бъдат интегрирани в различни стъпки и процедури на DFI. Друга част от изследователите също са съгласни, че ML и AI имат капацитета да улеснят, подобрят и автоматизират редица дейности, типични за DFI, но препоръчват внимателно и подходящо използване на напреднали технологии. Тази загриженост идва от факта, че AI може да помогне на експертите-криминалисти, но ако се използва злонамерено от нападател, може да причини значителни щети;
- Може да се обобщи, че през последните няколко години интересът към тази тема силно привлича изследователи, като водещите автори в тази област са предимно от Индия, Великобритания, Саудитска Арабия, Ирландия, Пакистан, Германия. Сред най-проучваните теми са тези, свързани с разработване на модели за класификация и прогнозиране чрез прилагане на ML алгоритми, разработване на архитектури на изкуствени невронни мрежи и разработване на архитектури на DL алгоритми, подобряване на NLP

техники и модели за извличане на данни, прилагане на алгоритми за откриване на аномалии, използване на LLM;

- Може да се каже, че ML и AI имат потенциала бързо да обработват и анализират събрани или извлечени данни в DFI, да реконструират местопрестъпление и времева линия, да откриват и свързват доказателства, да предсказват насилствено поведение, да осигуряват верига за менажиране на доказателства, да подпомагат подготовката на документация, както и за подобряване на някои параметри на DFI.

Създадена рамка за приложение на AI в DFI

Въз основа на направените проучвания по-горе е създадена рамка, която обобщава основните проблеми и изследователски насоки, в които работи научната общност, в контекста на използване на предимствата на AI за процеса на DFI (Фигура 24).



Фиг. 24 Рамка за приложение на AI в DFI

От прегледа на литературата може да се види, че съществуващите AI техники непрекъснато се подобряват, както и че се търсят и създават нови решения. Алгоритми от ML, DL и RL често са полезни инструменти за решаване на проблеми в DFI. NLP също е сред интензивно изследваните техники за подпомагане на дейности в DFI. Напоследък, LLMs стават популярни, защото са в състояние да работят ефективно с големи набори от данни, връщайки разумен отговор или обобщение на човешки език.

Анализиране на цифрови доказателства чрез техники от машинно обучение и изкуствен интелект

Намирането на следи от киберпрестъпления, идентифицирането на цифрови доказателства и извършване на техния допълнителен анализ е неразделна част от DFI и включва много важни стъпки за изготвяне на компютърна експертиза.

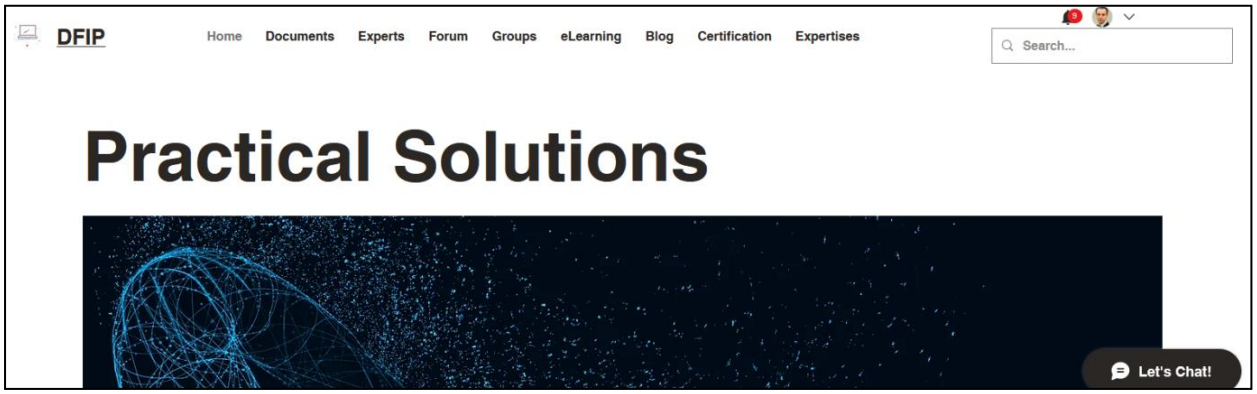
Извършени са няколко експеримента, като първият показва как голям брой различни типове файлове на машината на жертвата или атакуващ могат бързо да бъдат класифицирани. Беше приложен алгоритъм Decision Tree от контролирано ML и 17 типа файлове бяха класифицирани с висока точност. Второто изследване се отнася до използване на NLP техники за анализ на съдържание, което е включено в научни статии в pdf формат и в синтетично генерирани pdf файлове. Извличането на изображения от конкретен pdf файл също е демонстрирано. Извършен е и сентимент анализ, за да се получи по-добро разбиране за чувствата и настроението на авторите, които са написали специално подбраната научна статия и синтетично генериран pdf документ. Показано е как един документ може да бъде напълно проучен от различни гледни точки за подпомагане на експерти в DFI, за които и най-малкият детайл може да бъде важен. В третия случай потенциалът на LLMs за разкриване на нови знания е представен, като е използвана рамката на Ollama и моделът llama3.

ПЕТА ГЛАВА. РАЗРАБОТВАНЕ И ОЦЕНКА НА СОФТУЕРНА СИСТЕМА ЗА ЦЕЛИТЕ НА ЦИФРОВАТА КРИМИНАЛИСТИКА

Целта на пета глава е да представи разработен прототип на софтуерна система за целите на цифровата криминалистика съобразно създадената методология за разследване в цифровата криминалистика от практическа гледна точка DFIP и извършване на оценка относно имплементираната функционалност от експерти-криминалисти.

Разработен софтуерен прототип

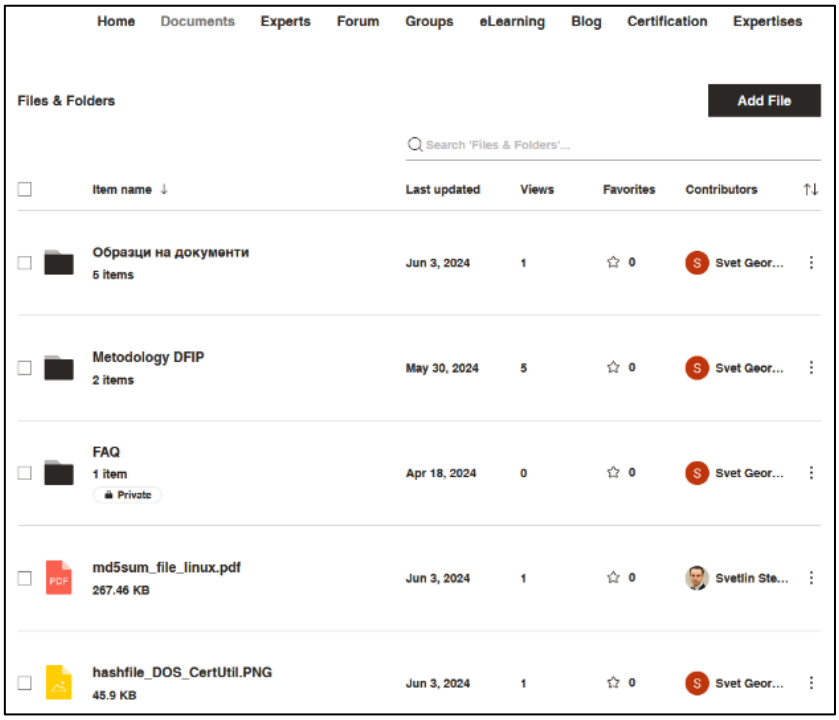
Софтуерната система включва множество компоненти, отговарящи на разработената функционална архитектура и архитектурния модел на софтуерен прототип, като следва описание на по-важните от тях. Входно/изходният компонент е вратата към системата. Използваният подход е, че само предварително регистрирани потребители от администратора могат да влизат в системата с имейл и парола. След като се влезе в системата, потребителят се установява на началната страница *Home*, на която има описание на разработената методология DFIP (Фигура 35). Също така, основните опции за избор на потребител се виждат под формата на меню.



Фиг. 35 Home page

Секцията *Documents* е място с възможност за споделяне на файлове от Експертите, като стандартни формуляри, работни книги, основни резултати от проведени изследвания. Освен това принципът на

конфиденциалност е спазен при контрола на достъпа до качените документи (Фигура 36).



Фиг. 36 Documents management

Секция *Experts* съдържа подробна информация за експертите, техните компетенции и опит. Този раздел е изключително полезен, когато трябва да бъдат избрани и подготвени членове на екипа за извършване на разследване по даден случай.

Разделът *Forum* гарантира, че всеки експерт може да създава публикации с актуално послание, да следва тези, написани от друг експерт, да коментира, харесва и споделя.

Разделът „*Groups*“ позволява на всеки член и администратор да създава групи, тъй като всяка група включва експерти за решаване на различни случаи на цифрова криминалистика.

В раздела за електронно обучение *eLearning,* всеки експерт има възможност да премине през процес на обучение по микрообучение с интерактивно съдържание и тест за оценка, ще получат значки за постижения след успешно изпълнение на курса, насоки за масивни отворени онлайн курсове (MOOC), които са достъпни за всеки, който може да се запише.

Компонентът *Expertise* предлага формуляри – вид шаблон, с вградени контроли за съдържанието на документите, използвани от Експертите при изземване на цифрови доказателства и изследването им в лаборатория.

Дадена е възможност за подпомагане на експерт-криминалист чрез предложение на съдържание за завършване на протокола чрез машинно обучение от налични изследователски модели. Използването на AI компонента е в подкрепа на търсенето на артефакти и предлага дестинации (пътеки) за тяхното откриване на изследваната памет.

Чатът може да се използва от всеки експерт за директна комуникация с останалите експерти за да си изпращат съобщения един на друг или да създават и управляват групови чатове.

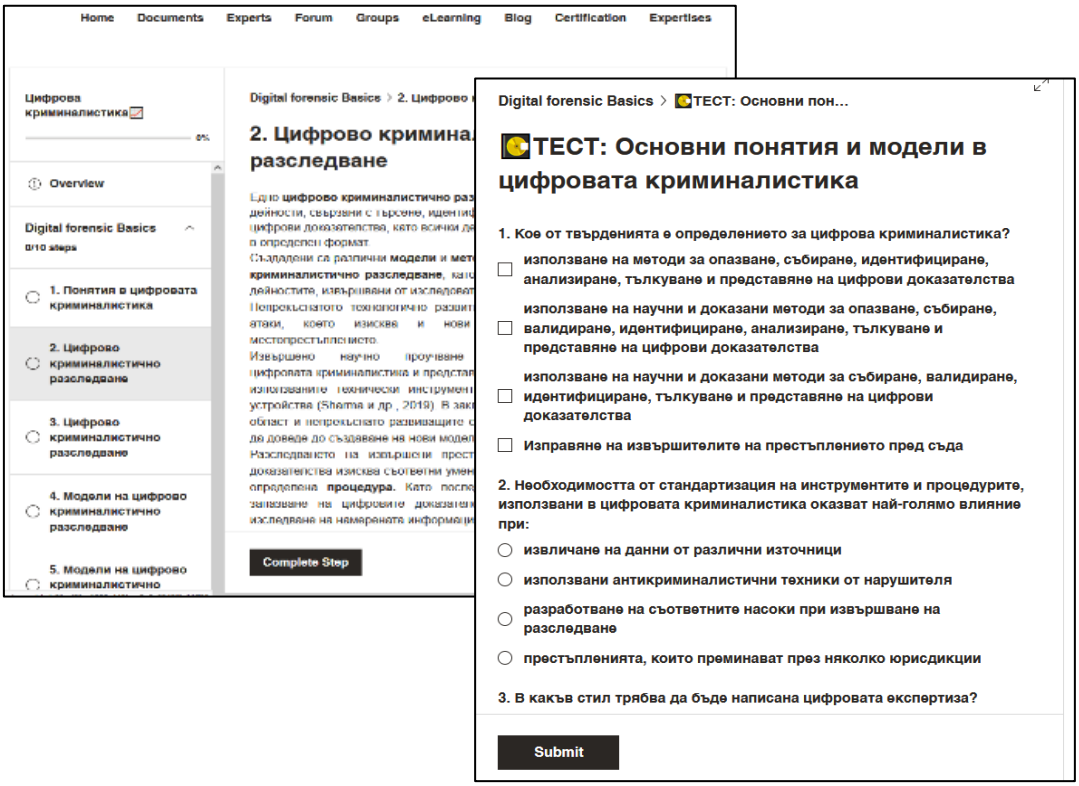
Разработената система може да се използва и от смартфон, което е предимство за експертите, когато е необходим незабавен достъп до материали и ресурси.

Микрообучение в курс по цифрова криминалистика

Цифровите експерти непрекъснато им се налага да учат по време на работа и в самия процес на разследване, но те също могат да бъдат включени в различни курсове за обучение, които ги запознават с новоизползваните технологии за атаки, техники за разследване или просто да дадат концептуализирани и обобщени аспекти в определена област на цифровата криминалистика.

В тази секция е представен разработен концептуален модел, подходящ за обучение на криминалисти за бързо и по време на работа придобиване на нови или обобщаване на съществуващи знания и за подобряване на тяхното обучение. Моделът се основава на стратегии за микрообучение, саморегулиращо обучение, използване на цифрови значки, както и участие в отворени онлайн курсове (Massive Open Online Courses - MOOC) и концепции за отворени образователни ресурси (Open Educational Resources - OER) за получаване на допълнителни знания и умения. Концептуалният модел е верифициран на практика чрез разработване на курс в софтуерна система за

подпомагане на цифрово криминалистично разследване и за улесняване на подготовката на компютърни експертизи. Курсът е част от областта за електронно обучение в софтуерната система, която предлага участие на криминалисти в саморегулирано обучение. Част от курса е представена на Фигура 46.



Фиг. 46 Част от създаден курс по цифрова криминалистика

Оценка функционалността на софтуерната система

Целта на тази секция е да представи изследване, съдържащо мнението и нагласите на криминалистите за полезността и ролята на разработената софтуерна система при извършване на цифрови криминалистични разследвания. Основният фокус е насочен към подпомагане на криминалистите в различните фази на разследванията, при извършване на дейности като комуникация, обмен на документи, търсене в документи, папки и експерти, изготвяне на компютърна експертиза, получаване на нова информация и обучение.

За да се оцени функционалността на първоначално разработената софтуерна система, която е изградена в съответствие с предварително

създадената методология DFIP, е разработен структуриран въпросник за получаване на мнение и отношение от регистрираните експерти относно функционалността на софтуерната система. Извършен е обобщение и анализ на получените отговори, за да се разбере полезността на системата в помощ на дейности по дигитално криминалистично разследване. Вотът на респондентите е много висок по отношение на:

(1) възможности за организиране на онлайн синхронна и асинхронна комуникация (в групи и на лична линия между криминалисти);

(2) възможност на системата за търсене на експерти, файлове, информация;

(3) функции относно управление, контрол и споделяне на папки и файлове;

(4) функции за създаване и управление на групи и екипи;

(5) предоставяне на новини и актуална информация в областта на цифровата криминалистика;

(6) организиране на саморегулирано обучение и участие в MOOCs;

(7) подпомагане на подготовката на компютърна експертиза;

(8) функции за организиране на лично виртуално пространство;

(9) функции за управление на различни дейности във фазите от методологията DFIP;

(10) реализиране на сигурност и поверителност чрез използване на различни нива на достъп според ролята на участниците: администратор, регистриран потребител и член на екипа.

Също така експертите-криминалисти споделят, че софтуерната система допринася за подобряване на тяхната ефективност, като ги улеснява при общуване, работа в екип, управление на документи, търсене в информация и документация и изготвяне на компютърна експертиза.

Може да се види, че създаването на софтуерна система, изградена на базата на теоретично издържана и практически приложима методология Digital Forensics Investigation from Practical Point of Practical View - DFIP е изключително важна стъпка в цифровата

криминалистика, позволяваща на експертите ефективно да организират и управляват дейности, типични за процес на разследване в DF, което беше потвърдено от самите експерти-криминалисти. Тази система беше разработена, защото беше идентифицирана липсата на интегрирано решение, комбиниращо множество инструменти във виртуалното пространство в помощ на разследващите органи.

Заключение

Дисертационният труд разглежда изключително важен и актуален проблем, свързан с подпомагане и автоматизиране на дейности, типични за разследване в цифровата криминалистика. Чрез разработената *методология за цифрово криминалистично разследване от практическа гледна точка* (DFIP) и последващото и имлементиране в софтуерна система се дава възможност на криминалистите да ускорят процеса на разследване, както и да бъдат по-ефективни при откриване и анализиране на цифрови доказателства в една усложнена обстановка на киберпрестъпност.

Познаването и използването на съвременни техники и методи от машинно обучение и изкуствен интелект в практиката на криминалистите понякога е от решаващо значение за коректността и точността на получените резултати и подготовка на компютърни експертизи.

Предложеният подход в дисертационния труд предоставя големи възможности за практическо използване на нови технологии и технологични решения за подобряване на организацията на разследванията като цяло, както и на дейности от отделните фази на методологията за постигане на навременност, качество и експертност при защита на компютърно-техническите експертизи пред съдебните органи.

Приноси

Научни и научно-приложни приноси:

1. Разработен е концептуален модел, представящ развитието на рамки и модели в цифрово криминалистично разследване, както и представящ значението на техники от изкуствен интелект, машинно и дълбоко обучение за подпомагане на експерт-разследващ.
2. Разработена е методология за цифрово разследване в цифровата криминалистика от практическа гледна точка – DFIP, включваща 12 фази, за подпомагане дейности на разследващи-експерти.
3. Предложен е подобрен модел за придобиване на цифрови доказателства за подпомагане изпълнението на фаза 2 от методологията.
4. Разработена е рамка за приложението на техники от изкуствен интелект в цифровата криминалистика, в цифрово криминалистично разследване и за подготовка на компютърни експертизи.
5. Създаден е класификационен модел за класификация на 17 вида файлови формати за подпомагане анализа на цифрови доказателства.
6. Създадени са два модела, съответно за изследване на текстовото съдържание и извличане на снимки от pdf файлове, за автоматизиране анализа на цифрови доказателства.
7. Създаден е модел за сентимент анализ на съдържанието на pdf файлове за подобряване на цифрово криминалистично разследване.

Приложни приноси:

1. Създаден е функционален архитектурен модел на софтуерна система, която е теоретично обоснована, интегрираща методология за разследване в цифровата криминалистика от практическа гледна точка DFIP и практически необходима съобразно изискванията на експерти-криминалисти.

2. Разработен е софтуерен прототип на система за автоматизиране на дейности в цифровата криминалистика въз основа на създадената преди това методология за разследване в цифровата криминалистика от практическа гледна точка.

ПУБЛИКАЦИИ ПО ТЕМАТА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Ivanova, M., and **Stefanov, S.**, "Digital Forensics Investigation Models: Current State and Analysis," 2023 8th International Conference on Smart and Sustainable Technologies (SpliTech), Split/Bol, Croatia, 2023, pp. 1-4, doi: 10.23919/SpliTech58164.2023.10193176. **Scopus**
   a. Забелязани са следните цитирания:
      i. Taavaldyev Kylychbek, Ismailova Rita, "Detecting Digital Footprints in Virtual Criminal Processes: A Review Of Digital Forensics Studies," Bulletin of Osh State University, ISSN: 1694-7452 e-ISSN: 1694-8610 №2/2024, 479-494, doi: 10.52754/16948610_2024_2_47.
      ii. Ogundiran Ayodeji, "A Goal-Oriented Visualization Approach to Digital Forensics Evidence Presentation," PhD Dissertation, Bowie State University, (2024), ProQuest, Number: 31562472.
2. **Stefanov, S.** and Ivanova, M., "Methodology for Digital Forensic Investigation DFIP: A Contemporary Glace from Practical Point of View," 49th International Conference Applications of Mathematics in Engineering and Economics, 10-16 June, 2023, Sozopol, Bulgaria (под печат)
3. **Stefanov, S.,** Ivanova, M., "An Architecture for Realization of Methodology Digital Forensics Investigation from Practical Point of View DFIP: A Requirement Analysis," In: Yang, XS., Sherratt, S., Dey, N., Joshi, A. (eds) Proceedings of Ninth International Congress on Information and Communication Technology. ICICT 2024, Lecture Notes in Networks and Systems, vol. 1013. Springer,

Singapore, (2024). https://doi.org/10.1007/978-981-97-3559-4_35. **Scopus SJR: 0.17, Q4**

4. **Stefanov, S.** and Ivanova, M., "A Software System to Facilitate Digital Forensics Investigation and to Support Preparation of Digital Expertise," 50th International Conference Applications of Mathematics in Engineering and Economics AMEE'2024, 7-13 June, (2024), Sozopol, Bulgaria (под печат)

5. **Stefanov, S.,** and Ivanova, M., "Implementation of Microlearning for Self-Regulated Course in Digital Forensics Investigation: In Support of Learning Performance and Workplace-Driven Tasks," 50th International Conference Applications of Mathematics in Engineering and Economics AMEE'2024, 7-13 June, 2024, Sozopol, Bulgaria (под печат)

6. Ivanova, M. and **Stefanov, S.**, "Regarding Artificial Intelligence in Digital Forensic Investigation: Applications and Solutions," 2024 XXXIII International Scientific Conference Electronics (ET), Sozopol, Bulgaria, (2024), pp. 1-6, doi: 10.1109/ET63133.2024.10721531. **Scopus**

7. **Stefanov, S.** and Ivanova, M., "Evaluation of Software System based on Methodology Digital Forensics Investigation from Practical Point of View DFIP," 10th International Congress on Information and Communication Technology ICICT 2025, 18-21 February, (2025), London, UK. (приета)

8. Ivanova, M. and **Stefanov, S.,** "Evidence Analysis through Artificial Intelligence Techniques to Facilitate Digital Forensic Investigation and Preparation of Computer Expertise," 10th International Congress on Information and Communication Technology ICICT 2025, 18-21 February, (2025), London, UK. (приета)

SUMMARY

The dissertation addresses an extremely important and topical issue related to the maintenance and automation of activities characteristic of investigation in digital forensics. The developed Methodology Digital Forensics Investigation from Practical Point of View (DFIP) and its subsequent implementation in a software system allows forensic scientists to accelerate the investigation process, as well as to be more effective in the discovery and analysis of digital evidence in a complex cybercrime environment.

In this dissertation, we have studied, analyzed and summarized contemporary scientific achievements regarding models for Digital Forensic Investigation (DFI) in recently published scientific articles, outlining some challenges and trends in the context of the research topic. We have also summarized the results in a conceptual model showing the current state of Digital Forensics (DF) and in conducting forensic investigations.

Based on the research conducted, a framework has been created that summarizes the main problems and research directions in which the scientific community is working, in the context of using the advantages of AI for the DFI process.

The functionality of the initially developed software system, which was built in accordance with the previously established DFIP methodology, was evaluated by forensic experts, who shared that the software system contributes to improving their efficiency by facilitating their communication, teamwork, document flow, information and documentation search, and preparation of digital expertise.

The approach proposed in the dissertation provides great opportunities for the practical use of new technologies and technological solutions to improve the organization of investigations as a whole, as well as activities in the individual phases of the methodology to achieve timeliness, quality and expertise in the defense of computer-technical expertise before judicial authorities.