УНИВЕРЗИТЕТ У НОВОМ САДУ

ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА

ОБЕЗБЕЂИВАЊЕ ВАЉАНОСТИ ФОРЕНЗИЧКЕ ИСТРАГЕ ПРИМЕНОМ ДЕСКРИПТИВНЕ ЛОГИКЕ

ДОКТОРСКА ДИСЕРТАЦИЈА

Ментор:
доц. др Жељко Вуковић

Кандидат:
Милица Матијевић Гостојић

Нови Сад, 2025. године

УНИВЕРЗИТЕТ У НОВОМ САДУ **ОБРАЗАЦ – 5а**
ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА

КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА[1]

Врста рада:	Докторска дисертација
Име и презиме аутора:	Милица Матијевић Гостојић
Ментор (титула, име, презиме, звање, институција):	др Жељко Вуковић, доцент, Факултет техничких наука у Новом Саду
Наслов рада:	Обезбеђивање ваљаности форензичке истраге применом дескриптивне логике
Језик и писмо рада:	српски ћирилица
Физички опис рада:	Унети број: Страница 219 Поглавља 8 Референци 121 Табела 6 Слика 54 Графикона 0 Прилога 2
Научна област:	Електротехничко и рачунарско инжењерство
Ужа научна област (научна дисциплина):	Примењене рачунарске науке и информатика
Кључне речи / предметна одредница:	дигитална форензика, прихватљивост дигиталних доказа, репрезентација знања, дескриптивна логика, аутоматско расуђивање
Апстракт на језику рада:	Истраживање описано овом дисертацијом посвећено је решавању проблема ангажовања неискусних форензичара у области информационих технологија у судском процесу, што потенцијално доводи до оспоравања или произвођења невалидних дигиталних трагова. Предлог решења је систем који се заснива на формалном опису искустава експерата и главних делова стандарда који прописују ваљано спровођење дигиталне форензичке истраге (ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042, ISO/IEC 27043), као и водича Националног института за стандарде и технологију САД-а и Међународне полицијске организације Интерпол. Овај формални опис чине конструкти дескриптивне логике SROIQ(D), те је расуђивањем над њиме омогућено аутоматизовано вођење неискусног форензичара кроз ваљану форензичку истрагу. Решење је верификовано спровођењем пост-тест експеримента са контролном групом у коме експериментални фактор представља употреба поменутог система.

[1] Аутор докторске дисертације потписао је и приложио следеће Обрасце:
5б – Изјава о ауторству;
5в – Изјава о истоветности штампане и електронске верзије докторског рада и дозвола за објављивање личних података;
5г – Изјава о коришћењу.
Ове Изјаве се чувају у институцији у штампаном и електронском облику и не кориче се са радом.

Датум прихватања теме од стране надлежног већа:	
Датум одбране: (Попуњава накнадно институција)	
Чланови комисије: (титула, име, презиме, звање, институција)	Председник: др Бранко Милосављевић, ред. проф, Факултет техничких наука Универзитета у Новом Саду Члан: др Братислав Предић, редовни професор, Електронски факултет Универзитета у Нишу Члан: др Илија Башичевић, редовни професор, Факултет техничких наука Универзитета у Новом Саду Члан: др Јелена Сливка, редовни професор, Факултет техничких наука Универзитета у Новом Саду Члан: др Марко Марковић, ванредни професор, Факултет техничких наука Универзитета у Новом Саду Члан, ментор: др Жељко Вуковић, доцент, Факултет техничких наука Универзитета у Новом Саду
Напомена:	

UNIVERSITY OF NOVI SAD
FACULTY OR CENTER

KEY WORD DOCUMENTATION[2]

Document type:	Doctoral dissertation
Author:	Milica Matijević Gostojić
Supervisor (title, first name, last name, position, institution)	PhD, Željko Vuković, assistant professor, Faculty of Technical Sciences, University of Novi Sad
Thesis title in English:	Ensuring the Soundness of Digital Forensic Investigations Using Description Logic
Language and script:	Serbian Cyrillic
Physical description:	Number of: Pages 219 Chapters 8 References 121 Tables 6 Illustrations 54 Graphs 0 Appendices 2
Scientific field:	Electrical engineering and computing
Scientific subfield (scientific discipline):	Applied computer science and informatics
Subject, Key words:	digital forensics, digital evidence admissibility, knowledge representation, description logic, automated reasoning
Abstract in English:	This dissertation addresses the issue of involving inexperienced digital forensic practitioners in judicial proceedings, which can compromise the integrity of the investigative process and result in the production of inadmissible or invalid digital evidence. To mitigate this risk, a knowledge-based system is proposed, based on a formal representation of expert-level knowledge and the normative requirements of internationally recognized digital forensic standards, including ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042, and ISO/IEC 27043. The model also incorporates guidelines issued by the U.S. National Institute of Standards and Technology (NIST) and the International Criminal Police Organization (INTERPOL). The formal representation of a sound forensic process is specified using the SROIQ(D) description logic, enabling automated reasoning over the knowledge base and facilitating standards-compliant guidance for novice forensic practitioners. The system was validated through a post-test randomized controlled trial, in which the independent variable was the use of the proposed system.

[2] The author of the doctoral dissertation has signed the following Statements:
5б – Statement on the authorship,
5в – Statement that the printed and e-version of the doctoral dissertation are identical and authorization to use personal data,
5г – Copyright statement.
The paper and e-versions of Statements are held at the institution and are not included into the printed thesis.

Date of endorsement by the scientific board:	
Date of defence: (Filled in by the institution)	
Thesis defence board: (title, first name, last name, position, institution)	Chair:, PhD, Branko Milosavljević, Full professor, Faculty of Technical Sciences University of Novi Sad Member: PhD, Bratislav Predić, Full professor, Faculty of Electronical Engineering University of Niš Member: PhD, Ilija Bašičević, Full professor, Faculty of Technical Sciences University of Novi Sad Member: PhD, Jelena Slivka, Full professor, Faculty of Technical Sciences University of Novi Sad Member: PhD, Marko Marković, Associate professor, Faculty of Technical Sciences University of Novi Sad Member, Mentor: PhD, Željko Vuković, Assistant professor, Faculty of Technical Sciences University of Novi Sad
Note:	

Захвалница

Захваљујем се својим драгим родитељима за безбрижан животни и академски пут.

Захваљујем се својим средњошколским професорима за подстрек да се у мени роди љубав према науци.

Захваљујем се комисији на удубљивању у рад и изузетно конструктивним коментарима.

Захваљујем се генерацији студената 2023 мастер студија, који су похађали курс Увод у дигиталну форензику, на доброј вољи за учешће у истраживању.

Посебно се захваљујем ментору, доц. др Жељку Вуковићу, за усмеравање и другарски приступ.

Садржај

Списак скраћеница

CCTV Closed Circuit Televison 18

ESN Electronic Serial Number 17

EVE The Emulated Virtual Environment 156

GPS Global Positioning System 23

GSM Global System for Mobile Communications 17

IMEI International Mobile Equipment Identity 17

JWT JSON Web Token 98

LAN Local Area Network 23

LLM Large Language Model 170

NAS Network Attached Storage 17

PDAs Personal Digital Assistants 16

PEAP Protected Extensible Authentication Protocol 89

PEDs Personal Electronic Devices 16

PIN Personal Identification Number 19, 23

PUK Personal Unblocking Key 19, 23

RADIUS Remote Authentication Dial-In User Service 89

RAID Redundant Array of Independent Disks 21

RAM Random Access Memory 23

SAN Storage Area Network 17

SIM Subscriber Identity Module 19, 23

SSD Solid-State Drive 25

SWGDE Scientific Working Group on Digital Evidence 1

UPS Uninterruptible Power Supply 19, 20

USIM Universal Subscriber Identity Module 23

VPN Virtual Private Network 23

XAI Explainable Artificial Intelligence 171

Списак слика

Списак табела

Речник појмова[1]

Потенцијални дигитални доказ	Податак ускладиштен или пренесен у бинарном формату, који још није подвргнут фазама прегледања и анализе у оквиру форензичке истраге, те још нема епитет релевантног податка за истрагу.
Дигитални доказ	Информација или податак ускладиштен или пренесен у бинарном формату, који може послужити као доказ за утврђивање чињеница.
Релевантност дигиталног доказа	Карактеристика дигиталног доказа, која се огледа у способности доказа да потврди или оповргне неку од хипотеза случаја који се истражује.
Поузданост дигиталног доказа	Карактеристика дигиталног доказа, која подразумева да су дигитални докази стварно оно што се тврди да јесу.
Довољност дигиталних доказа	Карактеристика скупа дигиталних доказа, која подразумева да су дигитални докази из скупа довољни да се истрага спроведе задовољавајуће, односно да се одговори на задатак вештачења.
Оправданост истражног процеса	Карактеристика форензичке истраге, која омогућава независним проценитељима да, на основу датог образложења за предузете активности, одреде да ли је примењен адекватан научни метод, техника или процедура.
Проверљивост дигиталног доказа	Карактеристика дигиталног доказа, која омогућава другим форензичарима да евалуирају активности предузете током истраге.
Поновљивост дигиталног доказа	Карактеристика дигиталног доказа, која подразумева произвођење истог тест резултата понављањем истражне активности коришћењем истог мерног метода и процедуре, истог алата и под истим условима, без обзира на период након којег се истражна активност понавља.
Обновљивост дигиталног доказа	Карактеристика дигиталног доказа, која подразумева произвођење истог тест резултата понављањем истражне активности коришћењем истог мерног метода, али других алата, под другим условима, без обзира на време које прође након прве истражне активности.

[1]Неки од коришћених појмова наведени су сабрано у овом речнику појмова, као помоћ читаоцу. Потпуне дефиниције појмова наведене су у тексту.

Ланац надлежности	Документ који садржи хронологију руковања потенцијалним дигиталним доказом од тренутка када је идентификован, па до момента престанка важења материјала као доказног. Минималан скуп информација које садржи ланац надлежности укључује јединствени идентификатор доказа, име и презиме лица које је приступало доказу, време и датум када је доказу приступљено, где се доказ налазио у тренутку приступања, име и презиме особе која је доказни материјал унела, односно изнела са места чувања и време и датум када се то десило, разлог због којег је доказни материјал изнет са места чувања и белешку и образложење сваке неизбежне измене потенцијалног дигиталног доказа, као и име и презиме особе за то одговорне.
Процена ризика	Систематична евалуација ризика и његовог потенцијалног утицаја на дигиталну истрагу.
Објашњивост	Способност модела машинског учења да разјасни начин доласка до својих предвиђања, као и да дā процену у којој мери се на дата предвиђања треба ослонити.
Интерпретабилност	Способност модела машинског учења да објасни значење својих предвиђања.
Сажетак (хеш-вредност)	Вредност која зависи од садржаја и омогућава утврђивање постојања измене садржаја.

1 Увод

- Није сигурно да ништа није сигурно.

Блез Паскал

Човекова тежња ка моралности сликовито се представља тежњом да се концентрични кругови који обухватају оно што се подразумева под правдом и правом проширују све више не би ли се стопили са кругом морала, који има исти центар, али астрономски већи пречник. Још од краја 19. века знало се за све битне елементе суђења по правичности, као практичној примени правде. У свом *Општем имовинском законику*, Валтазар Богишић, између осталог, каже: „Судија у суђењу треба да пази на разум и мишљење народа или разреда људи којима су обични послови те руке" (Богишић, 1898), мислећи при томе на доказе проистекле из професионалних схватања вештака ангажованих у судском поступку. Тежиште ове дисертације управо је на њима – вештацима, и то у области информационих технологија, тј. стручњацима за дигиталну форензику.

Федерални истражни биро (енг. *FBI*) је 1984. године, заједно са другим правним телима САД-а, започео увођење појма дигиталног, односно рачунарског доказа, а 1991. године, правна тела САД-а су се састала ради дискусије о истрази дигиталних трагова, односно дигиталној форензици, као научној дисциплини у оквиру које је неопходно развити стандардне процедуре и протоколе (Noblett и сар., 2000). Дакле, у оквиру дигиталне форензике, која је до тада имала претежно технички и практички карактер, јавља се потреба за сређивањем и систематизацијом знања, тј. за научним приступом. Потом је уследило дефинисање основних појмова дигиталне форензике, као и стандардних процедура форензичке истраге у дигиталном домену од стране Радне групе за дигиталне доказе, SWGDE (Whitcomb, 2002).

Тиме је почетком овога века заподенут убрзани развој дигиталне форензике као науке, која своја знања примењује над складиштима података у дигиталном облику и чији је циљ проналажење информација. Када се узме у обзир даљи пут информација проистеклих из форензичке истраге дигиталних уређаја, потреба за вештачењем у области информационих технологија отвара читаву нову димензију. Вештак за информационе технологије мора да буде не само експерт у области информационих технологија, већ је неопходно и познавање права, као и поседовање реторичких вештина.

Међутим, данас је поље дигиталне форензике изузетно широко и у сталном је развоју, па се поставља питање да ли је уопште могуће звати се експертом у области дигиталне форензике. Свако ко себе сматра експертом у поменутој области требало би да је у стању да фактима о свом знању и искуству подупре тврђење о експертизи, како би се о њој могло судити (Horsman и Shavers, 2022). У факта о знању и искуству форензичара свакако спадају претходни случајеви који, да би се сматрали искуством, морају бити бројни и морају имати одговарајући исход (Horsman, 2019).

У литератури (Ferrazzano и сар., 2021) се среће и конкретнији правац у дискусији о појму форензичког експерта у дигиталном домену. Наводе се карактеристике експерта међу којима су: савесност, компетентност, поузданост, непристрасност, независност, транспарентност, професионална комуникативност и поверљивост. Овоме се додају праћење актуелног стања у области уз различиту стручну литературу, као и фамилијарност са алатима и техникама које је заједница форензичара у дигиталном домену одобрила.

1.1 Мотивација

Ако експертиза не сме изостати приликом ангажовања форензичара дигиталних уређаја у правном поступку, како омогућити неискусним форензичарима да стичу искуство? Како потпомоћи постојеће квалитете форензичара када је у питању проналажење релевантних трагова и писање налаза и мишљења тако да они буду равни експерту? До сада су неискусни форензичари у својим извештајима и исказима проналазили потпору у праћењу стандарда и прописаних процедура, међутим, све то заснива се на интерпретацији самог форензичара, која услед неискуства или тренутних неповољних околности може бити погрешна.

Извештај, односно налаз и стручно мишљење форензичара, као продукт истраге који се разматра на суду, има кључну улогу у превођењу пронађених дигиталних трагова у доказе. Међутим, истраживање је показало да је неопходно да се писање налаза и мишљења међу форензичарима подигне на виши ниво како би се смањила могућност њиховог оспоравања на суду (Sunde, 2021).

Овде запажамо да је понекад и форензичару-експерту у области информационих технологија добродошла помоћ или сигурност у ваљаном спровођењу форензичке истраге и произвођењу доказа. Оно што се под помоћи подразумева, има два правца. Један је аутоматизована помоћ у виду вештачке интелигенције, а други се води изреком – две главе су паметније од једне, односно чињеницом да би два или више експерата у области дигиталне форензике спровела истрагу ваљаније него што би то урадио форензичар самостално.

Проблем употребе алатā који се заснивају на вештачкој интелигенцији правна бранша препознаје као проблем црне кутије (енг. *black-box*). Другим речима, неспособност форензичара да са сигурношћу објасни начин на који је алат произвео излазни податак, чини пронађене трагове неприхватљивим на суду. Ипак, у литератури (Solanke, 2022) се јављају предлози метода којима је могуће оправдати употребу оваквих система, но, остаје обавеза форензичара, који користи алат базиран на вештачкој интелигенцији, да изврши валидацију произведених трагова (Hall и сар., 2022).

Тако се наново враћамо на проблем неискусног, несигурног или недовољно компетентног форензичара, који има велику одговорност приликом спровођења форензичке истраге и сведочења о продуктима истраге на суду. Уз то, јасно је да је за сваког форензичара у дигиталном домену немогуће обезбедити партнера који ће у свакој истрази бити она друга глава.

Дакле, као решење се издваја систем који у својој бази интегрише знање и искуство више форензичара и у чије расуђивање је прихватљиво поуздати

се нарочито када се у обзир узме објашњивост начина расуђивања.

Значај проблема је очевидан, а значај представљеног решења огледа се у непобитности и складности тврђења ускладиштених у бази знања, што форензичару омогућује да се у њих поуздa и искористи их приликом састављања свог налаза и мишљења о реконструисаним догађајима. Такође, база знања се карактерише проширљивошћу како тврдњама из литературе, тако и искуством форензичара са успешним исходом у пракси, односно форензичара који су одговорили на задатке истраге дигиталним траговима који потврђују или оповргавају неку хипотезу.

Успех предложеног решења огледа се у његовој практичној примени од стране неискуснх форензичара који могу да посведоче о његовој корисности.

1.2 Предмет истраживања

Скуп проблема који чини предмет истраживања ове дисертације проистиче из систематичног прикупљања сазнања о ваљаном спровођењу форензичке истраге, као и из поседовања искуства у форензичкој пракси. Неискуство, несигурност или некомпетентност форензичара у дигиталном домену ангажованог у судском процесу, може довести до оспоравања дигиталних трагова који би требало да буду декларисани као дигитални докази или пак до произвођења невалидних дигиталних трагова.

Значај истраживања са циљем решавања ових проблема огледа се двојако, с обзиром на то да дигитална форензика повезује право и информационе технологије. Из угла права, у коме се огледа друштвени допринос истраживања на ову тему, недопустиво је да и један случај буде препуштен неискусном форензичару чије мишљење умногоме утиче на одлуку суда. Међутим, почетак каријере је неминовност у професионалном развоју сваког форензичара.

Најзначајнија прихваћена хипотеза која се среће у литератури, јесте да се ваљаност форензичке истраге огледа у конформацији стандардима и прописаним водичима и процедурама форензичке истраге (Makura и сар., 2021; McKemmish, 2008). Уз то, постоји запажање о потреби за формалним моделима форензичке истраге (Horsman, 2019), где је уочени проблем стандардизација формалних модела (Sikos, 2021).

Одабир теорија које су креирале мисаони стил овог истраживања, проистиче из ове хипотезе и отвореног питања, те је теоријско полазиште предмета овог истраживања креирање формалних модела прописаних стандарда и процедура ваљане форензичке истраге.

Операционално одређење предмета истраживања даље проистиче из конкретизације појмова који најопштије указују на предмет истраживања, а уткани су у наслов ове дисертације. Изабрани метод креирања формалних модела је дескриптивна логика и то SROIQ(D) дескриптивна логика, а одабрани стандарди и процедуре за извођење ваљане форензичке истраге су ISO/IEC 27037 (2015), ISO/IEC 27041 (2016), ISO/IEC 27042 (2016), ISO/IEC 27043 (2016), „Guide to Integrating Forensic Techniques into Incident Response" (Kent и сар., 2006) и „Guidelines for Digital Forensics First Responders" (Interpol, 2021).

С обзиром на то да форензичка истрага може укључивати различите диги-

талне уређаје и уређаје на којима су складиштени подаци, дигитална форензика као дисциплина дели се на више поддисциплина. Међу њима су форензика масовне меморије која трагове тражи међу подацима ускладиштеним у трајној меморији, форензика радне меморије, која се фокусира на несталне податке, форензика оперативних система, која се бави артефактима оперативних система, форензика рачунарских мрежа, која рукује подацима који се преносе преко мреже или их логују мрежни уређаји, форензика апликација, чији су фокус различите корисничке апликације, форензика мобилних телефона и др.

Дакле, научни допринос у пољу информационих технологија, односно допринос увећању фонда научног сазнања истраживања на поменуту тему огледа се у следећем:

1. смањењу могућности оспоравања дигиталних доказа који проистекну из тврдњи неискусних форензичара,

2. смањењу могућности произвођења невалидних дигиталних трагова услед неискуства или несигурности форензичара,

3. доприносу тачној интерпретацији стандарда у домену дигиталне форензике као текстуалних докумената креирањем формалног модела истих,

4. запажању о применљивости дескриптивне логике на процес форензичке истраге,

5. запажању о применљивости дескриптивне логике на појединачне фазе форензичке истраге.

1.3 Хипотеза истраживања

Хипотеза овог истраживања гласи: употреба водича кроз истрагу базираног на аутоматском расуђивању формалног модела форензичких стандарда од стране студената, који су у процесу учења о дигиталној форензици, обезбеђује већу ефективност и ефикасност у проналажењу и документовању дигиталних трагова.

При томе се под ефективношћу подразумева укупан број бодова које су студенти завредили решавајући задати случај, а ефикасност се мери временом које је студентима било потребно за решавање случаја.

Верификација хипотезе овог истраживања спроведена је у оквирима форензике рачунарских мрежа. Разлог за то лежи у енормној количини уређаја који су умрежени и имају приступ Интернету, те енормној количини података који се преносе преко мреже, што имплицира велики значај ове области. Међутим, истраживање се може проширити на било коју поддисциплину дигиталне форензике.

1.4 Циљеви истраживања

Постигнути циљ овог истраживања може се посматрати са друштвеног и научног аспекта.

Научни циљ сваког истраживања је стицање научног сазнања које се среће у различитим облицима. Тако је за ово истраживање везано откриће узрочно-последичне везе између истраге вођене аутоматским расуђивањем базираним на формалном моделу форензичких стандарда и ваљано спроведене форензичке истраге. У ужем смислу, узрочно-последична веза огледа се у спровођењу истраге од стране неискусног форензичара успешније када као водич кроз истрагу форензичар користи систем базиран на формалном моделу форензичких стандарда.

Постигнути друштвени циљ овог истраживања огледа се у примени поменутог открића. Под тим се подразумева алат иза кога стоји реализација овог истраживања, који је везан за почетак каријере форензичара у дигиталном домену, вештака за информационе технологије или будућих форензичара.

Реализација овог истраживања обухватила је следеће: развој базе знања која формално описује главне делове стандарда за спровођење форензичке истраге, спецификацију захтева информационог система који служи као водич кроз форензичку истрагу, дизајн и пројектовање информационог система базираног на знању као водича кроз форензичку истрагу, прототипску имплементацију информационог система базираног на знању и верификацију прототипске имплементације информационог система.

1.5 Метод истраживања

Тежиште методологије овог истраживања је формално описивање знања из домена дигиталне форензике и омогућавање аутоматског расуђивања над њим. Стога, иако се успех овог система огледа у његовој практичној примени, не треба занемарити и способност система да покаже у којој мери је одабрана методологија применљива на решавање поменутог проблема.

Мисаоно-логички приступ овоме истраживању одликују основне методе анализе, апстракције и специјализације, односно дефиниције, као и методе развоја софтвера.

Метод који претходи осталима је анализа и то анализа поменутих стандарда и процедура који прописују ваљано спровођење истраге. Резултат анализе је издвајање битних компоненти из целокупног документа и уочавање односа међу њима.

Затим следи метод апстракције којим се међу издвојеним битним компонентама издвајају најопштије. У овом истраживању то подразумева издвајање и формулисање четири главне оперативне форме које се везују за четири фазе форензичке истраге, као и формулисање критеријума ваљаности које је у свакој фази форензичке истраге потребно задовољити.

Метод апстракције се потом преусмерава са општих компоненти на посебне. Другим речима, ниво апстракције оперативних форми форензичке истраге, фаза и критеријума ваљаности форензичке истраге спушта се ниже све до појединачних представника (инстанци).

На крају, методом специјализације појмова, односно дефинисања, врши се повезивање оперативних форми форензичке истраге, фаза форензичке истраге и критеријума ваљаности, чиме се обезбеђује дедуктивно закључивање о

ваљаности дате форензичке истраге.

Поменутим методама утврђене су чињенице и односи међу њима у документима који представљају међународно прихваћене стандарде и процедуре за извођење ваљане форензичке истраге. Следеће у мисаоно-логичком приступу истраживању је креирање формалног модела ових чињеница и њихових односа употребом дескриптивне логике SROIQ(D).

Дескриптивна логика SROIQ(D) пружа могућност неколико типова расуђивања. Међу њима су закључивање о инстанцама појмова, одређивање потпојмова појмова и одређивање појмова на основу дате везе међу појмовима.

Реализација хипотезе коначно се завршава применом метода објектно-оријентисаног развоја софтвера – развојем водича за спровођење истраге. Резултат прве фазе развоја софтвера је спецификација захтева, односно структуре и понашања система, који су проистекли из циљева овог истраживања, као и анализе окружења у коме ће систем бити коришћен. Спецификација захтева описана је случајевима коришћења, који су потом приказани дијаграмом. Друга фаза развоја софтвера подразумева дизајн пословне логике, односно његову логичку структуру и понашање. Логичка структура система описана је концептуалним моделом који се заснива на концептима формалног описа форензичке истраге, док је логичко понашање система описано дијаграмом секвенци. Из фазе развоја софтвера која следи, фазе пројектовања, проистиче архитектура система, чије компоненте су имплементиране у фази имплементације. Фаза имплементације описана је дијаграмом компоненти и дијаграмом распоређивања.

За прикупљање података на основу којих се вршила верификација хипотезе, која је горе поменутим методама реализована, коришћен је експериментални метод.

Уз етичку дозволу за спровођење експеримента, узорковани су студенти мастер академских студија Факултета техничких наука Универзитета у Новом Саду, који су слушали предмет Увод у дигиталну форензику. Величина узорка је 60 студената једнако подељених на експерименталну и контролну групу.

Експериментални фактор представља употреба система као водича за спровођење истраге. Истрага је, у овом случају, решавање задатака на тему форензике рачунарских мрежа и одговарање на питања представљена тестом. Свако питање у тесту вреди један бод.

Да би студентима било омогућено спровођење истраге, креирано је окружење које симулира рачунарску мрежу са траговима које студенти морају пронаћи да би одговорили на питања теста.

Ефекат експерименталног фактора мерен је упоређивањем ефективности студената, односно средњом вредношћу бодова студената експерименталне и контролне групе завређених решавањем теста. Такође, експериментални фактор мерен је и упоређивањем ефикасности студената мерењем времена које им је било потребно за истрагу и решавање теста. Поред ових квантитативних података, студенти експерименталне групе допринели су квалитативним подацима који осликавају њихова лична искуства у вези са употребом система.

Анализа резултата експеримента укључила је и извођење статистичког теста да би се испитао њихов статистички значај. Како постоје две групе сту-

дената и како се упоређују средње вредности освојених бодова у обе групе, адекватна је примена t-теста са независним узорцима. При томе се за нулту хипотезу узело тврђење да употреба система не доприноси ефективности и ефикасности спровођења истраге. t-тест се применио над студентским резултатима целокупне истраге, али и над резултатима појединачних фаза форензичке истраге – идентификацијом доказа, прикупљањем доказа, прегледањем доказа и анализом доказа.

1.6 Оправданост истраживања

Већ је било речи о значају истраживања на наведену тему уопште. Међутим, овај одељак се односи на научни и друштвени допринос овог истраживања.

Научни допринос овог истраживања, који истраживање оправдава, огледа се у резултатима истраживања, а остварио се у виду хеуристичког резултата и у виду верификаторног резултата. Хеуристички резултат је утврђивање применљивости аутоматског расуђивања дескриптивне логике $SROIQ(D)$ на вођење форензичке истраге. Верификаторни резултат је реализација ове примене у виду система, који је спреман за коришћење од стране неискусних форензичара.

Друштвени проблем чијим решавањем се оправдава ово истраживање огледа се у ослањању на несигурне налазе и мишљења неискусних форензичара. Проблематика добија на значају ако се у обзир узму истраживања која показују да је сајбер криминал све напреднији, а да су циљеви сајбер криминалаца све критичнији и профитабилнији (Europol, 2019). Нарочит пораст бележи се у контексту високотехнолошког криминала и безбедносних инцидената (Normurod o'g'li и сар., 2023). Дакле, употреба програма којим се реализовала хипотеза овог истраживања оправдава се доприносом кредибилитету форензичара ангажованог у судском поступку и смањењу могућности оспоравања трагова које је открио или могућности произвођења невалидних трагова.

1.7 Структура дисертације

Ова дисертација је организована у осам поглавља. Поглавље 2 даје теоријску основу истраживања, односно увод у дигиталну форензику и дескриптивну логику. При томе се акценат ставља на појмове дигиталног доказа, дигиталне истраге, дигиталне форензичке истраге, као и на дефинисање ваљане форензичке истраге. С друге стране, нагласак је на појму дескриптивне логике и на синтакси и семантици формализама који омогућују развој формалног модела.

Поглавље 3 пружа дискусију на тему ваљане форензичке истраге уз осврт на литературу, као и преглед литературе која се бави формалним описивањем домена дигиталне форензике са тежиштем на стандарде и процедуре у домену дигиталне форензике и информационе безбедности.

Поглављем 4 представља се модел форензичке истраге, који укључује фазе идентификације, прикупљања, прегледања и анализе доказа, као и формални опис главних делова стандарда и процедура за ваљано спровођење форензичке

истраге кроз поменуте четири фазе.

У поглављу 5 описан је развој система заснованог на формалном моделу главних делова стандарда и процедура за ваљано спровођење форензичке истраге. Дата је спецификација корисничких захтева и представљени су дизајн, пројектовање и имплементација система.

Поглавље 6 представља емпиријску валидацију система. Под тим се подразумева опис поставке експеримента и представљање резултата.

У поглављу 7 дискутован је избор стандарда и водича који су коришћени за креирање формалног модела форензичке истраге, оправдана је употреба симболичке вештачке интелигенције у односу на друге облике вештачке интелигенције, а затим су анализирани резултати експеримента и дискутоване су претње по валидност истраживања.

Дисертација се завршава поглављем 8 којим је извршена рекапитулација главних питања истраживања и одговора на њих, затим циљева истраживања и начина постизања циљева, резултата истраживања и њиховог значаја и ефекта, доприноса истраживања, објављених радова, као и предметā даљњих истраживања.

2 Теоријске основе

- Сваки контакт оставља траг.

Едмонд Локард

2.1 Преглед

Наредним одељцима разматрају се основни теоријски концепти ове дисертације. У одељку Дигитална форензика најпре је дата и дискутована дефиниција дигиталне форензике као једне од форензичких дисциплина. Изнета је дистинкција између појмова дигиталне истраге и дигиталне форензичке истраге и у складу са тим, објашњен је појам дигиталног доказа са освртом на правни систем Републике Србије. Потом су разматрани критеријуми ваљано спроведене дигиталне форензичке истраге на основу међународно признатих стандарда, водича и процедура, али и на основу правне регулативе у Републици Србији. У одељку Дескриптивна логика представљена је дескриптивна логика уопште, затим конкретно SROIQ(D) дескриптивна логика и њене синтакса и семантика, као и типови расуђивања.

2.2 Дигитална форензика

Не постоји јединствена формулација дефиниције дигиталне форензике, те је објашњење овог појма у овој дисертацији резултат обједињења више тумачења из литературе.

Дигитална форензика подразумева примену научно изведених и доказаних метода у очувању, прикупљању, валидацији, идентификацији, анализи, интерпретацији, документовању и презентовању дигиталних доказа проистеклих из дигиталних уређаја, са циљем реконструкције догађаја криминалне природе или антиципирања малициозних активности, а уз очување интегритета оригиналног доказа и ланца надлежности. (Palmer, 2001; Kent и сар., 2006).

Комплексност дигиталне форензике као науке расла је са порастом броја дигиталних уређаја који омогућују складиштење података (Makura и сар., 2021). Дакле, предмет дигиталне форензике нису само рачунари, већ се потенцијалним извором доказа сматра сваки медијум који омогућује складиштење података у дигиталном облику (Hayes, 2020).

Уз то, дигитални докази могу имати есенцијални значај у правном поступку, те је форензичар у области информационих технологија (у даљњем тексту: форензичар) у обавези да ваљано спроведе процес форензичке истраге. Треба напоменути да и истрага, која испрва није укључена у правни поступак, потенцијално може постати правни случај. Стога је и приликом корпорацијске истраге препоручљиво истрагу дигиталних уређаја спровести са мишљу да ће пронађени трагови бити разматрани на суду. Прихватљиви докази продукт

су истраге искусног форензичара који, имајући експертско знање у области информационих технологија, поседује знање и у области права, па се може претпоставити да је вештачење у области информационих технологија изазов за неискусног форензичара.

2.2.1 Дигитални доказ, дигитална истрага, дигитална форензичка истрага

У овом одељку прави се дистинкција између дигиталне истраге и дигиталне форензичке истраге, па се са оба ова аспекта посматра и појам дигиталног доказа.

Дигитална (сајбер) истрага подразумева систематично прикупљање, прегледање и евалуацију свих информација релевантних за успостављање чињеница о инцидентима повезаним са Интернетом или могућим сајбер злочином и идентификацију починилаца или учесника истих (Årnes, 2023). Другим речима, дигитална истрага се спроводи када рачунарски систем представља алат, циљ или део места злочина. Предмет дигиталне истраге је било која врста дигиталног уређаја укљученог у инцидент или злочин у смислу његове употребе током почињења физичког злочина или током дигиталних активности које нарушавају законско или друго правило (Carrier, 2005). Дигитална истрага захтева испитивање дигиталних уређаја које се састоји од постављања хипотезе и потраге за доказима (дигиталним доказима) који ће хипотезу оповргнути (Brooks, 2015).

Употреба термина дигиталног доказа врло је осетљива јер, како каже Brooks (2015): „нема видљиве линије раздвајања правног и техничког". Зато је овде нужно разјаснити значење термина доказ у правном контексту и у контексту форензичке истраге. У контексту форензичке истраге, дигитални доказ је било који дигитални податак који представља поуздане информације којима се потврђује или одбацује хипотеза у вези са неким инцидентом или злочином (Carrier и Spafford, 2004). Формулација која је примеренија правној бранши гласи: дигитални или електронски доказ је свака доказна информација која се складишти или се преноси у дигиталном облику таква да се може искористити на суду (Casey, 2011).

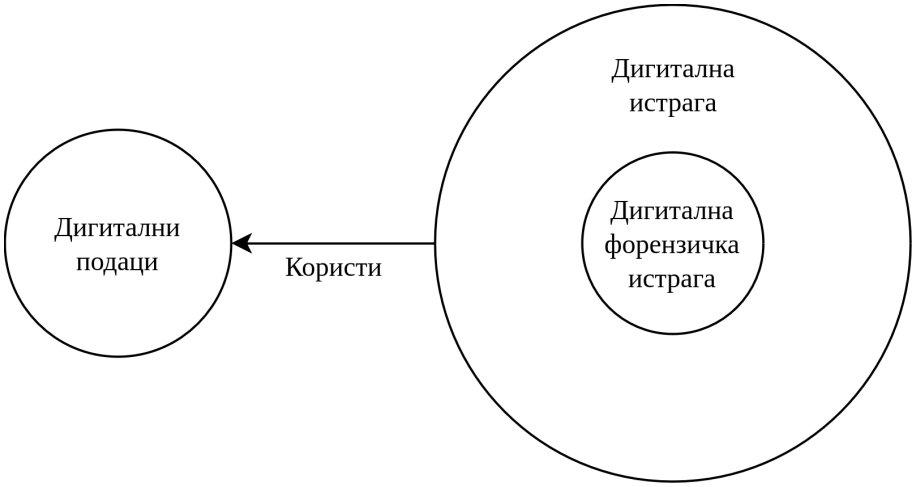
Такође, потребно је напоменути да у водичима Министарства правде САД-а, који се тичу руковања рачунарима у правне сврхе, постоји дистинкција између термина електронски и дигитални доказ. Електронским доказом сматра се сваки облик хардвера, односно свака физичка компонента рачунара, док се дигиталним доказом означава информација – подаци или програми складиштени у рачунару или пренесени помоћу рачунара. У складу са тим, Casey (2004) даје следећу поделу рачунарских доказа:

- хардвер као доказ,
- хардвер као инструмент криминалне активности,
- хардвер као забрањени материјал или плод криминалне активности,
- информација као доказ,

- информација као инструмент криминалне активности,
- информација као плод криминалне активности.

У правном систему Републике Србије, у тренутку писања ове дисертације, не постоји појам дигиталног доказа. Термин који се помиње у Законику о кривичном поступку, а који сличи малочас дефинисаном појму дигиталног доказа, јесте исправа. Дакле, „исправа је сваки предмет или рачунарски податак који је подобан или одређен да служи као доказ чињенице која се утврђује у поступку" (члан 83. ст. 1. и 2). Међутим, Савет Европе је у оквиру пројекта „iPROCEEDS" из 2018. године, којим је извршена процена у вези са прибављањем и коришћењем електронских доказа у кривичном поступку, препоручио уврштивање дигиталних или електронских доказа на списак врста доказа и некоришћење других термина у ову сврху.

Однос између појмова дигиталне истраге и дигиталне форензичке истраге најбоље приказује слика 1. Значење појма дигиталне форензичке истраге је подскуп значења појма дигиталне истраге јер форензички процес уводи бројне рестрикције (Carrier, 2005).



Слика 1: Однос појмова дигиталне истраге и дигиталне форензичке истраге.

Додавање придева „форензички" дигиталној истрази указује на употребу науке или технологије и успостављање чињеница прихватљивих као доказ на суду (Houghton Mifflin Company, 2000). Дакле, дигитална форензичка истрага је процес анализе дигиталних података употребом науке и технологије, који води развијању и тестирању теорија које на суду могу бити искоришћене да би се одговорило на питања у вези са догађајима од интереса (Carrier, 2005).

Према типу судског поступка, односно почињеног дела, у оквиру кога је неопходна дигитална форензичка истрага, разликују се истрага кривичног дела и истрага у оквиру корпорације. Истрага кривичног дела односи се на дело кршења одређеног закона, док корпорацијска истрага укључује кршење корпорацијског правила (Brooks, 2015).

2.2.2 Ваљана дигитална форензичка истрага

Као што је већ напоменуто, да би се дигитална истрага сматрала форензичком, она мора да произведе ваљане дигиталне доказе, односно дигиталне доказе који су прихватљиви на суду. Како се научна заједница слаже око тога да се ваљаност постиже конформацијом стандардима (Makura и сар., 2021; McKemmish, 2008), у овом одељку дата је сумирана интерпретација изабраних стандарда и водича (ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042, ISO/IEC 27043, „Guide to Integrating Forensic Techniques into Incident Response" и „Guidelines for Digital Forensics First Responders") у један скуп инструкција за ваљано спровођење дигиталне форензичке истраге.

Главни критеријуми ваљаности дигиталне форензичке истраге, а тиме и проистеклих дигиталних доказа су релевантност доказа, поузданост доказа, интегритет доказа, довољност доказа и оправданост доказа. Поузданост доказа постиже се задовољењем критеријума проверљивости, поновљивости (енг. *repeatability*) и обновљивости доказа (енг. *reproducibility*) (ISO/IEC 27037, 2015), а задовољење ових критеријума постиже се документовањем сваке истражне активности и завођењем ланца надлежности (ISO/IEC 27043, 2016). Уколико критеријуми поновљивости и обновљивости дигиталних доказа не могу бити задовољени, на пример, услед примене потпуно новог метода, процедуре или алата, потребна је адекватна валидација (ISO/IEC 27041, 2016). Поред тога, интегритет и поузданост потенцијалних дигиталних доказа форензичар осигурава праћењем документације коју сачињавају процедуре, односно водичи за руковање изворима потенцијалних дигиталних доказа, а које се заснивају на основним принципима руковања доказним материјалом: тежња ка минималним руковањем оригиналног доказног материјала, документовање свих активности предузетих током истраге, примена процедура очувања доказа, којима се осигурава непроменљивост доказа и гарантује непостојање могућности измене доказа, али и образлагање или оправдавање било каквих нужних измена података које су се десиле током истраге, затим поседовање овлашћења за спровођење истражних активности (ISO/IEC 27043, 2016), придржавање локалних правила за руковање доказима и непредузимање активности за које форензичар није компетентан (ISO/IEC 27037, 2015).

Да би се обезбедила увереност у подобност и адекватност методā које форензичар током истраге користи, било који процес који форензичар намерава спровести током истраге требало би да се састоји од фаза прикупљања и анализе захтева, дизајна процеса, имплементације процеса, верификације процеса, валидације процеса, конфирмације, примене, рецензије и одржавања.

Захтеви се могу поделити у неколико категорија: функционални захтеви, захтеви који се тичу перформанси истраге, захтеви који се тичу интеракције са другим системима, процесни захтеви и нефункционални захтеви. Поред ових захтева, потребно је одредити границе оперисања над одређеним потенцијалним дигиталним доказом (максимална величина датотека, максималан и минималан број улазних вредности итд.). Функционални захтеви подразумевају задатке које током истраге треба извршити, као и све што је за из-

вршавање задатака потребно и што би требало да буде резултат извршавања задатака. Захтеви у вези са перформансама извођења истраге треба да дефинишу обим посла, ниво задовољења и услове за извршавање задатака, односно функционалних захтева. Процесни захтеви су уствари захтеви за усаглашеношћу са законом или другим процедурама и правилима. Нефункционални захтеви односе се на преносивост, поузданост, одрживост, безбедност дигиталних уређаја, али и на безбедност и здравље људи (ISO/IEC 27041, 2016).

Продукт дизајна истражног процеса је детаљан приказ начинā на које ће методе бити примењене узимајући у обзир наведене нефункционалне захтеве. Другим речима, дизајн подразумева идентификацију тока активности које треба спровести над одређеним доказним материјалом. У овом стадијуму истраге идентификују се сви алати који ће бити употребљени укључујући и доступне алате са истим или сличним функцијама. При томе је обавезно да се идентификује и квантификује ризик који са собом носе одређене функције одабраних алата (ISO/IEC 27041, 2016). Приликом одабира алата, предност треба дати онима који имају најмањи утицај на систем. На пример, уместо алата са графичким корисничким интерфејсом, за аквизицију података из радне меморије треба користити алат који не изискује много радне меморије да би функционисао. Затим, боље је користити алате који имају сопствене извршне датотеке, а не користе оне које су инсталиране на систему под истрагом (Interpol, 2021). Поред тога, мора се узети у обзир упознатост форензичара са алатом који користи током истраге, јер то може да утиче на повећање вероватноће грешке. Ово доприноси несигурности у квалитет спроведене истраге или, другим речима, чини мане спроведене истраге. Зато је неопходно формално разумевање слабости истраге да би се грешке ефикасно контролисале (ISO/IEC 27041, 2016).

Како је дизајном истражног процеса одређен скуп алата који се могу искористити током истраге, у стадијуму имплементације се дају упутства како одабрати адекватан алат у условима који се стекну током истраге. У креирању оваквог упутства свакако помажу претходно процењени ризици и наведене несигурности у функционисање алата. Међутим, треба бити опрезан, јер недостатак забележених мана неког алата може значити да тај алат само није био довољно у употреби од стране стручњака (ISO/IEC 27041, 2016).

Верификација подразумева одређивање нивоа сигурности у то да је одређени процес или алат усаглашен са својом спецификацијом. Ово није гарант да ће процес или алат и функционисати на жељени начин у контексту конкретне истраге, али добар почетни индикатор за то је верификација у односу на захтеве истражног процеса, који треба да су слични захтевима који одређују за шта је алат намењен. Верификација није довољна да би се сматрало да је процес или алат валидиран (ISO/IEC 27041, 2016).

Под валидацијом се подразумева провера да ли процес производи тачне излазне податке за дефинисан скуп улазних података. Поред тога, валидацијом се одређују гранични услови и учесталост грешке. За валидацију је карактеристично тзв. тестирање црне кутије (енг. *black box testing*), које обезбеђује да знање имплементационих детаља не утиче на поступак тестирања или на коначне резултате тестирања. Дакле, план валидације мора бити неза-

висан од фаза дизајна и имплементације процеса. Разликују се свеобухватна и довољна валидација. Свеобухватна валидација тестира процес под свим могућим условима (на пример, на свим могућим конфигурацијама хардвера за све могуће улазне податке). Наравно, није увек неопходно спровести свеобухватну валидацију током истраге, јер би она могла бити инхибиторни фактор истраге у смислу времена и потребних ресурса. Случај у коме би свеобухватна валидација требало да се изврши је постојање процесā који се спроводе у оквиру више фаза истраге и од стране више форензичких тимова. За остале процесе, који се не спроводе изнова током истраге, треба извршити довољну валидацију.

Довољна валидација односи се на валидацију спрам функционалних и нефункционалних захтева и то под условима који су тренутно актуелни у истрази. Дакле, метод није неопходно валидирати за софтверске и хардверске конфигурације које неће бити релевантне за дату истрагу или за податке који неће бити обрађени током дате истраге. Довољна валидација показује да процес даје тачне резултате за тип улазних података карактеристичан за дату истрагу, чиме се такође показује да је процес подобан за употребу јер задовољава идентификоване захтеве. Било који процес не би требало да се примени ако није валидиран. Ако процес не прође валидацију, форензичар треба да ревидира захтеве, дизајн и имплементацију и да их адекватно допуни, а затим да процес поново подвргне валидацији (ISO/IEC 27041, 2016).

Валидацијски сет укључује план валидације и валидацијске узорке. Пре спровођења валидације неопходно је утврдити валидацијски сет. Креирање валидацијског сета не сме бити поверено укљученима у дизајн, имплементацију и верификацију процеса да би се избегао конфликт интереса. Ако то није могуће, валидацијски поступак мора бити јасно и концизно документован да би се омогућила независна ревизија. План валидације дефинише серију тестова за чије се извођење не познају имплементациони детаљи (енг. *black-box tests*), а који су у складу са утврђеним захтевима. Сваки тест везује информацију о улазним подацима и очекиваним излазним подацима. Тестови треба да сведоче о робусности и подобности процеса и алата укључених у процес за дату истрагу. Адекватност и довољност валидацијског сета мора бити тврђена јер представља гарант да сет задовољава идентификоване захтеве. Ово је нарочито важно када валидацију не спроводи форензичар укључен у истрагу. Скуп резултата тестова заједно са забелешком свих уочених проблема или извршених измена, чини доказ валидације. Валидацијски сет са доказом валидације мора бити периодично ревидиран, како би се у датом тренутку гарантовала њихова адекватност. Поред тога, и процеси морају бити ревидирани, а резултат ревизије забележен да би се могло гарантовати да је валидацијски сет повезан са процесом и даље исправан и да процес остаје валидиран (ISO/IEC 27041, 2016).

Доказу о валидацији процесā који чине истрагу мора се додати доказ о компетентности и професионалности самог форензичара да би се истрага сматрала валидном (ISO/IEC 27041, 2016).

Конфирмација процеса представља формалну процену задовољења идентификованих захтева, а тиме и формални доказ да је процес подобан за дату

истрагу. За конфирмацију је неопходно приложити доказе о валидацији процеса, била она изведена од стране форензичара који спроводи тренутну истрагу или од стране других форензичара/научника. Ако је процес већ валидиран од стране других форензичара, нема потребе за поновном валидацијом уколико она одговара датој истрази (ISO/IEC 27041, 2016).

Примена процеса у истрази значи да је процес валидиран за дату истрагу. Сваки облик одступања од очекиваног понашања мора бити забележен и морају се спровести додатне активности које могу укључивати измену процеса и/или поновну валидацију. Уколико је дизајном истражног процеса одређено више алата са сличним функцијама, долазак у фазу примене процеса је време када форензичар одабира један од њих и, наравно, образлаже свој избор (ISO/IEC 27041, 2016).

На крају, у оквиру фазе рецензирања и одржавања, посматра се учинак процеса у истрази како би се потенцијално идентификовали додатни захтеви или извршиле измене, нпр. у случају измене коришћених алата (аутоматска надоградња алата, енг. *upgrade*, престанак важења услова претходно узетих у обзир итд.). Током одржавања процеса, потребно је вратити се у фазе прикупљања и анализе захтева, дизајна процеса и имплементације процеса, а све са циљем да се постигну валидација и конфирмација процеса (ISO/IEC 27041, 2016).

ISO/IEC 27037 (2015) сугерише да свака истражна активност буде пропраћена валидацијом, документовањем, свесношћу о свакој опасности од нарушавања интегритета или неочувања првобитног стања потенцијалних извора доказа и проценом ризика, затим узимањем у обзир тренутних околности при сваком одлучивању током истражне активности и приоритизовањем спровођења активности. Приоритизација истражних активности врши се у односу на процењену доказну вредност уређаја, период перзистирања података и количину труда који је потребно уложити. Доказну вредност дигиталног уређаја форензичар процењује на основу свог разумевања ситуације услед које је неопходна дигитална истрага, као и на основу свог искуства у сличним ситуацијама. Узимање у обзир периода перзистирања података значи давање предности подацима из радне меморије, тј. подацима који нестају са искључењем уређаја са напајања. Међутим, и подаци који се складиште у трајној меморији могу бити изгубљени у кратком временском року, на пример, уколико се ради о логовима чији се постојећи садржај преписује са доласком новог. Количина труда који је потребно уложити односи се не само на време које је потребно утрошити, већ и на цену потребне опреме и сервиса за спровођење истражне активности (Kent и сар., 2006). Такође, према стандарду ISO/IEC 27042 (2016), потребно је проценити и степен несигурности у резултат истраге, који је обрнуто пропорционалан квалитету и квантитету потенцијалних дигиталних доказа проистеклих из истраге у корист хипотезе случаја.

Од почетка истраге, од фазе идентификације, потребно је предузимати мере чувања потенцијалних дигиталних доказа, односно уређаја који потенцијално садрже дигиталне доказе. Под тим се подразумева очување поверљивости, интегритета и доступности потенцијалних дигиталних доказа, као и предузимање мера за спречавање било каквог утицаја окружења, односно

места чувања, на потенцијалне дигиталне доказе.

2.2.2.1 Истрага на месту догађаја

Понекад форензичар дигиталних уређаја има потребу да своју истрагу започне на месту догађаја, најчешће по ангажовању правног или физичког лица. У том случају, ISO/IEC 27037 (2015) налаже посебан начин поступања. Пре доласка на место догађаја, форензичар треба да претпостави и припреми опрему која ће затребати. По доласку на место догађаја, на коме се налазе потенцијални дигитални докази, односно уређаји који потенцијално садрже дигиталне доказе, форензичар треба да изврши процену ризика. На пример, под тим се подразумева разматрање могућности конфигурисања уређаја за уништење података након искључења уређаја или других акција над којима форензичар нема контролу. Након процене ризика и поступањем у складу са тим, генерално правило је да сваки уређај, који је до доласка форензичара био укључен, форензичар не искључује и обрнуто, сваки уређај који је био искључен, форензичар не укључује. Такође, по доласку на место догађаја, треба фотографисати или скицирати положај каблова и портова, како би се по завршетку истраге место могло реконструисати. Добра је пракса и претражити и узети у обзир недигиталне доказе, који би могли бити од користи током истраге (белешке, дневници, упутства за употребу) у смислу да садрже есенцијалне информације као што су лозинке или пинови (ISO/IEC 27037, 2015). Поред тога, ако за то постоји овлашћење, форензичар треба да упита за лозинке или пин-кодове и да на месту догађаја провери њихову коректност (Interpol, 2021).

Уколико на месту догађаја постоји велики број дигиталних уређаја, те би истрага свих била изузетно временски захтевна, разумно је на месту догађаја укључити уређаје (уколико су били искључени) и извршити преглед који би резултирао проценом релевантности датог уређаја за дигиталну истрагу. Уколико дигитални уређај покреће батерија и постоји могућност да се она испразни током прегледања, форензичар би требало да, уколико је могуће, предупреди тај сценарио довођењем напајања путем исправљача како би се осигурали подаци похрањени на уређају, а који потенцијално представљају дигиталне доказе (ISO/IEC 27037, 2015).

2.2.2.2 Идентификација доказа

Прва фаза дигиталне форензичке истраге је идентификација доказа, односно потрага за потенцијалним изворима доказа, њихово препознавање и документовање. Потенцијални извори доказа представљају складишта података и уређаје који обрађују податке, који потенцијално представљају информације релевантне за дати случај. Ту спадају складишта података карактеристична за рачунаре (магнетни, оптички и полупроводнички уређаји), мобилни телефони, дигитални асистенти (енг. PDAs), лични електронски уређаји (енг. PEDs), меморијске картице, мобилни навигациони системи, фотоапарати и камере, стандардни рачунари са могућношћу мрежног повезивања, рачунарске мреже засноване на TCP/IP и другим протоколима, али и други уређаји

слични наведенима (ISO/IEC 27037, 2015).

Након препознавања дигиталних уређаја који потенцијално садрже доказе, форензичар је у обавези да забележи њихове детаље. Ове карактеристике обухватају: информацију о произвођачу, моделу и серијском броју уређаја (уколико она није јасно видљива, корисно је уочити и забележити јединствене карактеристике дизајна уређаја), идентификационе информације које се могу очитати са уређаја, а које су повезане са базама података које носе додатне информације (нпр. са мобилног телефона може се очитати IMEI број [2], а са сигурносног чипа ESN [3] број), информацију о интерфејсима уређаја (нпр. конектор напајања), затим информације о оператору мреже (уколико је познат телефонски број). Уколико се ради о уређају за складиштење података, потребно је забележити његов капацитет, затим информације о затеченом стању и локацији уређаја, информације о присутним безбедносним контролама и коментаре који могу помоћи у разумевању контекста (ISO/IEC 27037, 2015; Interpol, 2021).

Ако је идентификовани уређај повезан у мрежу, потребно је проценити ризик његовог искључивања из исте. Под тим се подразумева утврђивање да ли постоје сервиси од којих зависи рад датог уређаја, као и степен критичности сервиса, ако постоје. Уколико се ове мере не предузму, могућ је губитак потенцијалних дигиталних доказа или штета која настаје у случају искључења, односно нефункционисања уређаја са критичном мисијом (ISO/IEC 27037, 2015).

Потрага за потенцијалним изворима доказа током фазе идентификације подразумева и потрагу за могућим скривеним изворима доказа. На пример, добра је пракса употребити детектор бежичног сигнала како би се открили уређаји за бежично повезивање (енг. *wireless devices*). Уколико није могуће употребити детектор бежичног сигнала (услед недостатка времена или новца), неопходно је да форензичар забележи образложење. Уз то, форензичар треба да узме у обзир предузимање активног скенирања уређаја повезаних на мрежу за случај да постоје скривени уређаји у мрежи. Пре тога, неопходно је проценити ризик, односно уверити се да активно скенирање неће изазвати нежељене последице по уређаје који су већ идентификовани. Велики изазов за форензичаре током спровођења фазе идентификације представља виртуелизација, односно рачунарство у облаку, складишта података повезана на мрежу (NAS) и мреже складишта података (SAN). Фаза идентификације треба да буде и почетак завођења ланца надлежности (енг. *chain of custody*) (ISO/IEC 27037, 2015).

Током идентификовања потенцијалних извора доказа потребно је формирати приоритете у односу на период перзистирања података у меморији, који ће се пратити током прикупљања и аквизиције потенцијалних извора доказа (ISO/IEC 27037, 2015).

[2] IMEI је 15-цифрени број који носи информацију о произвођачу и моделу уређаја, као и о држави задуженој за издавање дозволе GSM оператору.

[3] ESN је јединствени 32-битни број код којег првих 8-14 бита идентификују произвођача, а остатак битова, серијски број уређаја.

2.2.2.3 Прикупљање доказа

Прикупљање доказа је фаза која следи фазу идентификације. У зависности од околности, форензичар у овој фази одлучује које податке ће прикупити са идентификованих потенцијалних извора доказа. При приоритизацији у прикупљању потенцијалних дигиталних доказа, форензичар треба да разуме разлог из кога се одређени доказ прикупља и мора да има на уму период перзистирања података у датом меморијском складишту, као и релевантност, односно потенцијалну доказну вредност уређаја који се прикупља (ISO/IEC 27037, 2015). Такође, током прикупљања потенцијалних дигиталних доказа, неопходно је да форензичар буде свестан природе инцидента који се истражује, техничког знања осумњичених и локације складишта података. Природа инцидента диктира потребну опрему и адекватност техничких процедура које ће бити примењене. Степен стручности осумњичених може указати на, на пример, начине покушаја сакривања или уништавања доказа, а локације складишта података могу диктирати потребу за посебним овлашћењем за прикупљање или за посебном опремом (Interpol, 2021).

Понекад није јасно да ли дигитални уређај садржи потенцијалне дигиталне доказе или није лако извршити приоритизацију. У том случају је потребно прегледати податке пре него што се започне са прикупљањем. Дигитални уређаји који могу бити узети у обзир у фази прикупљања доказа су: ИТ опрема и дигитални уређаји за складиштење података, уређаји за видео-надзор (CCTV), портабилни електронски уређаји, електронски уређаји у аутомобилу, контролни системи и импровизована електроника (ISO/IEC 27037, 2015).

Уколико не постоји фактор спречавања, у овој фази се идентификовани потенцијални извори доказа премештају у лабораторију или неко друго контролисано окружење након што се прописно упакују и означе. Паковање мобилних уређаја би требало да укључи контејнере који функционишу као Фарадејев кавез, како би се спречио нежељени приступ уређају на даљину. С друге стране, понекад је најбоље искључити мобилни уређај како би се спречила било каква измена затеченог стања. Треба напоменути да неки неперзистентни подаци могу да се измене променом локације уређаја, након неког времена или услед присуства других дигиталних уређаја. Дакле, потребно је такве податке очувати пре премештања уређаја на коме су складиштени (ISO/IEC 27037, 2015). Поред физичког транспорта потенцијалних доказа, транспорт може бити обављен и електронски. Транспортовање доказа електронски мора бити пропраћено мерама очувања интегритета доказа и ланца надлежности над доказима. Ове мере укључују, на пример, шифровање и дигитално потписивање података (ISO/IEC 27043, 2016). Уколико пак није могуће преместити идентификоване уређаје у фази прикупљања, потребно је забележити образложење за то. Такође, дигитални уређаји могу да буду извор физичких доказа (отисци прстију, DNA, итд.), те форензичар дигиталних уређаја мора да буде у контакту са форензичарима других профила. Уз то, важно је напоменути да је, у случају сумње да су подаци на меморијском складишту шифровани или да у рачунарском систему постоји малициозни програм, битно прикупити неперзистентне податке, с обзиром на то да се у радној меморији могу налазити фразе и кључеви неопходни за дешифровање.

Такође, у случају шифрованог меморијског складишта, потребно је размотрити логичко прикупљање података (ISO/IEC 27037, 2015).

Поред идентификованих дигиталних уређаја, форензичар би требало да прикупи и документује и друге изворе података или помоћне уређаје који су неопходни за наредне фазе истраге, као што су недигитални докази (лозинка исписана на папиру, оригинална паковања мобилних телефона, која могу садржати информацију о PIN или PUK-коду), исправљачи и уређаји и каблови за пуњење, меморијске картице, SIM-картице. Такође, форензичар треба да узме у обзир и вербално прикупљање доказа (разговор са администратором мреже, власницима или корисницима дигиталних уређаја), уколико за то постоји могућност (ISO/IEC 27037, 2015).

Кључно питање у фази прикупљања јесте да ли је уређај који је идентификован укључен или искључен. Уколико је уређај укључен, форензичар најпре треба да се упита да ли је за истрагу релевантно прикупљање података из радне меморије и ако јесте, да прикупљање и изврши (ISO/IEC 27037, 2015). У случају да је уређај закључан, форензичар би могао да примени напад којим је могуће прочитати садржај радне меморије након искључења уређаја и пронађе криптографске кључеве (енг. *cold boot attack* (Halderman и сар., 2009)) (Interpol, 2021). Овај напад се спроводи тако што се укључени рачунар отвори и модул радне меморије се расхлади спрејом за расхлађивање да би се продужило време перзистирања података. Након тога се уређај „насилно" искључи одвођењем напајања и оперативни систем се поново учита користећи меморијско складиште које садржи алат за снимање радне меморије.

Након прикупљања неперзистентних података или уколико их није потребно прикупити, форензичар треба да процени да ли је безбедно искључити уређај (ISO/IEC 27037, 2015). На пример, постоје алати који могу да помогну да се одговори на то питање, односно да детектују било коју врсту опструкције истраге искљученог уређаја, у шта спадају енкрипција, активан програм за брисање података из трајне меморије, подаци складиштени у облаку или умреженим уређајима за складиштење, као и виртуелизација (Interpol, 2021). Такође, форензичар би требало да, увидом у конфигурацију уређаја, провери да ли би уклањање извора напајања довело до губитка података. Ако не би, форензичар може одспојити везу са извором напајања најпре одстрањивањем краја везе на уређају, а потом и краја у утичници. Овај редослед је важан уколико је уређај повезан са UPS уређајем, који може проузроковати измену података ако се напајање одспоји најпре са краја повезаног са утичницом. Искључивање лап-топ рачунара, односно уређаја који напаја батерија, требало би извршити уклањањем батерије, а не притиском на дугме за искључивање јер ова акција може да покрене малициозна скрипта која би изменила или обрисала есенцијалне податке или би обавестила други систем који би довео до уништења потенцијалних доказа или би, у најгорем случају, могла довести до физичких повреда особља. Након уклањања батерије, уколико постоји прикључен адаптер, треба уклонити и адаптер. Стање слота за CD или други преносиви медијум за складиштење података на укљученом рачунару треба забележити. Ако лежиште диска извире из слота, треба забележити да ли оно садржи CD или DVD диск, уклонити диск из лежишта и забележити за-

течено стање, затим слот прелепити траком како би се спречио било какав улаз података. Случај за који ова акција форензичара може бити значајна јесте постављен бутабилан диск, када је могуће да се, у зависности од поставки BIOS-а, уместо оперативног система чврстог диска, покрене оперативни систем бутабилног диска (ISO/IEC 27037, 2015).

Ако је уређај искључен, форензичар би требало да одспоји везу са извором напајања најпре одстрањивањем краја везе на уређају, а потом и краја у утичници, да обележи, а затим одспоји и обезбеди све каблове и портове са уређаја како би обезбедио каснију реконструкцију и траком прекрије свич за укључивање, уколико постоји, како би се спречила промена стања свича. Са одстрањивањем трајног меморијског складишта из кућишта рачунара треба сачекати до започињања аквизиције података, с обзиром на то да ризик од оштећења диска расте ван кућишта рачунара. Посебан случај чини лап-топ рачунар и на њега се мора обратити нарочита пажња. Његово стање хибернације грешком се може третирати као искључено стање, а постоје и лап-топ рачунари који се након подизања поклопца аутоматски укључују. Даље, ако је на месту догађаја потребно преузети чврсти диск из кућишта рачунара, форензичар би требало да уземљи уређај како би се спречило оштећење података на диску услед статичког електрицитета. Након што се диск одстрани из кућишта рачунара, потребно га је обележити и забележити његове идентификационе детаље (произвођач, модел, серијски број и капацитет). Приликом обележавања уређаја, ознака се не сме поставити директно на механичке делове уређаја и не сме прекрити идентификационе детаље. Након овог треба да уследе исте активности у вези са екстерним меморијским складиштима који се могу наћи у слоту за CD/DVD, а који су потенцијално бутабилни (ISO/IEC 27037, 2015).

Постоје уређаји који омогућују да се укључени уређај пренесе у лабораторију. На пример, уређај који омогућава одспајање везе са напајањем, а прикључивање уређаја на преносиви UPS уређај без прекидања довода напајања. С тим у вези, користан може бити и уређај који имитира миш (енг. *mouse-jiggler*) и тако спречава закључавање екрана. Приликом преношења укљученог уређаја, потребно је водити рачуна о карактеристикама окружења које могу захтевати појачано хлађење уређаја, заштиту од механичких шокова итд. Ако постоји ризик од губитка или измене података у случају одспајања везе напајања, онда форензичар треба прописно да искључи уређај. Након тога, форензичар треба да обележи, а затим одспоји и обезбеди све каблове и портове са уређаја како би обезбедио каснију реконструкцију и да траком прекрије свич за укључивање, уколико постоји, како би се спречила промена стања свича (ISO/IEC 27037, 2015).

Да би се у фази прикупљања постигла релевантност доказа, потребно је показати да прикупљени материјал садржи информације битне за истрагу одређеног случаја, те навести разлоге због којих је дати материјал прикупљен. Даље, да би се постигле оправданост и проверљивост доказа, потребно је образложити одлуку да се прикупи дати материјал и документовати све спроведене активности. Довољност доказа постиже се провером и образложењем разлога прикупљања датог материјала (ISO/IEC 27037, 2015).

Околности под којима, на пример, није разумно извршити прикупљање потенцијалних дигиталних доказа су непоседовање правне дозволе за прикупљање доказног материјала, постојање обавезе, коју налаже наручилац услуге да се користе друге методе, постојање потребе бележења малициозног деловања у реалном времену, постојање обавезе да се прикупљање или аквизиција података изврши тајно, без знања лица која користе уређаје, случај када дигитални уређај припада критичној инфраструктури, те не трпи периоде искључења, случај када је капацитет меморијског складишта превелик (на пример ако се ради о серверу, дата-центру или систему RAID), случај када се ради о безбедносно критичном дигиталном уређају, те би искључење било опасно и случај када дигитални уређај опслужује и друга лица, која се ни за шта не терете (ISO/IEC 27037, 2015).

2.2.2.4 Аквизиција доказа

Аквизиција података следи након фазе прикупљања доказа и подразумева прављење форензичке копије прикупљених дигиталних доказа (чврстог диска, партиције диска, одабраних датотека и сл.) и документовање коришћених метода и алата, образложења за употребу наведених метода и алата, као и образложење хронологије аквизирања појединачних меморијских складишта. Препоручљиво је да искоришћени метод буде обновљив (енг. *reproducible*) и да га је могуће верификовати. Излишно је и наводити да могућност измена података услед употребе изабраних метода и алата мора бити сведена на минимум. Уколико је пак неизбежна измена података током аквизиције, она мора бити образложена (ISO/IEC 27037, 2015). Резултат прављења форензичке копије може бити клон или слика. Клон се још карактерише као „уређај на уређај" копија јер се у претходно „очишћени" меморијски уређај истог или већег капацитета у односу на оригинални меморијски уређај, похрани истоветна бит по бит копија оригиналног меморијског уређаја (енг. *bit stream imaging, disk imaging*) (Interpol, 2021). Форензичка копија – клон може бити директно повезана са рачунаром и монтирана (енг. *mount*) тако да је могуће прегледати њен логички садржај (Kent и сар., 2006).

С друге стране, форензичка слика подразумева једну датотеку или више повезаних датотека које представљају идентичну копију оригиналног меморијског складишта. Предности прављења форензичке слике која се састоји од више датотека огледају се у могућности одређивања величине датотека у зависности од карактеристика одредишног меморијског уређаја, затим у могућности компресије без губитака података, као и у могућности обезбеђивања садржаја датотека енкрипцијом (Interpol, 2021). Међутим, да би се прегледао логички садржај форензичке копије – слике, потребно је да се на основу слике реконструише диск или да се употреби форензички алат који је способан да прочита и прикаже логички садржај форензичке слике (Kent и сар., 2006).

У случају да прављење форензичке копије, било клона или слике, није могуће (у случају сервера, складишта података повезаних са мрежом, виртуелних дискова или шифрованих меморијских уређаја), решење је прављење логичке копије диска (енг. *logical backup*). Треба напоменути да у случају енкриптованог меморијског складишта, уређај мора бити укључен да би се

извршило логичко прикупљање података. На овај начин, форензичар подацима приступа као и корисник датог уређаја. Такође, решење може бити и логичка копија датотека за које форензичар сматра да су релевантне за истрагу. Мана овог приступа је неукључивање слек простора датотеке (енг. *slack space*) и обрисаних датотека, као и потенцијална измена метаподатака датотеке. У сваком случају, прављење логичке копије мора бити пропраћено употребом адекватног метода и алата, заштитом од писања, максималним могућим очувањем метаподатака и коришћењем криптографског алгоритма за верификацију интегритета аквизираних података (Interpol, 2021).

Током прављења форензичке копије, клона или слике, као и логичког прикупљања података, форензичар мора предузети мере очувања интегритета оригиналног складишта података, односно складишта података чији се садржај копира. Под тим се подразумева употреба блокатора писања (енг. *write-blocker*) – хардверског или софтверског алата који спречава да се садржај складишта података повезаног са рачунаром измени. Хардверски блокатор писања физички се повезује са рачунаром и са складиштем података које се копира, док се софтверски блокатор писања инсталира на форензичкој радној станици. Треба напоменути да неки оперативни системи могу бити конфигурисани тако да се секундарна складишта података не монтирају (енг. *mount*) приликом покретања рачунара, те софтверски блокатор писања у том случају није потребан (Kent и сар., 2006).

При приоритизацији у аквизицији потенцијалних дигиталних доказа, форензичар треба да разуме разлог из кога се одређени доказ аквизира и мора да има на уму период перзистирања података у датом меморијском складишту, као и релевантност, односно потенцијалну доказну вредност уређаја који се аквизира (ISO/IEC 27037, 2015). Услед великог капацитета меморијског складишта које се аквизира и које потенцијално садржи доказе, прављење форензичке копије може да траје сатима. Зато са аквизицијом идентификованог потенцијалног извора доказа не треба чекати, већ је треба започети док идентификација и прикупљање других извора доказа трају (Interpol, 2021). У случају да није могуће направити форензичку копију читавог диска, форензичар треба да направи форензичку копију оних датотека или партиција диска које потенцијално садрже дигиталне доказе. Продукт аквизиције података треба да буду једна главна копија (енг. *master copy*) и две радне копије. Главна копија треба да буде одложена и да се над њом не спроводи истрага. Она може послужити за верификовање радних копија или као замена за другу радну копију у случају оштећења прве (ISO/IEC 27037, 2015).

Поступак аквизиције података зависи од стања уређаја, односно од тога да ли је уређај искључен, укључен или је укључен и има критичну мисију, па га није препоручљиво искључити (ISO/IEC 27037, 2015).

Уколико је уређај укључен, форензичар најпре треба да обезбеди уређај тако да се не закључа или не пређе у режим хибернације, употребом, на пример, уређаја који имитира миш (енг. *mouse-jiggler*). Овде је потребно напоменути да употреба уређаја за спречавање закључавања или преласка у режим хибернације мора довести до измене података на уређају који се аквизира, што је неопходно документовати (ISO/IEC 27037, 2015).

Такође, уколико је уређај повезан у мрежу, треба га повезаног и оставити како би се забележила активност уређаја у мрежи. Међутим, ако активност уређаја у мрежи није релевантна, форензичар може изоловати уређај тако што одспоји мрежни кабел или прекине везу са приступном тачком за бежично повезивање. Поред тога, може бити потребно спречити пренос радио сигнала (на пример код уређаја који подржавају GPS). Методе изоловања радио сигнала могу довести до појачаног трошења струје, с обзиром на сталне покушаје да се успостави веза са мрежом. Зато овим уређајима мора бити обезбеђено адекватно напајање. Ове методе укључују употребу уређаја за ометање (енг. *jamming device*), заштићених подручја, заштићених контејнера и маскирних SIM или USIM картица. Уређаји за ометање блокирају трансмисију радио сигнала тако што стварају јаку интерференцију (шум) када уређај емитује сигнал фреквенцијског опсега који користе мобилни уређаји. Заштићено подручје подразумева заштићени радни простор као што је лабораторија, у оквиру кога није могућа трансмисија радио сигнала. Овакав простор може бити и портабилан, али тада проблем могу представљати скученост и доведени каблови који, ако нису прописно изоловани, могу опструирати заштиту и функционисати као антена. Пример заштићеног контејнера је Фарадејева врећа. Маскирне SIM или USIM картице морају се пре употребе валидирати за конкретан уређај и конкретну мрежу. Уколико не постоји опасност за њихову употребу, оне могу омогућити безбедну истрагу. Крајња опција би била укидање мрежних сервиса од стране провајдера, али то скоро у сваком случају инхибира ефикасност истраге. Треба напоменути да, пре уклањања батерије и SIM картице, форензичар треба да изврши живу аквизицију података, како се потенцијални докази не би изгубили уколико су смештени у радној меморији или уколико је уређај заштићен PIN или PUK-кодом (ISO/IEC 27037, 2015).

Пре искључивања уређаја из мреже, потребно је обавити логичку аквизицију података који се тичу мрежних конекција. То укључује IP конфигурацију, табеле рутирања и сл. Ово је нарочито важно због потребе за идентификовањем свих метода комуникације уређаја (физичка веза са мрежом, VPN итд.). Наравно, пре него што се мрежни кабел одспоји, форензичар треба да означи портове и каблове тако да буде могућа реконструкција мреже. У случају да уређај користи више комуникационих метода (жично на LAN мрежу или бежично преко модема), форензичар треба све да их идентификује и да предузме мере спречавања уништења потенцијалних дигиталних доказа услед повезаности уређаја у мрежи (ISO/IEC 27037, 2015).

Након предузимања активности везаних за мрежу у којој је уређај повезан, форензичар треба да изврши аквизицију најпре неперзистентних података, као што су подаци о покренутим процесима, мрежним конекцијама, поставкама датума и времена, лозинкама, и дешифрованим апликацијама, који су смештени у радну меморију (RAM) или део трајне меморије која се по потреби користи као радна меморија (енг. *swap memory*). Нарочито је важно аквизирати податке радне меморије у случају постојања енкрипције, што није на одмет најпре проверити употребом валидираног алата за детекцију енкрипције. Форензичар треба да буде опрезан када очитава датум и

време на дигиталним уређајима које истражује, с обзиром на то да време и датум могу бити погрешно конфигурисани или са другом временском зоном. Све што уочи у вези са конфигурацијом датума и времена, форензичар треба да документује. Такође, да би се очитала конфигурација датума и времена на уређају, понекад је неизбежно начинити измену података на уређају, те је и овај случај обавезно забележити. Све што је видљиво на екрану уређаја у тренутку приступања, форензичар треба да забележи (покренути програми и процеси, отворени документи и др.).

Аквизиција неперзистентних података врши се на укљученом уређају и тада се назива живом аквизицијом. Приликом живе аквизиције, уређај не би требало искључивати из мреже на коју је повезан. Жива аквизиција се може извршити кроз конзолу или на даљину преко мреже. У случају да је уређај закључан, могуће је физички приступити подацима кроз посебан интерфејс (енг. *firewire*). Алати који се при томе користе морају бити поуздани и форензичар никако не би требало да користи програме већ инсталиране у систему са којег аквизира податке. Форензичар мора бити компетентан за употребу одређеног алата и мора бити свестан последица до којих употреба алата може довести, а које су неминовне јер се стање меморијског складишта покретањем форензичког алата мора променити. Свака промена затеченог стања се мора разумети, образложити и документовати. Такође је неопходно документовати и разлоге због којих није могуће јасно представити и образложити ефекат који је употреба форензичког алата произвела. Пре започињања живе аквизиције, потребно је форматирати меморијско складиште које ће похранити резултат аквизиције (пожељно је да меморијско складиште буде ново), а након копирања неперзистентних података, неопходно је израчунати и документовати сажетак меморијског складишта. Аквизиција перзистентних података (података похрањених у трајној меморији уређаја) мора бити извршена употребом валидираног алата. Слика трајне меморије се, као и слика радне меморије, складишти у (ново) меморијско складиште, које је форматирано (ISO/IEC 27037, 2015).

Уколико је уређај искључен, аквизиција података из радне меморије се искључује, а врши се само аквизиција перзистентних података из трајне меморије (чврстог диска). Пре започињања аквизиције, потребно је уверити се да је уређај искључен. Уколико је прихватљиво, пожељно је одстранити складиште података из уређаја, адекватно га означити и документовати информације као што су произвођач, модел, серијски број и капацитет. Аквизиција се мора вршити употребом поузданог, односно валидираног алата (ISO/IEC 27037, 2015).

Уколико се ради о укљученом уређају са критичном мисијом, као што су сервери у дата-центрима, који опслужују кориснике који нису ни на који начин укључени у случај који се истражује, надзорни системи, медицински уређаји и сл., форензичар треба да спроведе само живу аквизицију на већ описани начин (ISO/IEC 27037, 2015).

Дā се закључити да се у случају искључених уређаја и уређаја са критичном мисијом предузима парцијална аквизиција. У првом случају аквизирају се само перзистентни подаци, а у другом случају, само неперзистентни. Пар-

цијална аквизиција се спроводи и када је меморијско складиште превеликог капацитета (нпр. код сервера који служе као база података), када постоје нерелевантни подаци које није потребно аквизирати или када не постоји правна дозвола за аквизицију података. Дакле, у случају парцијалне аквизиције, форензичар би требало да је у стању да идентификује директоријуме, датотеке или друге системске опције релевантне за дату истрагу и да спроведе логичку аквизицију тих података (ISO/IEC 27037, 2015).

Поред дела меморијских складишта видљивог оперативном систему, аквизиција доказа требало би да укључи прављење форензичке копије и неалоцираног меморијског простора (ISO/IEC 27037, 2015).

Након прављења копије потенцијалних дигиталних доказа или уређаја који потенцијално садрже дигиталне доказе, копију је потребно верификовати верификаторном функцијом, која је у датом тренутку прихватљива од стране научне заједнице, али и од стране индивидуа које ће разматрати продукте истраге (ISO/IEC 27037, 2015). Верификаторна функција је у овом случају хеш-функција или функција сажетка, која се користи за рачунање јединственог отиска скупа података (енг. *message digest, summary*), који потом служи верификацији интегритета података. Верификација интегритета података се врши утврђивањем истоветности сажетака копије и оригиналних података. При томе, форензичар треба да буде свестан да полупроводнички дискови (SSD), који су у широкој употреби, имају способност чишћења података без икаквог иницирања, услед повезаности путем интерфејса, дакле, само услед постојања напајања, те обезбеђивање интегритета целокупног садржаја диска употребом сажетака може бити онемогућено. Зато је добра пракса да у случају полупроводничких дискова форензичар прибегне рачунању сажетка релевантних партиција или појединачних датотека (Interpol, 2021).

Потребно је напоменути да понекад није могуће верификовати оригинал и копију потенцијалних дигиталних доказа, односно уређаја који садрже потенцијалне дигиталне доказе (на пример када се врши аквизиција укљученог система, када оригинал није у потпуности исправан, те је немогуће направити копију или кад је прављење копије онемогућено услед недостатка времена, тј. услед превеликог меморијског капацитета прикупљених уређаја). Тада је неопходно да форензичар јасно и логично образложи метод за који сматра да је могућ и најбоља опција. На пример, уколико је могуће направити само делимичну копију складишта података (услед грешака које садрже поједини сектори меморијског складишта), прихватљиво је да форензичар верификује копију исправног дела меморијског складишта. Такође, уколико је капацитет меморијског складишта превелик или је у питању складиште система са критичном мисијом, који је укључен, разумна одлука форензичара је да спроведе логичку аквизицију, односно да направи копију одабраних меморијских локација (датотека или партиција) за које сматра да садрже дигиталне доказе (ISO/IEC 27037, 2015).

2.2.2.5 Анализа доказа

Анализа, као фаза истраге, подразумева идентификацију и евалуацију дигиталних доказа. Дакле, треба приметити да је уз термин дигитални доказ до

сада стајао епитет потенцијални. За продукт анализе не би требало да постоји сумња да се може искористити као доказ. Анализа је често итеративан процес јер нови утврђени доказ може довести до поновног разматрања, којим ће се оснажити постојећи докази (ISO/IEC 27042, 2016).

Процес анализе, који се примењује, не сме узроковати промену садржаја потенцијалних дигиталних доказа. Наравно, уколико постоји шанса да се потенијални докази униште, потребно је предузети одговарајуће мере да до тога не дође, односно да се вероватноћа за то умањи или да се умање ефекти потенцијалне штете. Ако су оштећења потенцијалних дигиталних доказа неизбежна, форензичар или тим форензичара треба да буде компетентан да настанак штете објасни и образложи (ISO/IEC 27042, 2016).

Форензичар мора бити компетентан за употребу алатā који се током анализе користе. Ако форензичар користи нови алат, са којим форензичари немају искуство, тај алат пре употребе мора проћи одређену валидацију и мора имати дозволу за употребу. При томе, алат мора бити валидиран узимајући у обзир и случај који се тренутно истражује. Стандардом је указано и на то да алат за чије мане се зна, може бити употребљен, ако се може показати да ће без негативних ефеката допринети анализи датог случаја (ISO/IEC 27042, 2016).

Поред ланца надлежности, форензичар током анализе треба да бележи хронологију активности током анализе са свим детаљима и резултатима појединачних активности. Ниво детаља треба да буде такав да омогући другом компетентном форензичару да понови дате активности и добије исте резултате. Овај опис активности анализе треба да садржи и информације о контексту, које је форензичар примио, као и образложење свих одлука које је током анализе донео (ISO/IEC 27042, 2016).

У зависности од врсте потенцијалних дигиталних доказа, анализа се дели на статичку и живу анализу. Статичка анализа спроводи се над форензичком копијом потенцијалних дигиталних доказа. Статичка анализа је прегледање потенцијалних дигиталних доказа са циљем одређивања доказне вредности. Активности које укључује статичка анализа су: идентификација артефаката, конструкција временске линије догађаја, прегледање садржаја датотека укључујући и обрисане датотеке итд. С тим у вези, адекватно је да се статичка анализа спроводи над подацима који су резултат неког деловања – лог-датотеке, мрежни пакети, датотека са извештајем грешака (енг. *memory dump*) и сл. и над метаподацима – временским ознакама (енг. *timestamp*), дозволама приступа датотекама и сл. Примери потенцијалних дигиталних доказа над којима треба спровести живу анализу су инстант поруке, паметни телефони и таблети, комплексне рачунарске мреже, шифровани уређаји за складиштење података, полиморфни кôд и сл. Жива анализа може да се спроводи над форензичком копијом или над оригиналним подацима, када прављење форензичке копије није могуће (ISO/IEC 27042, 2016).

Разлози из којих није могуће направити форензичку копију могу бити техничке природе (јединствен хардвер), оперативне природе (неповољан ефекат на функционисање организације) или постојање ризикā по потенцијалне дигиталне доказе (када је једина опција коришћење алатā већ инсталираних у

систему чији се подаци копирају). С друге стране, анализа форензичке копије система би требало да се одвија директно у оперативном окружењу система. Ако то није могуће, онда форензичар треба да емулира хардвер и софтвер оригиналног окружења колико је могуће верније користећи верификоване виртуелне машине или копије оригиналног хардвера. При томе форензичар треба да буде уверен да било какве измене копије система неопходне за покретање система у оквиру емулатора ни у ком случају не мењају функционисање система и саме податке под анализом, који представљају потенцијалне дигиталне доказе. Треба имати на уму да постоји могућност да је на систему под истрагом инсталиран малициозни програм, који ће променити своје понашање уколико детектује извршавање система у оквиру емулатора (ISO/IEC 27042, 2016).

У оквиру анализе, форензичар врши интерпретацију пронађених података. Под тим се подразумева евалуација података и анализа у односу на контекст. Одавде произилазе чињенице, односно поткрепљења чињеница, што чини форензичарево мишљење. Наравно, и интерпретација је репетитиван процес и не мора да буде само део анализе, већ и других фаза истраге, као што је прикупљање. У стандарду се налаже да је потребно извршити дистинкцију између пронађених чињеница и изведених информација. На пример, чињеницу представља констатација да у датом систему датотека постоји одређена датотека. С друге стране, изведена иноформација би била продукт очитавања метаподатака дате датотеке, који говоре о кориснику који ју је креирао, изменио итд. Дакле, чињенице морају поткрепити изведене информације и морају бити проверене (верификоване). Током давања стручног налаза и мишљења, ова дистинкција би требало да буде јасно изражена, а логички процес који је резултовао извођењем информација мора бити јасно описан и поновљив. (ISO/IEC 27042, 2016).

2.2.2.6 Интерпретација доказа

Након фазе прегледања и анализе доказа, више се не користи термин „потенцијални" дигитални доказ. Доказна вредност би у овој фази истраге требало да буде извесна и утврђује се интерпретацијом дигиталних доказа. Интерпретација мора укључити доступне информације о околностима које су довеле до тога да се одређени податак сматра доказом. Ове информације могу доћи од људи који су били укључени у функционисање система који се истражује. Поред тога, форензичар мора бити упознат са сврхом и доменом истраге која му је поверена. Један од циљева интерпретације дигиталних доказа је да, употребом научно доказаних метода, изгради објашњења за присуство одређених дигиталних артефаката који су идентификовани. Такође, циљ фазе интерпретације је да класификује интерпретиране доказе спрам њихове релевантности. Другим речима, да се одреди који су дигитални докази важнији у односу на остале. Главни резултат интерпретације доказа је извештај, односно стручни налаз и мишљење форензичара, који треба да садржи апсолутно све дигиталне доказе. Извештај треба да буде написан једноставним језиком, јасно, концизно и недвосмислено. Тако да га разумеју и они који немају никаквог додира са струком. Укратко, овај извештај треба детаљно да представи

потенцијалне доказе, који су прикупљени и/или аквизирани, технике анализе, које су употребљене, које информације, односно исказе је форензичар узео у обзир и од кога те информације потичу. Ако није могуће са апсолутном сигурношћу дати мишљење на основу изнесених доказа, форензичар треба да представи своје претпоставке, као и да процени њихову вероватност (ISO/IEC 27043, 2016).

Према стандарду ISO/IEC 27042 (2016), извештај о истрази, односно стручни налаз и мишљење, треба да садржи следеће:

- јасан израз форензичареве компетентности за дату истрагу и сведочење;
- почетне информације о контексту истраге, које су форензичару предочене пре започињања истраге;
- навођење природе инцидента који се истражује;
- време почетка и период трајања инцидента под истрагом;
- локацију инцидента;
- предмете истраге;
- учеснике у истрази, као и њихове улоге;
- време почетка и завршетка истраге;
- место спровођења истраге;
- главне детаље о дигиталним уређајима над којима се спроводи истрага;
- опис било ког вида оштећења потенцијалних дигиталних доказа, која су примећена током истраге и утицај оштећења на ток истраге;
- ограничавајуће факторе анализе;
- листу свих извршених процеса и коришћених алата;
- интерпретацију дигиталних доказа од стране форензичара. Уколико форензичар сматра да постоји више могућих сценарија, треба да наведе све, као и процену вероватности да се сваки од њих догодио. Треба напоменути да у овом случају форензичар мора јасно да представи дистинкцију између чињеница које је утврдио и свог мишљења и да дā образложење за свако мишљење;
- закључке;
- препоруке за допунску истрагу ако је потребна.

Стога, ваљаност експертског мишљења треба да се заснива на следећим принципима:

- теорије и технике употребљене од стране експерта су тестиране;

- теорије и технике употребљене од стране експерта су рецензиране од стране колега у пољу и јавно објављене;
- ако постоји утврђена вероватноћа грешке за одређену технику, она је забележена у извештају;
- теорије и технике употребљене од стране експерта су регулисане одговарајућим стандардима;
- теорије и технике употребљене од стране експерта су у широкој употреби.

2.2.3 Дигитално форензичко вештачење у Републици Србији

Према Закону о судским вештацима („Сл. гласник РС", бр. 44/2010), „вештачење представља стручну активност, чијим се обављањем, уз коришћење научних, техничких и других достигнућа, пружају суду или другом органу који води поступак, потребна стручна знања која се користе приликом утврђивања, оцене или разјашњења правно релевантних чињеница. Вештачење могу обављати физичка и правна лица која испуњавају одређене услове, државни органи и научне и стручне установе". Чланом 6. овог закона одређени су посебни услови под којима физичко лице може бити именовано за вештака уколико:

- „има одговарајуће стечено високо образовање на студијама другог степена, односно на основним студијама за одређену област вештачења;
- има најмање пет година радног искуства у струци;
- поседује стручно знање и практична искуства у одређеној области вештачења;
- је достојан за обављање послова вештачења".

При томе је чланом 7. овог закона одређено да „кандидат за вештака своје стручно знање и практична искуства за одређену област вештачења доказује стручним и научним радовима, потврдама о учешћу на саветовањима у организацији стручних удружења, као и мишљењима и препорукама судова или других државних органа, стручних удружења, научних и других институција или правних лица у којима је кандидат за вештака радио, односно за које је обављао стручне послове".

Овакав садржај Закона о судским вештацима може се чинити штур с обзиром на то да суд може имати потребу за форензичким испитивањима из више области, као што су ДНК, општа биологија, медицина, трасологија, балистика, физичка хемија, токсикологија, акустика, електронска и информатичка форензичка испитивања итд., па се дā закључити да је неопходно увести правила која су специфична за ове области.

Коментар на садржај поменутих чланова Закона о судским вештацима дају Комлен Николић и сар. (2010) истичући да ће се у области информационих

технологија посебно знање и искуство пре срести код људи који немају високо образовање, већ огроман ентузијазам за праћење свих иновација у пољима информационих технологија. Casey (2012) и Turvey (2011) додају да вештак у области информационих технологија, поред искуства у овој широкој области, мора да има и посебну обуку и вештине из специфичне области коју сведочи, односно вештачи. Такође, Петровић (2001) истиче потребу за мултидисциплинарним тимским приступом с обзиром на широк спектар знања за која може бити претерано очекивати да поседује један човек. Шаркић и Николић (2011) наглашавају да није довољно опште информатичко знање, већ је неопходно да вештак поседује вештине коришћења информатичких технологија. Такође, Шаркић и Николић (2011) предлажу да се у новом закону уведе ограничено бављење вештачењем на четири–пет година, као и категоризација вештака, која укључује њихово лиценцирање. Периодичан избор вештака би омогућио преиспитивање компетентности вештака, с обзиром на брзе технолошке промене.

У правном систему Републике Србије, вештачење се сматра видом доказног средства, при чему је одређење процедуре вештачења везано за појединачне законе. На пример, Закон о парничном поступку предвиђа процедуру вештачења одредбама чл. 249. до 262. У процесном решењу које доноси суд када сматра да је вештачење неопходно, тачно се наводи предмет и обим вештачења, као и тачан задатак вештаку. Вештак је у обавези да, након преузимања предмета вештачења, проучи предмет и процени своју компетентност. У случају да вештак није компетентан, дужан је да предмет врати. Након завршетка вештачења, вештак је дужан да сачини писмени налаз, који треба да садржи опис свих стручних радњи које је обавио. На крају налаза, вештак износи мишљење, које је директан одговор на задатак вештачења. Поред Закона о парничном поступку, закони који се такође баве вештачењем су Законик о кривичном поступку, Закон о прекршајима, Закон о ванпарничном поступку и др.

Компетентност форензичара за анализу потенцијалних дигиталних доказа, према стандарду ISO/IEC 27042 (2016), може бити дефинисана за посебан случај који се тренутно истражује или то може бити општа листа способности према којој се компетентност форензичара може процењивати. У водичу Националног института за стандардизацију и технологију САД-а (Kent и сар., 2006) се додаје да форензичар треба да поседује знање о форензичким принципима, водичима и процедурама, форензичким алатима и техникама, као и антифорензичким техникама. Такође, наводи се да није на одмет да форензичар поседује знање из информационе безбедности и да познаје специфичности најзаступљенијих објеката истраге, као што су најчешће коришћени оперативни системи, системи датотека, најзаступљеније апликације и мрежни протоколи.

2.3 Дескриптивна логика

Да би се схватила улога дескриптивне логике у решавању проблема дигиталне форензике, неопходно је њено разумевање, те следи кратак увод.

Дескриптивна логика је фамилија формалних језика за репрезентацију доменског знања, чија синтакса се састоји од конструката за описивање доменских концепата и веза између концепата, а семантика, која се не разликује од семантике логике првог реда, омогућује опис доменских концепата (Markus и сар., 2013).

Дескриптивна логика јесте фамилија формалних језика, но сви језици се базирају на основном – атрибутивном језику (енг. *Attribute Language*, $\mathcal{AL}$) (Baader, 2003). Основни синтактички елементи су имена индивидуа, имена концепата и имена веза међу њима. Семантички, имена индивидуа означавају појединачне ентитете домена од интереса, имена концепата се односе на типове, категорије или класе поменутих ентитета и имена веза представљају бинарне релације које могу постојати међу ентитетима домена (Rudolph, 2011). Мапирање синтактичких елемената на домен интерпретације одвија се на следећи начин: сваком имену индивидуе придружује се одговарајући ентитет из домена од интереса, сваком имену концепта придружује се скуп доменских ентитета, а сваком имену везе придружује се скуп уређених парова доменских ентитета (Rudolph, 2011).

Доменско знање представљено дескриптивном логиком, тзв. база знања ($\mathcal{KB}$), састоји се од два дела – концептуалног ($TBox$) и чињеничног ($ABox$). Концептуални део обухвата концепте или категорије ентитета одређеног домена, док чињенични део обухвата појаве поменутих концепата, односно њихове конкретизације (Baader и сар., 2017).

Највећи значај дескриптивне логике огледа се у могућности резоновања, односно извођења имплицитног знања на основу експлицитно дефинисаног знања (Baader, 2003). Дескриптивна логика одликује се одлучивошћу (енг. *decidability*). То значи да се процедуре закључивања увек завршавају, те је кориснику увек могуће дати одговор, био он позитиван или негативан. Међутим, у вези са одлучивошћу дескриптивне логике неопходно је имати на уму сложеност процедура одлучивања у оквиру базе знања неког домена и водити рачуна о балансирању између сложености закључивања и степена формалне изражајности доменског знања (Baader и сар., 2017). Закључивање укључује проверу контрадикторности концептуалног дела и проверу односа општи–конкретнији међу појмовима, према чему се појмови организују у хијерархијску структуру (Baader, 2003). Постоје различити типови закључивања међу којима су произвођење одговора на питања који ентитети припадају одређеном скупу, ком скупу припада одређени ентитет и који ентитет/ентитети је у одређеној вези/везама са одређеним ентитетом/ентитетима.

2.3.1 $SROIQ(D)$ дескриптивна логика

$SROIQ(D)$ дескриптивна логика је једна од најекспресивнијих одлучивих дескриптивних логика. База знања састављена од формализама $SROIQ(D)$ дескриптивне логике, поред концептуалног ($TBox$) и чињеничног дела ($ABox$) садржи и део који се односи на везе међу концептима или њиховим конкретизацијама ($RBox$) (Rudolph, 2011).

Да би се разумела дефиниција $SROIQ(D)$ базе знања, потребно је најпре дефинисати појмове *концептуалног израза* (енг. *concept expression*) и *аксиома*

(енг. *axiom*). Појам *концептуалног израза* представља следеће (Rudolph, 2011):

- свако име концепта C $\in \mathbf{N}_C$;
- најопштији концептуални израз $\top$ (израз који означава проширење концепта које обухвата све индивидуе, односно конкретизације; проширење концепта које је тачно за сваку индивидуу; $\top^I = \Delta^I$);
- најрестриктивнији концептуални израз $\bot$ (израз који означава проширење концепта које не садржи ни једну индивидуу, $\bot^I = \emptyset$);
- номиналне концепте $\{a_1, \ldots, a_n\}$ (концептуални израз који означава сваки коначни скуп имена индивидуа, а који представља коначан скуп индивидуа, $\{a_1, \ldots, a_n\} = \{a_1^I, \ldots, a_n^I\}$);
- негацију $\neg C$ (скуп индивидуа који није део проширења концептуалног израза C, $\Delta^I \backslash C^I$);
- пресек $C \sqcap D$ (скуп индивидуа који је истовремено део проширења концептуалног израза C и проширења концептуалног израза D, $(C \sqcap D)^I = C^I \sqcap D^I$);
- унија $C \sqcup D$ (скуп индивидуа који је део проширења концептуалног израза C или проширења концептуалног израза D или оба, $(C \sqcup D)^I = C^I \sqcup D^I$);
- егзистенцијално ограничење индивидуе $\exists r.C$ (постоји индивидуа садржана у проширењу концептуалног израза C која је везом r повезана са датом индивидуом, $(\exists r.C)^I = \{\delta \in \Delta^I | \exists \delta' \in \Delta^I.(\langle \delta, \delta' \rangle \in r^I \wedge \delta' \in C^I)\}$);
- универзално ограничење индивидуе $\forall r.C$ (ако је дата индивидуа повезана са неком индивидуом везом r, онда је та индивидуа садржана у проширењу концептуалног израза C, $(\forall r.C)^I = \{\delta \in \Delta^I | \forall \delta' \in \Delta^I.(\langle \delta, \delta' \rangle \in r^I \rightarrow \delta' \in C^I)\}$);
- саморестрикција $\exists r.\texttt{Self}$ (индивидуе из домена које су везом r повезане саме са собом, $(\exists r.\texttt{Self})^I = \{x \in \Delta^I | \langle x, x \rangle \in r^I\}$);
- ограничење кардиналитета $\geqslant nr.C$ (скуп индивидуа из домена у коме постоји бар n индивидуа које су повезане са неком индивидуом садржаном у проширењу концептуалног израза C везом r, $(\geqslant nr.C)^I = \{\delta \in \Delta^I | \ \# \ \{\delta' \in \Delta^I | \langle \delta, \delta' \rangle \in r^I \wedge \delta' \in C^I\} \geq n\}$);
- ограничење кардиналитета $\leqslant nr.C$ (скуп индивидуа домена у коме постоји не више од n индивидуа које су повезане са неком индивидуом садржаном у проширењу концептуалног израза C везом r, $(\leqslant nr.C)^I = \{\delta \in \Delta^I | \ \# \ \{\delta' \in \Delta^I | \langle \delta, \delta' \rangle \in r^I \wedge \delta' \in C^I\} \leq n\}$).

Ако су C и D концептуални изрази $SROIQ(D)$ дескриптивне логике, израз $C \sqsubseteq D$, који се назива *општим концептом подскупа*, означава скуп индивидуа садржан у проширењу концептуалног израза C, који је подскуп скупа

индивидуа садржаног у проширењу концептуалног израза D, а израз $C \equiv D$, тј. израз $C \sqsubseteq D, D \sqsubseteq C$ назива се *аксиомом еквиваленције*, онда појам *аксиом* представља или аксиом еквиваленције или општи концепт подскупа (Baader и сар., 2017). Дакле, коначан скуп општих концепата подскупа чини концептуални део базе знања ($TBox$) (Baader и сар., 2017).

Ако је $\mathbf{N}_I$ скуп имена индивидуа који нема пресек са скуповима $\mathbf{R}$ и $\mathbf{C}$, ако су $a, b \in \mathbf{N}_I$ имена индивидуа, $\mathbf{C}$ је име концепта и $r \in \mathbf{R}$ је име везе, онда се израз $C(a)$ назива *конкретизацијом концепта* а израз $r(a, b)$ зовемо *конкретизацијом везе*. Коначан скуп конкретизација концепата и конкретизација веза чини чињенични део $SROIQ(D)$ базе знања ($ABox$) (Baader и сар., 2017). Дакле, ако су a и b имена индивидуа, C је концептуални израз и r је веза, онда $ABox$ обухвата следеће изразе (Rudolph, 2011):

- конкретизацију концепта $C(a)$ (индивидуа a је инстанца, односно конкретизација проширења концептуалног израза C, $a^I \in C^I$);
- конкретизација везе $r(a, b)$ (индивидуа a је повезана са индивидуом b везом r, $(a^I, b^I) \in r^I$);
- негација конкретизације везе $\neg r(a, b)$ (индивидуа a није повезана са индивидуом b везом r, $(a^I, b^I) \notin r^I$);
- израз једнакости $a \approx b$ (индивидуа a и индивидуа b су једна иста индивидуа, $a^I = b^I$);
- израз неједнакости $a \not\approx b$ (индивидуа a и индивидуа b нису једна иста индивидуа, $a^I \neq b^I$).

Да би се схватила дефиниција дела $SROIQ(D)$ дескриптивне логике који обухвата везе међу концептима или њиховим конкретизацијама, потребно је дефинисати појам аксиома везе. Ако су r и s имена веза, аксиом везе је израз који има неку од следећих форми:

- подскуп везе $r_1 \circ \cdots \circ r_n \sqsubseteq r$ (ако је, у низу индивидуа, сваки пар суседних индивидуа међусобно повезан, онда прва и последња индивидуа морају бити такође повезане, $r_1^I \circ \cdots \circ r_n^I \subseteq r^I$);
- разлика везе $\texttt{Disj}(r, s)$ (сваки пар индивидуа из домена који је повезан везом r није повезан везом s, $r^I \cap s^I = \emptyset$);
- транзитивност веза $\texttt{Trans}(r)$ (ако је индивидуа d повезана са индивидуом e везом r и ако је индивидуа e повезана са индивидуом f везом r, онда је индивидуа d повезана са индивидуом f везом r,
$(d, e) \in r^I \wedge (e, f) \in r^I \Rightarrow (d, f) \in r^I$);
- функционалне везе $\texttt{Func}(r)$ (ако је индивидуа d повезана са индивидуом e везом r, онда индивидуа d не сме бити повезана са било којом другом индивидуом везом r,
$(d, e) \in r^I \wedge (d, f) \in r^I \Rightarrow e = f$);

- рефлексивност везе $\texttt{Ref}(r)$ (постоји индивидуа из домена која је повезана сама са собом везом r, $d \in \Delta^I \Rightarrow (d,d) \in r^I$);
- нерефлексивност везе $\texttt{Irref}(r)$ (не постоји индивидуа из домена која је повезана сама са собом везом r, $d \in \Delta^I \Rightarrow (d,d) \notin r^I$);
- симетричност везе $\texttt{Sym}(r)$ (ако је индивидуа d повезана са индивидуом e везом r, онда је индивидуа e повезана са индивидуом d везом r, $(d,e) \in r^I \Rightarrow (e,d) \in r^I$);
- асиметричност везе $\texttt{Asym}(r)$ (ако је индивидуа d повезана са индивидуом e везом r, онда индивидуа e није повезана са индивидуом d везом r, $(d,e) \in r^I \Rightarrow (e,d) \notin r^I$).

Скуп аксиома везе у бази знања представља део $SROIQ(D)$ базе знања која обухвата везе између концепата или њихових конкретизација (Baader и сар., 2017). Дакле, база знања креирана помоћу формализама $SROIQ(D)$ дескриптивне логике састоји се од три дела означена са $RBox$, $TBox$ и $ABox$. Другим речима, она се дефинише као триплет $\mathcal{KB} = (\mathcal{R}, \mathcal{T}, \mathcal{A})$ (Baader и сар., 2017). Над базом знања могуће је применити расуђивач, који омогућава закључивање о знању представљеном у бази знања (Baader и сар., 2017).

2.3.2 Расуђивање над SROIQ(D) базом знања

Дескриптивна логика пружа могућност расуђивања о концептима, везама и конкретизацијама концепата (Baader, 2010). Међу типовима расуђивања су произвођење одговора на питања који ентитети припадају одређеном скупу, ком скупу припада одређени ентитет и који ентитет/ентитети је у одређеној вези/везама са одређеним ентитетом/ентитетима.

Одређивање инстанци (ентитета) које припадају одређеном скупу односи се на инстанце тј. конкретизације било концепата или веза. Ако постоји база знања $\mathcal{KB}$ и концептуални израз C, одређивање инстанци као тип расуђивања даје сва имена индивидуа $a \in \mathbf{N}_I$, где је $\mathbf{N}_I$ скуп имена индивидуа који означава појединачне ентитете из домена од интереса за које важи $a^I \in C^I$. У том случају, одговор је име индивидуе a које је у бази знања описано као конкретизација концепта C, $\mathcal{KB} \models C(a)$. Ово захтева следећу проверу базе знања: $|\mathbf{N}_I(\mathcal{KB})|$. С друге стране, одређивање инстанци примењено над везама резултује свим паровима (a,b) имена индивидуа a и $b \in \mathbf{N}_I$ за које важи $(a^I, b^I) \in r^I$. Ово захтева проверу базе знања $\mathcal{KB} \models r(a,b)$ (Rudolph, 2011).

Имена концепата садржана у бази знања могу бити организована хијерархијски. Стога, одређивање скупа коме припада одређени ентитет врши се следећом провером над базом знања: $\mathcal{KB} \models A \sqsubseteq B$ за сваки пар имена концепата A, B (Rudolph, 2011).

Одговор на питање који ентитет/ентитети је у одређеној вези/везама са одређеним ентитетом/ентитетима може бити вредност из бинарног скупа вредности (тачно или нетачно) или торка имена индивидуа. Тип одговора зависи од постојања карактеристичних променљивих. За разлику од некарактеристичних променљивих, за карактеристичне променљиве је везано егзистенцијално

ограничење. На пример, у изразу $\exists y \exists z(\texttt{role1}(x, y) \wedge \texttt{role1}(x, z) \wedge \texttt{role2}(y, z))$, x је карактеристична променљива, а y и z су некарактеристичне променљиве. Ако су све променљиве у упиту некарактеристичне, одговор је бинарне природе. У супротном, одговор је торка имена индивидуа у коме су променљиве замењене именима индивидуа (Rudolph, 2011).

2.4 Сажетак

Свакој дигиталној истрази требало би доделити епитет форензички, с обзиром на то да сценарија, која захтевају дигиталну истрагу, а испрва нису укључена у правни поступак, то у будућности могу постати. Подразумева се да је дигитална форензичка истрага ваљано спроведена и да производи дигиталне доказе прихватљиве на суду. Стога је консензус научника и форензичара у расправи о ваљаности дигиталне форензичке истраге постигнут око конформације стандардима, водичима и процедурама за ваљано спровођење дигиталне истраге. У овој дисертацији обрађени су одабрани стандарди и водичи, а међу њима су ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042, ISO/IEC 27043, Guide to Integrating Forensic Techniques into Incident Response и Guidelines for Digital Forensics First Responders.

Правна регулатива у Републици Србији у вези са спровођењем дигиталне форензичке истраге изнета је Законом о судским вештацима („Сл. гласник РС", бр. 44/2010), као и појединим члановима Закона о парничном поступку, Закона о прекршајима, Закону о ванпарничном поступку и др. Међутим, многи аутори се слажу око тога да ова регулатива има много мана и да ју је потребно ревидирати и допунити, како би се вештачење у области информационих технологија, односно дигитално форензичко вештачење у Републици Србији, подигло на виши ниво у смислу компетентности форензичара и ваљаности дигиталне форензичке истраге. Како дескриптивна логика, као средство формалног описа ваљане форензичке истраге, може допринети побољшању дигиталног форензичког вештачења, у овом поглављу дате су основе дескриптивне логике.

3 Сродна истраживања

- Технологија рађа криминал и ми стално покушавамо да развијемо технологију како бисмо били корак испред особе која покушава да је злоупотреби.

Френк Абагнејл

3.1 Преглед

Пројекат овог истраживања захтева познавање различитих дисциплина као што су инжењеринг знања и дигитална форензика и повезује различите теме, међу којима су формално описивање одређеног домена и ваљано спровођење форензичке истраге. У складу са тим, ово поглавље обухвата преглед релевантних истраживања која су утицала на развој идеје и имплементацију истраживања ове дисертације. Истраживања су наведена хронолошки и укратко представљена са аспекта проблема, хипотезе и верификације хипотезе. Потом је дат коментар у вези са утицајем датог истраживања на истраживање ове дисертације.

У одељку Формална репрезентација знања у области дигиталне форензике, дат је преглед општих и специјалних онтологија као формалних репрезентација знања у области дигиталне форензике, које имају различите сврхе. У односу на овај одељак, у одељку Формална репрезентација критеријума ваљаности дигиталне форензичке истраге, издвајају се истраживања која онтологију користе као средство за формално описивање критеријума ваљаности дигиталне форензичке истраге. Одељак Формална репрезентација стандарда, представља преглед истраживања у којима се интегришу идеје из претходна два одељка, те се обрађује формална репрезентација стандарда у области дигиталне форензике, чија се сврха своди на представљање критеријума ваљаности дигиталне форензичке истраге. Одељак Критички осврт на сродна истраживања, узима у обзир најважније радове из литературе и концизно представља њихове теме. Затим следе запажања о недостацима ових радова која правдају потребу за истраживањем описаним овом дисертацијом.

3.2 Формална репрезентација знања у области дигиталне форензике

Проблем који исказују аутори Schatz и сар. (2004b) је енормна количина информација о догађајима, међу којима се крију и информације о инцидентима које форензичар треба да докучи. Поред тога информације су складиштене у најразличитијим формама. Аутори сматрају да експертски систем базиран на онтологији представља начин аутоматизације корелирања информација о догађајима који су предмет истраге. Ову хипотезу верификовали су студијом случаја за чије потребе су имплементирали прототип овог система.

За развој онтологије, која се не ослања ни на коју претходно развијену онтологију и која је специјализована за логове догађаја, аутори су користили стандард OWL [4], а за развој апликационог интерфејса аутори су користили радни оквир JENA [5]. Онтологија је веома једноставна и практично се своди на таксономију с обзиром на то да нису коришћени конструкти као што су ограничења и својства класа. Мана онтологије коју представљају ови аутори је недефинисана структура онтологије, што уноси конфузију и ствара тешкоће у разумевању описаног знања. Организовање структуре онтологије доприноси конзистентности и у увођењу новог знања. Приступ аутора Schatz и сар. (2004b) проширују аутори Schatz и сар. (2004a) додајући друге типове логова, али и могућност интеграције онтологија других поддомена, парсера и правила корелирања, које би сачињавали експерти за то компетентни, те би на тај начин своју експертизу могли искомуницирати са другим неискусним форензичарима.

Аутори Brinson и сар. (2006) као проблем виде непостојање дефинисаних критеријума компетентности форензичара у дигиталном домену и сматрају да специјална онтологија која представља нивое специјализовања, сертификовања и едукације форензичара у дигиталном домену, може допринети свесности о томе које критеријуме треба задовољити да би се форензичар сматрао компетентним за рад у овом пољу. Аутори узимају у обзир различите професије које могу бити укључене у дигиталну форензичку истрагу. Међутим, улоге форензичара у различитим професијама површно су обрађене. За разлику од овог истраживања, појам експерта у овој дисертацији везује се за појам стручњака који је компетентан да учествује у истрази сајбер инцидената независно од тога да ли свом позиву служи у оквиру војске, полиције или академске заједнице.

Проблемом компетентности форензичара у дигиталном домену индиректно се баве и аутори Kahvedžić и Kechadi (2009), који констатују да су инциденти у дигиталном пољу све чешћи и напреднији, те је њихова истрага изузетно компликована и временски захтевна. То даље обавезује дигиталне форензичаре да буду у корак са широким спектром алата, техника, опреме и уређаја, што представља велики изазов. Као решење овог проблема аутори предлажу логички коректну базу знања у области дигиталне форензике, која је имплементирана као онтологија под називом DIALOG и која служи репрезентовању и анализи знања у домену дигиталне истраге. Употреба ове онтологије демонстрирана је у истрази регистара оперативног система Windows. Онтологија садржи главне концепте дигиталне форензике и односе међу њима, а независна је од конкретне истраге и могуће ју је проширивати новим концептима. За евалуацију онтологије аутори су јој прилагодили форензички алат за анализу Windows регистара, RPCompare (Kahvedžić и Kechadi, 2008). Сама онтологија није објављена, али идеја њених аутора да сврха онтологије може бити и вођење форензичара кроз истрагу са циљем спречавања грешака, среће се и у овој дисертацији.

Форензика рачунарских мрежа се као тема истраживања среће и у ра-

[4] https://www.w3.org/TR/owl-features/
[5] https://jena.apache.org/

ду аутора Saad и Traore (2010). Ови аутори примећују да је фаза анализе у истрази рачунарске мреже умногоме мануелан процес, који отежава огромна количина података из различитих извора и различитих формата, те је потребна аутоматизација. Предложено решење за аутоматизацију су онтологије које садрже знање из домена форензике рачунарских мрежа и репрезентацију методологија за спровођење истраге у оквиру различитих сценарија форензике рачунарских мрежа. Студијом случаја показано је да знање описано онтологијама, као и изведено знање добијено расуђивањем, доприноси аутоматизацији у фази анализе обезбеђујући значења пронађених трагова. Имплементације онтологија нису објављене, те поновна искористљивост ове онтологије за опис домена форензике рачунарских мрежа у раду описаном овом дисертацијом није могла бити разматрана.

Аутори Kahvedžić и Kechadi (2011) надограђују онтологију DIALOG тако да се може искористити као помоћ при писању извештаја, односно стручног налаза и мишљења форензичара, пре свега у смислу образлагања релевантности доказа. Да би се онтологија похранила подацима о резултатима истраге, који укључују значење података, односно контекстуалне информације, аутори су развили окружење за манипулисање онтологијом. За разлику од система DIALOG, аутори сада користе механизме извођења новог знања, класификацију и категоризацију знања представљеног онтологијом, те тако доприносе разумевању и лакоћи постављања упита над базом знања.

Идеја вођења форензичара кроз истрагу среће се у истраживању чији је продукт уско специјализована онтологија аутора Chu и сар. (2011). Њихов научни допринос пољу дигиталне форензике огледа се у моделу дигиталне форензичке истраге вођеним онтологијом у контексту свеприсутног рачунарства. Дакле, модел у својој бази садржи кључне елементе свеприсутног рачунарства, који се гранају информацијама које потенцијално имају доказну вредност. Ради евалуације модела, аутори представљају студију случаја форензичке истраге, која се спроводи вођењем поменутом онтологијом.

Аутори Alzaabi (2013) претендују на решење проблема обимности и комплексности података које треба анализирати у оквиру дигиталне форензичке истраге. Предлог решења је радни оквир који асистира истражитељу тако што аутоматски анализира садржај мобилног уређаја. Аутор користи онтологију која садржи основне концепте мобилних уређаја и везе међу њима, те тако омогућава стварање базе података као потенцијалних доказа екстракованих из мобилних уређаја. Сврха такве онтологије је да открије нове информације механизмом расуђивања.

Аутори Dosis и сар. (2013) увиђају да је фаза анализе дигиталне форензичке истраге у најмањој мери формализована и да се умногоме ослања на форензичареву експертизу и искуство, што представља узрок честих грешака. Зато предлажу метод за семантичко анотирање и интеграцију дигиталних доказа који потичу из различитих извора. Овај метод се састоји од креирања уско специјализованих онтологија које моделују различите типове извора потенцијалних дигиталних доказа. Над овим онтологијама се, у зависности од тренутног типа извора доказа, примењују специјализовани алати за парсирање и трансформацију података у њихове семантичке репрезентације кре-

ирајући базу знања над којом је потом могуће аутоматско расуђивање. Како OWL језик за семантичку репрезентацију знања има ограничену експресивну моћ, то су аутори интегрисали расуђивање над комплекснијим правилима, чији резултат потом бива уметнут у постојећу базу знања. На крају, систем омогућава да форензичар постави упите над базом знања формулишући их језиком SPARQL. У датом истраживању аутори нису обезбедили кориснички интерфејс који би форензичару омогућио лаку навигацију кроз повезани граф и постављање упита.

Аутори Slay и Schulz (2014) су развили једноставну специјализовану онтологију како би верификовали хипотезу која гласи – употреба онтологије доприноси ефективности филтрирања потенцијалних дигиталних доказа. Сврха ове онтологије је да идентификује потенцијално сумњиве податке и на тај начин скрене пажњу форензичару који даље потврђује доказну вредност идентификованих података или их одбацује. Употребу онтологије омогућава њена уградња у алат са графичким корисничким интерфејсом, који форензичари могу искористити за скенирање уређаја на месту догађаја пре наставка истраге у лабораторији.

Такође, у истраживању аутора Turnbull и Randhawa (2015) као проблем се јавља огромна количина података, која представља предмет истраге за једног форензичара. Поставља се питање како повећати ефикасност форензичке истраге, а да се не снизи њен квалитет. Аутори представљају концепт система који се базира на формалној репрезентацији знања, а чија је сврха да послужи истражитељима који нису форензички експерти у тријажи дигиталних уређаја. Аутори наводе да, док год процес расуђивања над формално описаним знањем може бити објашњен, ваљаност употребе оваквог система на суду не би требало да буде доведена у питање.

Разумевање и дефинисање термина у области дигиталне форензике аутори Talib и Alomary (2015) препознају као проблем, те предлажу свеобухватну онтологију, која, између осталог садржи термине различитих типова инцидената информационе безбедности, као и модела дигиталних форензичких процеса и процедура. Ови термини се не гранају у дубину, већ је сврха онтологије да повеже неизоставне појмове који чине дигиталну форензику.

Док се у истраживањима представљеним на почетку овог прегледа недефинисаност структуре онтологије сматрала маном, сада аутори Brady и сар. (2015) тврде да је предност то што онтологија нема строго одређену форму, јер ју је тада лакше надограђивати новим форензичким артефактима који током истрага буду пронађени. Проблем који ови аутори онтологијом претендују да реше је енормна количина дигиталних уређаја који се све више појављују као циљ или средство криминалних активности. Тако они тврде да онтологија као репозиторијум и класификатор дигиталних форензичких артефаката доприноси редукцији података пре њихове екстракције. Студијом случаја аутори су показали како онтологија под називом DESO, постављајући над њоме SPARQL упите, може послужити форензичару да одговори на питања у вези са локацијом и типом форензичких артефаката одређеног складишта података али и да постигне корелацију између артефаката са различитих складишта података. Мана овог система је потреба да форензичар сам поставља SPARQL

упите, као и то што је онтологија само делимично попуњена знањем.

Даље, аутори Cuzzocrea и Pirrò (2016) препознају два главна проблема: прикупљени доказни материјал најчешће се одликује значајном разликом у формату, па га је теже интегрисати ради анализе и несвесност форензичара о имплицитном знању које се може извести из прикупљеног доказног материјала. С тим у вези, предлажу радни оквир који се састоји од четири модула: модула знања, модула интеграције података, модула расуђивања и модула постављања упита, који може да се комбинује са постојећим алатима у дигиталној форензици. Модул знања чини скуп специјализованих онтологија који форензичару помаже у формулисању хипотеза истраге и тестирању. У развоју онтологија учествовали су експерти у пољу дигиталне форензике, као и правници. Да би се овај радни оквир верификовао, аутори су симулирали рачунарски напад користећи виртуелизацију. На основу специјализованих онтологија, извршили су конверзију форензичких артефаката у формат RDF, а затим су различити артефакти интегрисани на основу дефинисаних правила. Над овако описаним случајем, могуће је, у зависности од хипотезе случаја, поставити SPARQL упит чији одговор води до потврђивања или одбацивања хипотезе. Мана и овог алата је непостојање корисничког интерфејса за постављање упита, па је форензичар принуђен да сам формулише SPARQL упите.

Проблем корелирања података услед хетерогености веће количине података из различитих извора препознају и аутори Mohammed и сар. (2016). Они предлажу радни оквир, који имплементира онтологију и који ће помоћи у разумевању веза између артефаката. Међутим, ова онтологија није елаборирана и мало тога се на основу описа истраживања о њој сазнаје.

3.3 Формална репрезентација критеријума ваљаности дигиталне форензичке истраге

Представници раних истраживања везаних за ваљаност дигиталне форензичке истраге, чија су запажања била корисна за развој истраживања описаног овом дисертацијом су радови аутора Meyers и Rogers (2005) и Ieong (2006). Meyers и Rogers (2005) сматрају да обрада дигиталних доказа кроз истрагу мора бити усклађена са оним што у овом пољу налаже право, као и наука да би из истраге проистекли докази који репрезентују релевантне чињенице. Ieong (2006) сматра да треба дефинисати основне принципе, који треба да буду задовољени кроз сваку активност истражног процеса. Као што су основни принципи информационе безбедности – поверљивост, интегритет и доступност, тако се форензичка истрага, сматрају аутори, мора заснивати на прописном извиђању, поузданости и релевантности. Аутори су били подстакнути проблемом исувише стручне природе извештаја форензичара о истрази, због чега извештај наилази на неразумевање од стране правника када дође до презентовања дигиталних доказа на суду.

Аутор Chaikin (2006) тврди да се, услед непостојања стандардних процедура за прикупљање, чување и анализу дигиталних доказа, повећава вероватноћа грешке у анализи и интерпретацији дигиталних доказа. Додатно, Hoss

и Carver (2009) примећују да не постоји свеобухватна формална репрезентација знања из области дигиталне форензике нити стандардизоване процедуре за спровођење истраге. То доводи до некомпатибилности форензичких алата као и до отежане поновне искористљивости знања у овој области. Зато ови аутори сматрају да се комбиновањем онтологија које садрже знање у области дигиталне форензике може допринети решавању проблема огромне количине података која се ставља пред форензичара, као и проблема стандардизације форензичких процедура и правне ваљаности дигиталних доказа.

Аутори Ćosić и сар. (2011) примећују да, како поред стручног налаза и мишљења и доказа валидности форензичког процеса, форензичар као продукт истраге треба да приложи и ланац надлежности, то вођење евиденције о руковању доказним материјалом има посебан значај за процену ваљаности дигиталне форензичке истраге. Аутори свој рад на унапређивању завођења ланца надлежности започињу креирањем онтологије, која садржи принципе завођења ланца надлежности доведене у везу са различитим уређајима као потенцијалним изворима доказа. Тиме доприносе разумевању ових принципа и структуре знања у области дигиталне форензике које је неопходно за ваљано завођење ланца надлежности.

Најзначајнија констатација за истраживање ове дисертације среће се у раду аутора Valjarevic и сар. (2014) и гласи да је већа прихватљивост доказа на суду сразмерна праћењу стандарда и формалних процедура током истраге, који су подвргнути јакој ревизији и који су међународно прихваћени. На ову констатацију надовезују се Antwi-Boasiako и Venter (2017), који кажу да стандарди дотад објављени, што укључује избор стандарда и процедура у овој дисертацији, не адресирају адекватно проблем прихватљивости дигиталних доказа јер се прихватљивост доказа не огледа само у конформацији стандардима и, додатно, постојећи стандарди не пружају могућност процене прихватљивости дигиталних доказа проистеклих из форензичке истраге. Као решење за овај проблем, аутори предлажу концепт радног оквира који интегрише техничке и правне захтеве ваљаности дигиталних доказа, који ће помоћи у развијању стандарда у области дигиталне форензике као и у хармонизацији правних и техничких аспеката дигиталне форензичке истраге.

Arshad и сар. (2020) се баве аутоматизацијом у области дигиталне форензике са аспекта њене прихватљивости на суду. Аутори закључују да аутоматизација мора бити заснована на формалним теоријама, а ове теорије су ретке у дотадашњем истраживању. Стога су аутори развили формалну теорију, односно онтологију, за аутоматизацију у пољу форензике социјалних мрежа. Како се ова аутоматизација заснива на формалној и објашњивој теорији, која је строго тестирана, то њени продукти не могу бити оспорени на суду као неваљано произведени. Онтологија се састоји од формалних репрезентација учесника у инцидентима везаним за социјалне мреже и веза између њих, те је њена сврха да објасни повезаност догађаја. Студијом случаја је показано да употреба онтологије доприноси ефикасности истраге редукујући скуп потенцијалног доказног материјала који треба анализирати.

Проблем неадекватног прикупљања дигиталних доказа и неуспешно одржање тачности, аутентичности и комплетности доказног материјала, што

доводи до одбацивања дигиталних доказа на суду као невалидних, увидели су аутори Yeboah-Ofori и Brown (2020). С тим у вези, поново се јавља тврдња да хармонизација правних и техничких фактора доводи до валидности доказа на суду. Надовезујући се на ову тврдњу, аутори Ramanauskaite и сар. (2022) чак уводе термин „сајбер јуриспруденција" којим желе да укажу на значај хармонизације техничких и правних аспеката форензичке истраге, који су кључни за ваљаност дигиталних доказа на суду.

3.4 Формална репрезентација стандарда

Први за ову дисертацију релевантни напори да се формално представи знање из стандарда вежу се за поље информационе безбедности. Аутори Fenz и сар. (2007) предлажу радни оквир базиран на онтологији развијен са циљем да се олакша прегледање стандарда ISO/IEC 27001 и тако допринесе бољој спремности компаније на сајбер нападе, али и проверу усклађености мера компаније са овим стандардом. Аутори у најави свог будућег рада наводе комбиновање других релевантних стандарда у дату онтологију. Исти мотив имају и аутори Pereira и Santos (2009), који су развили систем базиран на онтологији чије знање представља концепте из стандарда ISO/IEC FDIS 27001 (2005).

Прво истраживање које препознаје преку потребу за стандардом за репрезентовање информација о дигиталној форензичкој истрази среће се код аутора Garfinkel (2010). Потом, аутори Casey и сар. (2015) примећују да се дотадашње формалне репрезентације информација о истрази обично фокусирају на исувише специфичне делове форензичког процеса, не подржавају интеграцију са другим репрезентацијама и нису структуриране. Аутори предлажу стандард за репрезентацију и размену знања у пољу дигиталне форензике под именом DFAX, који се ослања на CybOX (Barnum и сар., 2012). DFAX уводи процедуралне појмове дигиталне форензичке истраге као што су евиденција ланца надлежности и управљање истражним процесом. Тиме овај рад нема преседана по питању увођења принципа ваљаности форензичке истраге у онтологију.

Иако у области информационе безбедности, рад аутора Syed и сар. (2016) изузетно је значајан за истраживање описано овом дисертацијом с обзиром на то да садржи идеју о инкорпорирању стандарда у онтологију. Онтологија под називом UCO покрива област информационе безбедности и важи за свеобухватну онтологију која олакшава дељење информација, проширивање и инкорпорирање садржаја више стандарда међу којима су CVE (Mann и Christey, 1999), CCE (Mann, 2008), CVSS (Forum of Incident Response and Security Teams, 2005), CAPEC (United States Department of Homeland Security, Office of Cybersecurity and Communications, 2007), CYBOX (Barnum и сар., 2012), KillChain (Barnum, 2012), STUCCO (Iannacone и сар., 2015). За развој ове онтологије узето је у обзир неколико постојећих онтологија, међу којима су Linked Open Data (Berners-Lee и сар., 2009), DBpedia (Auer и сар., 2007), Yago knowledge base (Suchanek и сар., 2008) и др.

Прво истраживање које у онтологију уграђује стандард ISO/IEC 27043

(2016), који се налази међу стандардима из избора у истраживању ове дисертације припада ауторима Ellison и Venter (2016). Аутори су мапирали стандард ISO 27043 на најапстрактније класе у онтологији, коју су потом специјализовали знањем о техникама које се примењују у пољу информационе безбедности и у пољу дигиталне форензике са циљем олакшавања истражитељима и научницима да стекну увид у сврху и начин примене поменутих техника.

Проблем истраге исте врсте информација из различитих извора и у различитим форматима, што отежава размену ових информација, њихову корелацију и анализу препознају аутори Casey и сар. (2018). Као решење овог проблема они предлажу платформу базирану на формалном језику CASE, која би допринела анализи доказног материјала. CASE превазилази све претходне формалне језике у домену дигиталне форензике и информационе безбедности као што су DOMEX (Office of the Director of National Intelligence, 2015), CybOX (Barnum и сар., 2012) и DFXML (Garfinkel, 2012). Аутори су искористили онтологију UCO за развој овог стандардизованог формалног језика за описивање и размену информација у различитим доменима међу којима је дигитална форензичка истрага и реаговање на безбедносне инциденте. Надоградњу репрезентације дигиталних трагова из онтологије UCO аутори су спровели угледајући се на модел платформе за дигиталну форензику „Ханскен" (Van Eijk, 2014).

Још једна група аутора која увиђа да у области дигиталне форензике постоји потреба за стандардизовањем и дефинисањем процеса јесте Ellison и сар. (2019). Ови аутори су прибегли формалној класификацији техника које се примењују након што се инцидент догоди. За поставку главних концепата, односно класа онтологије, аутори су се угледали на стандард ISO 27043. Amato и сар. (2020) такође се баве проблемом стандардизације онтологије. Базирајући се на стандарду ISO/IEC 27037, они спроводе семантичко анотирање података који су резултат рада форензичких алата.

Даље, аутори Akremi и сар. (2020) примећују да је, услед импресивног пораста сајбер криминала, енормно порасла количина података која је предмет форензичке истраге, те је отежана анализа података. Аутори сматрају да онтологија, која садржи доменско знање и базира се на ISO/IEC 27037 стандарду, доприноси анализи података током форензичке истраге тако што олакшава откривање и корелирање информација. Тестирање ефективности и ефикасности свог приступа аутори су спровели анализирајући лог-датотеке.

Дакле, литература око стандардизације и формализације знања у области дигиталне форензике подељена је на две идеје – једна се огледа у развоју стандардног језика за формализацију знања, а друга у формализацији постојећих међународно признатих стандарда.

Не треба изоставити напор аутора Kabaale и сар. (2018) и Mussmann и сар. (2020). Рад аутора Kabaale и сар. (2018) је значајан јер се бави питањем како обезбедити конформацију стандардима кроз формалну верификацију без обзира на то што не обрађују стандарде у области дигиталне форензике. Mussmann и сар. (2020) су извршили преглед литературе у којој се износе истраживања на тему усклађивања више безбедносних стандарда. Њихово запажање је да се хармонизација стандарда углавном врши ручно или се

развијају онтологије.

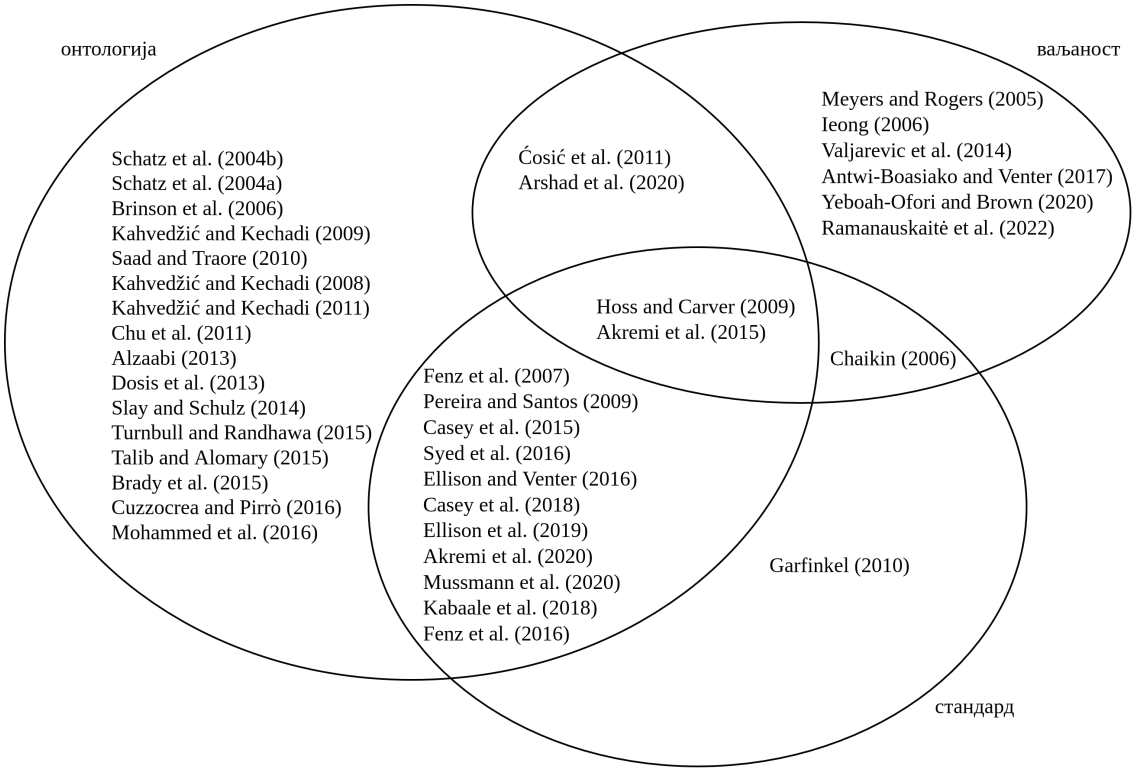
Следи преглед истраживања која интегришу више аспеката битних за истраживање ове дисертације.

Аутори Akremi и сар. (2015) у свом раду у обзир узимају следећа три аспекта – формализацију кроз онтологију, међународно признате стандарде и критеријуме прихватљивости дигиталних доказа на суду. Фокусирајући се на веб-сервисе, аутори увиђају да је, у случају безбедносног инцидента, форензичарима отежано спровођење истраге над логовима с обзиром на то да формат логова није униформан. Такође, форензичке процедуре нису стандардизоване, а форензичарима нису доступна искуства других форензичара, који су истраживали сличне случајеве. Стога аутори закључују да стандардни модел података, који се обрађују током форензичке истраге веб-сервиса, у виду проширљиве онтологије, омогућава аутоматизацију процеса анализе тако да докази који из ње проистекну буду прихватљиви на суду. Да би верификовали ову хипотезу, аутори су имплементирали алат са графичким корисничким интерфејсом који врши логовање активности веб-сервиса са којима је повезан и складишти их у онтологију. Потом, овај алат иницира расуђивање над онтологијом описаним знањем у складу са SWRL правилима и SPARQL упитима. Цео систем тестиран је у једној студији случаја. На овај начин, алат аутоматски детектује и реконструише малициозне догађаје. Студијом случаја је показано да употреба онтологије доприноси ефикасности истраге редукујући скуп потенцијалног доказног материјала који треба анализирати.

С друге стране, аутори Fenz и сар. (2016), поред формализације кроз онтологију и међународно признатих стандарда, у своје истраживање уводе и развој алата базираног на онтологији, који учествује у верификацији хипотезе на основу података прикупљених експерименталним методом. Хипотеза њиховог истраживања гласи – принцип управљања ризиком који се заснива на онтологији, омогућава да се аутоматски изведе степен усклађености предузетих мера са одговарајућим стандардима. Верификација ове хипотезе одвила се на следећи начин. Развијен је прототип система који се базира на UCO онтологији, који је потом примењен у оквиру неколико студија случаја. Прототип система је имплементиран као веб-апликација, која пружа графички интерфејс за интеракцију са корисником и који обезбеђује улаз у систем као опис форензичког случаја. Валидацију система аутори су спровели у реалном окружењу организације чија је специјалност високо безбедна софтверска решења и која је ауторима омогућила увид у своје пословне процесе. Међу учесницима у овом процесу валидације била су два истраживача и пет запослених у поменутој организацији. Први корак валидације је мапирање организацијске инфраструктуре и имплементираних противмера за безбедносне инциденте у онтологију, како би се обезбедило расуђивање над базом знања и провера усклађености са стандардом. Затим је уз помоћ алата, односно система базираног на овој онтологији, израчунат степен усклађености, који је потом коментарисан са учесницима процеса валидације, односно запосленима различитих специјалности. Тиме су добијени квалитативни резултати који су указивали на успех предложеног решења.

3.5 Критички осврт на сродна истраживања

Потрага за релевантном литературом своди се на потрагу за трима елементима који карактеришу истраживање описано овом дисертацијом. Први елемент је формализација знања, која се имплементира онтологијом, други елемент је стандардизација, а трећи елемент представља тема ваљаности дигиталне форензичке истраге на суду. Ради прегледности, ови елементи означени су као: (1) онтологија; (2) стандард; (3) ваљаност. На слици 2 приказан је Венов дијаграм најважнијих радова обрађених у овом одељку, који садрже један или више ових елемената.



Слика 2: Најважнији радови релевантне литературе.

С тим у вези, могуће је недостатке радова са овим темама поделити у неколико група: уска специјализација у оквиру подобласти дигиталне форензике, нпр. логови веб-сервиса (Akremi и сар., 2020), социјалне мреже (Arshad и сар., 2020) или регистар оперативног система Windows (Kahvedžić и Kechadi, 2009), затим, ограничавање на један стандард (Akremi и сар., 2020; Alzaabi, 2013; Amato и сар., 2020; Arshad и сар., 2020), нереференцирање на међународно признате стандарде и процедуре приликом креирања онтологије (Alzaabi, 2013; Amato и сар., 2020), ограничавање на један критеријум ваљаности истраге (Kahvedžić и Kechadi, 2011) и ограничавање на једну фазу форензичке истраге (Akremi и сар., 2020; Alzaabi, 2013; Amato и сар., 2020; Arshad и сар., 2020). Дакле, колико је познато, не постоји истраживање које дескриптивном логиком формално описује област форензике рачунарских мрежа, а при томе у обзир узима међународно признате стандарде и процеду-

ре за ваљано спровођење форензичке истраге, подробно обрађује сваку фазу форензичке истраге и у обзир узима све критеријуме ваљаности форензичке истраге које је научна заједница у области дигиталне форензике препознала.

3.6 Сажетак

Ово поглавље интегрише три групе сродних истраживања која као објекат формалне репрезентације имају различите теме обрађене истраживањем ове дисертације. Прву групу радова чине они који се баве формалном репрезентацијом знања у области дигиталне форензике. Другу групу чине радови чији је фокус на анализи критеријума ваљаности дигиталне форензичке истраге и њиховој формалној репрезентацији, а трећа група радова бави се формалном репрезентацијом међународно признатих стандарда. Радови су коментарисани са аспекта проблема истраживања, хипотезе, верификације хипотезе и резултата истраживања. На крају поглавља дат је критички осврт на поменуте радове где су концизно представљене теме оних најважнијих радова и потом коментарисане мане њихових истраживања.

4 Предложени формални модел форензичке истраге

- Живот се може објашњавати тек када је проживљен.

Серен Кјеркегор

4.1 Преглед

Дигитална форензика је дуг период била пре свега пракса, зато, када је реч о иновативности у овој области, њој свакако мора претходити практично искуство. С тим у вези, Кјеркегорову мисао можемо применити по аналогији, па рећи: рад на развоју дигиталне форензике као науке, започиње у лабораторији, радом на различитим случајевима који обогаћују искуство.

Искуство у Лабораторији за дигиталну форензику Факултета техничких наука Универзитета у Новом Саду равноправно је са теоријским разматрањима утицало на појаву идеје описане овом дисертацијом. Концептуална идеја онтологијом вођене истраге објављена је у раду Matijević и Gostojić (2021), док је радом Matijević Gostojić и Vuković (2023) идеја унапређена структурираношћу онтологије и проширена увођењем међународно признатих стандарда и водича.

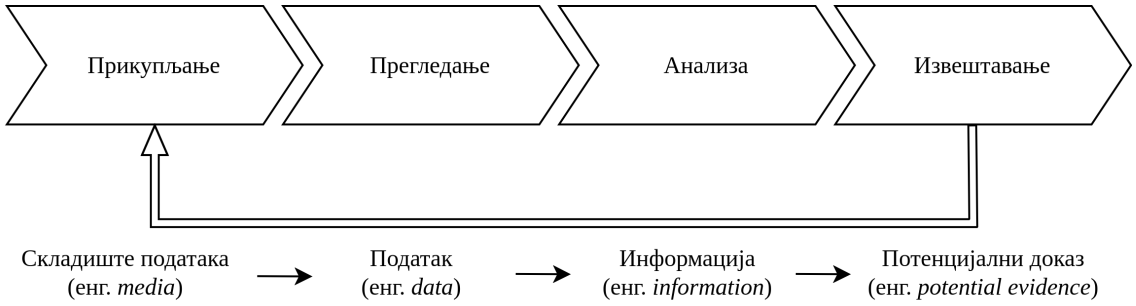
За почетак, ово поглавље даје увид у концепт истраживања представљајући формални модел форензичке истраге, који садржи главне делове међународно признатих стандарда, водича и процедура који прописују ваљано спровођење дигиталне форензичке истраге. Међу њима су стандарди Међународне организације за стандардизацију (ISO) ISO/IEC 27037 (ISO/IEC 27037, 2015), ISO/IEC 27041 (ISO/IEC 27041, 2016), ISO/IEC 27042 (ISO/IEC 27042, 2016), ISO/IEC 27043 (ISO/IEC 27043, 2016) и водичи Националног института за стандарде и технологију NIST (Kent и сар., 2006) и Међународне полицијске организације INTERPOL (Interpol, 2021).

Онтологија као имплементација дескриптивне логике у сврху формалног описивања форензичке истраге састоји се од четири модула, односно подонтологије: (1) онтологија форензике, (2) онтологија рачунарских мрежа, (3) онтологија система и (4) онтологија инстанци. Ове подонтологије сабирају се у свеобухватну онтологију форензике рачунарских мрежа. У наставку је свака од њих представљена својим најважнијим деловима.

4.2 Онтологија форензике

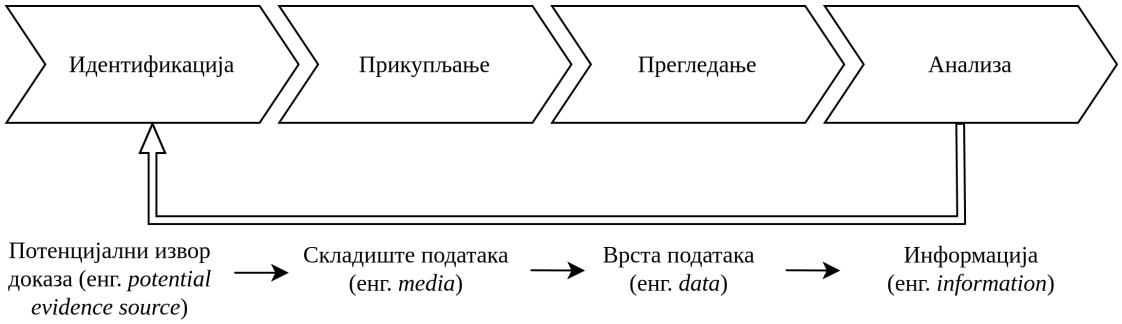
Модел форензичке истраге инспирисан је НИСТ-овим моделом форензичке истраге, који се састоји од четири фазе: прикупљања доказа, прегледања доказа, анализе доказа и извештавања о доказима (слика 3). За сваку фазу истраге везана је одређена форма трага над којом се у тренутној фази

спроводи истрага. Према НИСТ-у, у фази прикупљања, то је складиште података, у фази прегледања – податак, у фази анализе – информација, а у фази извештавања – потенцијални доказ.



Слика 3: НИСТ-ов модел форензичке истраге.

За усклађивање формалних описа поменутих стандарда и процедура у овом истраживању, погодна је измена НИСТ-овог модела, која се састоји у искључењу фазе извештавања, с обзиром на то да ова фаза садржи опсежну документацију свих активности у претходним фазама истраге и рукује конкретним информацијама о случају. Уместо тога, моделу на почетак истражног процеса додата је фаза идентификације доказа. На слици 4 приказан је модификовани модел форензичке истраге, који се састоји од фаза идентификације, прикупљања, прегледања и анализе доказа. Форме трагова над којима се у свакој фази спроводи истрага (у даљњем тексту, оперативне форме) сада су потенцијални извор доказа, складиште података, врста података и информација, респективно.



Слика 4: Модел форензичке истраге.

Развој онтологије форензике прати принцип да свака фаза форензичког процеса рукује одговарајућом оперативном формом података и да се дата оперативна форма података може извести из претходне оперативне форме, односно оперативне форме којом се рукује у претходној фази истраге. Такође, у свакој фази форензичке истраге постоје захтеви који се морају задовољити да би се истрага окарактерисала ваљаном. Ове активности називамо захтевима ваљаности. Сви захтеви ваљаности се, према ISO стандарду (ISO-/IEC 27037, 2015), могу груписати у захтеве поновљивости (енг. *repeatability*),

захтеве репродукције (енг. *reproducibility*), захтеве аудитабилности (енг. *auditability*), захтеве оправданости (енг. *justifiability*), захтеве довољности (енг. *sufficiency*) и захтеве поузданости (енг. *reliability*).

Тумачење ових захтева у даљњем тексту дато је са допуном или кларификацијом у односу на формулацију из стандарда. Дакле, захтев поновљивости подразумева да је исти или други форензичар у могућности да понови читаву истрагу на основу документације која је начињена током претходне истраге. Захтев репродукције се односи на могућност истог или другог форензичара да понављањем првобитно спроведених истражних активности, добије идентичне резултате. Захтев аудитабилности подразумева да је други форензичар у могућности да на основу документације о спроведеној истрази ревидира, односно евалуира читав поступак.

За овако формулисане захтеве дата су додатна појашњења у наставку. Наиме, захтев поновљивости не обухвата резултате форензичке истраге, већ само понављање целокупног поступка држећи се верно описа активности и употребљених метода, техника и алата. Захтев репродукције рестриктивнији је у односу на захтев поновљивости, јер укључивањем захтева поновљивости подразумева и долазак до истих резултата и закључака истраге. За разлику од ових захтева, задовољење захтева аудитабилности налаже постојање другог форензичара, који је у могућности да употребом истих или других метода, техника и алата дође до истих резултата и закључака у истрази над истим предметом.

Даље, захтев оправданости подразумева обавезу истражитеља да образложи и оправда предузете активности током истраге. Захтевом довољности налаже се форензичару да размотри да ли поседује довољан материјал да би се истрага адекватно спровела. Коначно, захтев поузданости налаже форензичару да објасни и демонстрира поузданост свих метода које су током истраге примењене.

У наставку су наведене класе које чине концептуални део онтологије форензике (*TBox*). За свако име концепта у онтологији везан је коментар, који се у оквиру графичког интерфејса система базираног на онтологији приказује кориснику.

Класа 1. Потенцијални извор доказа

Име	`PotentialEvidenceSource`
Дефиниција	`PotentialEvidenceSource` $\sqsubseteq \top$ $\forall$ *comment*.''`Potencijalni izvor dokaza`'' $\sqsubseteq$ `PotentialEvidenceSource` `PotentialEvidenceSource` $\equiv \exists$ `potentialEvidenceSourceProcessedBy.Identification` $\wedge \exists$ `hasMedia.Media`
Опис	Потенцијални извор доказа

Класа 2. Складиште података

Име	Media
Дефиниција	Media $\sqsubseteq \top$ $\forall$ *comment*.”Skladište podataka’’ $\sqsubseteq$ Media Media $\equiv \exists$ mediaProcessedBy.Collection $\wedge \exists$ hasData.Data
Опис	Складиште података

Класа 3. Врста података

Име	Data
Дефиниција	Data $\sqsubseteq \top$ $\forall$ *comment*.”Vrsta podataka’’ $\sqsubseteq$ Data Data $\equiv \exists$ dataProcessedBy.Examination $\wedge \exists$ hasInformation.Information
Опис	Врста података

Класа 4. Системски подаци

Име	SystemData
Дефиниција	SystemData $\sqsubseteq$ Data $\forall$ *comment*.”Sistemski podaci’’ $\sqsubseteq$ SystemData
Опис	Системски подаци

Класа 5. Кориснички подаци

Име	UserData
Дефиниција	UserData $\sqsubseteq$ Data $\forall$ *comment*.”Korisnički podaci’’ $\sqsubseteq$ UserData
Опис	Кориснички подаци

Класа 6. Конфигурација системских сервиса

Име	SystemConfigurationData
Дефиниција	SystemConfigurationData $\sqsubseteq$ SystemData $\forall$ *comment*.”Konfiguracija sistemskih servisa’’ $\sqsubseteq$ SystemConfigurationData
Опис	Конфигурација системских сервиса

Класа 7. Конфигурација корисничких сервиса

Име	`UserConfigurationData`
Дефиниција	`UserConfigurationData` $\sqsubseteq$ `UserData` $\forall$ *comment*.”`Konfiguracija korisničkih servisa’’` $\sqsubseteq$ `UserConfigurationData`
Опис	Конфигурација корисничких сервиса

Класа 8. Информација

Име	`Information`
Дефиниција	`Information` $\sqsubseteq \top$ $\forall$ *comment*.”`Informacija’’` $\sqsubseteq$ `Information`
Опис	Информација

Класа 9. Фаза истраге

Име	`InvestigationPhase`
Дефиниција	`InvestigationPhase` $\sqsubseteq \top$ $\forall$ *comment*.”`Faza istrage’’` $\sqsubseteq$ `InvestigationPhase` `InvestigationPhase` $\equiv \exists$ `satisfies.SoundnessRequirement`
Опис	Фаза истраге

Класа 10. Идентификација доказа

Име	`Identification`
Дефиниција	`Identification` $\sqsubseteq$ `InvestigationPhase` $\forall$ *comment*.”`Identifikacija dokaza’’` $\sqsubseteq$ `Identification`
Опис	Идентификација доказа

Класа 11. Идентификација начина повезивања

Име	`AccessIdentification`
Дефиниција	`AccessIdentification` $\sqsubseteq$ `Identification` $\forall$ *comment*.”`Identifikacija načina povezivanja’’` $\sqsubseteq$ `AccessIdentification`
Опис	Идентификација начина повезивања

Класа 12. Физичко повезивање са уређајем

Име	PhysicalAccessIdentification
Дефиниција	PhysicalAccessIdentification $\sqsubseteq$ AccessIdentification $\forall$ *comment*."Fizičko povezivanje sa uređajem'' $\sqsubseteq$ PhysicalAccessIdentification
Опис	Физичко повезивање са уређајем

Класа 13. Даљинско повезивање са уређајем

Име	RemoteAccessIdentification
Дефиниција	RemoteAccessIdentification $\sqsubseteq$ AccessIdentification $\forall$ *comment*."Daljinsko povezivanje sa uređajem'' $\sqsubseteq$ RemoteAccessIdentification
Опис	Даљинско повезивање са уређајем

Класа 14. Одређивање произвођача уређаја

Име	BrandIdentification
Дефиниција	BrandIdentification $\sqsubseteq$ Identification $\forall$ *comment*."Određivanje proizvođača uređaja'' $\sqsubseteq$ BrandIdentification
Опис	Одређивање произвођача уређаја

Класа 15. Идентификација релевантних карактеристика уређаја

Име	CharacteristicsIdentification
Дефиниција	CharacteristicsIdentification $\sqsubseteq$ Identification $\forall$ *comment*."Identifikacija relevantnih karakteristika uređaja'' $\sqsubseteq$ CharacteristicsIdentification
Опис	Идентификација релевантних карактеристика уређаја

Класа 16. Идентификација комуникационих интерфејса

Име	CommunicationInterfaceIdentification
Дефиниција	CommunicationInterfaceIdentification $\sqsubseteq$ Identification $\forall$ *comment*."Identifikacija komunikacionih interfejsa'' $\sqsubseteq$ CommunicationInterfaceIdentification
Опис	Идентификација комуникационих интерфејса

Класа 17. Идентификација активних сервиса

Име	`ConfiguredServiceIdentification`
Дефиниција	`ConfiguredServiceIdentification` $\sqsubseteq$ `Identification` $\forall$ *comment*.”`Identifikacija aktivnih servisa`’’ $\sqsubseteq$ `ConfiguredServiceIdentification`
Опис	Идентификација активних сервиса

Класа 18. Провера постојања иницијалних оштећења

Име	`DamageExistanceIdentification`
Дефиниција	`DamageExistanceIdentification` $\sqsubseteq$ `Identification` $\forall$ *comment*.”`Provera postojanja inicijalnih oštećenja`’’ $\sqsubseteq$ `DamageExistanceIdentification`
Опис	Провера постојања иницијалних оштећења

Класа 19. Идентификација партиција на складишту података

Име	`DiskPartitionIdentification`
Дефиниција	`DiskPartitionIdentification` $\sqsubseteq$ `Identification` $\forall$ *comment*.”`Identifikacija particija na skladištu podataka`’’ $\sqsubseteq$ `DiskPartitionIdentification`
Опис	Идентификација партиција на складишту података

Класа 20. Идентификација додатне опреме

Име	`EquipmentIdentification`
Дефиниција	`EquipmentIdentification` $\sqsubseteq$ `Identification` $\forall$ *comment*.”`Identifikacija dodatne opreme`’’ $\sqsubseteq$ `EquipmentIdentification`
Опис	Идентификација додатне опреме

Класа 21. Одређивање модела уређаја

Име	`ModelIdentification`
Дефиниција	`ModelIdentification` $\sqsubseteq$ `Identification` $\forall$ *comment*.”`Određivanje modela uređaja`’’ $\sqsubseteq$ `ModelIdentification`
Опис	Одређивање модела уређаја

Класа 22. Идентификација оперативног система

Име	`OperatingSystemIdentification`
Дефиниција	`OperatingSystemIdentification` $\sqsubseteq$ `Identification` $\forall$ *comment*.”`Identifikacija operativnog sistema`’’ $\sqsubseteq$ `OperatingSystemIdentification`
Опис	Идентификација оперативног система

Класа 23. Идентификација портова

Име	`PortIdentification`
Дефиниција	`PortIdentification` $\sqsubseteq$ `Identification` $\forall$ *comment*.”`Identifikacija portova`’’ $\sqsubseteq$ `PortIdentification`
Опис	Идентификација портова

Класа 24. Идентификација серијског броја уређаја

Име	`SerialNumberIdentification`
Дефиниција	`SerialNumberIdentification` $\sqsubseteq$ `Identification` $\forall$ *comment*.”`Identifikacija serijskog broja uređaja`’’ $\sqsubseteq$ `SerialNumberIdentification`
Опис	Идентификација серијског броја уређаја

Класа 25. Идентификација топологије

Име	`TopologyIdentification`
Дефиниција	`TopologyIdentification` $\sqsubseteq$ `Identification` $\forall$ *comment*.”`Identifikacija topologije`’’ $\sqsubseteq$ `TopologyIdentification`
Опис	Идентификација топологије

Класа 26. Прикупљање доказа

Име	`Collection`
Дефиниција	`Collection` $\sqsubseteq$ `InvestigationPhase` $\forall$ *comment*.”`Prikupljanje dokaza`’’ $\sqsubseteq$ `Collection`
Опис	Прикупљање доказа

Класа 27. Прикупљање података о приступању

Име	`AccessLogCollection`
Дефиниција	`AccessLogCollection` $\sqsubseteq$ `Collection` $\forall$ *comment*.”`Prikupljanje podataka o pristupanju`’’ $\sqsubseteq$ `AccessLogCollection`
Опис	Прикупљање података о приступању

Класа 28. Прикупљање података са шифрованог складишта

Име	`EncryptedMediaCollection`
Дефиниција	`EncryptedMediaCollection` $\sqsubseteq$ `Collection` $\forall$ *comment*.”`Prikupljanje podataka sa šifrovanog skladišta`’’ $\sqsubseteq$ `EncryptedMediaCollection`
Опис	Прикупљање података са шифрованог складишта

Класа 29. Логичко прикупљање

Име	`LogicalCollection`
Дефиниција	`LogicalCollection` $\sqsubseteq$ `Collection` $\forall$ *comment*.”`Logičko prikupljanje (kopiranje podataka iz određenih delova skladišta - ne svih)`’’ $\sqsubseteq$ `LogicalCollection`
Опис	Логичко прикупљање (копирање података из одређених делова складишта – не свих)

Класа 30. Прикупљање података са складишта уређаја критичне инфраструктуре

Име	`MissionCriticalDeviceCollection`
Дефиниција	`MissionCriticalDeviceCollection` $\sqsubseteq$ `Collection` $\forall$ *comment*.”`Prikupljanje podataka sa skladišta uređaja kritične infrastrukture`’’ $\sqsubseteq$ `MissionCriticalDeviceCollection`
Опис	Прикупљање података са складишта уређаја критичне инфраструктуре

Класа 31. Прикупљање мрежног саобраћаја

Име	`NetworkTrafficCollection`
Дефиниција	`NetworkTrafficCollection` $\sqsubseteq$ `Collection` $\forall$ *comment*.”`Prikupljanje mrežnog saobraćaja`’’ $\sqsubseteq$ `NetworkTrafficCollection`
Опис	Прикупљање мрежног саобраћаја

Класа 32. Физичко прикупљање

Име	PhysicalCollection
Дефиниција	PhysicalCollection ⊑ Collection ∀ *comment*."Fizičko prikupljanje (bit po bit prikupljanje celokupnog sadržaja skladišta podataka)'' ⊑ PhysicalCollection
Опис	Физичко прикупљање (бит по бит прикупљање целокупног садржаја складишта података)

Класа 33. Прикупљање података са складишта искљученог уређаја

Име	PoweredOffDeviceCollection
Дефиниција	PoweredOffDeviceCollection ⊑ Collection ∀ *comment*."Prikupljanje podataka sa skladišta isključenog uređaja'' ⊑ PoweredOffDeviceCollection
Опис	Прикупљање података са складишта искљученог уређаја

Класа 34. Прикупљање података са складишта укљученог уређаја

Име	PoweredOnDeviceCollection
Дефиниција	PoweredOnDeviceCollection ⊑ Collection ∀ *comment*."Prikupljanje podataka sa skladišta uključenog uređaja'' ⊑ PoweredOnDeviceCollection
Опис	Прикупљање података са складишта укљученог уређаја

Класа 35. Прегледање доказа

Име	Examination
Дефиниција	Examination ⊑ InvestigationPhase ∀ *comment*."Pregledanje dokaza'' ⊑ Examination
Опис	Прегледање доказа

Класа 36. Прегледање мапирања приватних IP адреса и портова на јавну IP адресу и портове

Име	NATTranslationExamination
Дефиниција	NATTranslationExamination ⊑ Examination ∀ *comment*."Pregledanje mapiranja privatnih IP adresa i portova na javnu IP adresu i portove'' ⊑ NATTranslationExamination
Опис	Прегледање мапирања приватних IP адреса и портова на јавну IP адресу и портове

Класа 37. Преīледање снимка мрежноī саобраћаја

Име	NetworkTrafficExamination
Дефиниција	NetworkTrafficExamination $\sqsubseteq$ Examination $\forall$ *comment*."Pregledanje snimka mrežnog saobraćaja'' $\sqsubseteq$ NetworkTrafficExamination
Опис	Прегледање снимка мрежног саобраћаја

Класа 38. Анализа доказа

Име	Analysis
Дефиниција	Analysis $\sqsubseteq$ InvestigationPhase $\forall$ *comment*."Analiza dokaza'' $\sqsubseteq$ Analysis
Опис	Анализа доказа

Класа 39. Анализа лоīа ūриснūуūања

Име	AccessLogAnalysis
Дефиниција	AccessLogAnalysis $\sqsubseteq$ Analysis $\forall$ *comment*."Analiza loga pristupanja'' $\sqsubseteq$ AccessLogAnalysis
Опис	Анализа лога приступања

Класа 40. Анализа лоīа сервиса NAT

Име	NATLogAnalysis
Дефиниција	NATLogAnalysis $\sqsubseteq$ Analysis $\forall$ *comment*."Analiza loga servisa NAT'' $\sqsubseteq$ NATLogAnalysis
Опис	Анализа лога сервиса NAT

Класа 41. Анализа мрежноī саобраћаја

Име	NetworkTrafficAnalysis
Дефиниција	NetworkTrafficAnalysis $\sqsubseteq$ Analysis $\forall$ *comment*."Analiza mrežnog saobraćaja'' $\sqsubseteq$ NetworkTrafficAnalysis
Опис	Анализа мрежног саобраћаја

Класа 42. Анализа NAT лоīа

Име	NATAnalysis
Дефиниција	NATAnalysis $\sqsubseteq$ NetworkTrafficAnalysis $\forall$ *comment*."Analiza NAT loga'' $\sqsubseteq$ NATAnalysis
Опис	Анализа NAT лога

Класа 43. Анализа пакета у снимку мрежног саобраћаја

Име	PacketAnalysis
Дефиниција	PacketAnalysis $\sqsubseteq$ NetworkTrafficAnalysis $\forall$ *comment*."Analiza paketa u snimku mrežnog saobraćaja'' $\sqsubseteq$ PacketAnalysis
Опис	Анализа пакета у снимку мрежног саобраћаја

Класа 44. Захтевваљаности

Име	SoundnessRequirement
Дефиниција	SoundnessRequirement $\sqsubseteq \top$ $\forall$ *comment*."Zahtev valjanosti'' $\sqsubseteq$ SoundnessRequirement
Опис	Захтев ваљаности

Класа 45. Аудитабилност

Име	Auditability
Дефиниција	Auditability $\sqsubseteq$ SoundnessRequirement $\forall$ *comment*."Auditabilnost (mogućnost revizije)'' $\sqsubseteq$ Auditability
Опис	Аудитабилност (могућност ревизије)

Класа 46. Завођење ланца доказа

Име	DocumentChainOfCustody
Дефиниција	DocumentChainOfCustody $\sqsubseteq$ Auditability $\forall$ *comment*."Zavedi lanac dokaza tako što ćeš prilikom pristupa potencijalnom izvoru dokaza navesti: (1) interni identifikator potencijalnog izvora dokaza, (2) ko je pristupio potencijalnom izvoru dokaza, (3) kada je pristupljeno potencijalnom izvoru dokaza, (4) gde je pristupljeno potencijalnom izvoru dokaza, (5) ko je odgovorna osoba, (6) potpis odgovorne osobe.'' $\sqsubseteq$ DocumentChainOfCustody
Опис	Завођење ланца доказа уз инструкцију

Класа 47. Документовање карактеристике уређаја

Име	DocumentCharacteristics
Дефиниција	DocumentCharacteristics $\sqsubseteq$ Auditability $\forall$ *comment*."Dokumentuj datu karakteristiku uređaja'' $\sqsubseteq$ DocumentCharacteristics
Опис	Документовање дате карактеристике уређаја

Класа 48. Документовање постојања/непостојања иницијалних оштећења уређаја

Име	`DocumentDamageExistance`
Дефиниција	`DocumentDamageExistance` $\sqsubseteq$ `Auditability` $\forall$ *comment*.”`Dokumentuj postojanje/nepostojanje inicijalnih oštećenja uređaja`’’ $\sqsubseteq$ `DocumentDamageExistance`
Опис	Документовање постојања/непостојања иницијалних оштећења уређаја

Класа 49. Оправданост

Име	`Justifiability`
Дефиниција	`Justifiability` $\sqsubseteq$ `SoundnessRequirement` $\forall$ *comment*.”`Opravdanost`’’ $\sqsubseteq$ `Justifiability`
Опис	Оправданост

Класа 50. Оправдавање немогућности прављења форензичке копије

Име	`JustifyUnabilityToMakeForensicCopy`
Дефиниција	`JustifyUnabilityToMakeForensicCopy` $\sqsubseteq$ `Justifiability` $\forall$ *comment*.”`Opravdaj nemogućnost pravljenja forenzičke kopije`’’ $\sqsubseteq$ `JustifyUnabilityToMakeForensicCopy`
Опис	Оправданост

Класа 51. Поузданост

Име	`Reliability`
Дефиниција	`Reliability` $\sqsubseteq$ `SoundnessRequirement` $\forall$ *comment*.”`Pouzdanost`’’ $\sqsubseteq$ `Reliability`
Опис	Поузданост

Класа 52. Жично повезивање са уређајем

Име	`CollectByConnectingDirectlyRatherThanRemotely`
Дефиниција	`CollectByConnectingDirectlyRatherThanRemotely` $\sqsubseteq$ `Reliability` $\forall$ *comment*.”`Poveži se sa uređajem putem kabla, ne bežično`’’ $\sqsubseteq$ `CollectByConnectingDirectlyRatherThanRemotely`
Опис	Жично повезивање са уређајем

Класа 53. Повезивање путем одговарајућег интерфејса

Име	`ConnectToRightInterface`
Дефиниција	`ConnectToRightInterface` $\sqsubseteq$ `Reliability` $\forall$ *comment*.”`Poveži se putem odgovarajućeg interfejsa''` $\sqsubseteq$ `ConnectToRightInterface`
Опис	Повезивање путем одговарајућег интерфејса

Класа 54. Прављење форензичке копије

Име	`MakeForensicCopy`
Дефиниција	`MakeForensicCopy` $\sqsubseteq$ `Reliability` $\forall$ *comment*.”`Napravi forenzičku kopiju''` $\sqsubseteq$ `MakeForensicCopy`
Опис	Прављење форензичке копије

Класа 55. Прављење главне форензичке копије

Име	`MakeMasterForensicCopy`
Дефиниција	`MakeMasterForensicCopy` $\sqsubseteq$ `MakeForensicCopy` $\forall$ *comment*.”`Napravi glavnu forenzičku kopiju''` $\sqsubseteq$ `MakeMasterForensicCopy`
Опис	Прављење главне форензичке копије

Класа 56. Прављење радне форензичке копије

Име	`MakeWorkingForensicCopy`
Дефиниција	`MakeWorkingForensicCopy` $\sqsubseteq$ `MakeForensicCopy` $\forall$ *comment*.”`Napravi radnu forenzičku kopiju''` $\sqsubseteq$ `MakeWorkingForensicCopy`
Опис	Прављење радне форензичке копије

Класа 57. Обезбеђивање интегритета података

Име	`PreserveIntegrity`
Дефиниција	`PreserveIntegrity` $\sqsubseteq$ `Reliability` $\forall$ *comment*.”`Obezbedi integritet podataka''` $\sqsubseteq$ `PreserveIntegrity`
Опис	Обезбеђивање интегритета података

Класа 58. Онемогућавање измене података

Име	`PreventAlteration`
Дефиниција	`PreventAlteration` $\sqsubseteq$ `Reliability` $\forall$ *comment*.”`Onemogući izmenu podataka`’’ $\sqsubseteq$ `PreventAlteration`
Опис	Онемогућавање измене података

Класа 59. Употреба поузданог алата

Име	`UseReliableTool`
Дефиниција	`UseReliableTool` $\sqsubseteq$ `Reliability` $\forall$ *comment*.”`Upotreba pouzdanog alata`’’ $\sqsubseteq$ `UseReliableTool`
Опис	Употреба поузданог алата

Класа 60. Валидација извршених активности

Име	`ValidateActions`
Дефиниција	`ValidateActions` $\sqsubseteq$ `Reliability` $\forall$ *comment*.”`Validiraj izvršene aktivnosti`’’ $\sqsubseteq$ `ValidateActions`
Опис	Валидација извршених активности

Класа 61. Поновљивост

Име	`Repeatability`
Дефиниција	`Repeatability` $\sqsubseteq$ `SoundnessRequirement` $\forall$ *comment*.”`Ponovljivost`’’ $\sqsubseteq$ `Repeatability`
Опис	Поновљивост

Класа 62. Репродукција

Име	`Reproducibility`
Дефиниција	`Reproducibility` $\sqsubseteq$ `SoundnessRequirement` $\forall$ *comment*.”`Reprodukcija`’’ $\sqsubseteq$ `Reproducibility`
Опис	Репродукција

Класа 63. Чување прикупљеног материјала

Име	`PreserveCollectedMaterial`
Дефиниција	`PreserveCollectedMaterial` $\sqsubseteq$ `Reproducibility` $\forall$ *comment*.”`Sačuvaj prikupljeni materijal`’’ $\sqsubseteq$ `PreserveCollectedMaterial`
Опис	Чување прикупљеног материјала

Класа 64. Довољност

Име	Sufficiency
Дефиниција	Sufficiency $\sqsubseteq$ SoundnessRequirement $\forall$ *comment*.''Dovoljnost'' $\sqsubseteq$ Sufficiency
Опис	Довољност

Класа 65. Упоређивање садржаја оперативне и трајне меморије

Име	CheckDifferenceBetweenOperatingAndDiskMemoryContent
Дефиниција	CheckDifferenceBetweenOperatingAndDiskMemoryContent $\sqsubseteq$ Sufficiency $\forall$ *comment*.''Proveri da li se sadržaj operativne i trajne memorije razlikuju'' $\sqsubseteq$ CheckDifferenceBetweenOperatingAndDiskMemoryContent
Опис	Упоређивање садржаја оперативне и трајне меморије

Класа 66. Упоређивање конфигурационих поставки у оперативној и трајној меморији

Име	CheckConfigurationDifferenceStoredInRAMAndDiskMemory
Дефиниција	CheckConfigurationDifferenceStoredInRAMAndDiskMemory $\sqsubseteq$ CheckDifferenceBetweenOperatingAndDiskMemoryContent $\forall$ *comment*.''Proveri da li se konfiguracione postavke smeštene u operativnoj memoriji razlikuju u odnosu na one smeštene u trajnoj memoriji'' $\sqsubseteq$ CheckConfigurationDifferenceStoredInRAMAndDiskMemory
Опис	Упоређивање конфигурационих поставки у оперативној и трајној меморији

4.3 Онтологија рачунарских мрежа

У оквиру одељка који представља подонтологију форензике приказани су концепти најопштијих оперативних форми података. У овом одељку, подонтологијом рачунарских мрежа ови концепти су специјализовани до најконкретнијих концепата. Стога у наставку следе њихове спецификације.

Класа 1. Уређај

Име	PotentialEvidenceSourceDevice
Дефиниција	PotentialEvidenceSourceDevice $\sqsubseteq$ PotentialEvidenceSource $\forall$ *comment*.''Uređaj'' $\sqsubseteq$ PotentialEvidenceSourceDevice
Опис	Физички уређај

Класа 2. Софтвер

Име	PotentialEvidenceSourceSoftware
Дефиниција	PotentialEvidenceSourceSoftware $\sqsubseteq$ PotentialEvidenceSource $\forall$ *comment*."Softver'' $\sqsubseteq$ PotentialEvidenceSourceSoftware
Опис	Софтвер

Класа 3. DRAM меморија

Име	DRAM
Дефиниција	DRAM $\sqsubseteq$ Media $\forall$ *comment*."DRAM memorija'' $\sqsubseteq$ Media
Опис	DRAM меморија

Класа 4. Flash меморија

Име	FlashMemory
Дефиниција	FlashMemory $\sqsubseteq$ Media $\forall$ *comment*."Flash memorija'' $\sqsubseteq$ FlashMemory
Опис	Flash меморија

Класа 5. Hot-swappable хард диск

Име	HotSwappableHardDisk
Дефиниција	HotSwappableHardDisk $\sqsubseteq$ Media $\forall$ *comment*."Hot-swappable hard disk'' $\sqsubseteq$ HotSwappableHardDisk
Опис	Hot-swappable хард диск

Класа 6. Хард диск

Име	MagneticDisk
Дефиниција	MagneticDisk $\sqsubseteq$ Media $\forall$ *comment*."Hard disk'' $\sqsubseteq$ MagneticDisk
Опис	Хард диск

Класа 7. Меморијска картица

Име	MemoryCard
Дефиниција	MemoryCard $\sqsubseteq$ Media $\forall$ *comment*."Memorijska kartica'' $\sqsubseteq$ MemoryCard
Опис	Меморијска картица

Класа 8. Перзистентна RAM меморија

Име	NonvolatileRAM
Дефиниција	NonvolatileRAM $\sqsubseteq$ Media $\forall$ *comment*."Perzistentna RAM memorija'' $\sqsubseteq$ NonvolatileRAM
Опис	Перзистентна RAM меморија

Класа 9. CD

Име	OpticalDisc
Дефиниција	OpticalDisc $\sqsubseteq$ Media $\forall$ *comment*."CD'' $\sqsubseteq$ OpticalDisc
Опис	CD

Класа 10. RAM меморија

Име	RAM
Дефиниција	RAM $\sqsubseteq$ Media $\forall$ *comment*."RAM memorija'' $\sqsubseteq$ RAM
Опис	RAM меморија

Класа 11. ROM меморија

Име	ROM
Дефиниција	ROM $\sqsubseteq$ Media $\forall$ *comment*."ROM memorija'' $\sqsubseteq$ ROM
Опис	ROM меморија

Класа 12. Thumb драјв

Име	ThumbDrive
Дефиниција	ThumbDrive $\sqsubseteq$ Media $\forall$ *comment*."Thumb drajv'' $\sqsubseteq$ ThumbDrive
Опис	Thumb драјв

Класа 13. Приступна тачка

Име	`AccessPointDevice`
Дефиниција	`AccessPointDevice` ⊑ `PotentialEvidenceSourceDevice` ∀ *comment*.”`Pristupna tačka`” ⊑ `AccessPointDevice`
Опис	Приступна тачка као физички уређај

Класа 14. Фајервол

Име	`FirewallDevice`
Дефиниција	`FirewallDevice` ⊑ `PotentialEvidenceSourceDevice` ∀ *comment*.”`Fajervol`” ⊑ `FirewallDevice`
Опис	Фајервол као физички уређај

Класа 15. Систем за детекцију упада

Име	`IDSDevice`
Дефиниција	`IDSDevice` ⊑ `PotentialEvidenceSourceDevice` ∀ *comment*.”`Sistem za detekciju upada`” ⊑ `IDSDevice`
Опис	Систем за детекцију упада као физички уређај

Класа 16. Мобилни уређај

Име	`MobileDevice`
Дефиниција	`MobileDevice` ⊑ `PotentialEvidenceSourceDevice` ∀ *comment*.”`Mobilni uređaj`” ⊑ `MobileDevice`
Опис	Мобилни уређај

Класа 17. Уређај за прислушкивање мрежног саобраћаја

Име	`PacketSnifferDevice`
Дефиниција	`PacketSnifferDevice` ⊑ `PotentialEvidenceSourceDevice` ∀ *comment*.”`Uređaj za prisluškivanje mrežnog saobraća-ja`” ⊑ `PacketSnifferDevice`
Опис	Уређај за прислушкивање мрежног саобраћаја

Класа 18. Прокси

Име	`ProxyDevice`
Дефиниција	`ProxyDevice` ⊑ `PotentialEvidenceSourceDevice` ∀ *comment*.”`Proksi`” ⊑ `ProxyDevice`
Опис	Прокси као уређај

Класа 19. Рутер

Име	`RouterDevice`
Дефиниција	`RouterDevice` $\sqsubseteq$ `PotentialEvidenceSourceDevice` $\forall$ *comment*.`''Ruter''` $\sqsubseteq$ `RouterDevice`
Опис	Рутер као уређај

Класа 20. Систем за управљање безбедносним догађајима

Име	`SEMDevice`
Дефиниција	`SEMDevice` $\sqsubseteq$ `PotentialEvidenceSourceDevice` $\forall$ *comment*.`''Sistem za upravljanje bezbednosnim događa-jima''` $\sqsubseteq$ `SEMDevice`
Опис	Систем за управљање безбедносним догађајима као уређај

Класа 21. Сервер

Име	`ServerDevice`
Дефиниција	`ServerDevice` $\sqsubseteq$ `PotentialEvidenceSourceDevice` $\forall$ *comment*.`''Server''` $\sqsubseteq$ `ServerDevice`
Опис	Сервер као уређај

Класа 22. Свич

Име	`SwitchDevice`
Дефиниција	`SwitchDevice` $\sqsubseteq$ `PotentialEvidenceSourceDevice` $\forall$ *comment*.`''Svič''` $\sqsubseteq$ `SwitchDevice`
Опис	Свич као уређај

Класа 23. Приступна тачка

Име	`AccessPointSoftware`
Дефиниција	`AccessPointSoftware` $\sqsubseteq$ `PotentialEvidenceSourceSoftware` $\forall$ *comment*.`''Pristupna tačka''` $\sqsubseteq$ `AccessPointSoftware`
Опис	Приступна тачка као софтвер

Класа 24. Фајервол

Име	`FirewallSoftware`
Дефиниција	`FirewallSoftware` $\sqsubseteq$ `PotentialEvidenceSourceSoftware` $\forall$ *comment*.`''Fajervol''` $\sqsubseteq$ `FirewallSoftware`
Опис	Фајервол као софтвер

Класа 25. Систем за детекцију упада

Име	IDSSoftware
Дефиниција	IDSSoftware $\sqsubseteq$ PotentialEvidenceSourceSoftware $\forall$ *comment*.''Sistem za detekciju upada'' $\sqsubseteq$ IDSSoftware
Опис	Систем за детекцију упада као софтвер

Класа 26. Софтверски алат за прислушкивање мрежног саобраћаја

Име	PacketSnifferSoftware
Дефиниција	PacketSnifferSoftware $\sqsubseteq$ PotentialEvidenceSourceSoftware $\forall$ *comment*.''Softverski alat za prisluškivanje mrežnog saobraćaja'' $\sqsubseteq$ PacketSnifferSoftware
Опис	Софтверски алат за прислушкивање мрежног саобраћаја

Класа 27. Прокси

Име	ProxySoftware
Дефиниција	ProxySoftware $\sqsubseteq$ PotentialEvidenceSourceSoftware $\forall$ *comment*.''Proksi'' $\sqsubseteq$ ProxySoftware
Опис	Прокси као софтвер

Класа 28. Рутер

Име	RouterSoftware
Дефиниција	RouterSoftware $\sqsubseteq$ PotentialEvidenceSourceSoftware $\forall$ *comment*.''Ruter'' $\sqsubseteq$ RouterSoftware
Опис	Рутер као софтвер

Класа 29. Систем за управљање безбедносним догађајима

Име	SEMSoftware
Дефиниција	SEMSoftware $\sqsubseteq$ PotentialEvidenceSourceSoftware $\forall$ *comment*.''Sistem za upravljanje bezbednosnim događajima'' $\sqsubseteq$ SEMSoftware
Опис	Систем за управљање безбедносним догађајима као софтвер

Класа 30. Сервер

Име	ServerSoftware
Дефиниција	ServerSoftware $\sqsubseteq$ PotentialEvidenceSourceSoftware $\forall$ *comment*.''Server'' $\sqsubseteq$ ServerSoftware
Опис	Сервер као софтвер

Класа 31. Веб-сервер

Име	`WebServerSoftware`
Дефиниција	`WebServerSoftware` $\sqsubseteq$ `ServerSoftware` $\forall$ *comment*.''`Veb-server`'' $\sqsubseteq$ `WebServerSoftware`
Опис	Веб-сервер као софтвер

Класа 32. Свич

Име	`SwitchSoftware`
Дефиниција	`SwitchSoftware` $\sqsubseteq$ `PotentialEvidenceSourceSoftware` $\forall$ *comment*.''`Svič`'' $\sqsubseteq$ `SwitchSoftware`
Опис	Свич као софтвер

Класа 33. Конфигурација мреже

Име	`NetworkConfigurationData`
Дефиниција	`NetworkConfigurationData` $\sqsubseteq$ `SystemConfigurationData` $\forall$ *comment*.''`Konfiguracija mreže`'' $\sqsubseteq$ `NetworkConfiguration-Data`
Опис	Конфигурација мреже

Класа 34. IP конфигурација

Име	`IPConfigurationData`
Дефиниција	`IPConfigurationData` $\sqsubseteq$ `NetworkConfigurationData` $\forall$ *comment*.''`IP konfiguracija`'' $\sqsubseteq$ `IPConfigurationData`
Опис	IP конфигурација

Класа 35. Целокупан траг мрежног саобраћаја

Име	`FullPacketCaptureData`
Дефиниција	`FullPacketCaptureData` $\sqsubseteq$ `UserData` $\forall$ *comment*.''`Celokupan trag mrežnog saobraćaja`'' $\sqsubseteq$ `Full-PacketCaptureData`
Опис	Целокупан траг мрежног саобраћаја

Класа 36. Метаподаци мрежних конекција

Име	`NetFlowData`
Дефиниција	`NetFlowData` $\sqsubseteq$ `UserData` $\forall$ *comment*.''`Metapodaci mrežnih konekcija`'' $\sqsubseteq$ `NetFlowData`
Опис	Метаподаци мрежних конекција

Класа 37. Лог корисничке активности у рачунарској мрежи

Име	UserNetworkActivityLogData
Дефиниција	UserNetworkActivityLogData $\sqsubseteq$ UserData $\forall$ *comment*."Log korisničke aktivnosti u računarskoj mreži'' $\sqsubseteq$ UserNetworkActivityLogData
Опис	Лог корисничке активности у рачунарској мрежи

Класа 38. Информација мрежног пакета

Име	PacketInformation
Дефиниција	PacketInformation $\sqsubseteq$ Information $\forall$ *comment*."Informacija mrežnog paketa'' $\sqsubseteq$ PacketInformation
Опис	Информација мрежног пакета

4.4 Онтологија система

Употреба система базираног на формалној репрезентацији знања у области форензике рачунарских мрежа изискује постојање концепта случаја и концепта корисника како би се за њих могле везати оперативне форме података релевантне за конкретан истражни случај одређеног корисника, односно форензичара.

Класа 1. Случај

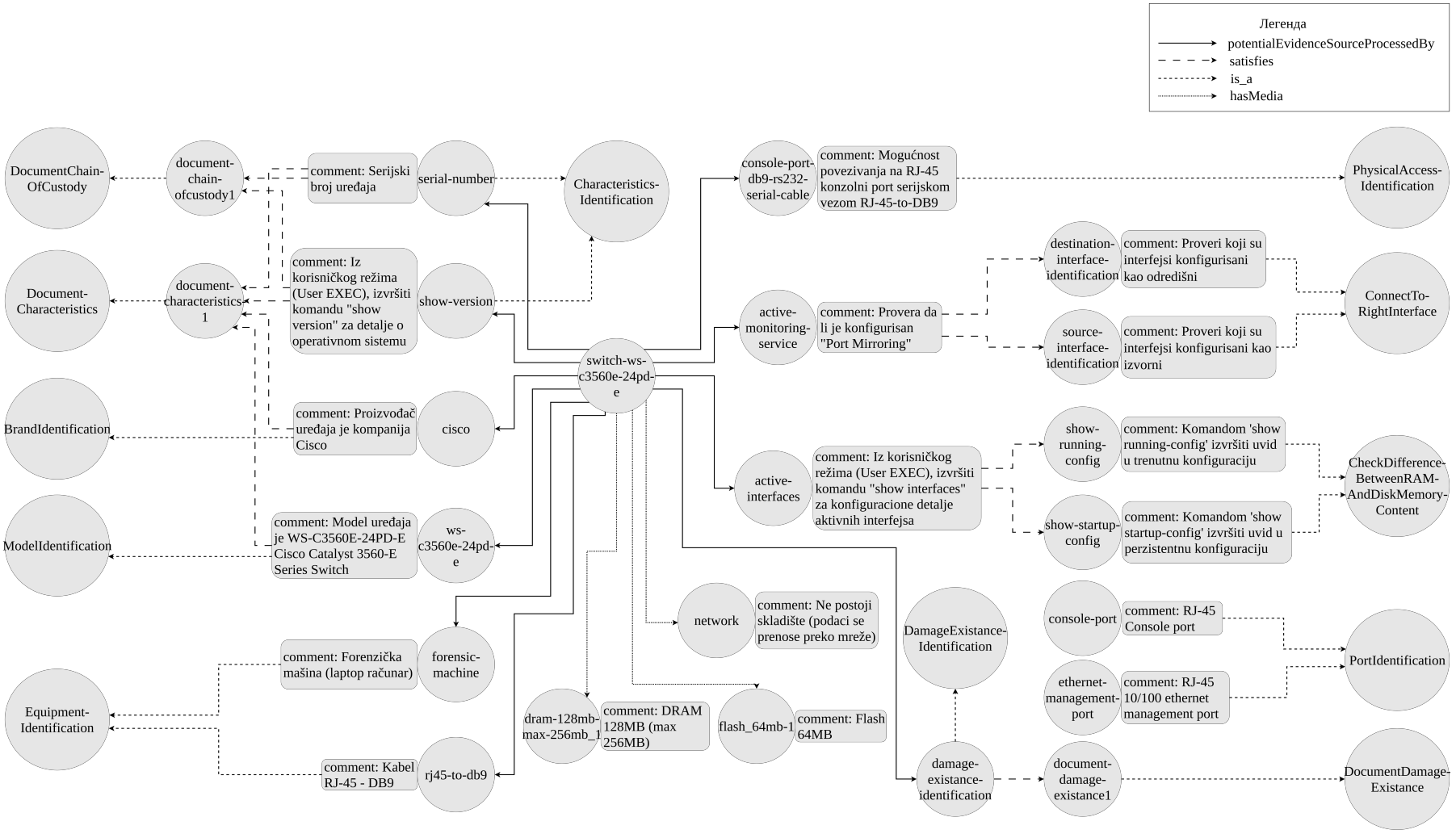
Име	Case
Дефиниција	Case $\sqsubseteq \top$ $\forall$ *comment*."Slučaj'' $\sqsubseteq$ Case Case $\equiv \exists$ caseHasMedia.Media $\wedge \exists$ caseHasData.Data $\wedge \exists$ caseHasInformation.Information
Опис	Случај

Класа 2. Корисник

Име	User
Дефиниција	User $\sqsubseteq \top$ $\forall$ *comment*."Korisnik'' $\sqsubseteq$ User Case $\equiv \exists$ userHasCase.Case
Опис	Корисник

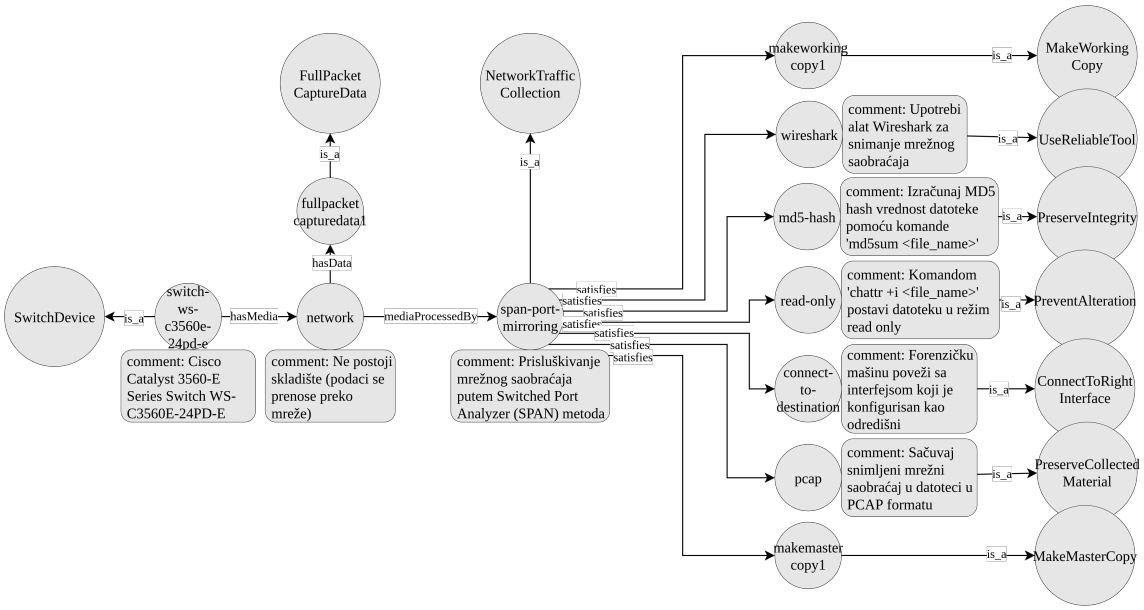
4.5 Онтологија инстанци

У овом одељку графом су приказани одабрани делови подонтологије инстанци. На слици 5 приказана је инстанца свича као потенцијалног извора доказа, који је у вези са инстанцама потконцепата концепта идентификације као фазе истраге као и са инстанцама концепта складишта података. Даље су дате везе између инстанци потконцепата концепта идентификације и инстанци потконцепата концепта захтева ваљаности.



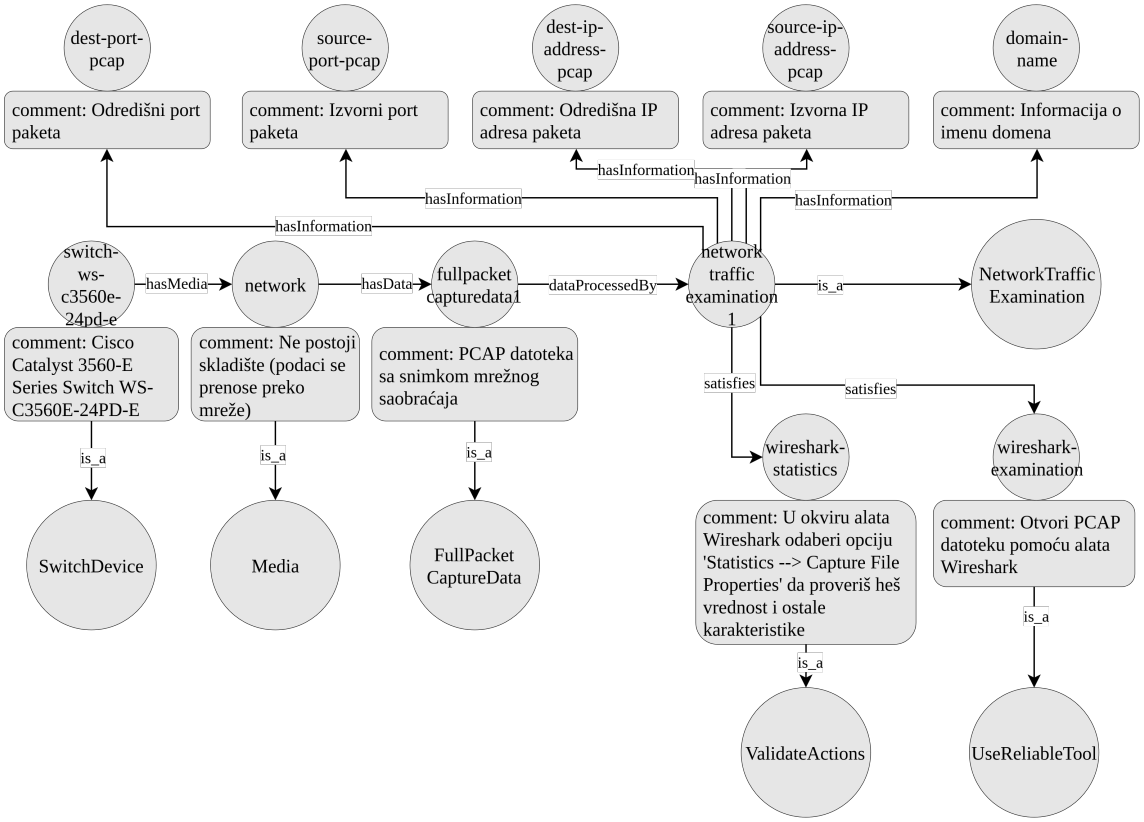
Слика 5: Део онтологије инстанци који укључује концепте потенцијалног извора доказа, фазе идентификације у истрази и захтева ваљаности истраге у поменутој фази.

На слици 6 приказана је одабрана инстанца концепта складишта података која је у вези са инстанцом свича са претходне слике. Ова инстанца концепта складишта података у вези је са инстанцама потконцепата концепта прикупљања као фазе истраге као и са инстанцама концепта врсте података. Затим су дате везе између инстанци потконцепата концепта прикупљања и инстанци потконцепата концепта захтева ваљаности.



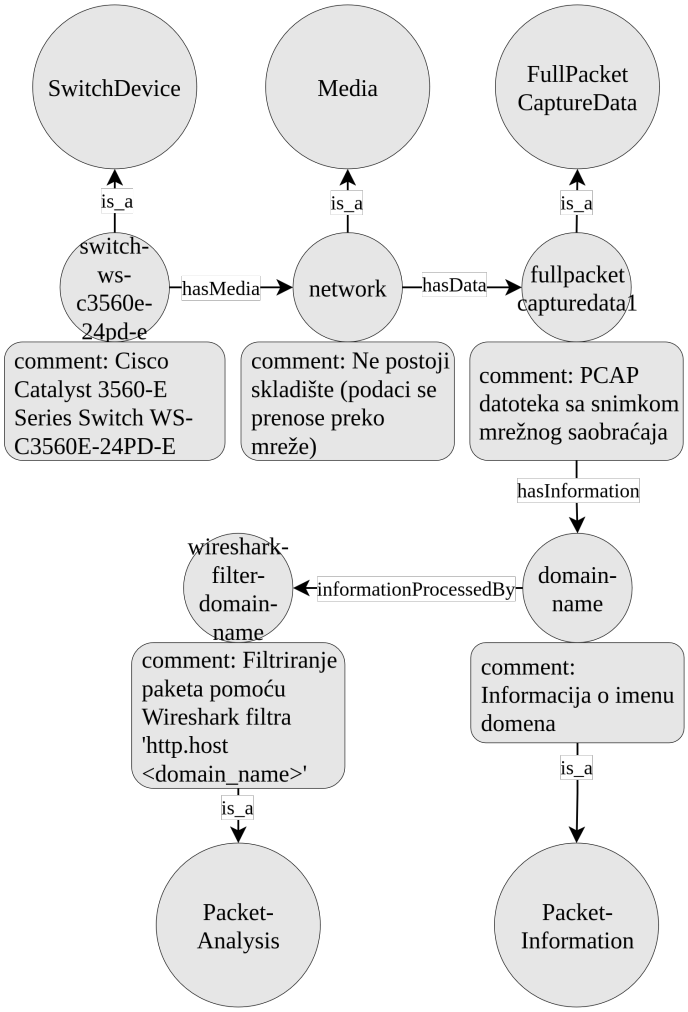
Слика 6: Део онтологије инстанци који укључује концепте складишта података, фазе прикупљања у истрази и захтева ваљаности истраге у поменутој фази.

На слици 7 приказана је одабрана инстанца концепта врсте података која је у вези са инстанцом складишта података са претходне слике. Ова инстанца концепта врсте података у вези је са инстанцама потконцепата концепта прегледања као фазе истраге као и са инстанцама концепта информације. Поред тога, приказане су везе између инстанци потконцепата концепта прегледања и инстанци потконцепата концепта захтева ваљаности.



Слика 7: Део онтологије инстанци који укључује концепте врста података, фазе прегледања у истрази и захтева ваљаности истраге у поменутој фази.

На крају, на слици 8 приказана је одабрана инстанца концепта информације која је у вези са инстанцом врсте података са претходне слике. Ова инстанца концепта информације у вези је са инстанцама потконцепата концепта анализе као фазе истраге.



Слика 8: Део онтологије инстанци који укључује концепте информације и фазе анализе у истрази.

4.6 Могућност проширења онтологије

На крају поглавља о предложеном формалном моделу форензичке истраге дато је бројно стање концепата, веза и инстанци у представљеној онтологији, као и упутство за њено проширивање.

Дакле, укупан број концепата износи 108, укупан број веза износи 23, а укупан број инстанци износи 123.

Треба напоменути да је онтологију могуће проширивати у два правца. Један представља допуну постојећих модула, којима се надограђује онтологија форензике рачунарских мрежа, а други подразумева увођење нових модула који представљају друге подобласти дигиталне форензике.

Да би се надоградила постојећа онтологија, експерт-форензичар треба да испрати одређена правила у зависности од припадности инстанце, односно потклассе класи. Уколико експерт жели да прошири онтологију новом класом, мора да је придружи одговарајућој наткласи, а уколико се онтологија проширује новом инстанцом, потребно ју је, не само придружити одговарајућој

класи, већ ју је потребно на прави начин повезати са другим инстанцама. Правила за повезивање инстанци дата су у наставку.

Уколико нова инстанца припада класи потенцијалног извора доказа, она се одговарајућом везом мора повезати са инстанцама класе фазе идентификације и са инстанцама класе складишта података. Уколико нова инстанца припада класи складишта података, она се одговарајућом везом мора повезати са инстанцама класе фазе прикупљања и са инстанцама класе врсте података. Уколико нова инстанца припада класи врсте података, она се одговарајућом везом мора повезати са инстанцама класе фазе прегледања и са инстанцама класе информације. Уколико нова инстанца припада класи информације, она се одговарајућом везом мора повезати са инстанцама класе фазе анализе. Уколико нова инстанца припада некој од класа фаза истраге, она се може, а не мора повезати са инстанцом/инстанцама класе захтева ваљаности. У сваком случају, експерт је у обавези да свакој новој класи или инстанци додели коментар, који служи локализацији система.

4.7 Сажетак

У овом поглављу представљен је концептуални модел система за вођење кроз ваљану форензичку истрагу, кога чине четири онтолошка модула. Модули су представљени конструктима дескриптивне логике тако што је за сваки концепт дата његова дефиниција. Модул онтологије форензике предочава концепте фаза истраге, најопштијих оперативних форми података којима се рукује у фазама истраге и концепата захтева ваљаног спровођења истраге. Модул онтологије рачунарских мрежа садржи концепте конкретнијих оперативних форми података којима се рукује у фазама форензичке истраге. Модул онтологије система чине концепти неопходни за функционисање система, док модул онтологије инстанци садржи инстанце, односно конкретизације концепата из свих претходних модула. На крају овога одељка предочена су упутства за потенцијално проширење целокупне онтологије.

5 Имплементација истраживања

- Логика као пропедевтика и чини, такорећи, само предсобље наука и кад је реч о сазнањима, онда се, додуше, ради њиховог оцењивања логика претпоставља, али њихово се проширивање мора тражити у наукама у правом и објективном смислу те речи.

Имануел Кант

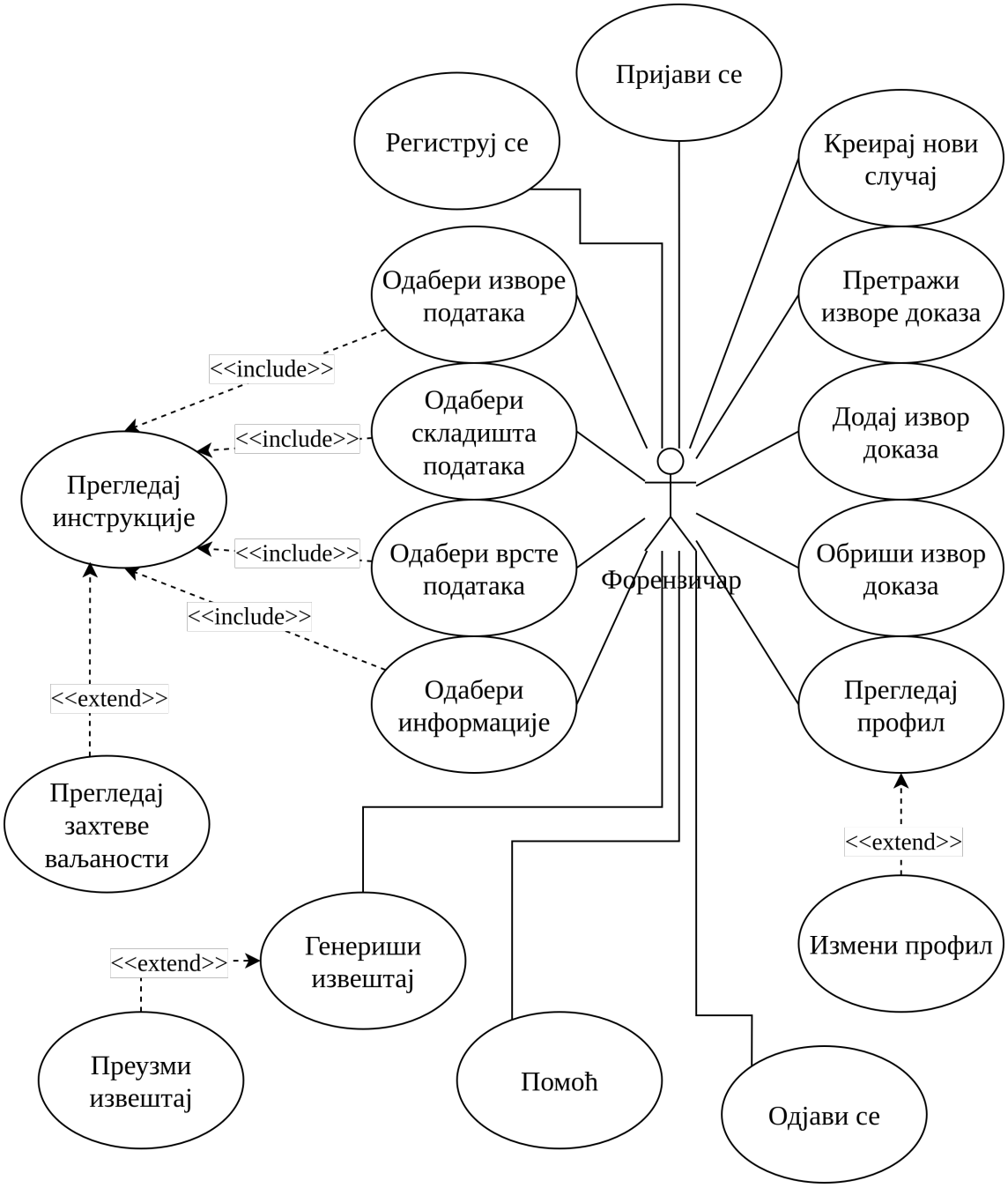
5.1 Преглед

Закорачивши претходним поглављима у, како Кант каже, предсобље унапређења дигиталне форензике, ово поглавље даје основ за проверу доприноса истраживања описаног овом дисертацијом. Основ за проверу идеје свакако је њена имплементација, у овом случају, у виду система који ће бити употребљив од стране форензичара, који ће тиме допринети валидацији идеје. Целокупан процес развоја поменутог система објављен је у раду Matijević Gostojić и сар. (2024a)

У првом делу овога поглавља дата је спецификација захтева система, а затим његов дизајн и пројекат, као и опис имплементације система. Други део овог поглавља чине студија случаја и демонстрација употребе система.

5.2 Спецификација захтева система

Функционалности система приказане су дијаграмом случајева коришћења на слици 9. Употреба апликације започиње регистровањем корисника у систем, односно пријавом у систем уколико је регистрација већ извршена. Следи креирање радног окружења у оквиру апликације у виду случаја. Информације о случају, које се притом наводе су назив случаја и главни актери случаја. Следећим кораком започиње се вођење форензичара кроз истрагу – систем ставља до знања да се ради о првој фази истраге – фази идентификације и форензичар одабира потенцијалне изворе доказа који се везују за његов случај. Уколико се потенцијални извор доказа грешком одабере, могуће је поништити одабир. Након тога, систем форензичару даје на увид активности које је пожељно спровести над одабраним потенцијалним изворима доказа током фазе идентификације доказа. Форензичар је тада у могућности да одабере активност за коју су везани захтеви ваљаности прописани стандардом како би добио увид у њих. На идентичном принципу одвија се интеракција форензичара и апликације за остале оперативне форме – складишта података, врсте података и информације, чије се инструкције и захтеви ваљаности дају на увид у оквиру прикупљања, прегледања и анализе доказа, респективно.



Слика 9: Дијаграм случајева коришћења.

Након увида у активности и захтеве ваљаности у оквиру анализе доказа, као последње оперативне фазе истраге, форензичар је у могућности да добије увид у генерисани извештај својих активности током рада са апликацијом.

Додатне функционалности апликације су преглед информација профила тренутно пријављеног форензичара, одјава из апликације и увид у документацију апликације.

У наставку је дата спецификација захтева система у виду случајева коришћења.

1. Картица случаја коришћења Регистрација корисника

Назив	Регистрација корисника
Предуслови	Корисник није регистрован у систем.
Кораци	1. Корисник отвара дијалог за регистрацију у систем. 2. Корисник уноси име. 3. Корисник уноси презиме. 4. Корисник уноси имејл адресу. 5. Врши се провера валидности унете имејл адресе. 6. Корисник уноси лозинку. 7. Врши се провера валидности унете лозинке. 8. Корисник потврђује лозинку. 9. Врши се провера истоветности потврде лозинке и првобитно унесене лозинке. 10. Корисник потврђује унете податке кликом на дугме за регистрацију.
Проширења	Нема.
Изузеци	Унесена имејл адреса или лозинка нису валидне.
Услови који важе након завршетка	Корисник је регистрован у систем.

2. Картица случаја коришћења Пријава корисника

Назив	Пријава корисника
Предуслови	1. Корисник је регистрован у систем. 2. Корисник није пријављен у систем.
Кораци	1. Корисник отвара дијалог за пријаву у систем. 2. Корисник уноси имејл адресу. 3. Корисник уноси лозинку. 4. Корисник потврђује унете податке кликом на дугме за пријаву.
Проширења	Нема.
Изузеци	Погрешно унесена имејл адреса или лозинка.
Услови који важе након завршетка	Корисник је пријављен у систем.

3. Картица случаја коришћења Увид у информације корисничког профила

Назив	Увид у информације корисничког профила
Предуслови	Корисник је пријављен у систем.
Кораци	1. Корисник отвара форму за приказ информација корисничког профила.
Проширења	Измена информација корисничког профила.
Изузеци	Нема.
Услови који важе након завршетка	Нема.

4. Картица случаја коришћења Измена информација корисничког профила

Назив	Измена информација корисничког профила
Предуслови	1. Корисник је пријављен у систем. 2. Корисник је отворио форму за приказ информација корисничког профила.
Кораци	1. Кликом на дугме за измену информација корисничког профила, форма за приказ информација корисничког профила дозвољава унос текста. 2. Ако је корисник изменио имејл адресу или лозинку, врши се провера валидности измене. 3. Кликом на дугме за потврду, измене ће бити сачуване.
Проширења	Нема.
Изузеци	Невалидно унесена имејл адреса или лозинка.
Услови који важе након завршетка	Измене су видљиве у форми за приказ информација корисничког профила.

5. Картица случаја коришћења Креирање новог случаја

Назив	Креирање новог случаја
Предуслови	Корисник је пријављен у систем.
Кораци	1. Кликом на дугме за креирање новог случаја, приказује се форма за унос података о случају. 2. Корисник уноси назив случаја.
Проширења	1. Случају се додељује идентификатор. 2. Случају се додељује тренутно пријављен корисник.
Изузеци	Нема.
Услови који важе након завршетка	Креиран је нови случај.

6. Картица случаја коришћења Претрага потенцијалних извора доказа

Назив	Претрага потенцијалних извора доказа
Предуслови	1. Корисник је пријављен у систем. 2. Креиран је случај.
Кораци	Уносом кључне речи за претрагу, врши се одабир потенцијалних извора доказа чији назив садржи унесену кључну реч.
Проширења	Нема.
Изузеци	Нема.
Услови који важе након завршетка	Кориснику се приказују подаци потенцијалних извора доказа одабраних на основу претраге.

7. Картица случаја коришћења Одабир потенцијалних извора доказа

Назив	Одабир потенцијалних извора доказа
Предуслови	1. Корисник је пријављен у систем. 2. Креиран је случај.
Кораци	1. Кликом на поље везано за одређени потенцијални извор доказа, корисник врши одабир потенцијалног извора доказа. 2. Кликом на дугме за потврду, корисник завршава одабир потенцијалних извора доказа.
Проширења	Нема.
Изузеци	Нема.
Услови који важе након завршетка	1. Одабрани потенцијални извори доказа придружени су креираном случају. 2. Кориснику су приказане карактеристике одабраних потенцијалних извора доказа.

8. Картица случаја коришћења Брисање одабраних потенцијалних извора доказа

Назив	Брисање одабраних потенцијалних извора доказа
Предуслови	1. Корисник је пријављен у систем. 2. Креиран је случај. 3. Постоје потенцијални извори доказа придружени случају.
Кораци	1. Кликом на поље везано за потенцијални извор доказа придружен случају, корисник врши одабир потенцијалног извора доказа. 2. Кликом на дугме за брисање, корисник поништава одабир потенцијалних извора доказа.
Проширења	Нема.
Изузеци	Нема.
Услови који важе након завршетка	Поништени потенцијални извори доказа нису придружени креираном случају.

9. Картица случаја коришћења Одабир складишта података

Назив	Одабир складишта података
Предуслови	1. Корисник је пријављен у систем. 2. Креиран је случај. 3. Корисник је одабрао потенцијалне изворе доказа. 4. Кориснику су приказане карактеристике одабраних потенцијалних извора доказа и складишта података која се у њима налазе.
Кораци	1. Кликом на поље везано за складиште података које се налази у неком од одабраних потенцијалних извора доказа, корисник врши одабир складишта података. 2. Кликом на дугме за потврду, корисник завршава одабир складишта података.
Проширења	Нема.
Изузеци	Нема.
Услови који важе након завршетка	1. Одабрана складишта података придружена су креираном случају. 2. Кориснику су приказане карактеристике одабраних складишта података.

10. Картица случаја коришћења Одабир врсте података

Назив	Одабир врсте података
Предуслови	1. Корисник је пријављен у систем. 2. Креиран је случај. 3. Корисник је одабрао потенцијалне изворе доказа. 4. Корисник је одабрао складишта података. 5. Кориснику су приказане карактеристике одабраних складишта података и врста података који се у њима налазе.
Кораци	1. Кликом на поље везано за врсту података који се налазе у неком од одабраних складишта података, корисник врши одабир врсте података. 2. Кликом на дугме за потврду, корисник завршава одабир врсте података.
Проширења	Нема.
Изузеци	Нема.
Услови који важе након завршетка	1. Одабране врсте података придружене су креираном случају. 2. Кориснику су приказане карактеристике одабраних врста података.

11. Картица случаја коришћења Одабир информација

Назив	Одабир информација
Предуслови	1. Корисник је пријављен у систем. 2. Креиран је случај. 3. Корисник је одабрао потенцијалне изворе доказа. 4. Корисник је одабрао складишта података. 5. Корисник је одабрао врсте података. 6. Кориснику су приказане карактеристике одабраних врста података и информације које се из њих могу добити.
Кораци	1. Кликом на поље везано за информацију која се може добити из неке од одабраних врста података, корисник врши одабир информације. 2. Кликом на дугме за потврду, корисник завршава одабир информација.
Проширења	Нема.
Изузеци	Нема.
Услови који важе након завршетка	1. Одабране информације придружене су креираном случају. 2. Кориснику су приказане одабране информације.

12. Картица случаја коришћења Приказивање инструкција

Назив	Приказивање инструкција
Предуслови	1. Корисник је пријављен у систем. 2. Креиран је случај. 3. Кориснику су приказане карактеристике одабраних потенцијалних извора доказа, складишта података, врста података или информација.
Кораци	1. Кликом на поље везано за потенцијални извор доказа, складиште података, врсту података или информацију, корисник врши одабир потенцијалног извора доказа, складишта података, врсте података или информације. 2. Након одабира потенцијалног извора доказа, складишта података, врсте података или информације, кориснику се приказује инструкција везана за одабир.
Проширења	1. Уколико је за инструкцију везан захтев ваљаности, кориснику се приказује лабела која указује на његово постојање. 2. Уколико су кориснику приказане карактеристике одабраних потенцијалних извора доказа, у линији напретка кориснику се указује на тренутну фазу истраге – фазу идентификације. 3. Уколико су кориснику приказане карактеристике одабраних складишта података, у линији напретка кориснику се указује на тренутну фазу истраге – фазу прикупљања. 4. Уколико су кориснику приказане карактеристике одабраних врста података, у линији напретка кориснику се указује на тренутну фазу истраге – фазу прегледања. 5. Уколико су кориснику приказане карактеристике одабраних информација, у линији напретка кориснику се указује на тренутну фазу истраге – фазу анализе.
Изузеци	Нема.
Услови који важе након завршетка	Нема.

13. Картица случаја коришћења Приказивање захтева ваљаности

Назив	Приказивање захтева ваљаности
Предуслови	1. Корисник је пријављен у систем. 2. Креиран је случај. 3. Кориснику су приказане карактеристике одабраних потенцијалних извора доказа, складишта података, врста података или информација. 4. Кориснику су приказане инструкције за одређени потенцијални извор доказа, складиште података, врсту података или информацију.
Кораци	1. Кликом на поље везано за инструкцију, корисник врши одабир инструкције. 2. Након одабира инструкције, кориснику се приказује захтев ваљаности везан за одабрану инструкцију.
Проширења	Нема.
Изузеци	За одабрану инструкцију не постоји захтев ваљаности.
Услови који важе након завршетка	Нема.

14. Картица случаја коришћења Генерисање извештаја

Назив	Генерисање извештаја
Предуслови	1. Корисник је пријављен у систем. 2. Креиран је случај.
Кораци	1. Кликом на дугме за генерисање извештаја, креира се документ у коме су забележене све корисничке активности након креирања случаја.
Проширења	Након креирања извештаја, могуће га је преузети.
Изузеци	Нема.
Услови који важе након завршетка	Нема.

15. Картица случаја коришћења Преузимање извештаја

Назив	Преузимање извештаја
Предуслови	Постоји генерисан извештај.
Кораци	1. Кликом на дугме за преузимање извештаја, врши се преузимање извештаја у формату PDF.
Проширења	Нема.
Изузеци	Нема.
Услови који важе након завршетка	Нема.

16. Картица случаја коришћења Помоћ

Назив	Помоћ
Предуслови	Нема.
Кораци	1. Кликом на дугме за помоћ, кориснику се приказује прозор са документацијом система.
Проширења	Нема.
Изузеци	Нема.
Услови који важе након завршетка	Нема.

17. Картица случаја коришћења Одјава са система

Назив	Одјава са система
Предуслови	Корисник је пријављен.
Кораци	1. Кликом на дугме за одјаву, врши се одјава корисника са система.
Проширења	Нема.
Изузеци	Нема.
Услови који важе након завршетка	Корисник је одјављен са система.

5.3 Дизајн и пројектовање система

5.3.1 Дијаграм компоненти

Архитектура система прилагођена је окружењу Лабораторије за дигиталну форензику и њеном особљу. На слици 10 приказана је архитектура система, која се састоји од четири компоненте – клијентске апликације, програмског интерфејса, пословне логике и базе података.

Клијентска апликација нуди графички кориснички интерфејс са циљем једноставне интеракције корисника са системом. Програмски интерфејс садржи крајње тачке које прихватају клијентске захтеве и прослеђују модулу пословне логике на обраду. Тиме програмски интерфејс представља спону клијентске апликације и пословне логике. Модул пословне логике система рукује формално описаним знањем ускладиштеним у бази података.

Слика 10: Архитектура система.

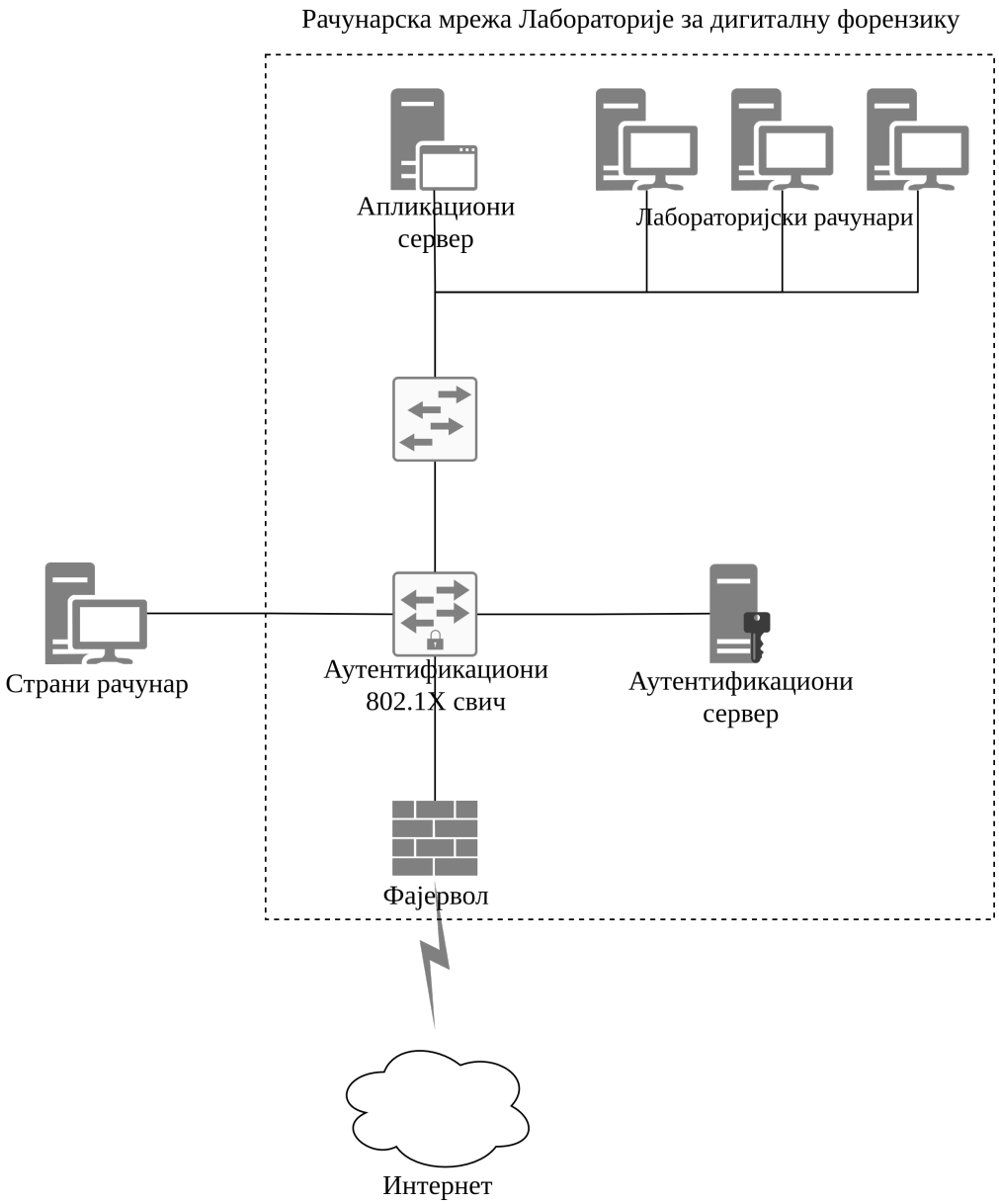
5.3.2 Дијаграм распоређивања

Рачунарска мрежа Лабораторије за дигиталну форензику (слика 11) састоји се од апликационог сервера на коме је инсталиран систем, аутентификационог сервера и аутентификатора који обезбеђује сигурност на нивоу везе (другом нивоу OSI референтног модела).

Механизам аутентификације система имплементиран је по узору на IEEE 802.1X стандард (Smith и сар., 2003) и то по типу аутентификације који се карактерише највишим степеном сигурности – аутентификацији базираној на сертификатима. Овај начин аутентификације захтева од клијента да приликом приступа систему приложи сертификат којим доказује идентитет којим се представља (Loos, 2012). Стога је део система и инфраструктура јавног кључа (енг. *Public Key Infrastructure*) задужена за управљање сертификатима.

Рачунарска мрежа Лабораторије садржи свич као мрежни уређај који има функцију аутентификатора. Комуникација између клијента и свича одвија се путем протокола EAPoLAN (Extensible Authentication Protocol over LAN) (IEEE Standards, 2001). Сертификат који је клијенту неопходан приликом комуникације аутоматски се инсталира у локално складиште сертификата клијента (Cisco, 2011).

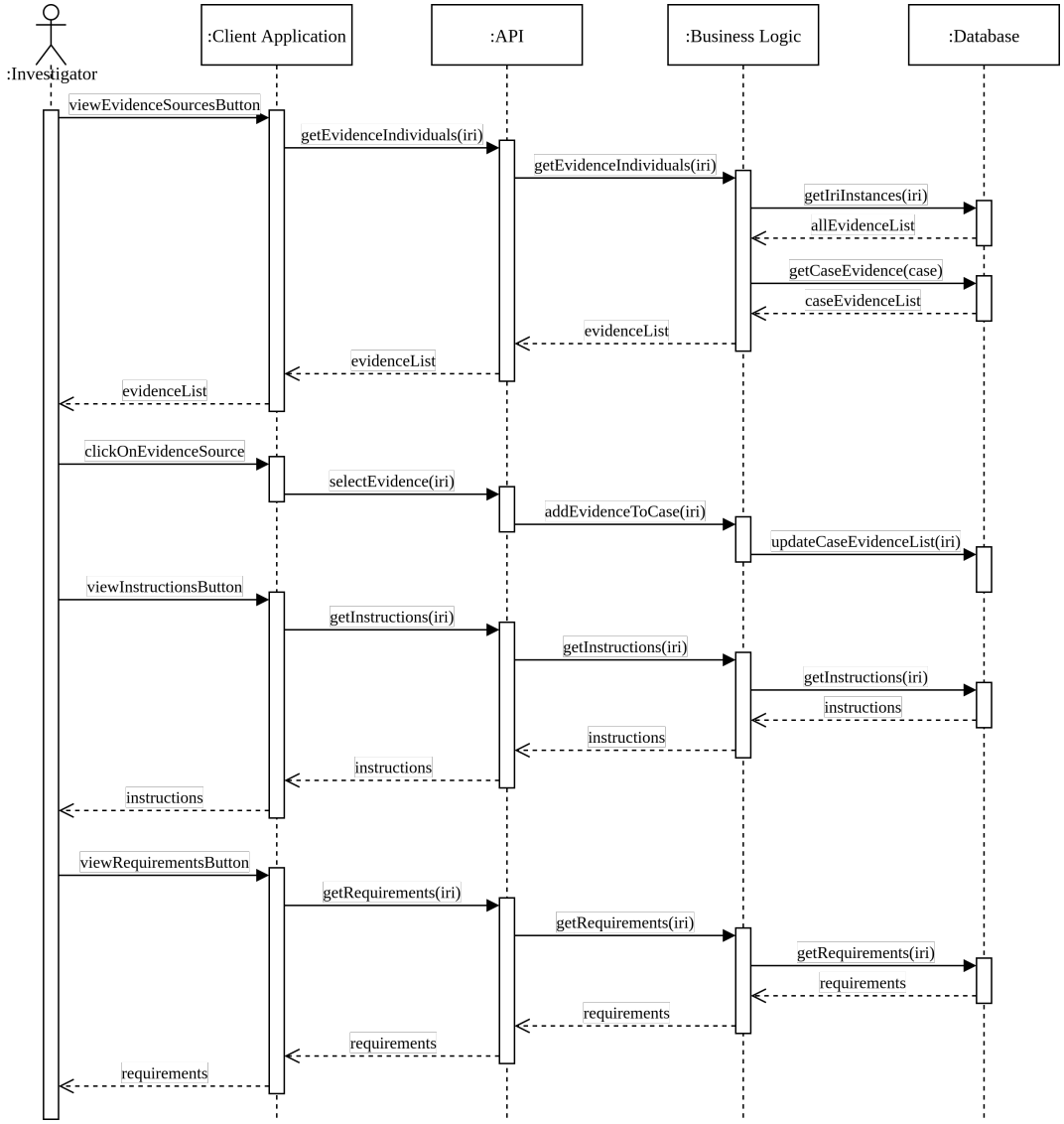
Аутентификациони сервер је RADIUS сервер (Zorn и Aboba, 1999). Сертификат RADIUS сервера користи се за доказивање идентитета клијента и креирање сигурног тока комуникације. Протокол који се користи за успостављање овог сигурног тока комуникације је PEAP (Palekar и сар., 2004). Након што се успостави сигуран ток комуникације, целокупан мрежни саобраћај размењен између клијента и RADIUS сервера бива шифрован.



Слика 11: Рачунарска мрежа Лабораторије за дигиталну форензику.

5.3.3 Дијаграм секвенце

Главне функционалности апликације су одабир оперативних форми и увид у инструкције у фазама истраге и захтеве ваљаности везане за инструкције. Стога је на слици 12 дат дијаграм секвенце који приказује начин реализације одабира потенцијалних извора доказа и увида у инструкције и њихове захтеве ваљаности.



Слика 12: Дијаграм секвенце за случајеве коришћења – одабир потенцијалних извора доказа и добављање инструкција и захтева ваљаности.

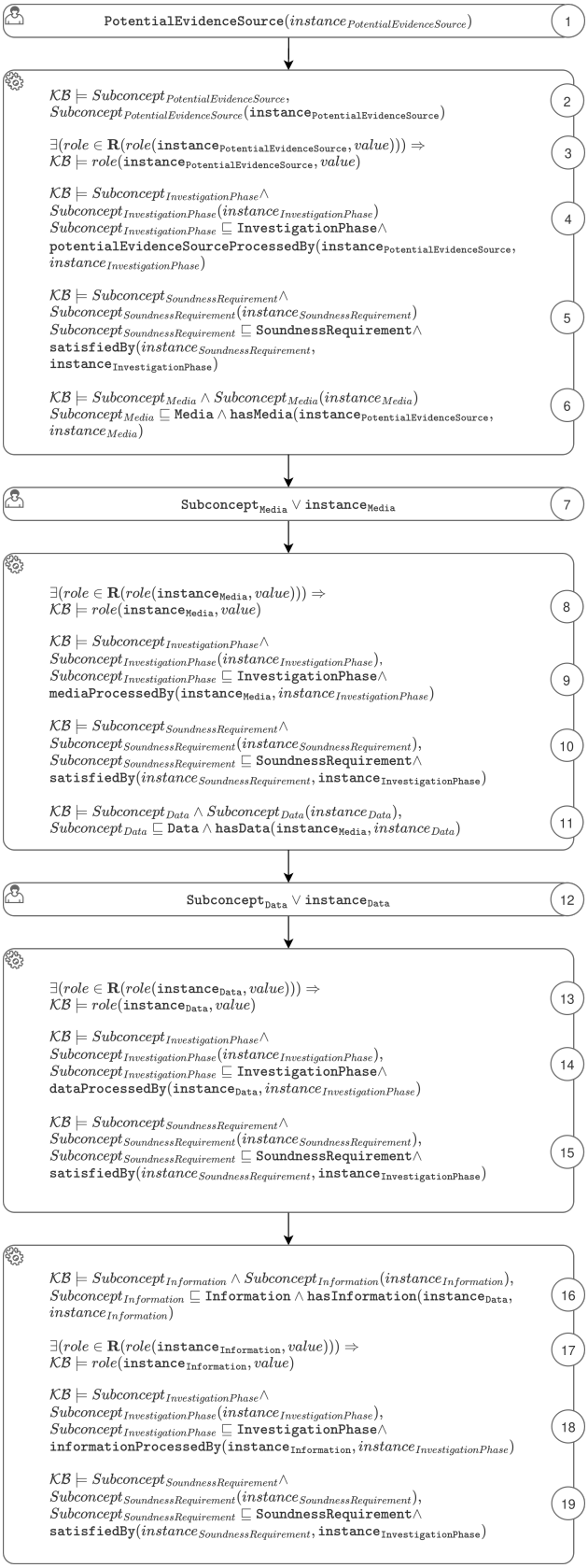
Колекција објеката дијаграма укључује форензичара, као учесника, инстанцу клијентске апликације, инстанцу класе апликационог програмског интерфејса, инстанцу класе пословне логике и базу података. Да би добио увид у све потенцијалне изворе доказа складиштене у онтологији, форензичар кроз одговарајућу компоненту графичког интерфејса шаље захтев одговарајућој тачки програмског интерфејса. Исти захтев програмски интерфејс шаље инстанци пословне логике, која захтева скуп потенцијалних извора доказа складиштених у онтологији, а који већ нису део тренутно активног случаја. Потом форензичар одабира потенцијалне изворе доказа које би требало да истражи, а инстанца програмског интерфејса, кроз операцију пословне логике и базу података, обезбеђује да се одабрани извори доказа прикључе тренутно активном случају.

Након прикључења потенцијалних извора доказа случају, форензичар,

кроз одговарајућу компоненту графичког интерфејса, врши одабир једне од њих како би добио увид у инструкције. Добављање инструкција одвија се путем операција програмског интерфејса и пословне логике, која директно комуницира са базом података. По сличном принципу, форензичар одабира добијену инструкцију како би се добавио скуп захтева ваљаности везаних за њу.

5.3.4 Дијаграм активности

Начин функционисања система осликан је и дијаграмом активности приказаним на слици 13. У исказима на дијаграму и у каснијим објашњењима промењљиве су приказане курзивом, док су продукти закључивања приказани писмовним резом. Постоје два типа активности – системске и корисничке. Ток активности започиње специфицирањем потенцијалних извора доказа од стране корисника (у даљњем тексту, форензичара). Тиме се допрема улазни параметар за различите типове расуђивања система: закључивање о инстанцама појмова, одређивање поткласа појмова и одређивање појмова на основу дате везе међу појмовима.



Слика 13: Дијаграм активности система.

У наставку следи објашњење појединачних активности.

Корисничка активност (1), представљена исказом `PotentialEvidenceSource`($instance_{PotentialEvidenceSource}$) означава одабир конкретног потенцијалног извора доказа, који је предмет истраге, односно означава одабир инстанце класе „потенцијални извор доказа".

Након што корисник одабере конкретан потенцијални извор доказа, следи системска активност, која се огледа у закључивању над онтологијом. Сви потконцепти концепта `PotentialEvidenceSource`, коме припада инстанца коју је корисник одабрао, бивају добављени закључивањем о инстанцама.

(2) $\mathcal{KB} \models Subconcept_{PotentialEvidenceSource}$, $Subconcept_{PotentialEvidenceSource}(\texttt{instance}_{\texttt{PotentialEvidenceSource}})$

У трећем кораку следи закључивање којим се инстанце одређују на основу дате везе са другим инстанцама. У конкретном случају, одабрани потенцијални извор доказа, као инстанца, у бази знања може бити повезана са инстанцама које представљају карактеристике потенцијалног извора доказа, те се њиховим добављањем оне стављају на увид кориснику.

(3) $\exists(role \in \mathbf{R}\ (role(\texttt{instance}_{\texttt{PotentialEvidenceSource}}, value))) \Rightarrow$ $\mathcal{KB} \models role(\texttt{instance}_{\texttt{PotentialEvidenceSource}}, value)$

Следи закључивање којим се одређује инстанца концепта „фаза истраге" ($instance_{InvestigationPhase}$) на основу везе са инстанцом потенцијалног извора доказа ($\texttt{instance}_{\texttt{PotentialEvidenceSource}}$). Другим речима, кориснику се на увид ставља фаза истраге у оквиру које корисник треба да истражи дати потенцијални извор доказа. Додатно, из базе знања бивају добављени директан концепт коме инстанца фазе истраге припада, као и његове инстанце, потконцепти и инстанце потконцепата.

(4) $\mathcal{KB} \models Subconcept_{InvestigationPhase} \wedge$ $Subconcept_{InvestigationPhase}(instance_{InvestigationPhase})$, $Subconcept_{InvestigationPhase} \sqsubseteq \texttt{InvestigationPhase} \wedge$ $\texttt{potentialEvidenceSourceProcessedBy}(\texttt{instance}_{\texttt{PotentialEvidenceSource}}, instance_{InvestigationPhase})$

Пети корак је део суштине система – закључивањем се одређује инстанца „захтева ваљаности" истраге који је везом `satisfiedBy` повезан са инстанцом „фазе истраге", односно инстанца „фазе истраге" је везом `satisfies` повезана са инстанцом „захтева ваљаности". Такође, из базе знања се закључивањем о класи којој инстанца припада добављају концепти захтева ваљаности истраге. Тиме се кориснику ставља до знања које захтеве у датој фази истраге треба да задовољи како би истрага била ваљана.

(5) $\mathcal{KB} \models Subconcept_{SoundnessRequirement} \wedge$
$Subconcept_{SoundnessRequirement}(instance_{SoundnessRequirement})$,
$Subconcept_{InvestigationPhase} \sqsubseteq \texttt{SoundnessRequirement} \wedge$
$\texttt{satisfiedBy}(instance_{SoundnessRequirement}, \texttt{instance}_{\texttt{InvestigationPhase}})$

У следећем кораку оперативна форма података над којима се врши истрага није више потенцијални извор доказа, већ складиште података. С тим у вези, закључивањем се одређују инстанце концепта „складиште података" (`Media`) које садржи дати потенцијални извор доказа, односно које су везом `hasMedia` повезане са датом инстанцом потенцијалног извора доказа.

(6) $\mathcal{KB} \models Subconcept_{Media} \wedge Subconcept_{Media}(instance_{Media})$,
$Subconcept_{Media} \sqsubseteq \texttt{Media} \wedge \texttt{hasMedia}(\texttt{instance}_{\texttt{PotentialEvidenceSource}},$
$instance_{Media})$

На кориснику је сада да одабере складиште података из одабраног потенцијалног извора доказа, за које мисли да ће га одвести до очекиваних трагова.

(7) $\texttt{Subconcept}_{\texttt{Media}} \vee \texttt{instance}_{\texttt{Media}}$

Наставак активности сличан је досадашњем току. Систем закључује о карактеристикама изабраних складишта података, које би могле бити корисне за форензичара, тако што одређује инстанце (вредности) које су повезане са инстанцама складишта података.

(8) $\exists(role \in \mathbf{R}\ (role(\texttt{instance}_{\texttt{Media}}, value))) \Rightarrow \mathcal{KB} \models role(\texttt{instance}_{\texttt{Media}}, value)$

Затим се из базе знања добављају инстанце концепта „фаза истраге" које су везом `mediaProcessedBy` повезане са одабраним складиштима података. Додатно се добавља директан концепт (класа) коме инстанца „фазе истраге" припада, потконцепти и инстанце потконцепата.

(9) $\mathcal{KB} \models Subconcept_{InvestigationPhase} \wedge$
$Subconcept_{InvestigationPhase}(instance_{InvestigationPhase})$,
$Subconcept_{InvestigationPhase} \sqsubseteq \texttt{InvestigationPhase} \wedge$
$\texttt{mediaProcessedBy}(\texttt{instance}_{\texttt{Media}}, instance_{InvestigationPhase})$

Кључни корак у тренутној фази истраге је одређивање захтева ваљаности, које би форензичар требало да задовољи. Тако се закључивањем у бази знања одређују инстанце концепта `SoundnessRequirement` које су везом `satisfiedBy` повезане са инстанцом тренутне фазе истраге. Поред тога, систем добавља и директан концепт, као класу којој добављена инстанца захтева ваљаности припада, потконцепте тог концепта и инстанце потконцепата, ако постоје.

(10) $\mathcal{KB} \models Subconcept_{SoundnessRequirement} \wedge$

$Subconcept_{SoundnessRequirement}(instance_{SoundnessRequirement})$,
$Subconcept_{InvestigationPhase} \sqsubseteq \texttt{SoundnessRequirement} \wedge$
$\texttt{satisfiedBy}(instance_{SoundnessRequirement}, \texttt{instance}_{\texttt{InvestigationPhase}})$

Следећа оперативна форма у истрази је „врста података" (`Data`). Кориснику се на увид стављају све врсте података које могу да се нађу у складишту података из претходног корака. Другим речима, из базе знања се закључивањем одређују инстанце концепта `Media` које су улогом `hasData` повезане са инстанцом концепта `Media`.

(11) $\mathcal{KB} \models Subconcept_{Data} \wedge Subconcept_{Data}(instance_{Data})$,
$Subconcept_{Data} \sqsubseteq \texttt{Data} \wedge \texttt{hasData}(\texttt{instance}_{\texttt{Media}}, instance_{Data})$

Тиме се кориснику даје могућност избора оне врсте података за које мисли да ће га одвести проналаску трагова важних за решење случаја.

(12) $\texttt{Subconcept}_{\texttt{Data}} \vee \texttt{instance}_{\texttt{Data}}$

Корак (13) сличан је корацима (8) и (3) – закључује се о постојању карактеристика одабраних врста података у бази знања и оне се стављају на увид кориснику.

(13) $\exists(role \in \mathbf{R}\ (role(\texttt{instance}_{\texttt{Data}}, value))) \Rightarrow \mathcal{KB} \models role(\texttt{instance}_{\texttt{Data}}, value)$

Са новом оперативном формом (врстом података), мења се и фаза истраге у оквиру које се спроводи истрага над врстама података. Тиме се у следећем кораку закључује о конкретној фази истраге, односно одређује се инстанца концепта `InvestigationPhase` која је улогом `DataProcessedBy` повезана са инстанцом концепта `Data`. Поред инстанце, закључује се о директном концепту коме инстанца припада, потконцептима и инстанцама потконцепата.

(14) $\mathcal{KB} \models Subconcept_{InvestigationPhase} \wedge$
$Subconcept_{InvestigationPhase}(instance_{InvestigationPhase})$,
$Subconcept_{InvestigationPhase} \sqsubseteq \texttt{InvestigationPhase} \wedge$
$\texttt{dataProcessedBy}(\texttt{instance}_{\texttt{Data}}, instance_{InvestigationPhase})$

Захтеви ваљаности које би у тренутној фази истраге требало испунити форензичару се стављају на увид тако што систем закључивањем одреди инстанце концепта `SoundnessRequirement` које су улогом `satisfiedBy` повезане са инстанцом концепта фазе истраге из претходног корака.

(15) $\mathcal{KB} \models Subconcept_{SoundnessRequirement} \wedge$
$Subconcept_{SoundnessRequirement}(instance_{SoundnessRequirement})$,
$Subconcept_{InvestigationPhase} \sqsubseteq \texttt{SoundnessRequirement} \wedge$
$\texttt{satisfiedBy}(instance_{SoundnessRequirement}, \texttt{instance}_{\texttt{InvestigationPhase}})$

Последња оперативна форма над којом се спроводи истрага је „информација" (`information`). Кориснику се на увид даје скуп информација које се из претходно одабраних врста података могу сазнати. То се постиже закључивањем над базом података којим се одређују инстанце концепта `Information` које су улогом `hasInformation` повезане са инстанцама концепта `Data`. Додатно се одређују и директан концепт добављаних инстанци, потконцепти и инстанце потконцепата.

(16) $\mathcal{KB} \models Subconcept_{Information} \wedge Subconcept_{Information}(instance_{Information})$, $Subconcept_{Information} \sqsubseteq \texttt{Information} \wedge \texttt{hasInformation}(\texttt{instance}_{\texttt{Data}}, instance_{Information})$

Уколико у бази знања постоје карактеристике претходно добављених типова информација, систем закључује о њима како би се приказале кориснику.

(17) $\exists(role \in \mathbf{R}\ (role(\texttt{instance}_{\texttt{Information}}, value))) \Rightarrow$
$\mathcal{KB} \models role(\texttt{instance}_{\texttt{Information}}, value)$

У последњим корацима, (18) и (19), систем закључује о фази истраге у којој је потребно истражити информације из претходних корака као и о захтевима ваљаности које у датим фазама истраге треба задовољити.

(18) $\mathcal{KB} \models Subconcept_{InvestigationPhase} \wedge$
$Subconcept_{InvestigationPhase}(instance_{InvestigationPhase})$,
$Subconcept_{InvestigationPhase} \sqsubseteq \texttt{InvestigationPhase} \wedge$
$\texttt{informationProcessedBy}(\texttt{instance}_{\texttt{Information}}, instance_{InvestigationPhase})$

(19) $\mathcal{KB} \models Subconcept_{SoundnessRequirement} \wedge$
$Subconcept_{SoundnessRequirement}(instance_{SoundnessRequirement})$,
$Subconcept_{InvestigationPhase} \sqsubseteq \texttt{SoundnessRequirement} \wedge$
$\texttt{satisfiedBy}(instance_{SoundnessRequirement}, \texttt{instance}_{\texttt{InvestigationPhase}})$

С обзиром на то да су се захтеви ваљаности истраге у описаним активностима одређивали на основу везе са одговарајућом фазом истраге (идентификацијом, прикупљањем, прегледањем или анализом доказа), то се ваљаност форензичке истраге може формално дефинисати као унија захтева ваљаности фазе идентификације, прикупљања, прегледања и анализе доказа:

$ForensicSoundness \equiv (IdentificationSoundnessRequirement \sqcup$
$CollectionSoundnessRequirement \sqcup ExaminationSoundnessRequirement \sqcup$
$AnalysisSoundnessRequirement)$

5.4 Имплементација система

Како је сигурносни аспект апликације веома важан, овај одељак је, поред софтверских технологија коришћених за имплементацију апликације по описаној архитектури, нарочито посвећен имплементацији сигурности.

Клијентска апликација система имплементирана је као једностранична апликација (енг. *single page application*) употребом радног оквира Angular (Jain и сар., 2014).

Програмски интерфејс система имплементиран је као Flask апликација (Pallets, 2010). Flask је радни оквир који омогућава имплементацију једноставних веб-апликација. За одабир овог радног оквира приликом имплементације система размотрени су његова величина и комплексност, потреба за скалабилношћу и перформансе. Како се систем може окарактерисати прототипом средње величине, употреба радног оквира Flask задовољава потребе система за једноставност и минималистички дизајн, као и за перформансе и скалабилност прилагођене употреби од стране форензичара Лабораторије за дигиталну форензику.

Модул пословне логике система имплементиран је употребом програмског језика Python у чијем је фокусу библиотека за манипулацију онтологијом – Owlready2 (Lamy, 2017). Ова библиотека омогућава учитавање онтологије као Python објекта након чега је могуће ажурирати онтологију, серијализовати је и спровести резоновање над знањем складиштеним у онтологији употребом расуђивача HermiT (Group, 2021). За упите над онтологијом, које није могуће извршити помоћу библиотеке Owlready2, модул пословне логике садржи SPARQL [6] упите.

Библиотека Owlready2 користи RDF графовску базу података, која је серијализована у SQLite [7] формату. База података у оквиру система не захтева имплементацију конкурентности с обзиром на то да систем не омогућава кориснику ажурирање онтологије као дељеног ресурса. Такође, не постоји потреба за распоређивање оптерећења мрежног саобраћаја јер је систем намењен употреби од стране форензичара који су део Лабораторије.

Поред имплементације механизама аутентификације, систем се одликује и механизмом ауторизације. Радни оквир који је коришћен за имплементацију ауторизације је OAuth (Hardt, 2012). OAuth радни оквир користи приступне токене (енг. access tokens), који представљају ауторизационе податке у складу са којима се ограничава приступ систему. Формат приступних токена који је коришћен је JWT (Jones и сар., 2015).

5.5 Студија случаја

Конкретан случај форензичке истраге, којим ће се у овом одељку показати начин на који систем помаже у истрази је вежба организације ENISA (ENISA, 2019) чија тема је форензика рачунарских мрежа.

[6] https://www.w3.org/TR/sparql11-query/
[7] https://www.sqlite.org/

Сценарио случаја везује се за цурење поверљивих информација једне компаније чему је узрок један од запослених. Поменуте поверљиве информације пронађене су на форуму мреже Дарквеб (енг. *dark web*). На основу садржаја објаве на форуму, познато је оквирно време деловања малициозног запосленог, а материјал за истрагу је лог-датотека безбедносног мрежног уређаја (енг. *firewall*) pfSense [8].

5.5.1 Фаза идентификације доказа

Прва фаза истраге је идентификација потенцијалних извора доказа. У описаном случају, то је рачунар на коме је инсталиран и активан безбедносни мрежни уређај pfSense Firewall. У првом кораку, у интеракцији форензичара са системом, форензичар бира дати безбедносни уређај као потенцијални извор доказа. У другом кораку, форензичару се од стране система даје на знање да је pfSense виртуелни безбедносни уређај, односно софтвер који се инсталира на вишенаменском рачунару. У кораку три, форензичару се даје на знање да pfSense треба најпре да буде подвргнут истражној фази идентификације. У наставку је дат формални опис поменутих активности.

$\texttt{PotentialEvidenceSource}(pfsense)$

$\mathcal{KB} \models VirtualizedPotentialEvidenceSource,$
$VirtualizedPotentialEvidenceSource(\texttt{pfsense})$

$\mathcal{KB} \models FirewallVirtualized,$
$FirewallVirtualized(\texttt{pfsense})$

$\mathcal{KB} \models Identification \wedge$
$Identification(identification\_of\_virtualized\_firewall),$
$Identification \sqsubseteq \texttt{InvestigationPhase} \wedge$
$\texttt{potentialEvidenceSourceProcessedBy}(\texttt{pfsense},$
$identification\_of\_virtualized\_firewall)$

$\mathcal{KB} \models VirtualizedPotentialEvidenceSourceIdentification \wedge$
$VirtualizedPotentialEvidenceSourceIdentification$
$(identification\_of\_virtualized\_firewall),$
$VirtualizedPotentialEvidenceSourceIdentification \sqsubseteq \texttt{Identification} \wedge$
$\texttt{potentialEvidenceSourceProcessedBy}(\texttt{pfsense},$
$identification\_of\_virtualized\_firewall)$

Већ је речено да је у обзир узето шест главних захтева ваљаности форензичке истраге – аудитабилност, оправданост, поузданост, поновљивост, репродукција и довољност. Неки од ових захтева могу се применити у конкретној фази идентификације доказа. Захтев аудитабилности подразумева документовање активности у току којих се руковало оригиналним изворима доказа (енг.

[8] https://www.pfsense.org/

chain of custody) као и документовање карактеристика потенцијалних извора доказа. Документ у коме се заводе активности у току којих се руковало оригиналним изворима доказа треба да садржи идентификатор извора доказа и ко је, када и где и из ког разлога руковао оригиналним извором доказа. Карактеристике извора доказа, у овом случају вишенаменског рачунара, које је потребно навести, су произвођач, модел и серијски број (ISO/IEC 27037, 2015).

④ $\mathcal{KB} \models IdentificationSoundnessRequirement$,
$IdentificationSoundnessRequirement \sqsubseteq$ `SoundnessRequirement`

$\mathcal{KB} \models IdentificationAuditability$,
$IdentificationAuditability \sqsubseteq$ `IdentificationSoundnessRequirement`

$\mathcal{KB} \models DocumentChainOfCustody \wedge$
$DocumentChainOfCustody(PC\_identifier, who, when, where,$
$responsible\_individual\_name)$,
$DocumentChainOfCustody \sqsubseteq$ `IdentificationAuditability` $\wedge$
`satisfiedBy`$(\{PC\_identifier, who, when, where,$
$responsible\_individual\_name\}$,
`identification_of_virtualized_firewall`)

$\mathcal{KB} \models DocumentPotentialEvidenceSourceCharacteristics \wedge$
$DocumentPotentialEvidenceSourceCharacteristics(type, name, version$
$DocumentPotentialEvidenceSourceCharacteristics \sqsubseteq$
`IdentificationAuditability` $\wedge$ `satisfiedBy`
$(\{type, name, version\}$, `identification_of_virtualized_firewall`)

Оправданост као захтев ваљаности истраге у фази идентификације односи се на објашњење релевантности потенцијалних извора података у конкретном случају. Вишенаменски рачунар са безбедносним софтвером pfSense Firewall јесте релевантан јер се у сценарију случаја ради о малициозним активностима спроведеним на Интернету кроз приватну мрежу. У наставку је дат формални опис наведеног.

$\mathcal{KB} \models IdentificationJustifiability$,
$IdentificationJustifiability \sqsubseteq$ `IdentificationSoundnessRequirement`

$\mathcal{KB} \models JustifyIdentificationRelevance \wedge$
$JustifyIdentificationRelevance(dealing\_with\_network\_intrusion,$
$attack\_beyond\_private\_network)$,
$JustifyIdentificationRelevance \sqsubseteq$ `IdentificationJustifiability` $\wedge$
`satisfiedBy`$(\{dealing\_with\_network\_intrusion,$
$attack\_beyond\_private\_network\}$,
`identification_of_virtualized_firewall`)

Захтев довољности у фази идентификације у датом случају односи се на

потребу да форензичар узме у обзир друге потенцијално релевантне изворе доказа и да наведе разлоге из којих су одабрани извори доказа довољни за решење конкретног случаја. Објашњење довољности вишенаменског рачунара са инсталираним безбедносним уређајем зависи од доступности других потенцијално релевантних доказа. Други уређаји или сервиси које би требало узети у обзир (ако су доступни) су они који чувају информације о природи конекција или о оштећеним (нападнутим) сервисима.

$\mathcal{KB} \models IdentificationSufficiency$,
$IdentificationSufficiency \sqsubseteq$ `IdentificationSoundnessRequirement`

$\mathcal{KB} \models ExplainNetworkSourcesSufficiency \wedge$
$ExplainNetworkSourcesSufficiency($
$can\_give\_information\_about\_suspicious\_connections$,
$cannot\_give\_information\_about\_attacked\_services$,
$cannot\_give\_information\_about\_nature\_of\_connections$),
$ExplainNetworkSourcesSufficiency \sqsubseteq$ `IdentificationSufficiency` $\wedge$
`satisfiedBy`($\{can\_give\_information\_about\_suspicious\_connections$,
$cannot\_give\_information\_about\_attacked\_services$,
$cannot\_give\_information\_about\_nature\_of\_connections\}$,
`identification_of_virtualized_firewall`)

Последњи захтев ваљаности истраге у фази идентификације, који се у овом случају може применити је поузданост. Под тиме се подразумева спречавање било каквих измена или оштећења оригиналног извора доказа, као и спречавање даљњих малициозних активности. То значи да вишенаменски рачунар на коме је инсталиран безбедносни софтвер, као и сам безбедносни софтвер, не смеју бити искључени, чиме рачунарска мрежа компаније остаје заштићена.

$\mathcal{KB} \models IdentificationReliability$,
$IdentificationReliability \sqsubseteq$ `IdentificationSoundnessRequirement`

$\mathcal{KB} \models \{RemainStateAsItIs, PreventThreats\} \wedge$
$\{RemainStateAsItIs, PreventThreats\}($
$dont\_switch\_off\_firewall$,
$dont\_switch\_off\_PC$),
$\{RemainStateAsItIs, PreventThreats\} \sqsubseteq$ `IdentificationReliability` $\wedge$
`satisfiedBy`($\{dont\_switch\_off\_firewall, dont\_switch\_off\_PC\}$,
`identification_of_virtualized_firewall`)

5.5.2 Фаза прикупљања доказа

Оперативна форма фазе прикупљања је складиште података. Захтеви ваљаности који су у овој фази применљиви су поузданост и довољност, за разлику од којих аудитабилност није применљив захтев с обзиром на то да не постоји потреба за прикупљањем складишта података, односно чврстог диска.

Задовољење захтева довољности изискује разматрање других складишта података поменутог вишенаменског рачунара. С обзиром на то да је уобичајено да се поред безбедносног софтвера pfSense Firewall користи и безбедносни сервис посредник Squid proxy [9], форензичар је у обавези да размотри локацију у складишту података коју користи овај сервис.

$\mathcal{KB} \models CollectionSufficiency$,
$CollectionSufficiency \sqsubseteq$ `CollectionSoundnessRequirement`

$\mathcal{KB} \models CollectSufficientMaterial \wedge$
$CollectSufficientMaterial(squid\_access\_logs)$,
$CollectSufficientMaterial \sqsubseteq$ `CollectionSufficiency` $\wedge$
`satisfiedBy({without_moving_media, collection_on_live_system},`
$squid\_access\_logs)$

$\mathcal{KB} \models Media$, $Media$(`pfsense_log, squid_log`)

$\mathcal{KB} \models HostMedia$, $HostMedia$(`pfsense_log, squid_log`)

$\mathcal{KB} \models HostMagneticDisk$, $HostMagneticDisk$(`pfsense_log, squid_log`)

$\mathcal{KB} \models HostMagneticDiskSystem$,
$HostMagneticDiskSystem$(`pfsense_log, squid_log`)

$\mathcal{KB} \models HostMagneticDiskSystemLog$,
$HostMagneticDiskSystemLog$(`pfsense_log, squid_log`)

$\mathcal{KB} \models HostMagneticDiskFirewallLog$,
$HostMagneticDiskFirewallLog$(`pfsense_log, squid_log`)

`pfsense_log, squid_log`

У следећем кораку систем предлаже метод прикупљања релевантних датотека, што је у овом случају прикупљање са укљученог рачунара без изоловања чврстог диска.

$\mathcal{KB} \models Collection \wedge$
$Collection(without\_moving\_media, collection\_on\_live\_system)$,
$Collection \sqsubseteq$ `InvestigationPhase` $\wedge$
`mediaProcessedBy(pfsense_log, squid_log,`
$\{without\_moving\_media, collection\_on\_live\_system\})$

$\mathcal{KB} \models PoweredOnDeviceCollection \wedge$
$PoweredOnDeviceCollection(without\_moving\_media,$
$collection\_on\_live\_system)$,

[9] https://www.squid-cache.org/

$PoweredOnDeviceCollection \sqsubseteq$ `Collection` $\wedge$
`mediaProcessedBy`(`pfsense_log, squid_log`,
$\{without\_moving\_media, collection\_on\_live\_system\}$)

Затим систем предлаже начине на које се може задовољити захтев поузданости у фази прикупљања овог случаја – прављење главне копије и прављење радне копије, као и спречавање измене података на оригиналном складишту података. Алати dd [10] и FTK Imager [11], који могу бити покренути са USB флеш меморије могу се искористити за прављење копија, а да при томе не наруше интегритет података. Након прављења копија, систем форензичару сугерише валидацију копија рачунањем хеш-вредности оригинала и копије испитивањем њихове идентичности. Пример алата који служи за рачунање хеш вредности је md5sum [12].

$\mathcal{KB} \models CollectionSoundnessRequirement$,
$CollectionSoundnessRequirement \sqsubseteq$ `SoundnessRequirement`

$\mathcal{KB} \models CollectionReliability$,
$CollectionReliability \sqsubseteq$ `CollectionSoundnessRequirement`

$\mathcal{KB} \models MakeForensicCopy \wedge$
$MakeForensicCopy(using\_dd, using\_FTK\_imager)$,
$MakeForensicCopy \sqsubseteq$ `CollectionReliability` $\wedge$
`satisfiedBy`(`{without_moving_media, collection_on_live_system}`,
$\{using\_dd, using\_FTK\_imager\}$)

$\mathcal{KB} \models MakeWorkingCopy$,
$MakeWorkingCopy \sqsubseteq$ `MakeForensicCopy`

$\mathcal{KB} \models MakeMasterCopy$,
$MakeMasterCopy \sqsubseteq$ `MakeForensicCopy`

$\mathcal{KB} \models PreventAlteration \wedge$
$PreventAlteration(use\_live\_distro)$,
$PreventAlteration \sqsubseteq$ `CollectionReliability` $\wedge$
`satisfiedBy`(`{without_moving_media, collection_on_live_system}`,
use_live_distro)

$\mathcal{KB} \models PreserveIntegrity \wedge$
$PreserveIntegrity(calculate\_hash\_values)$,
$PreserveIntegrity \sqsubseteq$ `CollectionReliability` $\wedge$
`satisfiedBy`(`{without_moving_media, collection_on_live_system}`,
$calculate\_hash\_values$)

[10] https://man7.org/linux/man-pages/man1/dd.1.html
[11] https://www.exterro.com/digital-forensics-software/ftk-imager
[12] https://man7.org/linux/man-pages/man1/md5sum.1.html

$\mathcal{KB} \models VerifyIntegrity \wedge$
$VerifyIntegrity(md5sum)$,
$VerifyIntegrity \sqsubseteq$ `PreserveIntegrity` $\wedge$
`satisfiedBy({without_moving_media, collection_on_live_system}`,
$md5sum)$

5.5.3 Фаза прегледања доказа

Оперативна форма фазе прегледања доказа је „врста података". Да би систем форензичару помогао у спровођењу ове фазе и руковању подацима, форензичар треба да специфицира врсте података које су релевантне за случај. У конкретном случају, то је садржај логова безбедносног софтвера pfSense и сервиса-посредника Squid.

(13) `pfsense_log_data, squid_log_data`

$\mathcal{KB} \models Data$, $Data($`pfsense_log_data`$)$

$\mathcal{KB} \models FirewallData$, $FirewallData($`pfsense_log_data`$)$

$\mathcal{KB} \models VirtualizedFirewallData$,
$VirtualizedFirewallData($`pfsense_log_data`$)$

$\mathcal{KB} \models VirtualizedFirewallLogData$,
$VirtualizedFirewallLogData($`pfsense_log_data`$)$

$\mathcal{KB} \models Examination \wedge$
$Examination(pfsense\_log\_examination)$,
$Examination \sqsubseteq$ `InvestigationPhase` $\wedge$
`dataProcessedBy`$(\texttt{pfsense\_log\_data}, pfsense\_log\_examination)$

$\mathcal{KB} \models FirewallExamination \wedge$
$FirewallExamination(pfsense\_log\_examination)$,
$FirewallExamination \sqsubseteq$ `Examination` $\wedge$
`dataProcessedBy`$(\texttt{pfsense\_log\_data}, pfsense\_log\_examination)$

$\mathcal{KB} \models VirtualizedFirewallExamination \wedge$
$VirtualizedFirewallExamination(pfsense\_log\_examination)$,
$VirtualizedFirewallExamination \sqsubseteq$ `FirewallExamination` $\wedge$
`dataProcessedBy`$(\texttt{pfsense\_log\_data}, pfsense\_log\_examination)$

$\mathcal{KB} \models VirtualizedFirewallLogExamination \wedge$
$VirtualizedFirewallLogExamination(pfsense\_log\_examination)$,
$VirtualizedFirewallLogExamination \sqsubseteq$
`VirtualizedFirewallExamination` $\wedge$ `dataProcessedBy`
$(\texttt{pfsense\_log\_data}, pfsense\_log\_examination)$

$\mathcal{KB} \models ExaminationSoundnessRequirement$,
$ExaminationSoundnessRequirement \sqsubseteq$ `SoundnessRequirement`

$\mathcal{KB} \models ExaminationAuditability$,
$ExaminationAuditability \sqsubseteq$ `ExaminationSoundnessRequirement`

Што се тиче захтева ваљаности које у фази прегледања треба задовољити, у конкретном случају су применљиви аудитабилност, поузданост и оправданост.

Аудитабилност изискује документовање свих активности спроведених током фазе прегледања доказа. Те активности укључују прегледање форензичке слике помоћу одговарајућег алата. Тако систем предлаже кориснику да употреби алат Autopsy, као најчешће коришћен форензички алат који служи за прегледање и анализу форензичких слика различитих формата. Како је pfSense виртуелна машина, то систем предлаже употребу модула алата Autopsy под називом Virtual Machine Extractor.

$\mathcal{KB} \models DocumentExamination \wedge$
$DocumentExamination(document\_all\_examination\_acitivities)$,
$DocumentExamination \sqsubseteq$ `ExaminationAuditability` $\wedge$
`satisfiedBy`$(document\_all\_examination\_activities,$
`pfsense_log_examination`$)$

На крају, форензичар би требало да оправда употребу поменутог софтвера како би задовољио захтев оправданости.

$\mathcal{KB} \models ExaminationReliability$,
$ExaminationReliability \sqsubseteq$ `ExaminationSoundnessRequirement`

$\mathcal{KB} \models ChooseMostSuitableExaminationTool \wedge$
$ChooseMostSuitableExaminationTool($
$autopsy\_virtual\_machine\_extractor)$,
$ChooseMostSuitableExaminationTool \sqsubseteq$ `ExaminationReliability` $\wedge$
`satisfiedBy`$(autopsy\_virtual\_machine\_extractor,$
`pfsense_log_examination`$)$

$\mathcal{KB} \models ExaminationJustifiability$,
$ExaminationJustifiability \sqsubseteq$ `ExaminationSoundnessRequirement`

$\mathcal{KB} \models JustifyDesicionForUsingExaminationTool \wedge$
$JustifyDesicionForUsingExaminationTool(widely\_adopted\_tool)$,
$JustifyDesicionForUsingExaminationTool \sqsubseteq$
`ExaminationJustifiability` $\wedge$ `satisfiedBy`
$(widely\_adopted\_tool,$ `pfsense_log_examination`$)$

5.5.4 Фаза анализе доказа

Продукт фазе анализе требало би да су информације добијене из података из претходне фазе истраге. Подаци из претходне фазе представљају садржај лог-датотека, те систем кориснику даје на увид формат записа у лог-датотекама како би могао да их анализира. Тако систем предочава да су редови лог-датотеке коју креира безбедносни софтвер pfSense, формата: <`Timestamp` ><`Hostname` >`filterlog:` <`CSVdata` > и да је формат реда у лог-датотеци сервиса-посредника: `remote_host remote_logname authenticated_username date request status content_length`.

$\mathcal{KB} \models hasLogEntryForm($`{pfsense_log_information,`
`''<Timestamp><Hostname>filterlog:<CSVdata>'')`

$\mathcal{KB} \models hasLogEntryForm($`{squid_log_information,`
`''remote_host remote_logname authenticated_username`
`date request status content-length'')`

$\mathcal{KB} \models Information, Information$
(`pfsense_log_information, squid_log_information`)

$\mathcal{KB} \models FirewallInformation,$
$FirewallInformation$(`pfsense_log_information`)

$\mathcal{KB} \models FirewallLogInformation,$
$FirewallLogInformation$(`pfsense_log_information,`
`rule_number, sub_rule_number, unique_id, anchor,`
`interface_name, reason_for_log_entry`)

$\mathcal{KB} \models ProxyInformation,$
$ProxyInformation$(`squid_log_information`)

$\mathcal{KB} \models ProxyLogInformation,$
$ProxyLogInformation$(`squid_log_information`)

$\mathcal{KB} \models Analysis \wedge$
$Analysis(pfsense\_log\_analysis),$
$Analysis \sqsubseteq$ `InvestigationPhase` $\wedge$
`informationProcessedBy`(`pfsense_log_information`, $pfsense\_log\_analysis$)

$\mathcal{KB} \models FirewallAnalysis \wedge$
$FirewallAnalysis(pfsense\_log\_analysis),$
$FirewallAnalysis \sqsubseteq$ `Analysis` $\wedge$
`informationProcessedBy`(`pfsense_log_information`,
check_ log_ file_ size, check_ number_ of_ lines, search_ for_ type_ of_ recorded_ traffic,
search_ for_ most_ frequent_ protocols,
search_ for_ source_ and_ destination_ IP_ addresses,

pfsense_log_analysis, *squid_log_analysis*,
analysis_with_MISP_alternatives)

Захтеви ваљаности који треба да се задовоље у фази анализе у овом случају су аудитабилност, поузданост, довољност, поновљивост и репродукција.

Аудитабилност у овом случају подразумева документовање свих активности спроведених током фазе анализе.

$\mathcal{KB} \models$ *AnalysisSoundnessRequirement*,
AnalysisSoundnessRequirement $\sqsubseteq$ `SoundnessRequirement`

$\mathcal{KB} \models$ *AnalysisAuditability*,
AnalysisAuditability $\sqsubseteq$ `AnalysisSoundnessRequirement`

$\mathcal{KB} \models$ *DocumentAnalysis* $\wedge$
DocumentAnalysis(*document_all_analysis_acitivities*),
DocumentAnalysis $\sqsubseteq$ `AnalysisAuditability` $\wedge$
`satisfiedBy`(*document_all_analysis_activities*,
`pfsense_log_analysis`)

Судећи по упутствима за спровођење истраге овог случаја, које је креирала организација ENISA, добра је пракса проверити најпре величину меморијског простора који заузима лог-датотека, као и број линија текста које чине лог-датотеку употребом алата командне линије `wc` [13].

$\mathcal{KB} \models$ *AnalysisReliability*,
AnalysisReliability $\sqsubseteq$ `AnalysisSoundnessRequirement`

$\mathcal{KB} \models$ *ChooseMostSuitableAnalysisTool* $\wedge$
ChooseMostSuitableAnalysisTool(
`''wc -l firewall_log''`),
ChooseMostSuitableAnalysisTool $\sqsubseteq$ `AnalysisReliability` $\wedge$
`satisfiedBy(''wc -l firewall_log'',`
`{check_log_file_size, check_number_of_lines}`)

Даље, систем форензичару предлаже да одреди тип снимљеног мрежног саобраћаја и најфреквентније мрежне протоколе који се у снимку јављају помоћу алата командне линије awk [14]. Такође, систем предлаже да се изворне и одредишне адресе из снимка мрежног саобраћаја упореде са сумњивим IP адресама из базе података MISP [15], за које је познато да представљају претњу по информациону безбедност.

$\mathcal{KB} \models$ *ChooseMostSuitableAnalysisTool* $\wedge$

[13] https://www.man7.org/linux/man-pages/man1/wc.1.html
[14] https://man7.org/linux/man-pages/man1/awk.1p.html
[15] https://www.misp-project.org/

$ChooseMostSuitableAnalysisTool($
''awk -F '{print $22}' firewall_log | sort | uniq -c | sort -n''),
$ChooseMostSuitableAnalysisTool \sqsubseteq$ AnalysisReliability $\wedge$
satisfiedBy(''awk -F '{print $22}' firewall_log | sort | uniq -c | sort -n'',
search_for_type_of_recorded_traffic)

$\mathcal{KB} \models ChooseMostSuitableAnalysisTool \wedge$
$ChooseMostSuitableAnalysisTool($
''awk -F '{print $17}' firewall_log | sort | uniq''),
$ChooseMostSuitableAnalysisTool \sqsubseteq$ AnalysisReliability $\wedge$
satisfiedBy(''awk -F '{print $17}' firewall_log | sort | uniq'',
search_for_most_frequent_protocols)

$\mathcal{KB} \models ChooseMostSuitableAnalysisTool \wedge$
$ChooseMostSuitableAnalysisTool($
''awk -F '{print $19}' firewall_log | sort | uniq -wc -l''),
$ChooseMostSuitableAnalysisTool \sqsubseteq$ AnalysisReliability $\wedge$
satisfiedBy(''awk -F '{print $19}' firewall_log | sort | uniq -wc -l'',
search_for_total_number_of_unique_source_IP_addresses)

$\mathcal{KB} \models ChooseMostSuitableAnalysisTool \wedge$
$ChooseMostSuitableAnalysisTool($
''awk -F '{print $20}' firewall_log | sort | uniq -wc -l''),
$ChooseMostSuitableAnalysisTool \sqsubseteq$ AnalysisReliability $\wedge$
satisfiedBy
(''awk -F '{print $20}' firewall_log | sort | uniq -wc -l'',
search_for_total_number_of_unique_destination_IP_addresses)

$\mathcal{KB} \models UseReliableKnowledgeShareServices \wedge$
$UseReliableKnowledgeShareServices($
$MISP\_database$),
$UseReliableKnowledgeShareServices \sqsubseteq$ AnalysisReliability $\wedge$
satisfiedBy ($MISP\_database$, search_for_suspicious_IP_addresses)

Да би се задовољио захтев довољности, систем форензичару предлаже да узме у обзир друге сервисе за дељење знања о инцидентима у информационој безбедности, као што су HELK [16] и CHIRON ELK [17]. Тиме би био задовољен и захтев за репродукцију, који може подразумевати да се помоћу других алата дође до истих закључака.

$\mathcal{KB} \models AnalysisSufficiency$,
$AnalysisSufficiency \sqsubseteq$ AnalysisSoundnessRequirement

[16] https://github.com/Cyb3rWard0g/HELK
[17] https://github.com/jzadeh/chiron-elk

$\mathcal{KB} \models AnalyseSufficientMaterial \wedge$
$AnalyseSufficientMaterial($
$take\_into\_account\_many\_knowledge\_sharing\_services,$
$AnalyseSufficientMaterial \sqsubseteq$ `AnalysisReliability` $\wedge$
`satisfiedBy`
$(take\_into\_account\_many\_knowledge\_sharing\_services$
`search_for_suspicious_IP_addresses`)

$\mathcal{KB} \models AnalysisReproducibility,$
$AnalysisReproducibility \sqsubseteq$ `AnalysisSoundnessRequirement`

$\mathcal{KB} \models AnalyseUsingToolsWithSameFunctions \wedge$
$AnalyseUsingToolsWithSameFunctions($
$analysis\_with\_MISP\_alternatives,$
$AnalyseUsingToolsWithSameFunctions \sqsubseteq$ `AnalysisReproducibility` $\wedge$
`satisfiedBy` $(\{HELK, CHIRONELK\},$
`analysis_with_MISP_alternatives`)

Даље систем налаже да се у оквиру анализе лог-датотека сервиса-посредника Squid провери постојање сумњивих локатора ресурса (енг. *Uniform Resource Locator, URL*).

$\mathcal{KB} \models ChooseMostSuitableAnalysisTool \wedge$
$ChooseMostSuitableAnalysisTool($
$grep\_ < suspecious\_URL > \_access.log),$
$ChooseMostSuitableAnalysisTool \sqsubseteq$ `AnalysisReliability` $\wedge$
`satisfiedBy`
$(grep\_ < suspecious\_URL > \_access.log$
`search_for_suspicious_urls`)

Захтев за поновљивост налаже да се омогући другом форензичару да спроведе анализу лог-датотека безбедносног софтвера pfSense Firewall и сервиса-посредника Squid и да дође до истих резултата као и форензичар који је пре њега спровео анализу.

$\mathcal{KB} \models AnalysisRepeatability,$
$AnalysisRepeatability \sqsubseteq$ `AnalysisSoundnessRequirement`

$\mathcal{KB} \models RepeatingAnalysisByAnotherInvestigator \wedge$
$RepeatingAnalysisByAnotherInvestigator($
$pfsense\_log\_analysis, squid\_log\_analysis,$
$RepeatingAnalysisByAnotherInvestigator \sqsubseteq$ `AnalysisRepeatability` $\wedge$
`satisfiedBy` $(repeating\_log\_analysis\_by\_another\_investigator,$
`pfsense_log_analysis, squid_log_analysis`)

На крају, информације које су кључне за решење овог случаја, а које могу

бити изведене из лог-датотека и базе података MISP су изворне и одредишне IP адресе сумњивих мрежних конекција и протокола, као и информације о ресурсима који су били предмет цурења података, у овом случају то представљају имена датотека које су „процурele" из компанијске базе података.

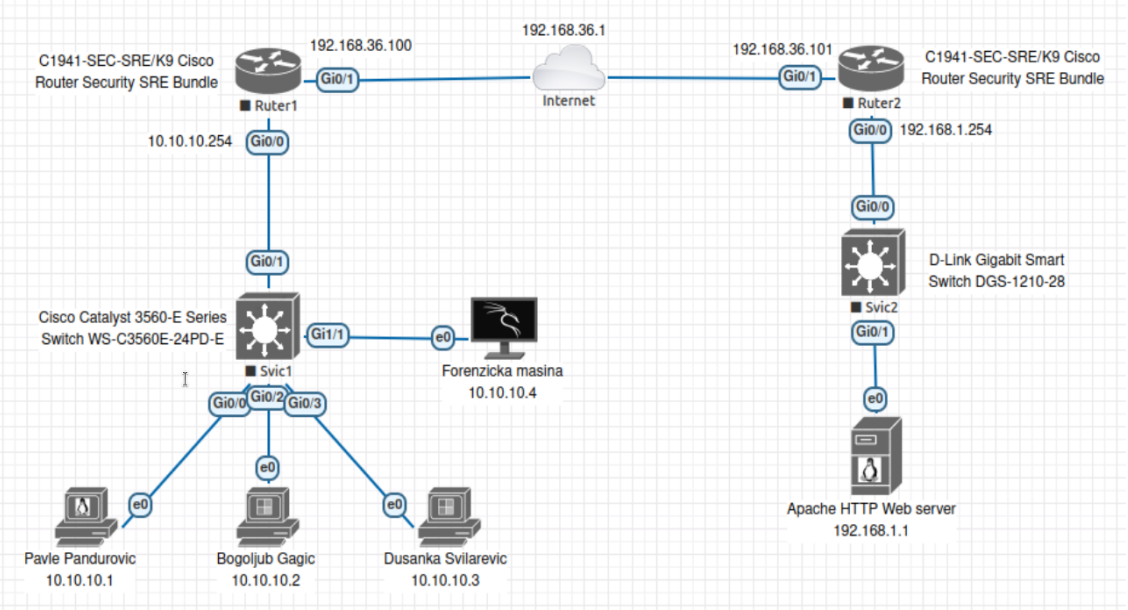
5.6 Демонстрација система

Илустрација употребе система дата је у овом одељку кроз решавање једног случаја, односно кроз спровођење једне форензичке истраге. Задаци поменуте форензичке истраге везани су за област рачунарских мрежа и укључују прикупљање мрежног саобраћаја конфигурисањем SPAN порта [18], анализу мрежног саобраћаја, прикупљање и анализу логова сервиса NAT [19] који је конфигурисан на рутеру и конфигурацију и анализу логова приступа веб-серверу. У наставку следи детаљан навод задатака:

1. Анализирати мрежни саобраћај приватне мреже предузећа, чија је IP адреса 10.10.10.0 (слика 14) и изјаснити се да ли је са рачунара приватне мреже приступано веб-сајту домена „domen.com" и, ако јесте, са ког рачунара и када.

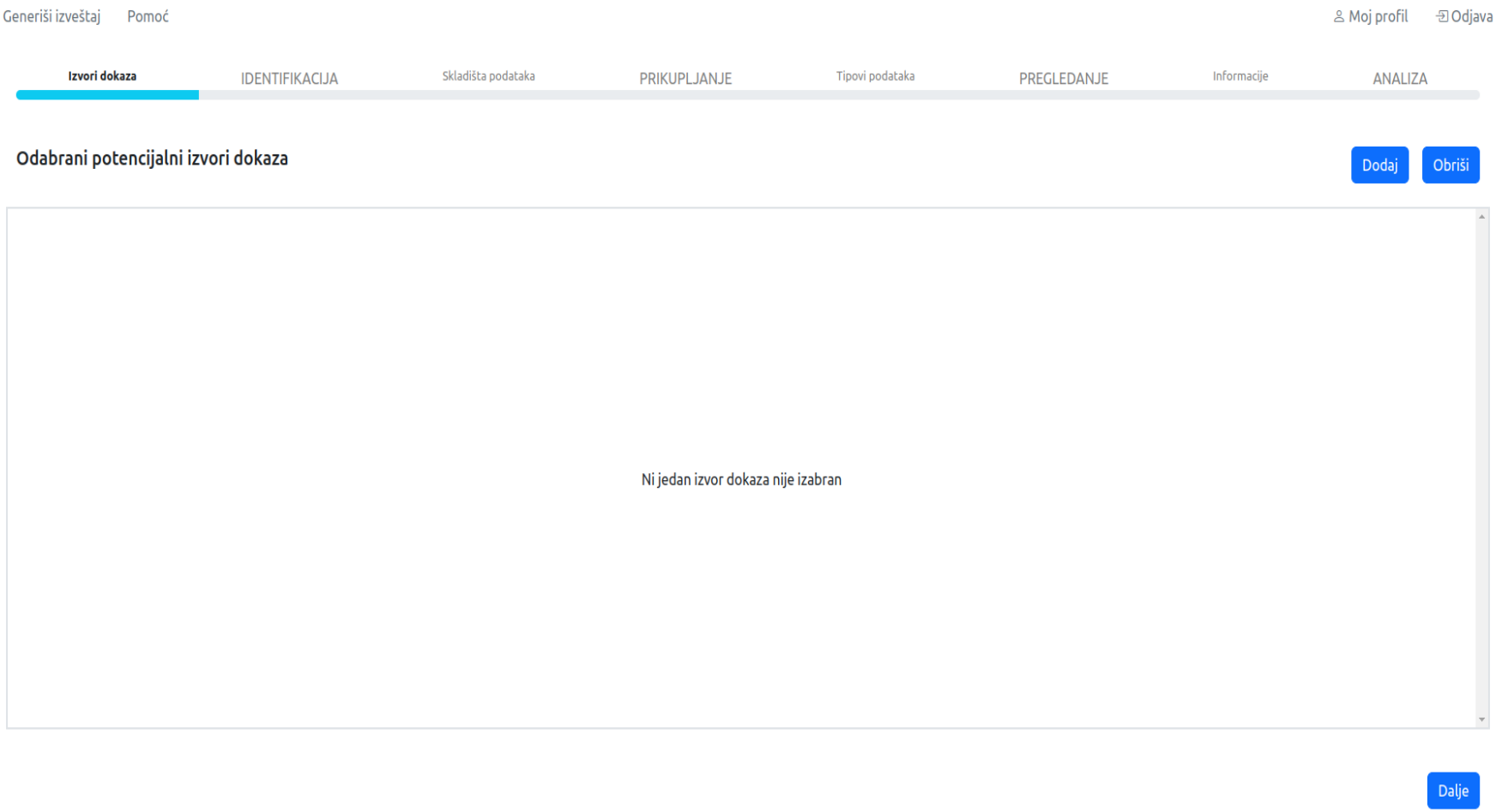
2. Потом се изјаснити у погледу приступања Apache HTTP веб-серверу са шеме топологије рачунарске мреже – да ли му је приступано са рачунара који не би требало да имају приступ веб-серверу (нико осим Богољуба Гагића не би требало да има приступ), а ако јесте, изјаснити се да ли је од сервера успешно добављен тражени ресурс. При томе користити лог приступања поменутом веб-серверу и потребне логове мрежних уређаја приватне мреже предузећа.

[18] https://www.cisco.com/c/en/us/td/docs/switches/lan/ catalyst_pon/software/configuration_guide/olt_ntw/b-gpon-config-olt-network/configuring_port_mirroring.pdf
[19] https://datatracker.ietf.org/doc/html/rfc2663



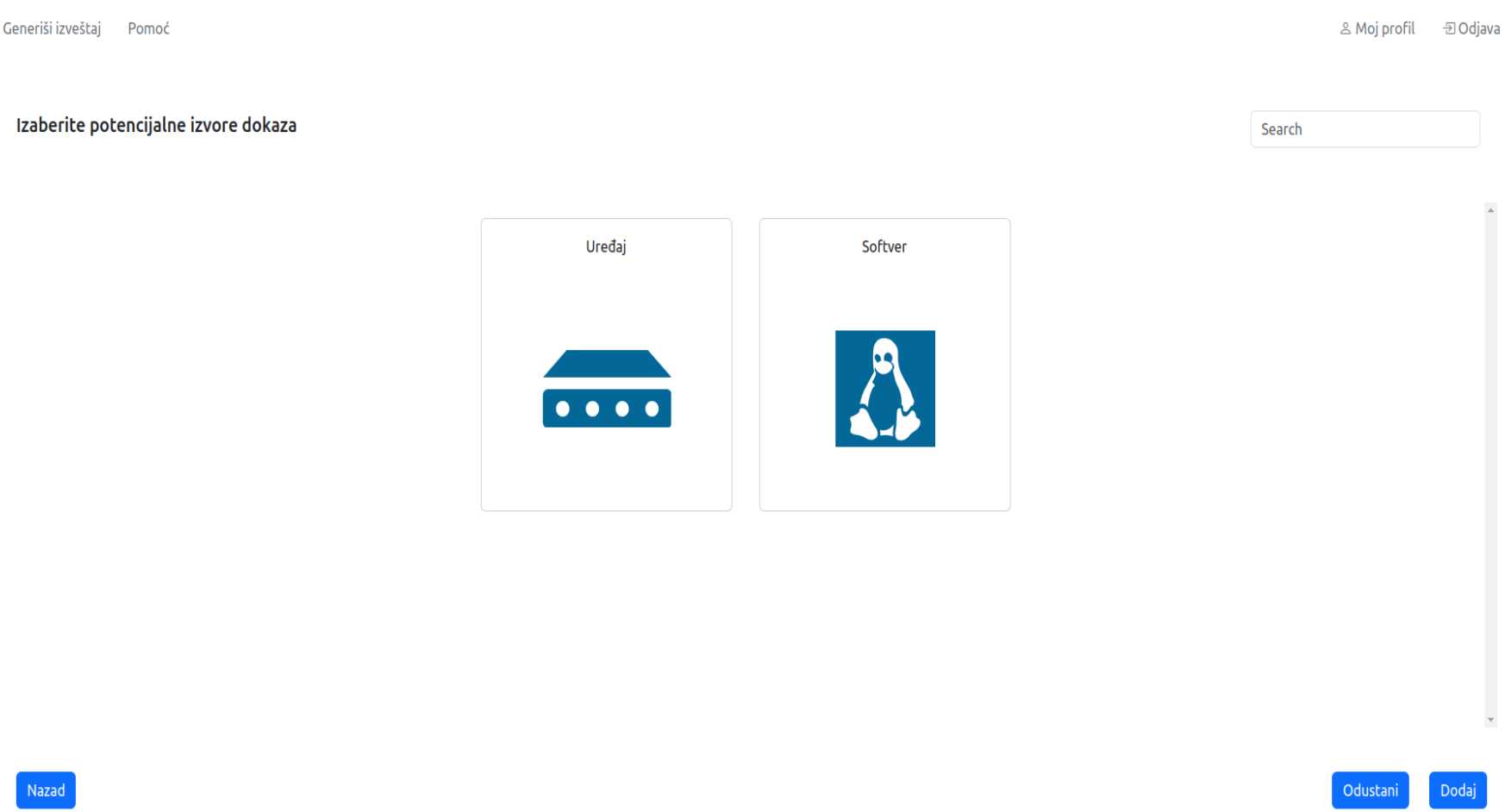
Слика 14: Шема топологије рачунарске мреже.

Употреба апликације започиње одабиром постојећег случаја или креирањем новог наводећи назив случаја. Уколико у оквиру постојећег случаја не постоје одабрани потенцијални извори доказа или уколико је креиран нови случај, кориснику се приказује одговарајућа порука (слика 15).



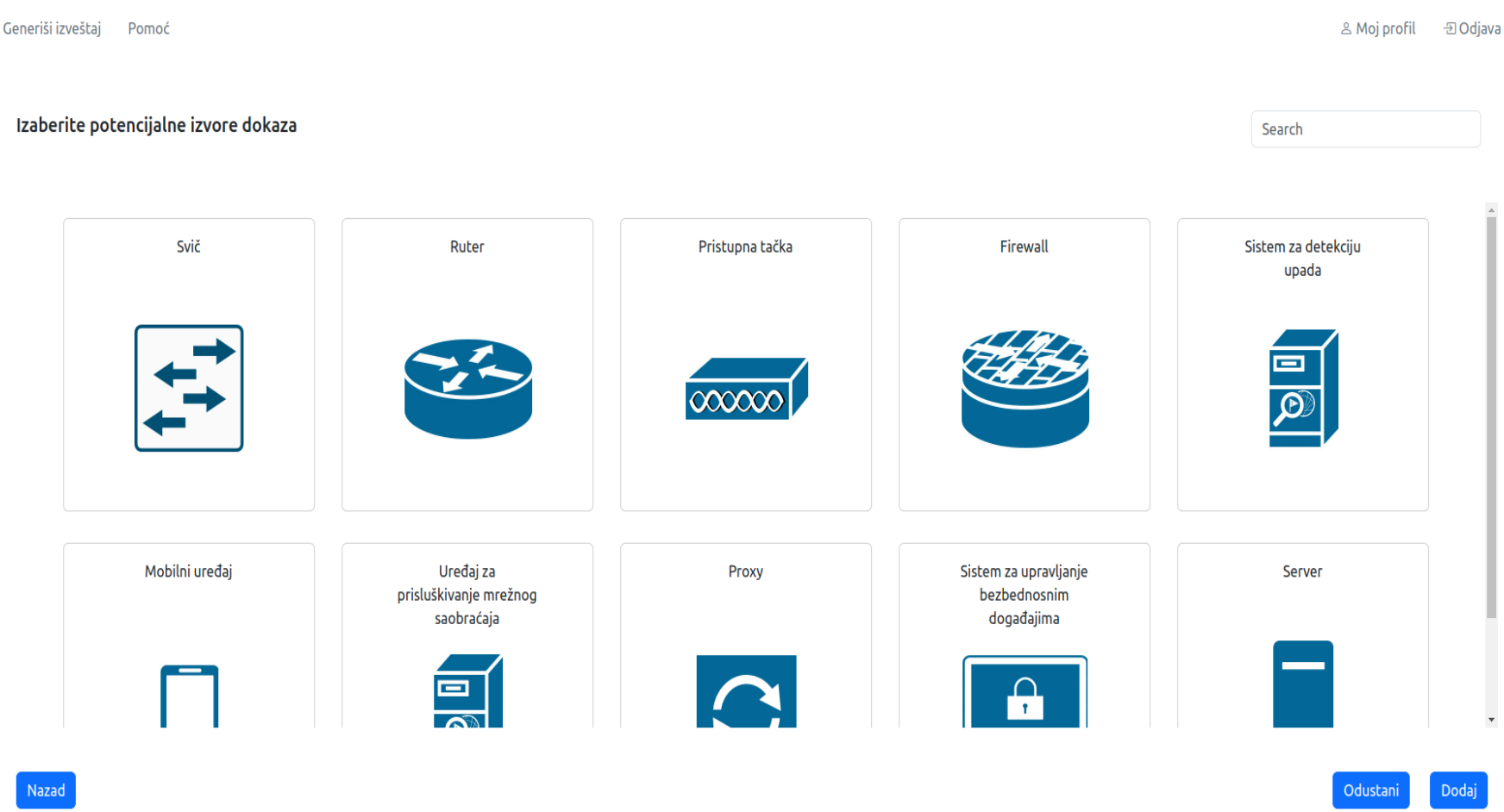
Слика 15: Порука кориснику уколико не постоје одабрани потенцијални извори доказа.

Одабир потенцијалних извора доказа започиње активацијом дугмета „Додај”, што доводи до странице са пољем за претрагу и указатељима на главне категорије потенцијалних извора доказа – уређај и софтвер (слика 16).



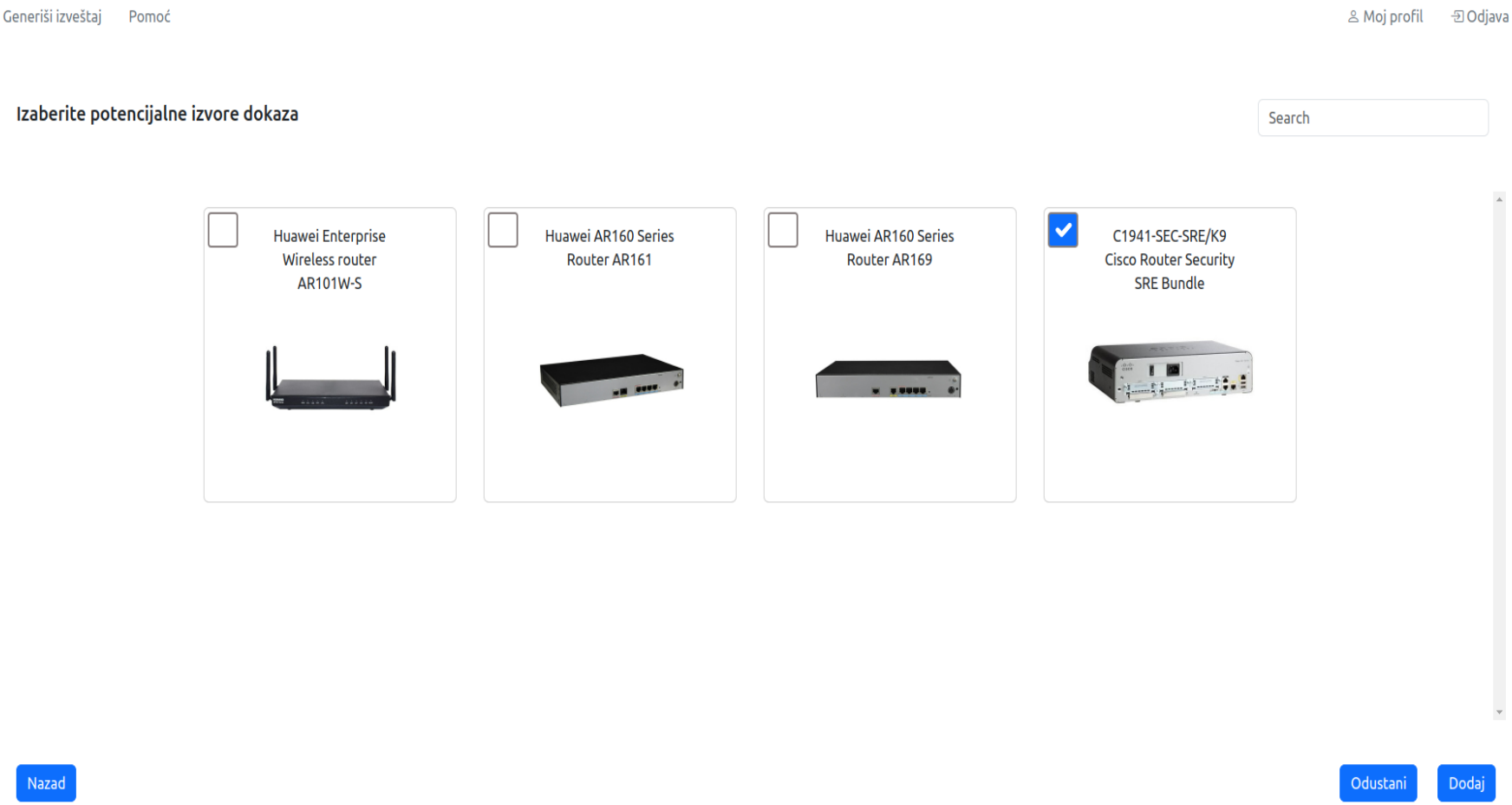
Слика 16: Приказ главних категорија извора доказа.

Категорије се даље продубљују, па тако одабиром категорије Уређај, корисник добија увид у поткатегорије (слика 17).



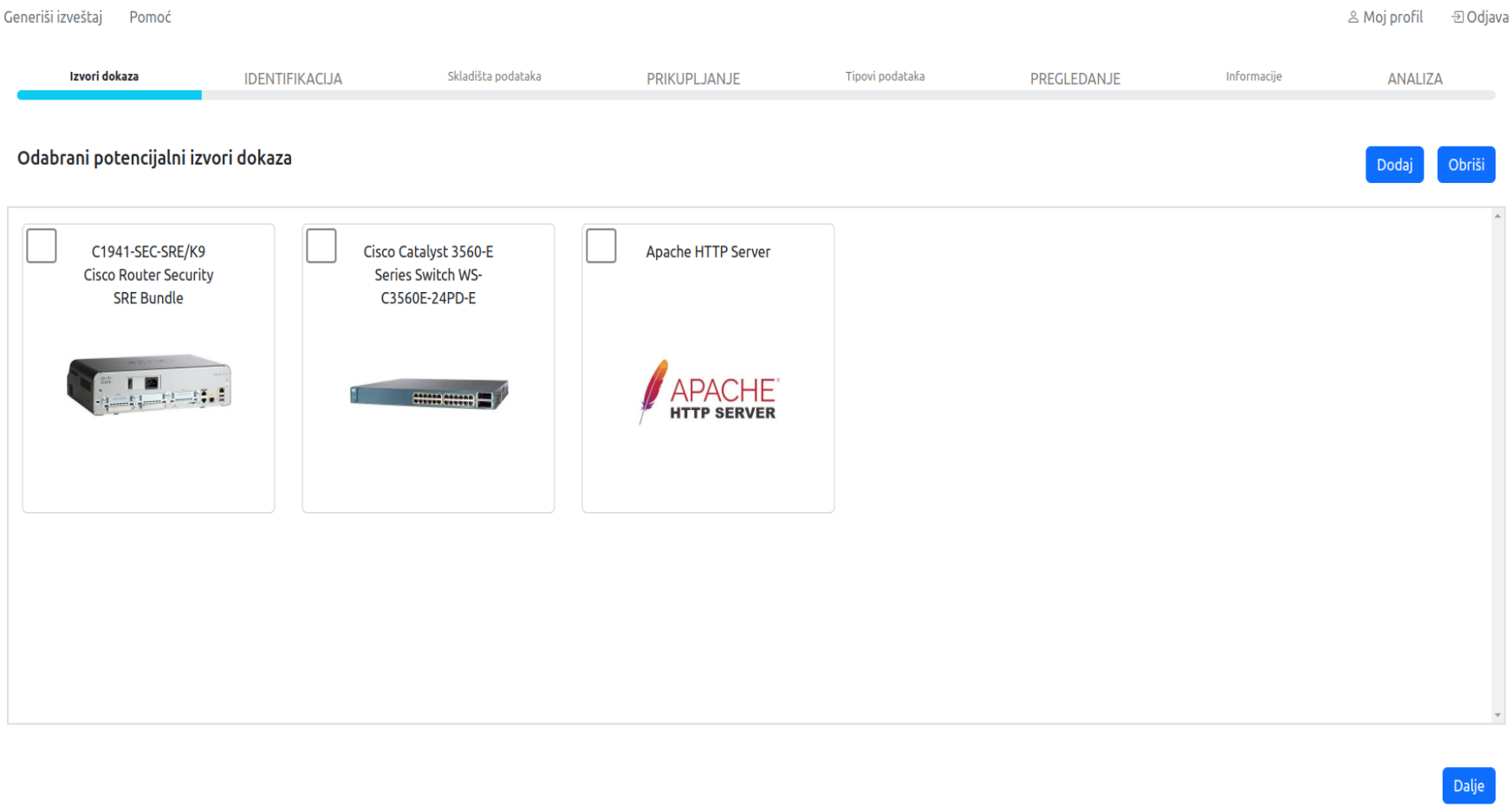
Слика 17: Приказ поткатегорија категорије Уређај.

Након одабира крајње поткатегорије, као што је на пример категорија Рутер, кориснику се приказују конкретни модели који припадају датој поткатегорији, а који се налазе у бази података система. На слици 18 приказани су модели рутера. Тада је корисник у могућности да одабере више уређаја који су релевантни за дати случај.



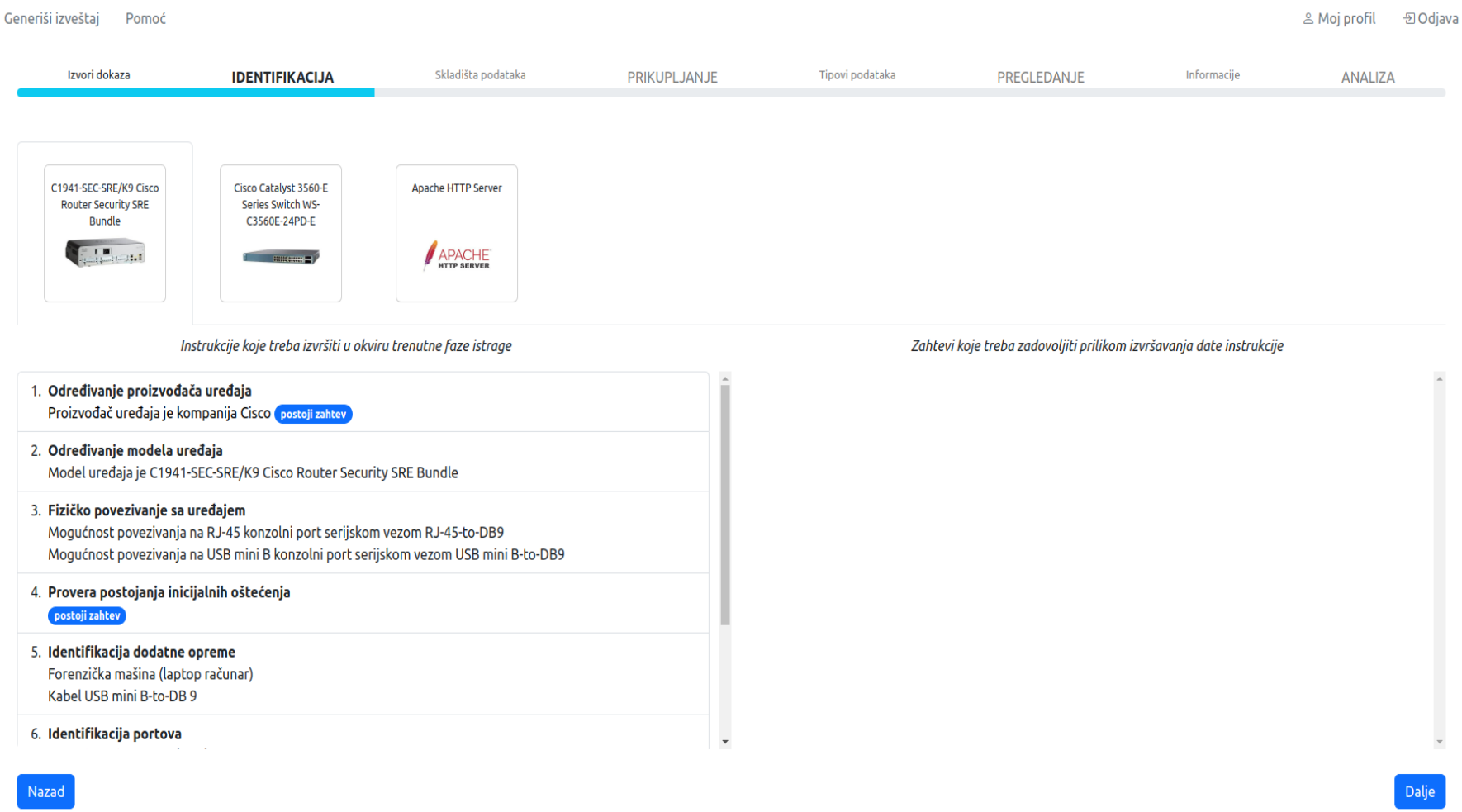
Слика 18: Модели рутера складиштени у бази података.

На исти начин, корисник бира припаднике других поткатегорија, док свом случају не придружи све релевантне изворе доказа. Тада се приказује страница која садржи одабране изворе доказа и омогућава наставак употребе апликације активацијом дугмета „Даље” (слика 19).

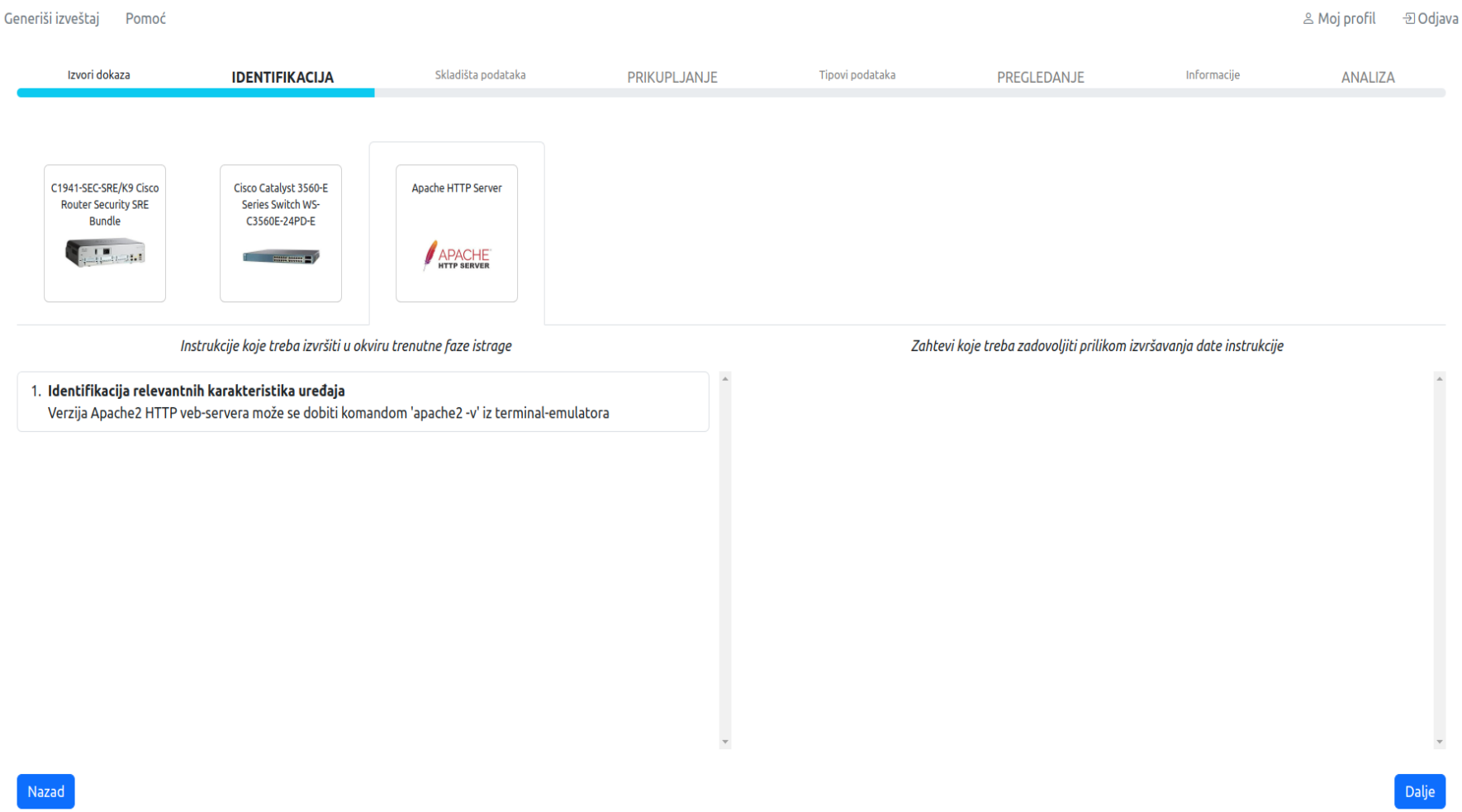


Слика 19: Одабрани потенцијални извори доказа.

Овим започиње фаза идентификације, што се кориснику и даје на увид линијом напретка у горњем делу странице апликације. Поред тога, у табове су распоређени одабрани потенцијални извори доказа, чијим активирањем се добија увид у инструкције за спровођење фазе идентификације. На пример, сликом 20 илустрован је случај одабира рутера Cisco C1941-SEC-SRE/K9 за који је неопходно очитати информације као што су произвођач, модел и серијски број. Затим су дате инструкције за повезивање са овим рутером у складу са интерфејсима које поседује, итд. Уколико је одабрани потенцијални извор доказа, софтвер, као у овом случају Apache HTTP веб-сервер, инструкција идентификације његових релевантних карактеристика садржи упутство за долазак до ових информација. У овом случају, до верзије софтвера помоћу алата командне линије (слика 21).

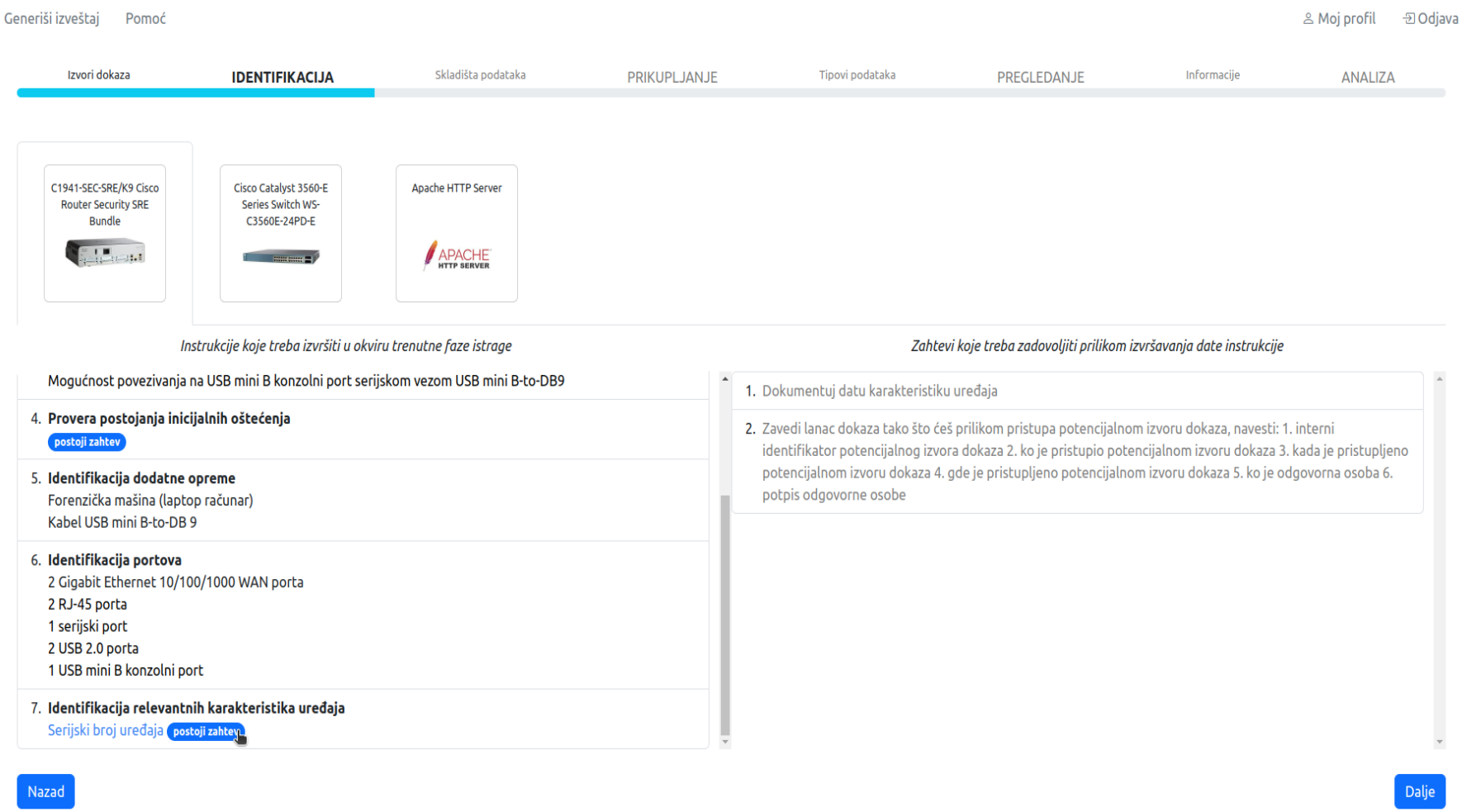


Слика 20: Приказ инструкција за спровођење фазе идентификације уређаја.



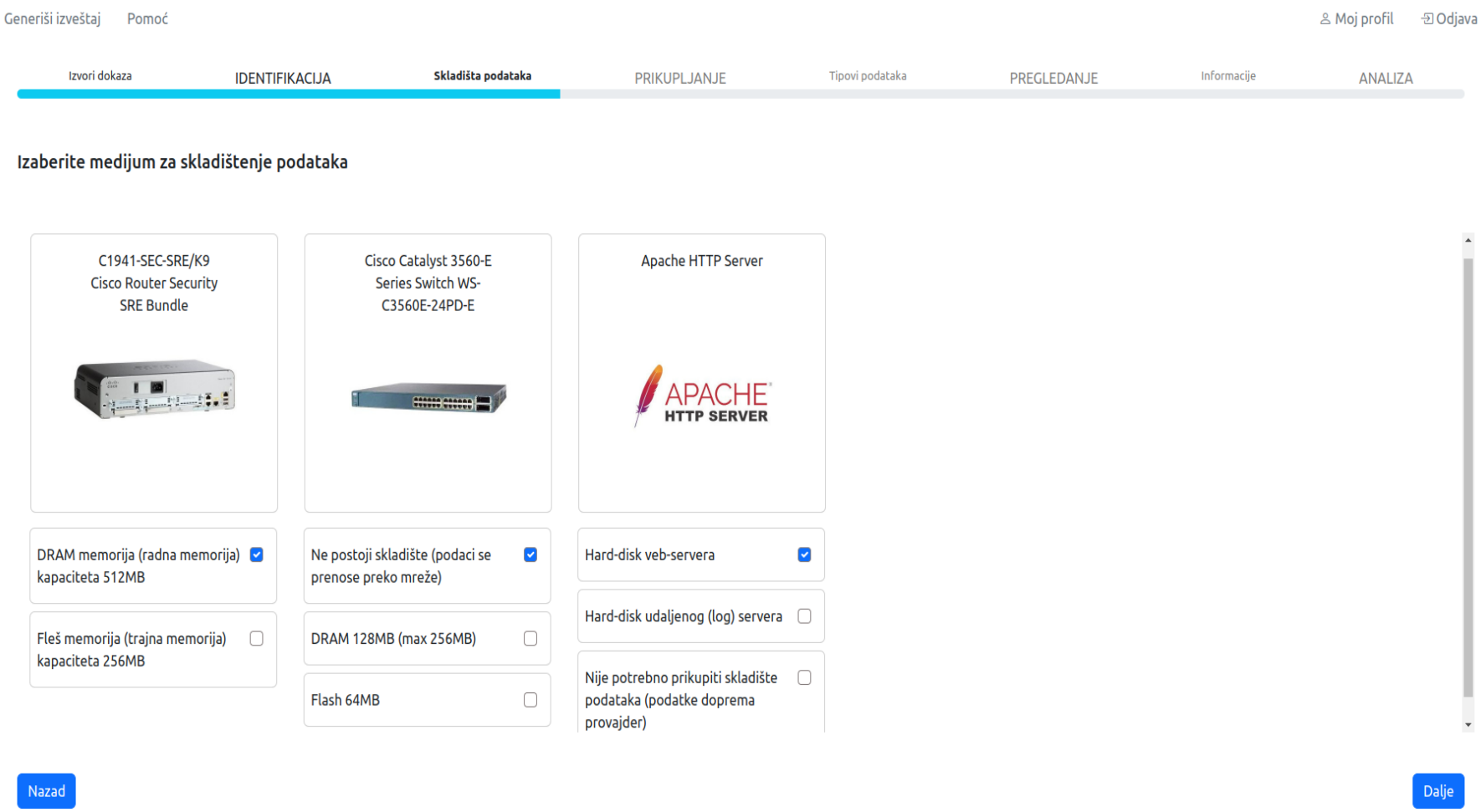
Слика 21: Приказ инструкција за спровођење фазе идентификације софтвера.

Да би истрага била ваљана, спровођење свих фаза мора бити ваљано. Тако поједине инструкције, које су кориснику у претходном кораку приказане, садрже додатне захтеве, односно напомене, на које форензичар треба да обрати пажњу. На пример, инструкција којом се форензичару налаже да у фази идентификације рутера очита његове релевантне карактеристике, садржи ознаку са текстом „постоји захтев". Активацијом инструкције, форензичару се с десна приказују додатне напомене као захтеви ваљаности. У овом случају, то је сугерисање документовања релевантних карактеристика рутера и при томе завођење евиденције руковања рутером, као оригиналним доказним материјалом (слика 22).



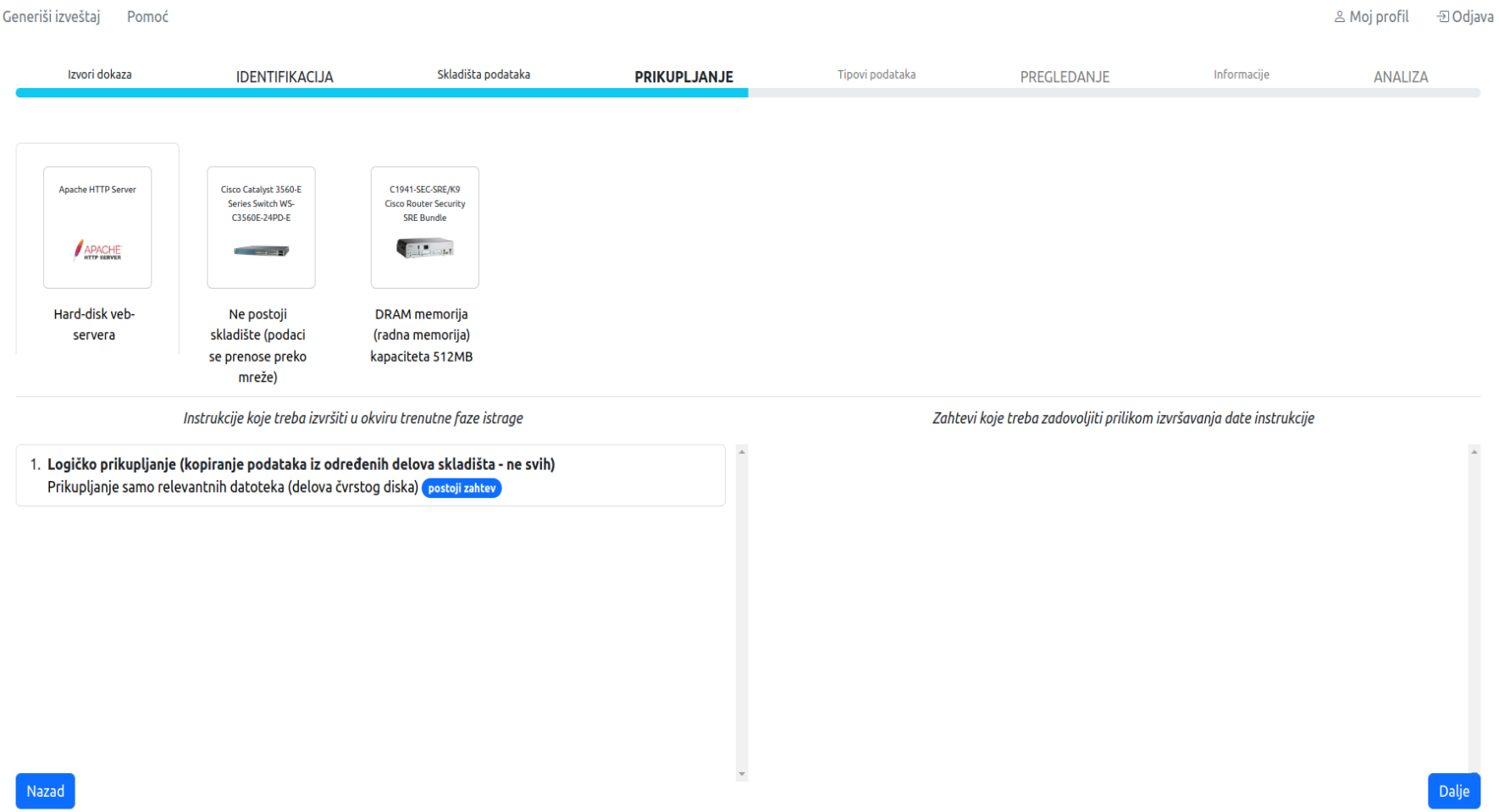
Слика 22: Приказ захтева ваљаности за спровођење инструкција фазе идентификације.

Овим се завршава фаза идентификације у истрази и форензичару се приказује страница са могућношћу одабира врсте складишта података које ће довести до информација потребних за решење случаја, а које се налази у претходно одабраним потенцијалним изворима доказа. У врсте складишта података спадају врсте трајне и оперативне меморије, што се да видети на слици 23.

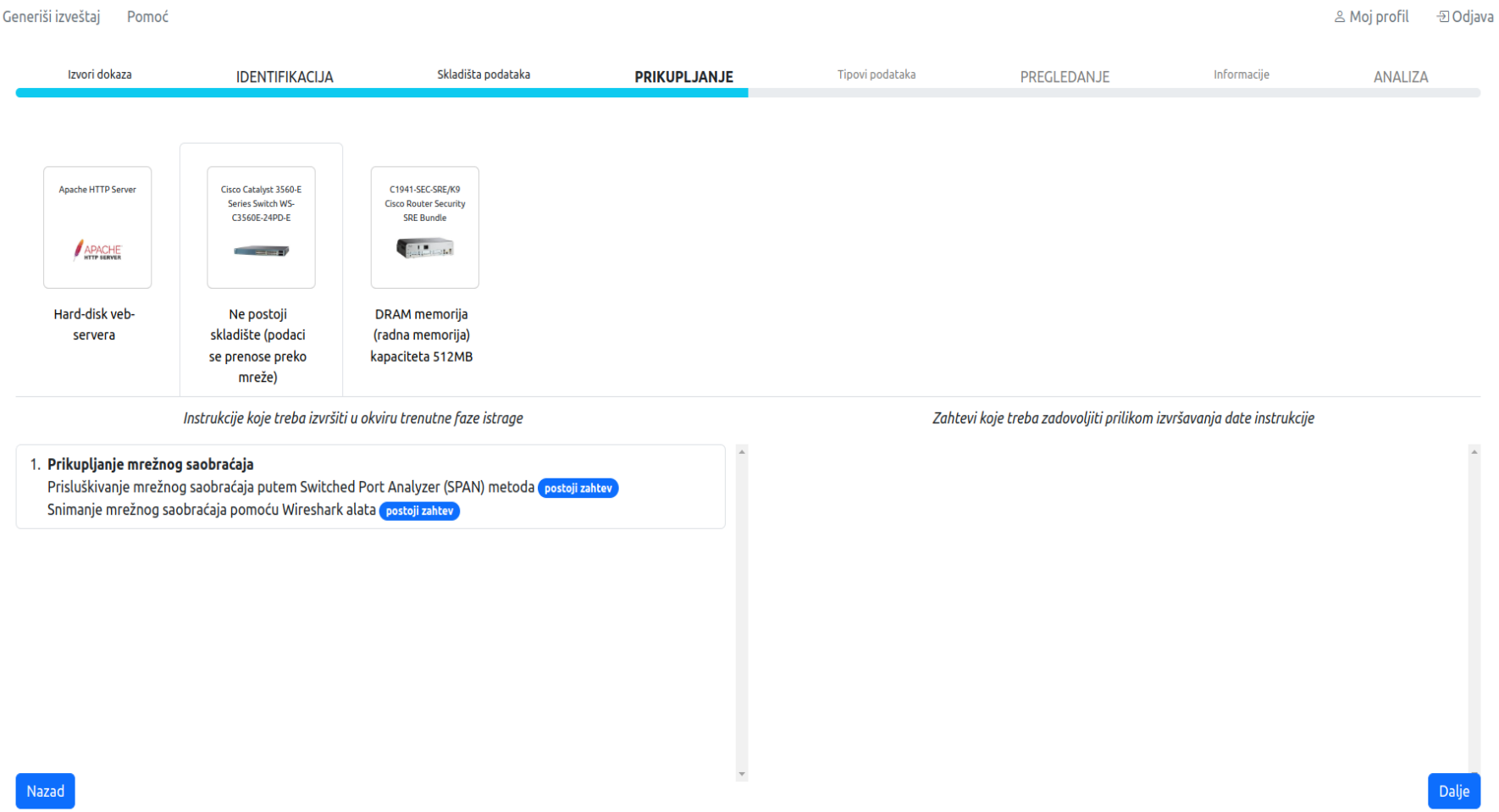


Слика 23: Приказ врста складишта података која се налазе у одабраним изворима доказа.

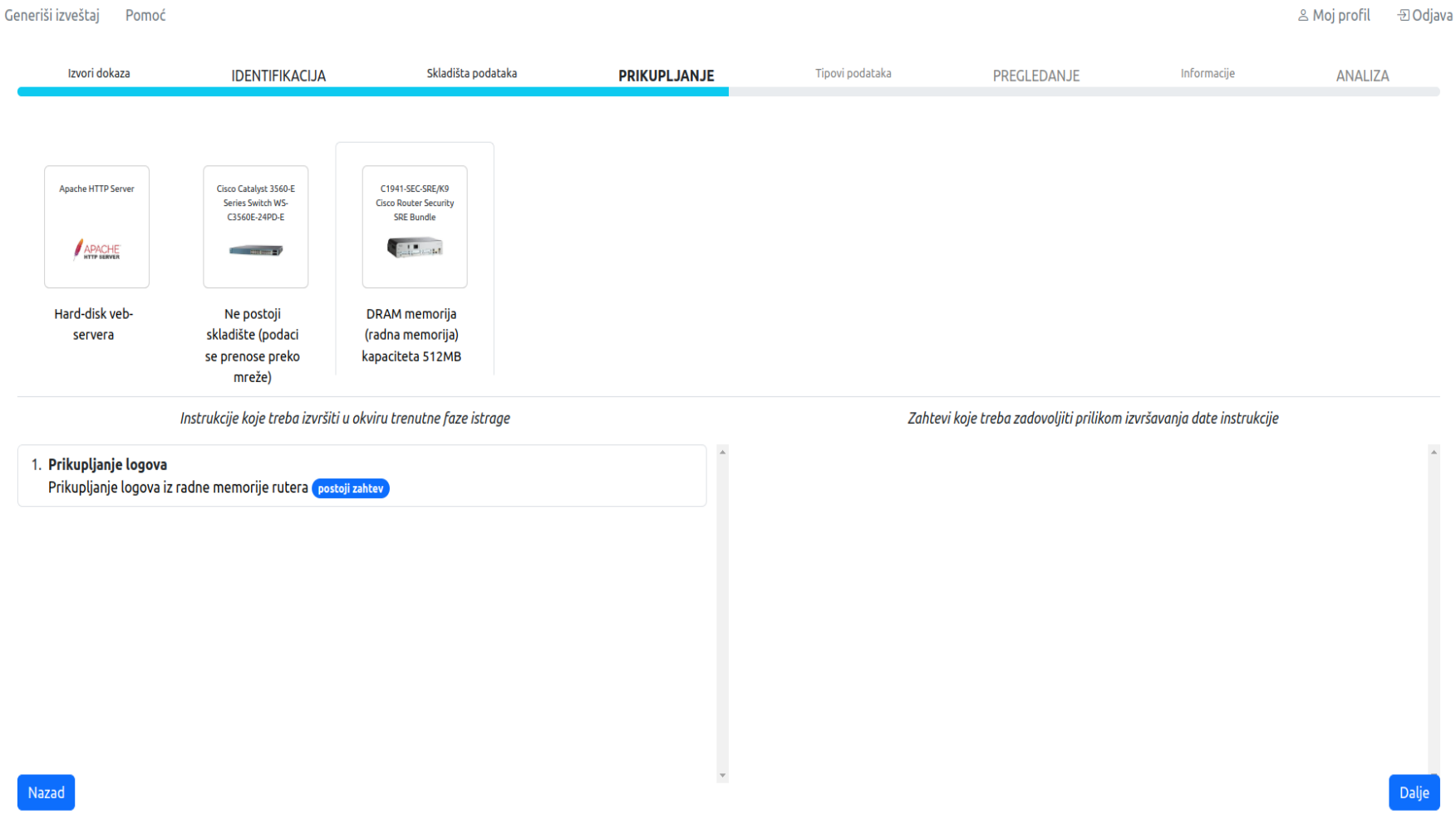
Као и након одабира потенцијалних извора података, када се форензичару приказују инструкције за спровођење фазе идентификације, тако се након одабира релевантних складишта података приказују инструкције за спровођење фазе прикупљања доказа. Форензичару се сугерише да изврши логичко прикупљање са чврстог диска Apache HTTP веб-сервера (слика 24). У вези са одабраним свичем као потенцијалним извором доказа, складиште података је сама мрежа, с обзиром на то да се подаци не складиште на овом уређају, већ се само преносе преко мреже. Форензичару се сугерише начин на који је могуће прикупити, односно снимити мрежни саобраћај (слика 25). На крају се форензичару предлаже прикупљање логова из оперативне меморије одабраног рутера (слика 26).



Слика 24: Приказ инструкција за спровођење фазе прикупљања у случају Apache HTTP веб-сервера.

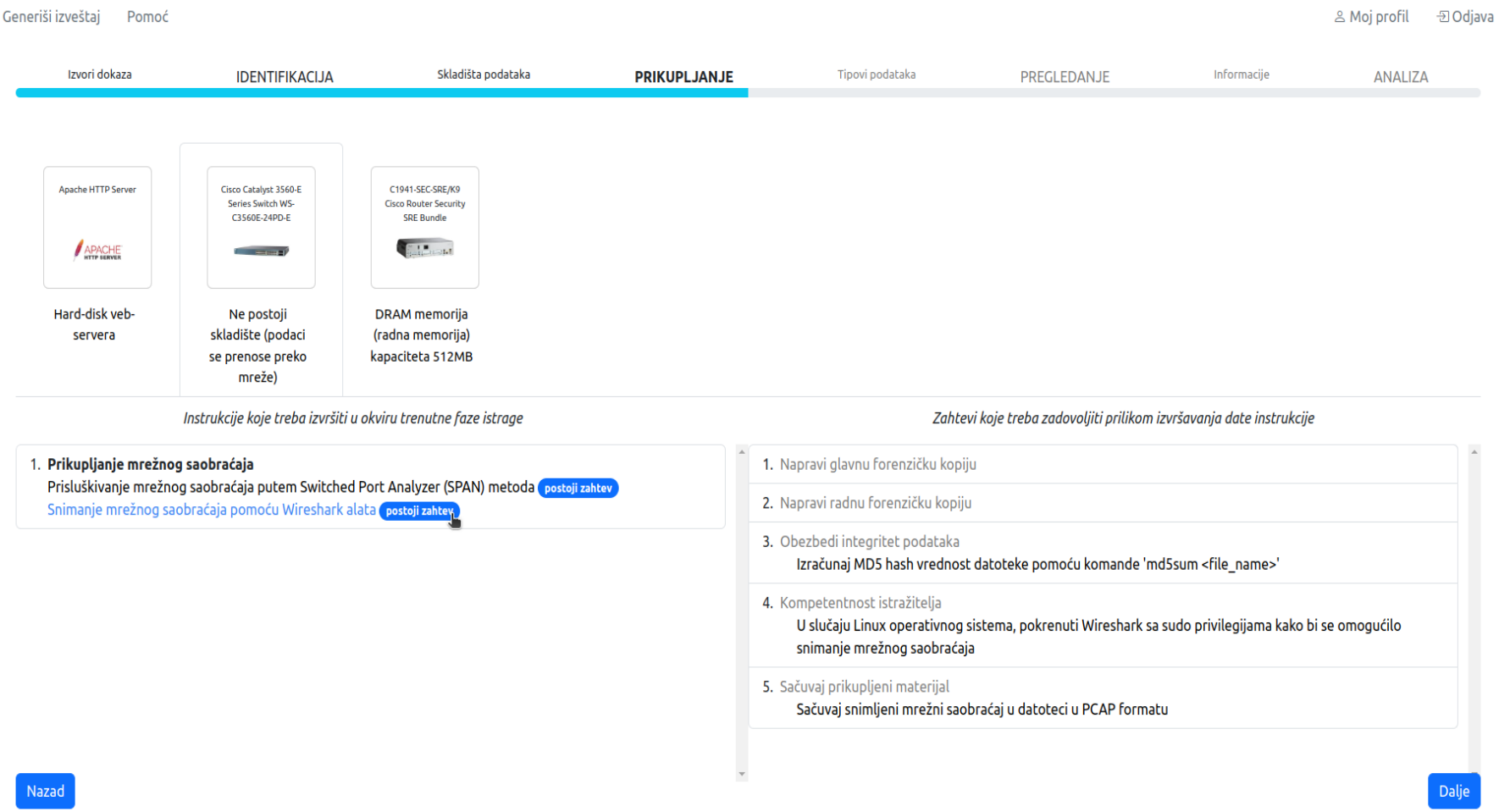


Слика 25: Приказ инструкција за спровођење фазе прикупљања у случају свича.



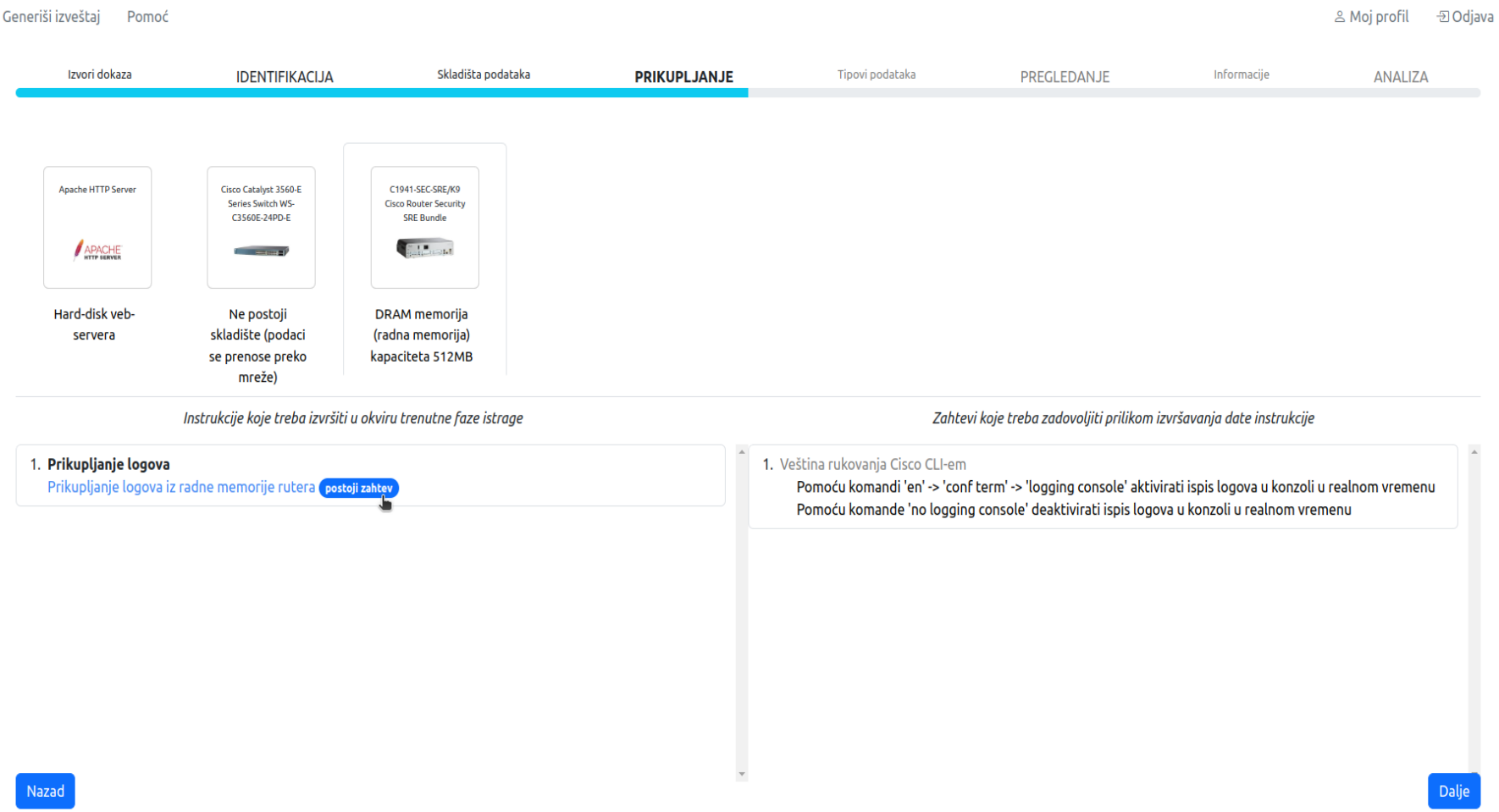
Слика 26: Приказ инструкција за спровођење фазе прикупљања у случају рутера.

Следи приказ захтева ваљаности за приказане инструкције. На пример, за инструкцију којом се форензичару предлаже прикупљање мрежног саобраћаја помоћу алата Wireshark, постоји неколико захтева ваљаности, међу којима су прављење главне и радне форензичке копије снимка мрежног саобраћаја, начин обезбеђивања интегритета података, правилан начин употребе алата предложеног инструкцијом и начин чувања снимка мрежног саобраћаја (слика 27).



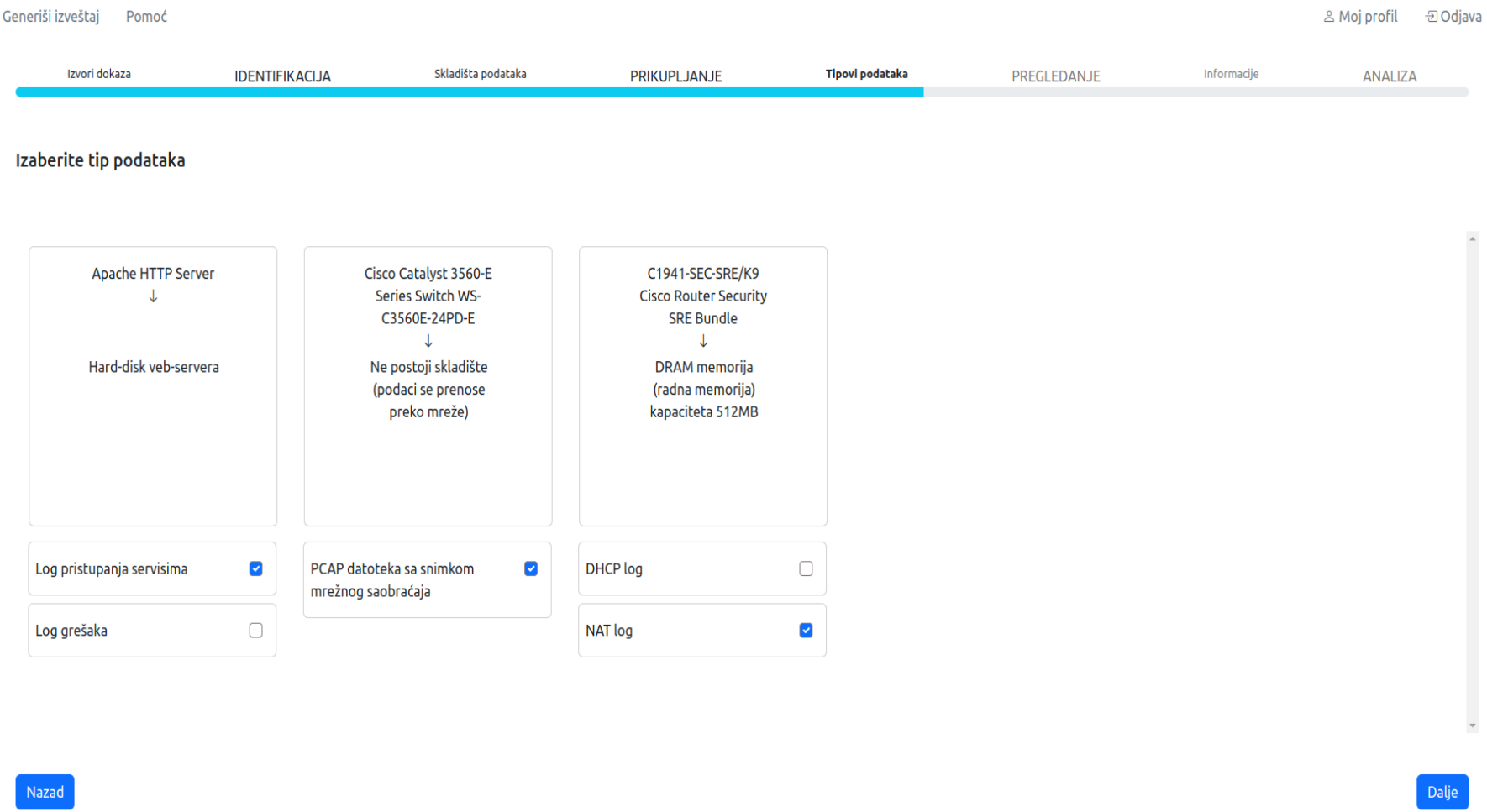
Слика 27: Приказ захтева ваљаности које треба испунити приликом прикупљања мрежног саобраћаја.

У случају прикупљања података из оперативне меморије рутера, форензичару се истиче начин на који је могуће добити увид у садржај логова (слика 28).



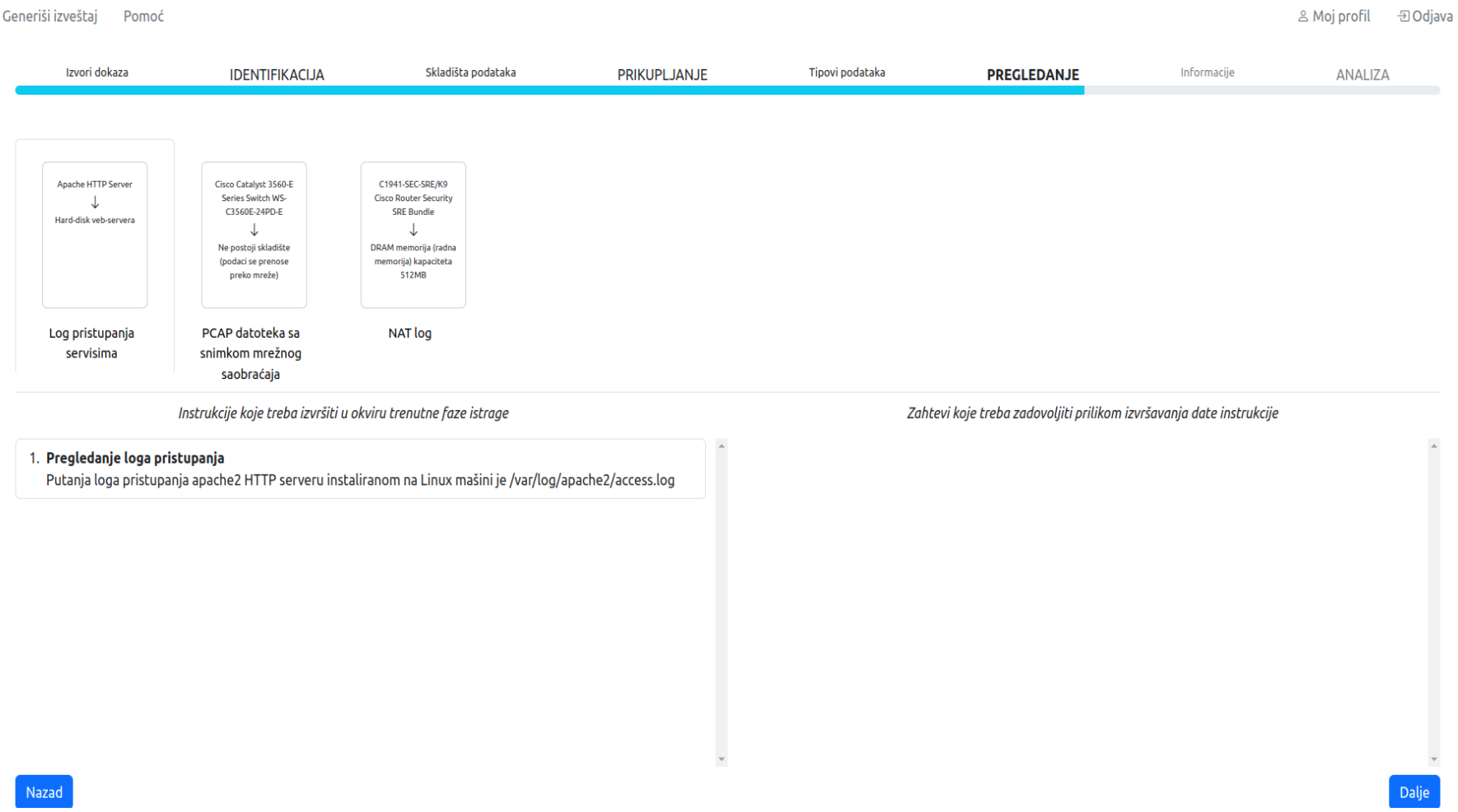
Слика 28: Приказ захтева ваљаности који треба испунити приликом прикупљања логова из радне меморије рутера.

Након фазе прикупљања, следи фаза прегледања доказа чији је предуслов одабир релевантних врста података које се могу наћи у одабраним складиштима података. Тако форензичар, у циљу решења случаја, бира лог приступања који се може наћи на чврстом диску Apache HTTP веб-сервера, датотеку са снимком мрежног саобраћаја који се преноси кроз мрежу чији је део одабрани свич и лог сервиса NAT који се може наћи у оперативној меморији одабраног рутера (слика 29).



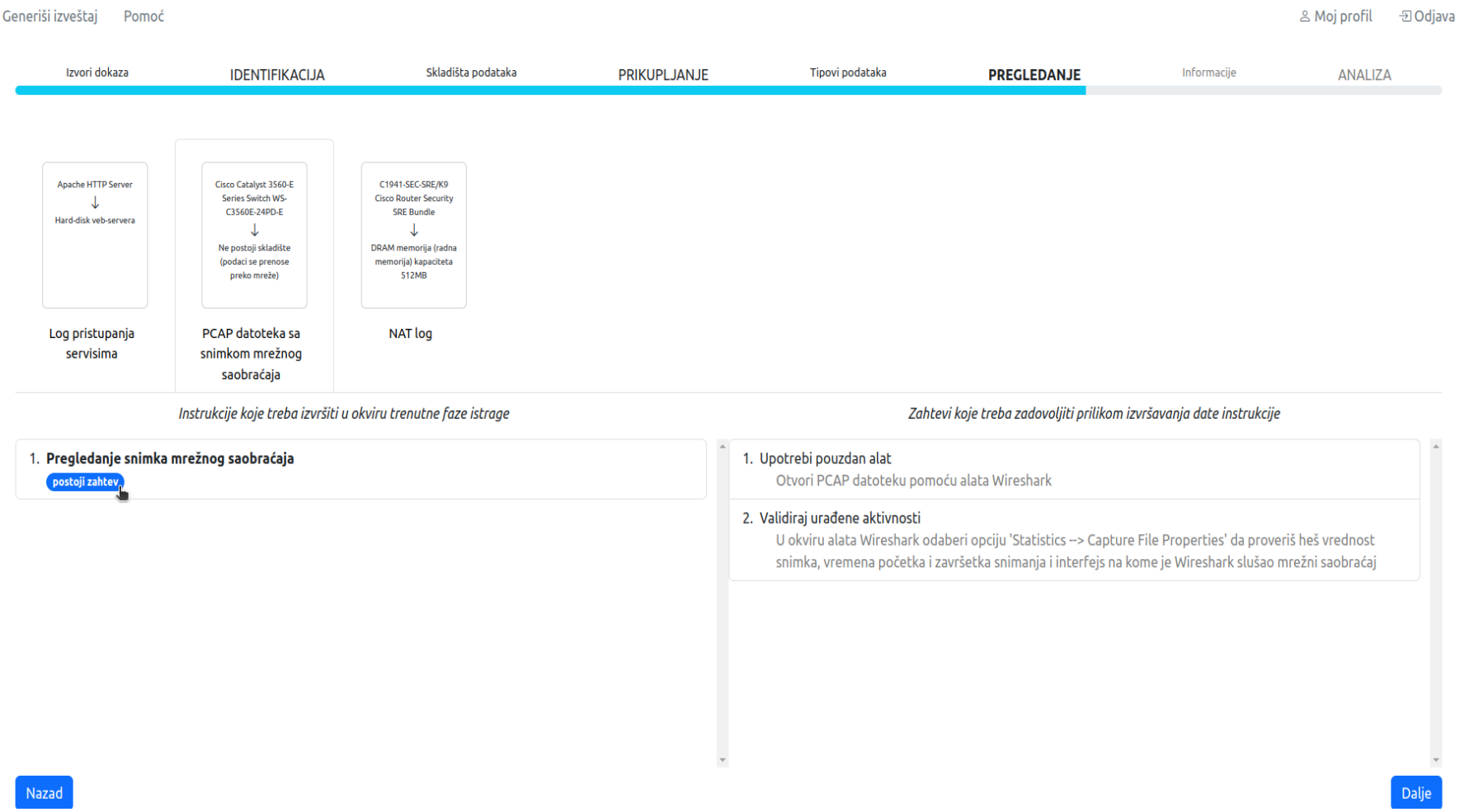
Слика 29: Одабир релевантних врста података који се могу прикупити из складишта података одабраних у претходном кораку.

Као и у претходним фазама спровођења форензичке истраге, форензичару се сада приказују инструкције за спровођење фазе прегледања, као и захтеви ваљаности, уколико постоје, које треба задовољити приликом праћења инструкција. Тако се, на пример, за прегледање лога приступања веб-сервера, форензичару сугерише путања у оквиру система датотека која је везана за лог приступања, уколико је веб-сервер инсталиран на некој од дистрибуција оперативног система Linux (слика 30).

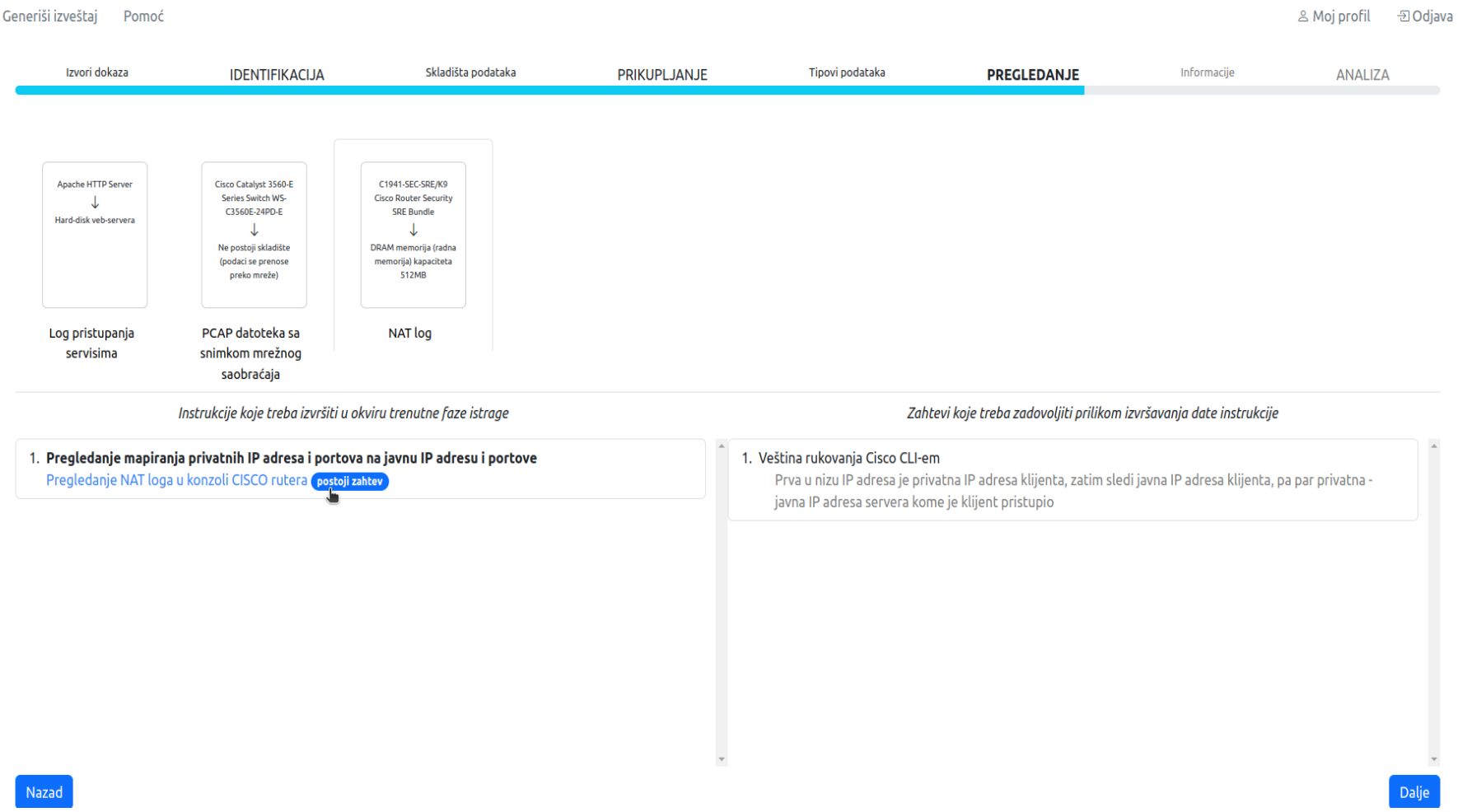


Слика 30: Приказ инструкције за прегледање лога приступања веб-серверу.

Инструкција прегледања снимка мрежног саобраћаја има за себе везан захтев ваљаности који налаже употребу поузданог алата и обезбеђивање валидације снимка мрежног саобраћаја наводећи информације које је неопходно документовати (слика 31). Поред тога, прегледање лога сервиса NAT од форензичара захтева вештину руковања интерфејсом командне линије оперативног система рутера, те апликација помаже у његовом тумачењу објашњењем формата овог лога (слика 32).

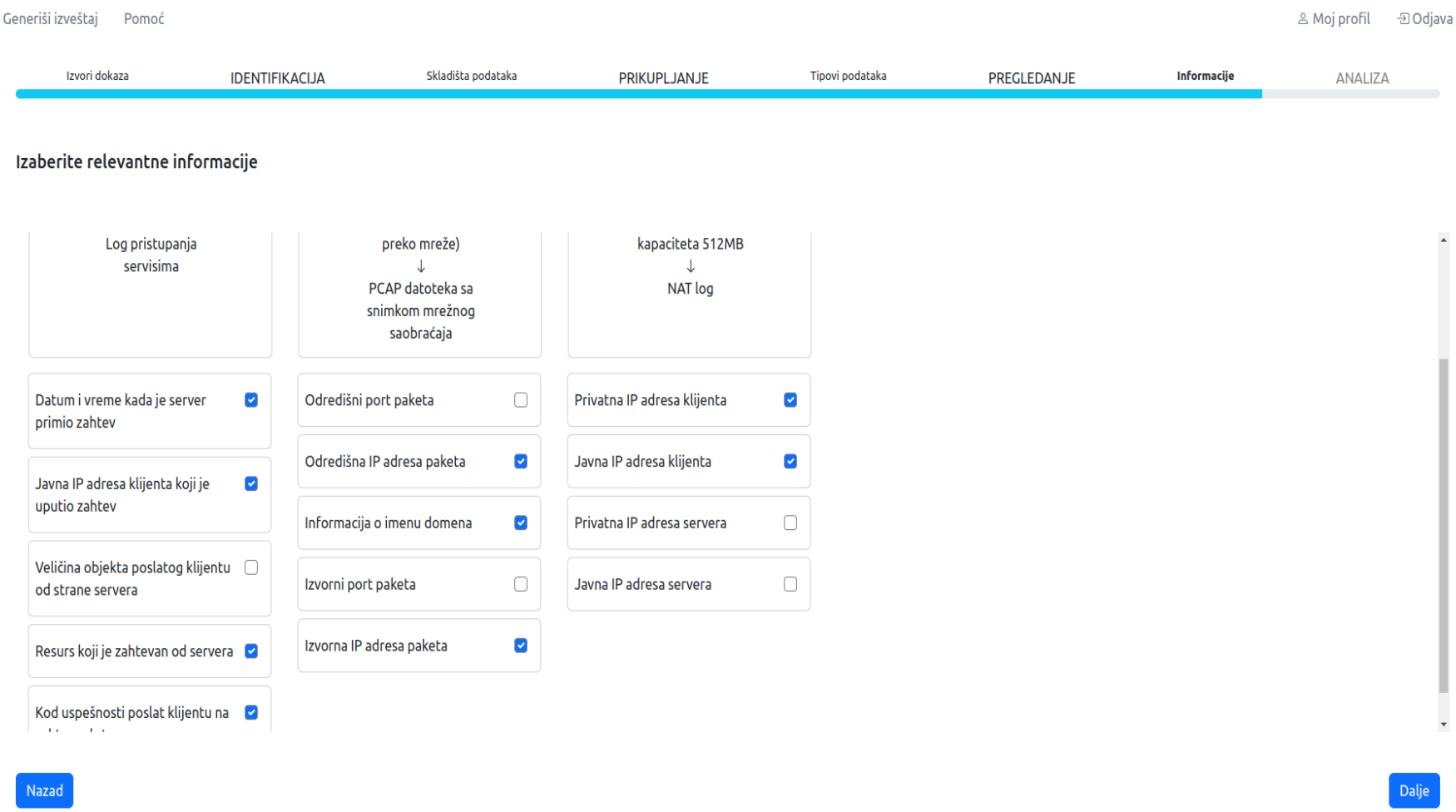


Слика 31: Приказ захтева ваљаности везаног за инструкцију прегледања снимка мрежног саобраћаја.



Слика 32: Приказ захтева вањаности везаног за инструкцију прегледања лога сервиса NAT.

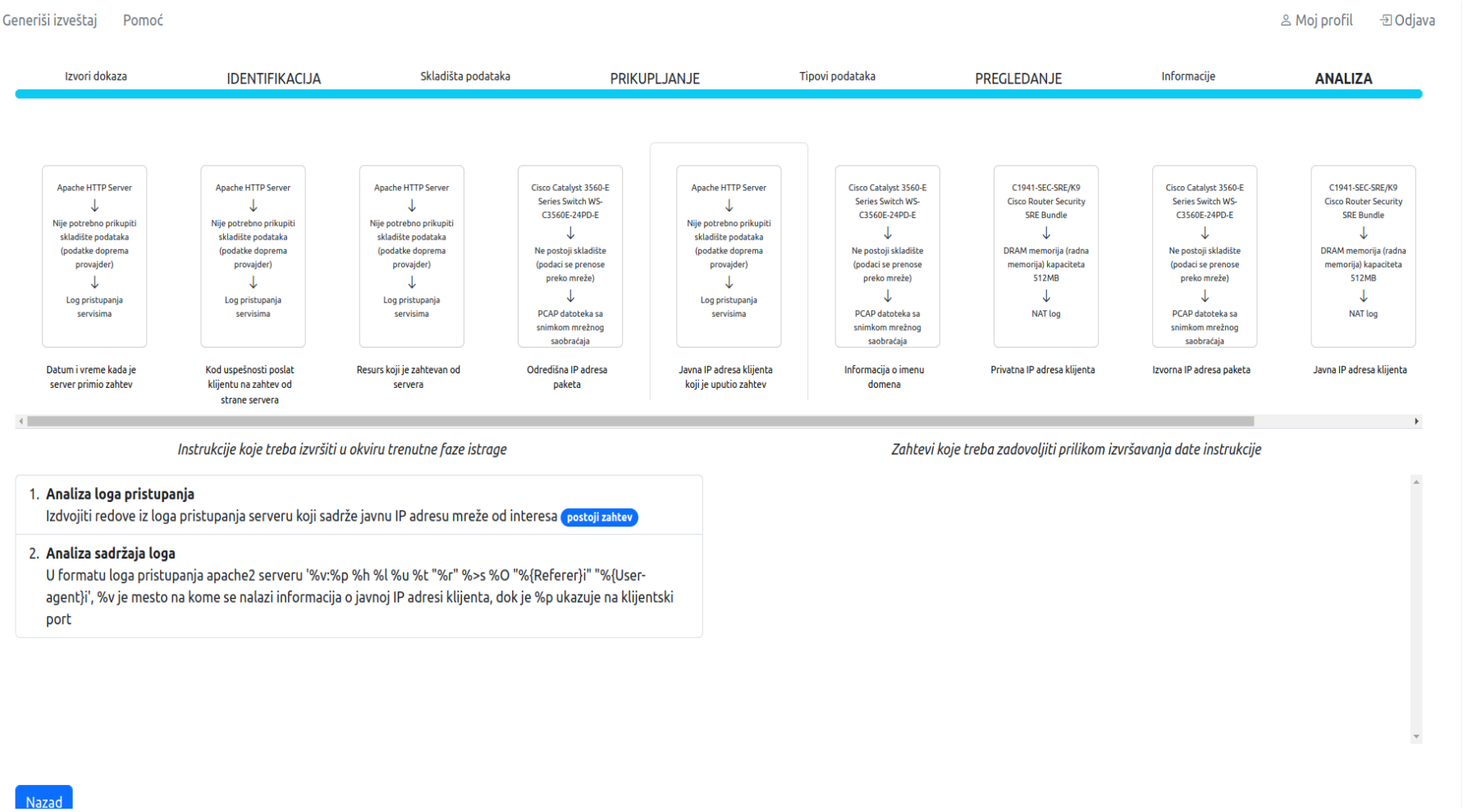
Последња фаза истраге кроз коју апликација води, је анализа доказа. Предуслов за приказ инструкција и захтева ваљаности у овој фази, је да форензичар одабере информације релевантне за свој случај, а које се могу добити из претходно одабраних типова података. Пример овог поступка илустрован је сликом 33.



Слика 33: Одабир релевантних информација.

Инструкције везане за анализу садржаја лога приступања веб-серверу односе се на указивање на његов формат, како би се лог могао протумачити. Стога се, у зависности од одабране информације, форензичару указује на колону у линији лог датотеке која садржи дату информацију (слике 34 и 35).

Слика 34: Инструкција за лоцирање информације о датуму и времену пријема захтева од стране веб-сервера.



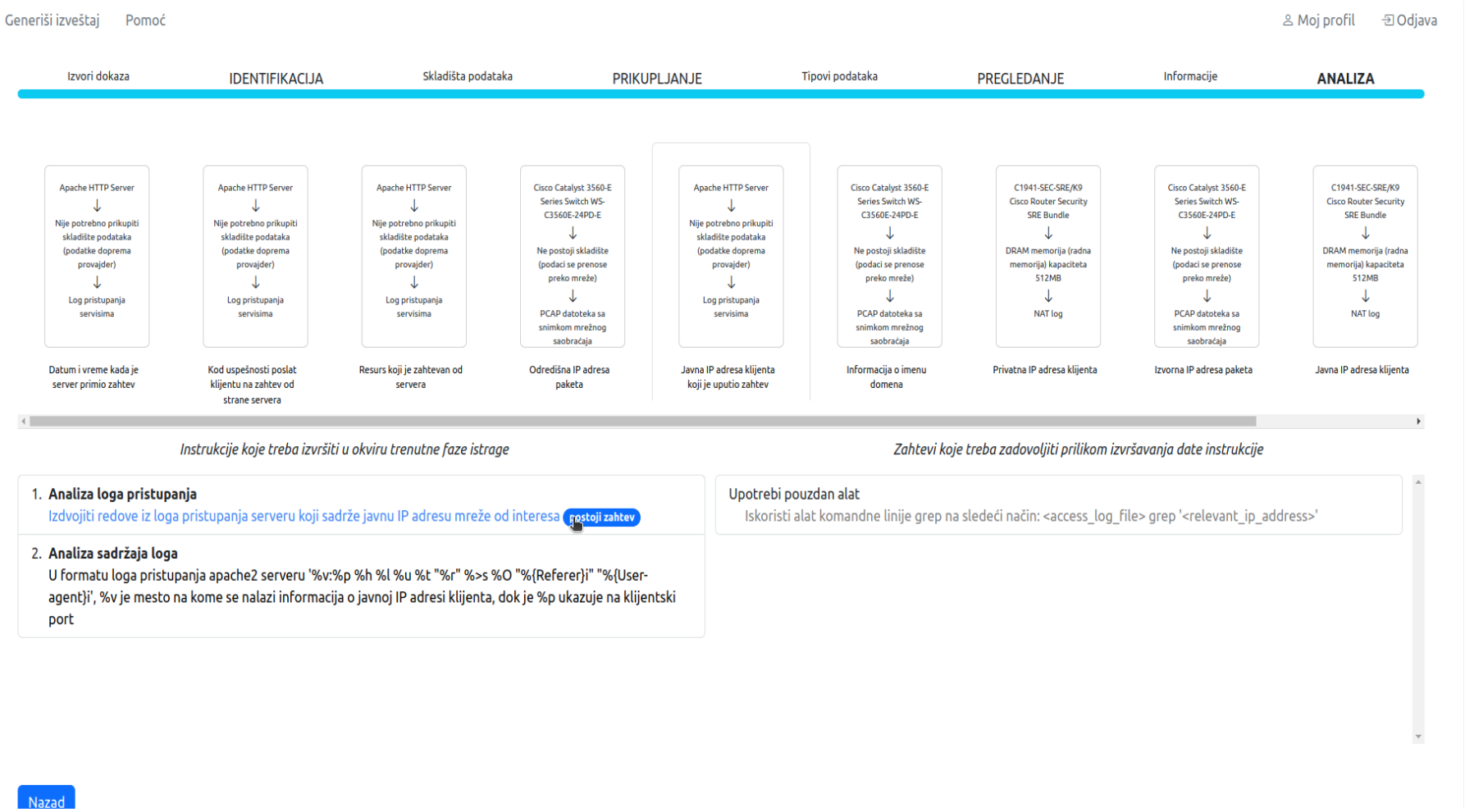
Слика 35: Инструкција за лоцирање информације о јавној IP адреси клијента који је упутио захтев веб-серверу.

Такође, анализу лога сервиса NAT прате инструкције у вези са тумачењем формата овог лога (слике 36 и 37).

Слика 36: Инструкција за лоцирање информације о приватној IP адреси клијента.

Слика 37: Инструкција за лоцирање информације о јавној IP адреси клијента.

На слици 38 приказан је пример захтева ваљаности који налаже начин употребе алата којим је могуће доћи до релевантних информација у логу приступања веб-серверу.



Слика 38: Захтев ваљаности који сугерише начин анализе лога приступања веб-серверу.

5.7 Сажетак

Имплементација истраживања описаног овом дисертацијом обухвата спецификацију захтева, дизајн, пројектовање и имплементацију система који се базира на формалној репрезентацији знања у области форензике рачунарских мрежа.

Спецификација захтева система описана је случајевима коришћења, при чему су они најпре приказани дијаграмом, а потом су изложена њихова сценарија. У оквиру дизајна, структура система представљена је дијаграмом компоненти и дијаграмом распоређивања, док је понашање система описано дијаграмом секвенце и дијаграмом активности. Ове активности представљене су конструктима дескриптивне логике како би се стекао увид у начин расуђивања над базом знања.

Неизоставни делови овога поглавља су студија случаја и демонстрација система. Студијом случаја је конкретизован дијаграм активности увођењем стварног сценарија са детаљима форензичког случаја, чиме се додатно разјашњава представљена идеја. Уз то, демонстрацијом система приказан је ток интеракције са корисником посредством графичког интерфејса.

6 Верификација хипотезе истраживања

6.1 Преглед

Ово поглавље садржи опис поступка верификације хипотезе, односно поступка прикупљања података експериментом и анализу резултата експеримента, што је делом представљено у раду Matijević Gostojić и сар. (2024b).

Поглавље започиње одељком Поставка експеримента, који описује узорак експеримента, као и независне и зависне променљиве. Следи представљање начина на који су прикупљени квантитативни и квалитативни подаци у виду теста са задацима и анкете, а на крају је дата напомена у вези са окружењем за рад на задацима теста.

У одељку који следи, Квантитативни резултати експеримента, извршена је анализа квантитативних резултата експеримента за сваку зависну променљиву, што укључује спровођење и анализу резултата статистичког теста. Резултати анкете, односно одговори на свако питање анкете графички су представљени у одељку Квалитативни резултати експеримента.

6.2 Поставка експеримента

Пре спровођења експеримента, поднесена је молба етичкој комисији Факултета техничких наука Универзитета у Новом Саду за спровођење експеримента у коме би учествовали студенти мастер студија Факултета техничких наука, који слушају предмет „Увод у дигиталну форензику". Након добијене сагласности, спроведено је узорковање студената који су претходно обавештени о предстојећим активностима. Величина узорка је 60 студената једнако подељених на експерименталну и контролну групу, где експериментални фактор представља употреба система за вођење кроз истрагу. Распоређивање студената у групе је потпуно случајно. Истрага се састојала од решавања задатака на тему форензике рачунарских мрежа и одговарања на питања теста у вези са задацима форензичке истраге. Навод задатака дат је у одељку 5.6.

Дакле, независне променљиве експеримента су студијски програм студената и година студирања. Зависне променљиве експеримента су ефективност и ефикасност студената приликом спровођења истраге и решавања теста. Ефективност студената огледа се у средњој вредности освојених бодова студената експерименталне и контролне групе, док се ефикасност мери временом које је студентима било потребно за спровођење истраге и решавање теста.

6.2.1 Тест и анкета

Питања теста, којима су прикупљани квантитативни подаци, креирана су тако да проверавају у којој мери је случај форензичке истраге решен у складу са ISO стандардима (ISO/IEC 27037, 2015; ISO/IEC 27041, 2016; ISO/IEC 27042, 2016; ISO/IEC 27043, 2016), водичима Интерпола (Interpol, 2021) и Националног института за стандардизацију и технологију САД-а (НИСТ) (Kent и сар., 2006). Питања теста су била подељена у четири групе које су одговарале различитим фазама форензичке истраге – идентификацији, прикупљању,

прегледању и анализи доказа. Свако од 28 питања теста вредновало је 1 бод, а преглед освојених бодова сваког студента је, поред укупне суме, подразумевао и рачунање сума освојених бодова у појединачним фазама истраге.

Анкета, којом су прикупљани квалитативни подаци, садржала је питања са вишеструким избором и отворена питања. Одговор на питања са вишеструким избором је број 1, 2, 3, 4 или 5, што градацијски означава у којој мери се студент слаже са одређеним тврђењем. При томе број 1 означава апсолутно неслагање, а број 5 – апсолутно слагање са тврђењем. На овај начин студенти су се изјашњавали у којој мери је: упознавање са начином употребе софтвера једноставно; коришћење софтвера једноставно; кориснички интерфејс софтвера интуитиван; фаза идентификације током истраге олакшана; фаза прикупљања олакшана; фаза прегледања олакшана; фаза анализе олакшана и колико би студент био рад да препоручи софтвер другим корисницима. С друге стране, отвореним питањима су се студенти слободно изјашњавали о недостацима, предностима и предлозима за унапређење софтвера.

6.2.2 Симулација окружења

Да би студенти били у могућности да спроведу форензичку истрагу и реше наведене задатке, рачунарска мрежа са неопходним подацима била је емулирана употребом платформе EVE [20]. С обзиром на то да емулација рачунарске мреже захтева истовремени рад више виртуелних машина и високе перформансе хост-рачунара, њена инсталација на студентске рачунаре није била могућа. Да би се обезбедио приступ емулираној рачунарској мрежи сваком студенту који је учествовао у експерименту, мрежа је инсталирана на платформи Google Cloud [21] у оквиру које је креирано онолико инстанци емулиране мреже, колико је било студената који су истовремено учествовали у експерименту.

6.3 Квантитативни резултати експеримента

6.3.1 Упоређивање ефективности студената

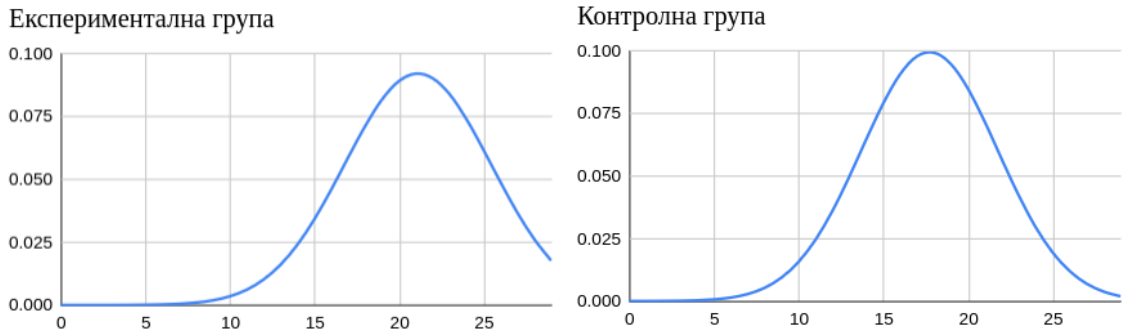
Резултати који осликавају ефективност студената експерименталне и контролне групе приликом спровођења истраге и решавања теста подлежу статистичком t-тесту. Томе сведоче независност експерименталне и контролне групе, случајни распоред студената у групе, нормална расподела података обе групе студената и приближно једнаке вредности варијанси група. На сликама 39–43 приказане су криве расподеле обе групе за резултате које су студенти постигли на целокупном тесту и на деловима теста који представљају спровођење појединачних фаза истраге – идентификације, прикупљања, прегледања и анализе доказа, а у табели 1 приказане су средње вредности и вредности стандардне девијације експерименталне и контролне групе студената.

Спровођењем статистичког теста, ствара се увид у информацију о популацији (Obradović и Sentić, 1959), што се у овом случају односи на дипломиране

[20] https://www.eve-ng.net/
[21] https://cloud.google.com/

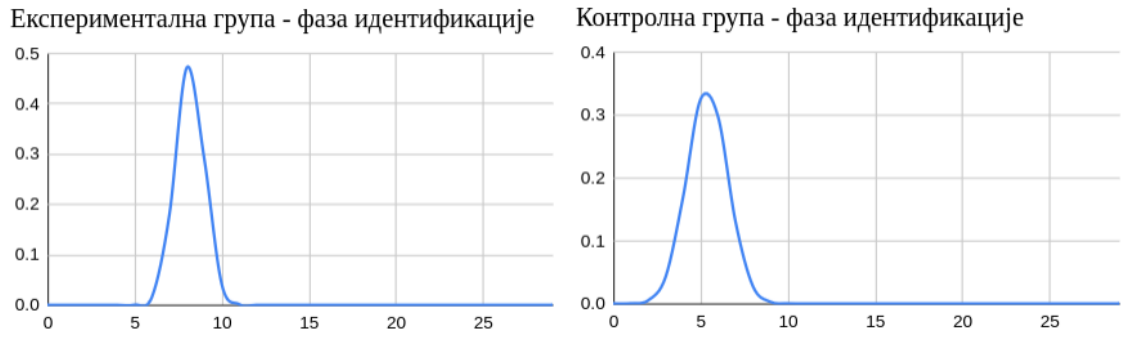
	Експериментална група		Контролна група	
	M	SD	M	SD
укупан резултат	21,12	4,34	17,73	4,02
резултат фазе идентификације	8,17	0,83	5,38	1,17
резултат фазе прикупљања	5,53	1,43	4,80	1,40
резултат фазе прегледања	4,37	1,97	3,75	1,89
резултат фазе анализе	3,05	1,51	3,80	1,27

Табела 1: Резултати теста експерименталне и контролне групе студената (средња вредност (M) и стандардна девијација (SD)).



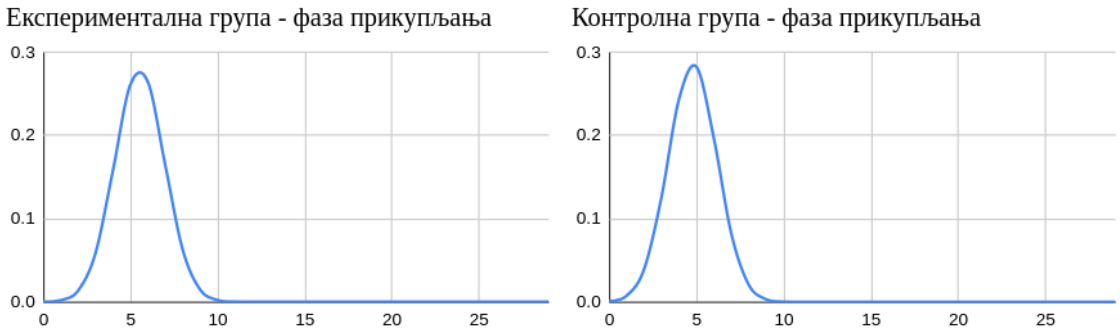
(а) (б)

Слика 39: Криве расподеле експерименталне и контролне групе за резултате постигнуте на целом тесту.



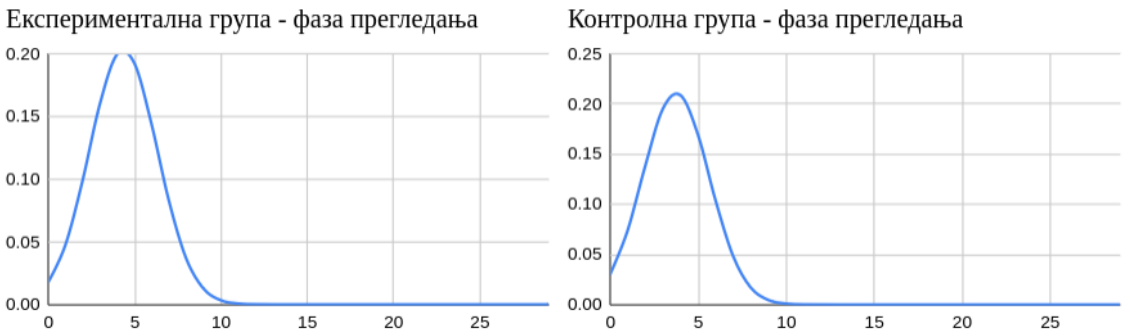
(а) (б)

Слика 40: Криве расподеле експерименталне и контролне групе за резултате постигнуте у оквиру фазе идентификације доказа.



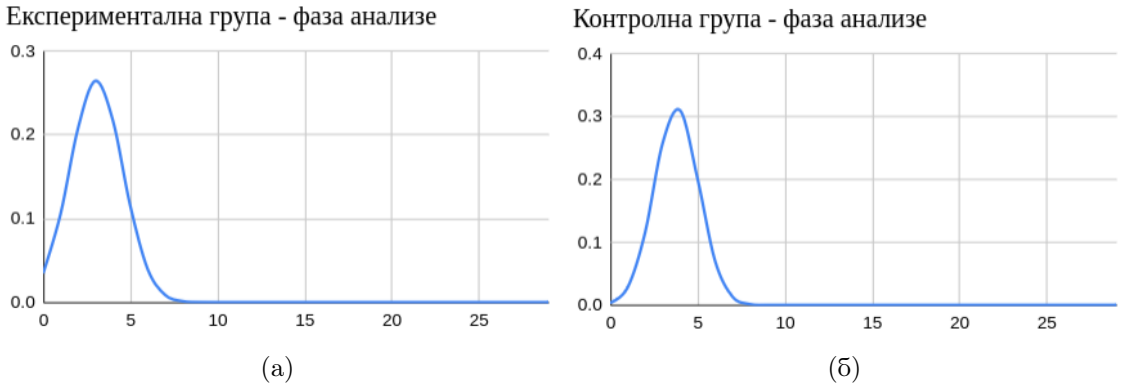
(а) (б)

Слика 41: Криве расподеле експерименталне и контролне групе за резултате постигнуте у оквиру фазе прикупљања доказа.



(а) (б)

Слика 42: Криве расподеле експерименталне и контролне групе за резултате постигнуте у оквиру фазе прегледања доказа.



(а) (б)

Слика 43: Криве расподеле експерименталне и контролне групе за резултате постигнуте у оквиру фазе анализе доказа.

укупан резултат	$t(58) = 3{,}079$, $p = 0{,}002$
резултат фазе идентификације	$t(58) = 10{,}468$, $p = 0{,}000$
резултат фазе прикупљања	$t(58) = 1{,}972$, $p = 0{,}027$
резултат фазе прегледања	$t(58) = 1{,}214$, $p = 0{,}115$
резултат фазе анализе	$t(58) =$ -2,041, $p = 0{,}023$

Табела 2: Резултати t-теста.

студенте рачунарства, који су слушали курс дигиталне форензике. Статистичка хипотеза гласи: употреба система – водича кроз истрагу, не доприноси ефективности студената. При томе је за ниво значајности теста узета вредност 0,05 ($\alpha = 0{,}05$).

У табели 2 приказани су резултати спровођења t-теста. С обзиром на одабрани ниво значајности, за сваки резултат за који се везује p-вредност мања од 0,05, одбацује се нулта хипотеза.

Експериментална група студената ($M = 21{,}12$, $SD = 4{,}34$), која је користила апликацију – водич кроз форензичку истрагу приликом решавања задатака је у односу на контролну групу студената ($M = 17{,}73$, $SD = 4{,}02$) постигла статистички значајно бољи резултат на целокупном тесту: $t(58) = 3{,}079$, $p = 0{,}002$. Стога, нулта хипотеза се одбацује и може се закључити да је експериментом показано да систем позитивно утиче на ефективност студената приликом спровођења форензичке истраге.

Током фазе идентификације, експериментална група студената ($M = 8{,}17$, $SD = 0{,}83$) у поређењу са контролном групом студената ($M = 5{,}38$, $SD = 1{,}17$) постигла је статистички значајно боље резултате: $t(58) = 10{,}468$, $p = 0{,}000$.

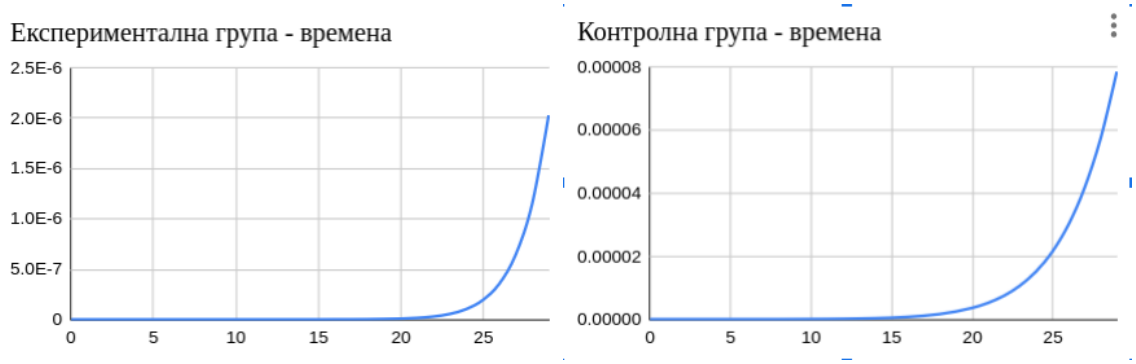
Током фазе прикупљања, експериментална група студената ($M = 5{,}53$, $SD = 1{,}43$) у поређењу са контролном групом студената ($M = 4{,}80$, $SD = 1{,}40$) постигла је статистички значајно боље резултате: $t(58) = 1{,}972$, $p = 0{,}027$.

Током фазе прегледања, експериментална група студената ($M = 4{,}37$, $SD = 1{,}97$) у поређењу са контролном групом студената ($M = 3{,}75$, $SD = 1{,}89$) постигла је боље резултате за које се не може рећи да су статистички значајни: $t(58) = 1{,}214$, $p = 0{,}115$.

С друге стране, током фазе анализе, контролна група студената ($M = 3{,}80$, $SD = 1{,}27$) у поређењу са експерименталном групом студената ($M = 3{,}05$, $SD = 1{,}51$) постигла је статистички значајно боље резултате: $t(58) =$ -2,041, $p = 0{,}023$.

Дакле, нулта хипотеза се може одбацити у случајевима фаза идентификације, прикупљања и анализе доказа, али не и у случају фазе прегледања доказа. Међутим, експериментом је показано да систем – водич кроз истрагу помаже студентима у истрази током фаза идентификације, прикупљања и прегледања доказа, али не помаже (или одмаже) у фази анализе доказа.

Другим речима, показано је да је вероватно да би сви студенти рачунарства са предзнањем из области дигиталне форензике, уз употребу система – водича кроз истрагу, ефективније спровели истрагу уопште, као и у фазама



(а) (б)

Слика 44: Криве расподеле експерименталне и контролне групе за времена потребна за спровођење истраге.

идентификације и прикупљања доказа, а да им у фази анализе доказа систем не би помогао или би им одмогао. За случај фазе прегледања, не постоје докази да се учинак студената из експеримента може применити на студенте тог профила уопште, али је много вероватније да би систем имао позитиван ефекат, него да не би утицао или да би одмогао.

Свакако је неопходно споменути недостатке експеримента, који би могли утицати на резултате. Разлог за узорковање студената дигиталне форензике лежи у претпоставци да они репрезентују неискусне форензичаре у дигиталном домену. Међутим, не може се тврдити да резултати проистекли из експеримента са студентима, могу да се примене на све неискусне форензичаре. Такође, потенцијална опасност за генерализовање на основу резултата експеримента је знање и способност исправног резоновања у сфери рачунарских мрежа од стране студената, с обзиром на то да су рачунарске мреже тема истраге у експерименту. Уколико студенти из експеримента нису имали довољно знања из ове подобласти рачунарства, резултати експеримента не одговарају реалној слици.

6.3.2 Упоређивање ефикасности студената

Констатацији да подаци произишли из експеримента подлежу t статистичком тесту значајности, предњачила је претпоставка о нормалној расподели података, што је доказано графичким поступком. Међутим, у случају посматрања ефикасности студената током истраге, графички поступак за подупирање претпоставке нормалне расподеле није одговарајући. Уместо тога примењен је статистички Лилиефорсов тест (Lilliefors) са нивоом значајности $\alpha = 0{,}05$. На слици 44 приказана је крива расподеле временā за експерименталну и контролну групу студената.

У табели 3 приказане су средње вредности и вредности стандардне девијације временā која су била потребна експерименталној и контролној групи студената за решавање задатака и теста.

Применом Лилиефорсовог теста над подацима експерименталне групе сту-

	M	SD
експериментална група	65,13	8,04
контролна група	68,57	11,32

Табела 3: Времена експерименталне и контролне групе студената (средња вредност (M) и стандардна девијација (SD)).

дената, закључено је да не постоји значајна разлика у односу на нормалну расподелу ($D(30) = 0{,}14$, $p = 0{,}17$). Такође, применом овог теста над подацима контролне групе студената, закључено је да не постоји значајна разлика у односу на нормалну расподелу ($D(30) = 0{,}12$, $p = 0{,}32$).

Како и у овоме случају важи независност експерименталне и контролне групе студената, у које су студенти случајно распоређени, остаје услов хомогености варијанси како би се могао применити t-тест. Статистичким F-тестом једнакости варијанси са нивоом значајности $\alpha = 0{,}05$ ($F(29, 29) = 0,5$, $p = 0,07$) показано је да се не може одбацити нулта хипотеза о једнакости варијанси експерименталне и контролне групе студената. Дакле, сви услови за примену t-теста су задовољени.

t-тестом је показано да је експериментална група студената ($M = 65{,}13$, $SD = 8{,}04$) у поређењу са контролном групом студената ($M = 68{,}57$, $SD = 11{,}32$) спровела форензичку истрагу ефикасније, односно за краће време, али да оно није статистички значајно: $t(58) = -1{,}33$, $p = 0{,}094$. Међутим, као и у случају упоређивања ефективности студената током фазе прегледања, ни у случају ефикасности студената не можемо занемарити позитиван ефекат система – водича кроз истрагу који је доказан експериментом, те закључујемо да је позитиван ефекат вероватнији и у читавој популацији неискусних форензичара у дигиталном домену.

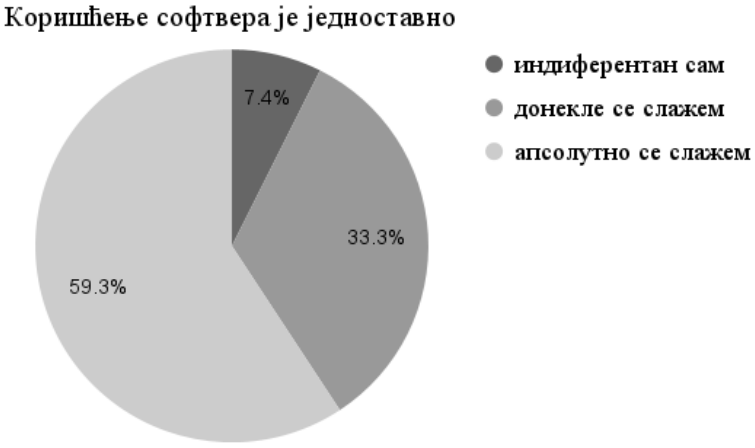
6.4 Квалитативни резултати експеримента

У овом одељку изнети су квалитативни резултати експеримента прикупљени анкетом. Како се анкета састојала из питања са вишеструким избором и отворених питања, најпре су представљени резултати изјашњавања студената на питања са вишеструким избором.

На питање у којој мери се студент слаже са тврђењем да је упознавање са начином употребе софтвера једноставно, 57,1% студената је одговорило да се апсолутно слаже, 35,7% студената се донекле сложило, а 7,1% студената је дало индиферентан одговор. На слици 45 је приказан дијаграм који графички представља наведене податке.

Слика 45: График изјашњавања студената.

График са слике 46 приказује како су се студенти изјаснили поводом тврдње да је коришћење софтвера једноставно. 59,3% студената апсолутно се сложило са тврдњом, 33,3% студената се донекле сложило са тврдњом, док је 7,4% студената било индиферентно.

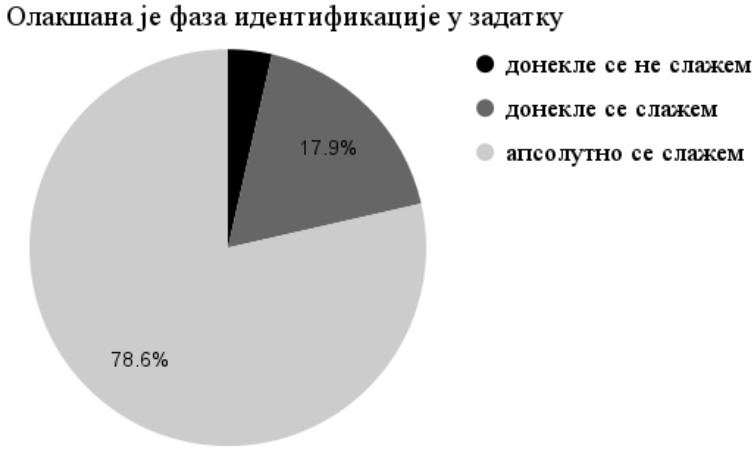


Слика 46: График изјашњавања студената.

Студенти су на питање да ли се слажу са тврдњом да је кориснички интерфејс софтвера интуитиван, одговорили на следећи начин. 50% студената се апсолутно сложило са тврдњом, 28,6% студената се донекле сложило са тврдњом, 17,9% студената је било индиферентно, а 3,6% студената се донекле није сложило са датом тврдњом (слика 47).

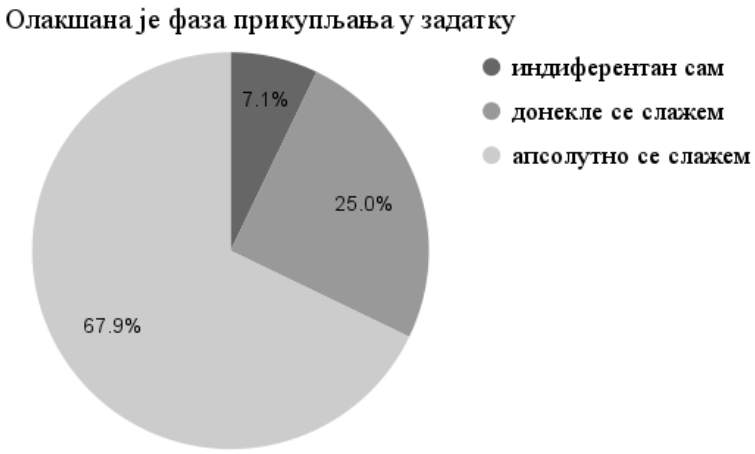
Слика 47: График изјашњавања студената.

Следе питања у вези са корисношћу софтвера у појединачним фазама истраге – идентификацији, прикупљању, прегледању и анализи доказа. 78,6% студената се апсолутно сложило са тврдњом да употреба софтвера олакшава спровођење фазе идентификације, 17,9% студената се донекле сложило са тврдњом, док се 3,6% студената донекле није сложило са тврдњом (слика 48).



Слика 48: График изјашњавања студената.

67,9% студената се апсолутно сложило са тврдњом да софтвер олакшава спровођење фазе прикупљања доказа, 25% студената се донекле сложило са овом тврдњом, а 7,1% студената је дало индиферентан одговор (слика 49).



Слика 49: График изјашњавања студената.

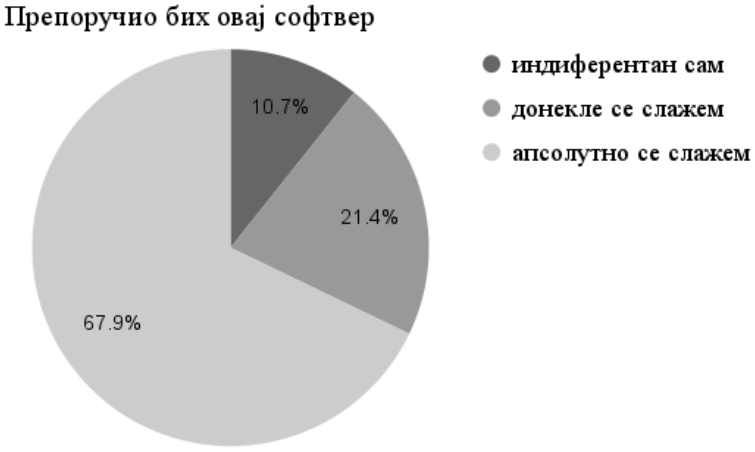
58,6% студената се апсолутно сложило са тврдњом да софтвер олакшава спровођење фазе прегледања доказа, 24,1% студената се донекле сложило са овом тврдњом, 13,8% студената је било индиферентно, док се 3,4% студената донекле није сложило са поменутом тврдњом (слика 50).

Слика 50: График изјашњавања студената.

Када је у питању спровођење фазе анализе током истраге, 50% студената се апсолутно сложило са тврдњом да је софтвер учинио лакшим спровођење те фазе, 30,8% студената се донекле сложило са овом тврдњом, а 19,2% студената није могло да се одлучи да ли је софтвер помогао или одмогао (слика 51).

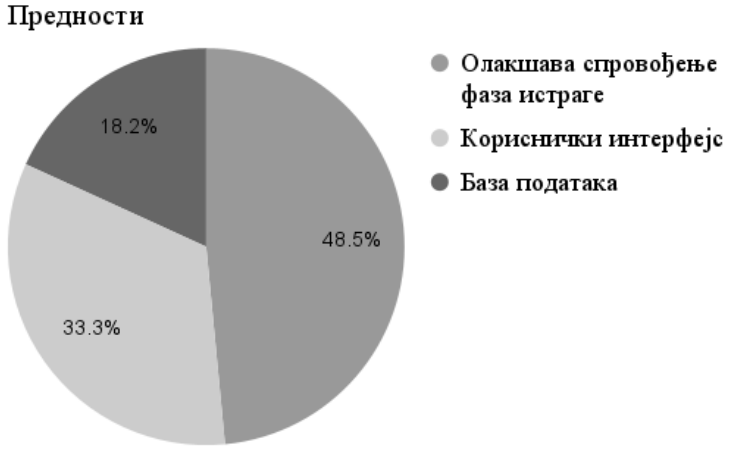
Слика 51: График изјашњавања студената.

На крају, студенти су упитани у којој мери се слажу са тврдњом да софтвер треба препоручити другим неикусним форензичарима. 67,9% студената се апсолутно сложило са овом тврдњом, 21,4% студената се донекле сложило, а 10,7% студената је дало индиферентан одговор (слика 52).



Слика 52: График изјашњавања студената.

Анкета се састојала од три отворена питања чијим одговорима би студенти требало да укажу на предности софтвера, мане софтвера и на предлоге за унапређење софтвера. На сликама 53 и 54 приказани су графици који осликавају изјашњавање студената о предностима и манама система – водича кроз форензичку истрагу.



Слика 53: График изјашњавања студената о предностима система.

Слика 54: График изјашњавања студената о манама система.

Када су у питању недостаци система, 40% студената сматра да систем нема недостатака, 45% студената је указало на недостатке графичког корисничког интерфејса система. Коментари ових студената указују на збуњујући и неинтуитиван интерфејс, као и на нереспонзивност интерфејса и премалу величину фонта. 15% студената је имало замерку на базу података. Тачније, замерке су се тицале инструкција за спровођење фаза истраге, које су, по мишљењу ових студената, биле недовољно јасне и богатства базе података потенцијалним изворима доказа.

С друге стране, студенти (48,5%) су као предност система навели да им је уз његову употребу било олакшано спровођење фаза истраге. Највише студената имало је овакав коментар за све фазе истраге, а од појединачних фаза, највише се спомињала фаза прикупљања, затим фазе идентификације и анализе доказа. 33,3% студената је навело предности графичког корисничког интерфејса система. При томе се највише понављао епитет једноставан, затим

интуитиван и конзистентан. На крају, 18,2% студената је наводило предности базе података система. Од тога су понајвише биле хваљене јасне и детаљно објашњене инструкције које су водиле кроз истрагу.

Предлози за унапређење софтвера највише су се тицали побољшања система помоћи и бољег објашњења начина употребе софтвера. Остале сугестије биле су конкретна упутства за побољшање интерфејса система.

6.5 Сажетак

Део овога поглавља, који треба истаћи, свакако чине резултати експеримента, те је у наставку табеларно дат преглед најважнијих. У табели 4 је за целокупан резултат теста, као и за појединачне фазе истраге наведена група студената која је ефективније решила тест, односно спровела истрагу. Такође, коментарисана је и статистичка значајност ових резултата. У табели 5 су за целокупан резултат теста предочени група студената која је била ефикаснија у изради теста и категорички коментар статистичке значајности овог резултата. Напослетку је у табели 6 приказан удео студената експерименталне групе који су на питања теста дали најпозитивнији одговор.

	група која је постигла већу ефективност	статистички значајан резултат
резултат целокупног теста	експериментална група	да
резултат фазе идентификације	експериментална група	да
резултат фазе прикупљања	експериментална група	да
резултат фазе прегледања	експериментална група	не
резултат фазе анализе	контролна група	да

Табела 4: Сажетак резултата упоређивања ефективности експерименталне и контролне групе.

	група која је постигла већу ефикасност	статистички значајан резултат
резултат целокупног теста	експериментална група	не

Табела 5: Сажетак резултата упоређивања ефикасности експерименталне и контролне групе.

	„апсолутно се слажем”
Упознавање са начином употребе софтвера је једноставно	57,1%
Коришћење софтвера је једноставно	59,3%
Кориснички интерфејс је интуитиван	50,0%
Олакшана је фаза идентификације у задатку	78,6%
Олакшана је фаза прикупљања у задатку	67,9%
Олакшана је фаза прегледања у задатку	58,6%
Олакшана је фаза анализе у задатку	50,0%
Препоручио/препоручила бих овај софтвер	67,9%

Табела 6: Сажетак резултата анкете.

7 Дискусија

7.1 Избор стандарда и водича

Скуп стандарда и водича који су коришћени у овој дисертацији чине ISO/IEC 27037 (ISO/IEC 27037, 2015), ISO/IEC 27041 (ISO/IEC 27041, 2016), ISO/IEC 27042 (ISO/IEC 27042, 2016), ISO/IEC 27043 (ISO/IEC 27043, 2016), Guide to Integrating Forensic Techniques into Incident Response (Kent и сар., 2006) и Guidelines for Digital Forensics First Responders (Interpol, 2021). Одговор на питање зашто је извршена баш оваква селекција лежи у кредибилитету који Међународна организација за стандардизацију, Међународна полицијска организација Интерпол и Национални институт за стандарде и технологију САД-а уживају у друштву на глобалном нивоу. Међународна организација за стандардизацију је највећа светска организација за развој стандарда која окупља националне институте у више од 160 земаља. Национални институт за стандардизацију Републике Србије такође базира националне стандарде и прописе на ISO стандардима. Даље, Интерполови водичи за поступање у случају рачунарског криминала не могу се занемарити с обзиром на то да ова организација окупља више од 190 земаља. На крају, НИСТ је организација која делује у оквиру Федералног министарства трговине САД-а и има за циљ промоцију америчке иновативности. Обрађени ISO стандарди су комплементарни, а уз додатак НИСТ-овог и Интерполовог водича онтологија је комплетирана.

Базирајући се на поменутим стандардима креирана је онтологија као имплементација предложеног модела форензичке истраге. Овде се поставља питање могућности преузимања делова других онтологија. У случају модула рачунарских мрежа онтологије описане овом дисертацијом, постојеће онтологије су делимично утицале на његово креирање. На пример, угледање на рад аутора De Paola и сар. (2003) било је могуће приликом креирања концепата који представљају информације у оквиру рачунарских мрежа. Такође, неки од потконцепата концепта „Потенцијални извор доказа" преузети су из онтологије представљене од стране аутора van Heerden и сар. (2012). У случају других модула онтологије, одговор је одричан јер, како се показало у поглављу 3, опште онтологије у области дигиталне форензике су ретке и неодговарајуће у смислу модела форензичке истраге у који се онтологија ове дисертације уклапа. Такође, постојеће онтологије махом садрже најопштије концепте информационе безбедности или дигиталне форензике, док онтологија ове дисертације у обзир узима и конкретне примере који се помињу у стандардима и водичима, те се тиме предупређује збуњивање форензичара апстракцијама.

Иако ниједна од организација не намеће употребу стандарда, у начелу би требало да је сваки стандард у вези са неким прописом који налаже да се стандард поштује. Тиме ова дисертација представља и апел националним надлежним институцијама да креирају прописе који намећу поштовање стандарда.

7.2 Употреба других облика вештачке интелигенције

У односу на симболичку вештачку интелигенцију, технике машинског учења подразумевају много ширу мрежу веза, која се заснива на односима између концепата, особинама и атрибутима концепата, који се налазе у енормно великим скуповима података за обучавање. Што већи скуп података за обучавање, то „паметнија" мрежа. У овом погледу, највећи значај имају велики језички модели (LLM).

Употреба машинског учења у форензичкој истрази нарочито је спорна уколико дође до испољавања проблема као што су: пристрасност (енг. *bias*), халуцинација (енг. *hallucation*) (Håkansson и Phillips-Wren, 2024), информисано претпостављање или одговор „нула покушаја" (енг. *zero-shot*) (Xian и сар., 2017) и проблем објашњивости (енг. *explainability*) (Barman и сар., 2024).

Пристрасност (енг. *bias*) вештачке интелигенције је проблем скупа података над којим она учи. Ако су у скуп података за обучавање модела уткане предрасуде које владају у друштву, оне кроз тренирање модела могу чак постати веће и учинити да систем који се на оваквом моделу заснива даје погрешне резултате. У пољу дигиталне форензике, за обучавање модела неопходна је колекција докумената који представљају извештаје форензичара. Како ови документи нису јавно доступни, обучавање модела, а самим тим и употреба вештачке интелигенције за вођење кроз форензичку истрагу, тешко су изводљиви.

Неспорно је говорити о недопустивости ослањања током форензичке истраге на вештачку интелигенцију која је склона халуцинацијама. Дезинформација, коју систем базиран на оваквом моделу вештачке интелигенције представи форензичару са великим уверењем у њену тачност, може да збуни форензичара, да га наведе на погрешан траг, а у најгорем случају, да га наведе на неистинито сведочење у поступку од чијег исхода зависи нечији живот.

Трећи проблем употребе вештачке интелигенције за вођење кроз форензичку истрагу је објашњивост (енг. *explainability*). Механизми функционисања машинског учења скривени су у „црној кутији". То значи да, чак и ако је могућ увид у целокупан скуп података који је коришћен за обучавање, није могуће поуздано знати на који начин је формирана предикција. Немогућност објашњења на који начин се дошло до одређеног резултата значи немогућност задовољења захтева ваљаности форензичке истраге. Дакле, уместо необјашњивог модела вештачке интелигенције, за област дигиталне форензике и вештачења много је адекватнији транспарентан принцип.

Ако вештачка интелигенција није обучавана над подацима који садрже њој тренутно постављено питање, она ће дати одговор, односно претпоставиће одговор на основу информација о значењу конкретног појма који се помиње у питању. Ове атрибуте она ће упоредити са знањем проистеклим из обучавања, односно података на којима јесте обучавана. Наравно да је вероватноћа грешке у учењу на основу нула покушаја обучавања много већа у односу на тренирано знање, па је очевидан значај овог проблема када се вештачка интелигенција употребљава у вођењу кроз форензичку истрагу која има удела у судском поступку.

Поједини аутори (Solanke, 2022) оправдавају употребу црних кутија ве-

штачке интелигенције методама поједностављивања модела, визуелизације, локализације и објашњавања најзначајнијих делова. Такође, концепт којим се тежи да се превазиђу проблеми интерпретабилности и објашњивости система базираних на вештачкој интелигенцији јесте објашњива вештачка интелигенција (XAI). Овај концепт обухвата методе и технике анализе процеса одлучивања модела машинског учења (Arrieta и сар., 2020), чији је крајњи циљ да се омогући исправно разумевање и интерпретација начина, као и резултата одлучивања модела машинског учења (Jinad и сар., 2024). Другим речима, објашњива вештачка интелигенција тежи да „црну кутију" машинског учења учини транспарентном и интерпретабилном тако што пружа објашњења за предвиђања система који се заснива на машинском учењу (Pfeifer и сар., 2023).

Као највећуману објашњиве вештачке интелигенције аутори Jinad и сар. (2024) наводе немогућност система да објасни узроке доласка до одређених предвиђања. Уз то, постоји и опасност од злонамерне употребе модела вештачке интелигенције који су, пратећи принцип објашњивости, изразито транспарентни те тако могу подстаћи сличне креације са неетичком сврхом или манипулације при употреби, које би довеле до штетног деловања. Ипак, Kelly и сар. (2020) као будући правац у употреби објашњиве вештачке интелигенције виде у унапређивању постојећих база знања креираних од стране експерата.

Тренутне имплементације вештачке интелигенције у дигиталној форензици захтевају валидацију од стране истражитеља (Hall и сар., 2022). Међутим, спорна је грешка коју форензичар, који валидира резултат алата заснованог на вештачкој интелигенцији, потенцијално може направити. Дакле, потребно је пронаћи начин да се људска грешка предупреди.

У систему базираном на симболичкој вештачкој интелигенцији описаном у овој тези оличена је транспарентна аутоматизована помоћ форензичарима током спровођења истраге. Валидација од стране истражитеља, која је неопходна у свакој употреби било ког вида вештачке интелигенције у правном поступку, у овом систему је већ задовољена јер систем у формалном облику, поред препорука из стандарда, инкорпорира и експертско знање и искуство.

7.3 Анализа резултата експеримента

Питање које се поставља јесте степен значајности појединачне фазе форензичке истраге у односу на остале фазе. С обзиром на то да су студенти експерименталне групе остварили лошији резултат у фази анализе у односу на контролну групу студената и да је овај резултат статистички значајан, прецизнију формулацију можемо конкретизовати, па се упитати да ли фаза анализе има већи или мањи значај у целокупној истрази у односу на било коју другу фазу.

Теза у корист ове дисертације гласи да без ваљано спроведених фаза идентификације, прикупљања и прегледања доказа, нема ни материјала за анализирање. Оперативна форма дигиталног трага у једној фази истраге изводи се из оперативне форме процесуиране у претходној фази истраге. С друге стране, теза на штету ове дисертације гласи да без ваљано спроведене фазе

анализе, нема ни комплетиране истраге, односно стручног налаза и мишљења које се евентуално презентује на суду.

Следи закључак да су све фазе истраге подједнако важне, те се ниједан резултат експеримента не сме занемарити. У случају фаза идентификације и прикупљања доказа, експериментална група студената била је успешнија у односу на контролну групу студената, при чему је овај резултат статистички значајан. То значи да би сви студенти Увода у дигиталну форензику спровели фазе идентификације и прикупљања доказа успешније уз употребу система базираног на формалном опису знања у односу на случај у коме изостаје његова употреба. Током фазе прегледања доказа, студенти експерименталне групе јесу били успешнији у односу на студенте контролне групе, али овај резултат није статистички значајан. Није могуће закључивати о резултату свих студената, већ само о конкретној генерацији. На крају, студенти контролне групе били су успешнији у фази анализе у односу на експерименталну групу студената и резултат који је на ово указао јесте статистички значајан. Дакле, свим студентима у фази анализе поменути систем не би помогао или би им одмогао.

Може се приметити да, како се форензичар (студент) примиче крају истраге користећи систем базиран на формалном опису знања, тако његова корисност опада. Једно од објашњења за ову појаву може бити све већа везаност оперативних форми трагова за конкретан случај како истрага одмиче. Последња оперативна форма, информација, обрађује се у фази анализе и најуже је везана за дати случај форензичке истраге, те знање и искуство из претходних форензичких случајева овде има најмањи значај. Оно што је од пресудне важности у фази анализе, јесте форензичарева експертиза и способност ваљаног закључивања на основу пронађених података, њихове ваљане интерпретације, те претварања у информације.

7.4 Претње по валидност истраживања

Овде је пригодно још једном навести један од циљева и хипотезу овог истраживања. Научни циљ је откриће узрочно-последичне везе између истраге вођене аутоматским расуђивањем базираним на формалном моделу форензичких стандарда и ваљано спроведене форензичке истраге. Другим речима, циљ је успешније спровођење истраге од стране неискусног форензичара када као водич кроз истрагу форензичар користи систем базиран на формалном моделу форензичких стандарда. У формулацији хипотезе овог истраживања, која је проверавана експериментом, неискусне форензичаре представљају студенти, који су у процесу учења о дигиталној форензици.

Из наведеног следи прва претња по валидност истраживања – изједначавање студената у процесу учења о дигиталној форензици са неискусним форензичарима, који обављају форензичку праксу. Техничко знање, којим располажу студенти и којим располажу неискусни форензичари – практичари, умногоме се поклапа, с обзиром на то да и једни и други имају исто звање дипломираног инжењера, а у Републици Србији је законски услов за обављање вештачења управо стечено високо образовање. Међутим, услов је и

најмање пет година радног искуства у било ком пољу у струци. Дакле, није неопходно да форензичар-практичар, у тренутку када започиње са радом као вештак за инормационе технологије, има искуство у обављању форензичке праксе. Оно што је сасвим сигурно, јесте да студенти ни у којој мери нису упознати са правним аспектом вештачења, док такво искуство у мањој мери могу имати неискусни форензичари-практичари. Међутим, тврдња која иде у прилог занемаривању ове примедбе, а са којом би требало да се сложи већина правника, гласи да мишљење вештака у судском поступку мора бити самоуверено и подупрто знањем и искуством у стопроцентној мери како би се осигурала правда. На основу свега наведеног, закључује се да студенти мастер студија који слушају курс дигиталне форензике представљају најнеискусније форензичаре у вештачењу у области информационих технологија.

Друга претња по валидност истраживања огледа се у теми форензичког случаја, која је одабрана да чини задатак студентима на основу кога су сачињена питања теста. Дакле, рачунарске мреже јесу специфична област рачунарства и степен савладавања ове материје на курсевима који се тичу рачунарских мрежа може умногоме утицати на квалитет спровођења форензичке истраге у области рачунарских мрежа. Уколико су дати студенти боље савладали рачунарске мреже, они ће боље и истрагу спровести, чиме се промаља питање да ли би студенти једнако приступили форензичкој истрази у другим областима рачунарства.

Трећа претња по валидност је инструмент експеримента у виду теста, као и изједначавање тачних одговора на тесту са ваљаношћу дигиталних доказа на суду. Тест је сачињен у складу са стандардом, али и са искуством у судској пракси Републике Србије. Лабораторија за дигиталну форензику била је ангажована у немалом броју судских случајева, те је ово искуство уткано у сам тест и задатке експеримента.

Поред ових претњи по валидност које се тичу извођења експеримента, треба навести и величину узорка, која представља минимум потребан за статистичко тестирање резултата експеримента. Међутим, у времену извођења експеримента, број студената који су у њему учествовали био је ограничен бројем студената који су тада слушали предмет „Увод у дигиталну форензику" и који су похађали вежбе на том предмету.

8 Закључак

Одговорност која је на форензичарима-вештацима у судским поступцима, не праштa несигурност и неискуство, па се поставља питање како омогућити неискусним форензичарима да стичу искуство? Питање које се такође поставља је како потпомоћи способност форензичара да пронађе релевантне трагове тако да истрага буде ваљана и да се смањи могућност оспоравања стручног налаза и мишљења на суду? Одговор на ова питања лежи у аутоматизацији вођења кроз истрагу, у које је уткано искуство других форензичара, експерата, и које садржи препоруке за ваљано спровођење дигиталне форензичке истраге из међународно признатих страндарда и водича.

Конкретизација аутоматизованог водича кроз дигиталну форензичку истрагу је систем који се заснива на формалном опису делова стандарда и водича за ваљано спровођење дигиталне форензичке истраге, као и искустава експерата. Дакле, циљеви овог истраживања били су креирање поменутог формалног описа, који чини базу података, односно базу знања система, затим спецификација захтева система, дизајн и пројектовање система, прототипска имплементација система и његова верификација. Формални опис стандарда, водича и искустава експерата постигнут је употребом дескриптивне логике SROIQ(D), па је научни циљ истраживања био и показати да ли неискусан форензичар спроводи истрагу успешније када као водич кроз истрагу користи поменути систем, те тиме проверити да ли аутоматско расуђивање над базом знања креираном помоћу конструката дескриптивне логике SROIQ(D) доприноси квалитету истраге. Друштвени циљ истраживања био је увођење система за вођење кроз дигиталну форензичку истрагу у употребу од стране неискусних форензичара, односно вештака за информационе технологије.

Постизање научног циља овог истраживања најпре је омогућило креирање модуларизоване онтологије која описује домен форензике рачунарских мрежа и ваљаног спровођења форензичке истраге рачунарских мрежа. Потом је реализован систем који, кроз расуђивање над онтологијом и интеракцију са корисником, води корисника кроз ваљано спровођење истраге. На крају је експериментом у коме су учествовали студенти мастер студија који су у датом тренутку похађали курс „Увод у дигиталну форензику" и који су представљали неискусне форензичаре, показано како употреба поменутог система утиче на ефективност и ефикасност спровођења истраге.

Технологија програмског и корисничког интерфејса система бирана је у складу са потребама, односно са капацитетом у људству и ангажовању Лабораторије за дигиталну форензику Факултета техничких наука Универзитета у Новом Саду, где је систем уведен у употребу. Графичким корисничким интерфејсом се активности из теорије, праксе, стандарда и водича, које су везане за фазе истраге, предочавају као инструкције, док се захтеви ваљаности стављају на увид као додаци инструкцијама. Одвајањем инструкција и захтева приликом вођења кроз форензичку истрагу стиче се утисак важности испуњења захтева ваљаности пре свега када је у питању вештачење у судском поступку. Омогућавањем практичне примене система од стране истражитеља Лабораторије за дигиталну форензику и тиме доприношењем њиховом кре-

дибилитету у вештачењима, постигнут је друштвени циљ овог истраживања.

Ово истраживање произвело је хеуристички и верификаторни резултат. Хеуристичким резултатом даје се на знање да је адекватна примена SROIQ(D) дескриптивне логике у сврху креирања система за вођење кроз ваљану форензичку истрагу. Другим речима, дескриптивна логика SROIQ(D) погодна је за формални опис главних делова форензичких стандарда и водича ISO/IEC 27037 (ISO/IEC 27037, 2015), ISO/IEC 27041 (ISO/IEC 27041, 2016), ISO/IEC 27042 (ISO/IEC 27042, 2016), ISO/IEC 27043 (ISO/IEC 27043, 2016), Guide to Integrating Forensic Techniques into Incident Response (Kent и сар., 2006) и Guidelines for Digital Forensics First Responders (Interpol, 2021). Наравно, потребно је образложити разлог употребе симболичке вештачке интелигенције у време процвата машинског учења и других видова вештачке интелигенције. Кроз дискусију се показало да други облици вештачке интелигенције не могу гарантовати ваљаност доказа на суду с обзиром на нетранспарентност начина функционисања и потенцијалне проблеме као што су пристрасност, халуцинације, проблем објашњивости и др.

Верификаторни резултат овог истраживања подупире тврђење да праћење стандарда ваљане форензичке истраге од стране форензичара који вештаче, гарантује ваљаност дигиталних доказа на суду и тиме смањује могућност оспоравања налаза и мишљења. У складу са хипотезом овог истраживања (специфицираном у одељку 1.3), којом употреба система базираног на формалном моделу форензичких стандарда и водича претендује на већу ефективност и ефикасност у проналажењу и документовању дигиталних трагова, експериментом је симулирана оваква форензичка истрага уз учешће студената као неискусних форензичара, који ваљаност својих поступака у истрази доказују тачним одговорима на питања теста. Дакле, употреба система базираног на поменутом формалном опису форензичких стандарда и водича позитивно је утицао на ефективност спровођења форензичке истраге рачунарских мрежа у целини. Међутим, верификаторни резултат овог истраживања има нарочит значај у погледу појединачних фаза истраге – идентификације, прикупљања, прегледања и анализе дигиталних доказа. Позитиван утицај система на ефективност неискусних форензичара констатован је у фазама идентификације, прикупљања и прегледања дигиталних доказа. Насупрот овим фазама, позитиван утицај на ефективност у спровођењу истраге не може се тврдити за фазу анализе дигиталних доказа. Поред тога, систем базиран на формалном опису форензичких стандарда позитивно утиче и на ефикасност спровођења форензичке истраге рачунарских мрежа. Тиме су резултати верификације наведене хипотезе, која је описана у поглављу 6, показали њену потврду.

Резултати истраживања описаног овом дисертацијом верификовани су објављивањем научних радова. Онтологија и дизајн система за вођење кроз форензичку истрагу објављени су у међународном часопису (Matijević Gostojić и Vuković, 2023), а рад који представља пројекат и имплементацију система базираног на онтологији, као и рад у коме је описан експеримент са резултатима, презентовани су на међународној конференцији (Matijević Gostojić и сар., 2024a,b).

За разлику од претходећих истраживања, за креирање онтологије овог ис-

траживања узето је у обзир више комплементарних стандарда и водича за ваљано спровођење дигиталне форензичке истраге. Такође, свака фаза истраге је подвргнута методу појединачно, чиме је свакој фази истраге придата једнака важност. Овоме се додаје и ширина области форензике рачунарских мрежа која је покривена онтологијом, као и могућност да се дата онтологија по истом принципу прошири на друге области дигиталне форензике.

У одељку 7.4 изнете су претње по валидност истраживања, које су и образложене. Међутим, постоје мане овог истраживања, које се могу превазићи у даљњим истраживањима. Мана онтологије, односно базе знања, тиче се ручног начина популисања онтологије инстанцама, што представља мукотрпан и обиман посао. Такође, опис домена дигиталне форензике онтологијом ограничен је на форензику рачунарских мрежа.

Визија за будуће унапређење продукта овога истраживања постоји у погледу онтологије и у погледу система који се базира на онтологији. Креирање концепата и инстанци онтологије изведено је увидом у стандарде и водиче, као и уграђивањем искуства стеченог радом у Лабораторији. Обогаћивање онтологије инстанцама у будућности се потенцијално може аутоматизовати креирањем парсера текста или употребом технологије обраде природног језика. Поред тога, комплетан систем би се могао унапредити тако да у потпуности буде вођен онтологијом. То значи да будући рад обухвата интеграцију постојеће онтологије која описује компоненте корисничког интерфејса и која би се надоградила и прилагодила постојећем систему. Тиме би се уклонила потреба за будућим редундантним радом над графичким корисничким интерфејсом у случају надограђивања концепата онтологије.

Такође, предмет даљњих истраживања свакако је проширење на друге подобласти дигиталне форензике, како онтологије, тако и система. Проширење онтологије на друге подобласти дигиталне форензике подразумева придруживање посебних модула постојећој интегришућој онтологији, који садрже концепте одређених подобласти дигиталне форензике, као и паралелно обогаћивање онтологије инстанци инстанцама ових концепата.

Као што се модел форензичке истраге који укључује фазу идентификације, прикупљања, прегледања и анализе доказа и оперативне форме података у овим фазама – потенцијални извор доказа, складиште података, врсту података и информацију, уклапа у област форензике рачунарских мрежа, по истом принципу би се уклопио са другим областима. На пример, увођење онтологије форензике мобилних телефона изискивало би најпре придруживање модула онтологије са концептима поменутих оперативних форми карактеристичних за мобилне телефоне. Затим би било потребно повезивање овог модула са модулом онтологије форензике мобилних телефона, који садржи концепте и дефиниције активности руковања оперативним формама, као и концепте и дефиниције ваљаног руковања оперативним формама у виду захтева ваљаности.

Како се систем тренутно користи у оквиру Лабораторије за дигиталну форензику као водич за ваљано спровођење истраге тако што кориснику предочава производ расуђивања над постојећом базом знања, отворена је могућност обогаћивања базе знања искуством форензичара у Лабораторији. Зато је пред-

мет даљњег истраживања и увођење посебног режима рада система који би био резервисан за обогаћивање онтологије искуством форензичара Лабораторије. Ово би захтевало разрађивање радног оквира који налаже форензичару строго праћење структуре онтологије како би новоунето знање било логички коректно.

Наравно, не треба се ограничити на употребу система само у оквиру Лабораторије за дигиталну форензику. Стога је у плану да систем убудуће буде коришћен од стране студената на курсу „Увод у дигиталну форензику", као и да се прикупљају квалитативни подаци о употреби система с циљем његовог унапређивања.

Како се прототипска имплементација система одликује избором технологије која је у складу са окружењем Лабораторије за дигиталну форензику, у перспективи постоји тежња да се развију и угради безбедносни механизми који би омогућили употребу система преко Интернета. У том случају, употреба система при вештачењу у правном поступку изискивала би правдање и преузимање одговорности за изношење поверљивих података изван зидова лабораторије.

Друштвени проблем чијем решењу доприноси ово истраживање најзначајнији је из перспективе актера у судским поступцима, који желе задовољење правде. Данас се дигитални уређаји ретко не налазе у потенцијалном доказном материјалу судских поступака. Понекад дигитални уређаји садрже доказе за почињена кривична дела која предвиђају строге казне, па је на форензичарима-вештацима изузетно велика одговорност и обавеза да истрагу спроведу ваљано. Дакле, решење проблема неваљане дигиталне форензичке истраге са аспекта задовољења правде на првом је месту друштвених доприноса овог истраживања. Ако се узму у обзир вештачења у области информационих технологија уопште, кредибилитет форензичара-вештака неретко може бити доведен у питање када је форензичар неискусан, односно на почетку каријере. Зато је неопходна аутоматизована помоћ, која нуди три најбитније компоненте форензичареве екпертизе, теоријско знање, познавање смерница добре праксе и практично знање, односно искуство.

9 Референце

Akremi, A., Sallay, H., Rouached, M., Bouaziz, R., Abid, M., 2015. Forensics-aware web services composition and ranking, in: Proceedings of the 17th International Conference on Information Integration and Web-based Applications & Services, pp. 1–10.

Akremi, A., Sriti, M.F., Sallay, H., Rouached, M., 2020. Ontology-based smart sound digital forensics analysis for web services, in: Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice. IGI Global, pp. 497–520.

Alzaabi, M., 2013. Ontology-based forensic analysis of mobile devices, in: 2013 IEEE 20th International Conference on Electronics, Circuits, and Systems (ICECS), IEEE. pp. 64–65.

Amato, F., Castiglione, A., Cozzolino, G., Narducci, F., 2020. A semantic-based methodology for digital forensics analysis. Journal of Parallel and Distributed Computing 138, 172–177.

Antwi-Boasiako, A., Venter, H., 2017. A model for digital evidence admissibility assessment, in: Advances in Digital Forensics XIII: 13th IFIP WG 11.9 International Conference, Orlando, FL, USA, January 30-February 1, 2017, Revised Selected Papers 13, Springer. pp. 23–38.

Arrieta, A.B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., cap., 2020. Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible ai. Information fusion 58, 82–115.

Arshad, H., Jantan, A., Hoon, G.K., Abiodun, I.O., 2020. Formal knowledge model for online social network forensics. Computers & security 89, 101675.

Auer, S., Bizer, C., Kobilarov, G., Lehmann, J., Cyganiak, R., Ives, Z., 2007. Dbpedia: A nucleus for a web of open data, in: international semantic web conference, Springer. pp. 722–735.

Baader, F., 2003. The description logic handbook: Theory, implementation and applications. Cambridge university press.

Baader, F., 2010. The Description Logic Handbook Theory, Implementation and Applications. Cambridge University Press.

Baader, F., Horrocks, I., Lutz, C., Sattler, U., 2017. An Introduction to Description Logic. Cambridge University Press.

Barman, K.G., Wood, N., Pawlowski, P., 2024. Beyond transparency and explainability: on the need for adequate and contextualized user guidelines for llm use. Ethics and Information Technology 26, 47.

Barnum, S., 2012. Standardizing cyber threat intelligence information with the structured threat information expression (stix). Mitre Corporation 11, 1–22.

Barnum, S., Martin, R., Worrell, B., Kirillov, I., 2012. The cybox language specification. The MITRE Corporation .

Berners-Lee, T., Bizer, C., Heath, T., 2009. Linked data - the story so far. International Journal on Semantic Web and Information Systems 5, 1–22.

Bogišić, V., 1898. Opšti imovinski zakonik za Knjaževinu Crnu Goru. Državna štamparija na Cetinju.

Brady, O., Overill, R., Keppens, J., 2015. Deso: Addressing volume and variety in large-scale criminal cases. Digital Investigation 15, 72–82.

Brinson, A., Robinson, A., Rogers, M., 2006. A cyber forensics ontology: Creating a new approach to studying cyber forensics. digital investigation 3, 37–43.

Brooks, C.L., 2015. CHFI Computer Hacking Forensic Investigator Certification All-in-One Exam Guide. All-in-one, McGraw-Hill Education. URL: http://gen.lib.rus.ec/book/index.php?md5=89ADA1EE22A1057E997E3F2D66F3CE89.

Carrier, B., 2005. File System Forensic Analysis. Addison-Wesley.

Carrier, B., Spafford, E., 2004. An event-based digital forensics investigation process. Digital Forensics Research Workshop (DFRWS) .

Casey, E., 2004. Digital evidence and computer crime: forensic science, computers and the Internet. 2nd ed ed., Academic Press. URL: http://gen.lib.rus.ec/book/index.php?md5=c586b7e1d9e81650fc62d8bfb73bea92.

Casey, E., 2011. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.

Casey, E., 2012. Cyberpatterns. Criminal Profiling , 361–378.

Casey, E., Back, G., Barnum, S., 2015. Leveraging cybox™ to standardize representation and exchange of digital forensic information. Digital Investigation 12, S102–S110.

Casey, E., Barnum, S., Griffith, R., Snyder, J., van Beek, H., Nelson, A., 2018. The evolution of expressing and exchanging cyber-investigation information in a standardized form. Handling and Exchanging Electronic Evidence Across Europe , 43–58.

Chaikin, D., 2006. Network investigations of cyber attacks: the limits of digital evidence. Crime, Law and Social Change 46, 239–256.

Chu, H.C., Deng, D.J., Chao, H.C., 2011. An ontology-driven model for digital forensics investigations of computer incidents under the ubiquitous computing environments. Wireless Personal Communications 56, 5–19.

Cisco, 2011. Wired 802.1X Deployment Guide. Available: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html.

Ćosić, J., Ćosić, Z., Bača, M., 2011. An ontological approach to study and manage digital chain of custody of digital evidence. Journal of Information and Organizational Sciences 35, 1–13.

Cuzzocrea, A., Pirrò, G., 2016. A semantic-web-technology-based framework for supporting knowledge-driven digital forensics, in: Proceedings of the 8th International Conference on Management of Digital EcoSystems, pp. 58–66.

De Paola, A., Gatani, L., Re, G.L., Pizzitola, A., Urso, A., 2003. A network ontology for computer network management. Tech. Rep. 22 .

Dosis, S., Homem, I., Popov, O., 2013. Semantic representation and integration of digital evidence. Procedia Computer Science 22, 1266–1275.

Ellison, D., Ikuesan, R.A., Venter, H.S., 2019. Ontology for reactive techniques in digital forensics, in: 2019 IEEE Conference on Application, Information and Network Security (AINS), IEEE. pp. 83–88.

Ellison, D., Venter, H., 2016. An ontology for digital security and digital forensics investigative techniques, in: Proceedings of the 11th international conference on cyber warfare and security, ICCWS, pp. 119–127.

ENISA, 2019. Introduction to Network Forensics. European Union Agency For Cybersecurity.

Europol, 2019. Internet organized crime threat assessment. The Hague: Europol .

Fenz, S., Goluch, G., Ekelhart, A., Riedl, B., Weippl, E., 2007. Information security fortification by ontological mapping of the iso/iec 27001 standard, in: 13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007), IEEE. pp. 381–388.

Fenz, S., Plieschnegger, S., Hobel, H., 2016. Mapping information security standard iso 27002 to an ontological structure. Information & Computer Security 24, 452–473.

Ferrazzano, M., Raffaella, B., cap., 2021. Digital forensics: best practices and perspective. COLLEZIONE DI GIUSTIZIA PENALE , 13–48.

Forum of Incident Response and Security Teams, 2005. Common vulnerability scoring system. URL: https://www.first.org/cvss/ .

Garfinkel, S., 2012. Digital forensics xml and the dfxml toolset. Digital Investigation 8, 161–174.

Garfinkel, S.L., 2010. Digital forensics research: The next 10 years. digital investigation 7, S64–S73.

Group, D..K., 2021. HermiT OWL Reasoner. Available: http://www.hermit-reasoner.com/.

Håkansson, A., Phillips-Wren, G., 2024. Generative ai and large language models-benefits, drawbacks, future and recommendations. Procedia Computer Science 246, 5458–5468.

Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W., 2009. Lest we remember: cold-boot attacks on encryption keys. Communications of the ACM 52, 91–98.

Hall, S.W., Sakzad, A., Choo, K.K.R., 2022. Explainable artificial intelligence for digital forensics. Wiley Interdisciplinary Reviews: Forensic Science 4, e1434.

Hardt, D., 2012. The OAuth 2.0 Authorization Framework. RFC 6749. URL: https://www.rfc-editor.org/info/rfc6749, doi:10.17487/RFC6749.

Hayes, D.R., 2020. A Practical Guide to Digital Forensics Investigations, 2nd Edition. Pearson IT Certification. URL: http://gen.lib.rus.ec/book/index.php?md5=90CFF242EE3DB14506856D08A08A01B0.

van Heerden, R.P., Irwin, B., Burke, I., 2012. Classifying network attack scenarios using an ontology, in: Proceedings of the 7th International Conference on Information-Warfare & Security (ICIW 2012), Academic Conferences and Publishing International Limited, Seattle, USA. pp. 311–324.

Horsman, G., 2019. Formalising investigative decision making in digital forensics: Proposing the digital evidence reporting and decision support (derds) framework. Digital Investigation 28, 146–151.

Horsman, G., Shavers, B., 2022. Who is the digital forensic expert and what is their expertise? Wiley Interdisciplinary Reviews: Forensic Science 4, e1453.

Hoss, A.M., Carver, D.L., 2009. Weaving ontologies to support digital forensic analysis, in: 2009 IEEE International Conference on Intelligence and Security Informatics, IEEE. pp. 203–205.

Houghton Mifflin Company, 2000. American Heritage Dictionary, 4th ed. Boston: Houghton Mifflin.

Iannacone, M., Bohn, S., Nakamura, G., Gerth, J., Huffer, K., Bridges, R., Ferragut, E., Goodall, J., 2015. Developing an ontology for cyber security knowledge graphs, in: Proceedings of the 10th annual cyber and information security research conference, pp. 1–4.

IEEE Standards, 2001. Ieee standard for port based network access control. IEEE Std 802.1X-2001 , 1–140doi:10.1109/IEEESTD.2001.92774.

Ieong, R.S., 2006. Forza–digital forensics investigation framework that incorporate legal issues. digital investigation 3, 29–36.

Interpol, 2021. Guidelines for Digital Forensics First Responders. Interpol.

ISO/IEC 27037, 2015. ISO/IEC 27037:2012 – Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Institute for Standardization of Serbia.

ISO/IEC 27041, 2016. ISO/IEC 27041:2016 – Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method. Institute for Standardization of Serbia.

ISO/IEC 27042, 2016. ISO/IEC 27042:2016 – Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence. Institute for Standardization of Serbia.

ISO/IEC 27043, 2016. ISO/IEC 27043:2016 – Information technology – Security techniques – Incident investigation principles and processes. Institute for Standardization of Serbia.

ISO/IEC FDIS 27001, 2005. ISO/IEC FDIS 27001 Information technology – Security techniques – Information security management systems. ISO copyright office. Geneva, Switzerland.

Jain, N., Bhansali, A., Mehta, D., 2014. Angularjs: A modern mvc framework in javascript.

Jinad, R., Islam, A., Shashidhar, N., 2024. Interpretability and transparency of machine learning in file fragment analysis with explainable artificial intelligence. Electronics 13, 2438.

Jones, M.B., Bradley, J., Sakimura, N., 2015. JSON Web Token (JWT). RFC 7519. URL: https://www.rfc-editor.org/info/rfc7519, doi:10.17487/RFC7519.

Kabaale, E., Wen, L., Wang, Z., Rout, T., 2018. Ensuring conformance to process standards through formal verification, in: Software Process Improvement and Capability Determination: 18th International Conference, SPICE 2018, Thessaloniki, Greece, October 9–10, 2018, Proceedings 18, Springer. pp. 248–262.

Kahvedžić, D., Kechadi, T., 2008. Extraction of user activity through comparison of windows restore points .

Kahvedžić, D., Kechadi, T., 2009. Dialog: A framework for modeling, analysis and reuse of digital forensic knowledge. digital investigation 6, S23–S33.

Kahvedžić, D., Kechadi, T., 2011. Semantic modelling of digital forensic evidence, in: Digital Forensics and Cyber Crime: Second International ICST Conference, ICDF2C 2010, Abu Dhabi, United Arab Emirates, October 4-6, 2010, Revised Selected Papers 2, Springer. pp. 149–156.

Kelly, L., Sachan, S., Ni, L., Almaghrabi, F., Allmendinger, R., Chen, Y.W., 2020. Explainable artificial intelligence for digital forensics: Opportunities, challenges and a drug testing case study [online first], in: Digital Forensic Science [Working Title]. IntechOpen.

Kent, K., Chevalier, S., Grance, T., Dang, H., 2006. Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology, Technology Administration, U. S. Department of Commerce.

Komlen Nikolić, L., Gvozdenović, R., Radulović, S., Milosavljević, A., Jerković, R., Živković, V., Živanović, S., Mr Reljanović, M., Aleksić, I., 2010. Suzbijanje visokotehnološkog kriminala. Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije.

Lamy, J., 2017. Owlready: Ontology-oriented programming in python with automatic classification and high level constructs for biomedical ontologies.

Loos, J., 2012. Implementing ieee 802.1x for wired networks. Global Information Assurance Certification Paper .

Makura, S., Venter, H., Kebande, V.R., Karie, N.M., Ikuesan, R.A., Alawadi, S., 2021. Digital forensic readiness in operational cloud leveraging iso/iec 27043 guidelines on security monitoring. Security and Privacy 4, e149.

Mann, D., 2008. An introduction to the common configuration enumeration. URL: http://cce.mitre.org/about/documents.html .

Mann, D.E., Christey, S.M., 1999. Towards a common enumeration of vulnerabilities, in: 2nd Workshop on Research with Security Vulnerability Databases, Purdue University, West Lafayette, Indiana, p. 9.

Markus, K., František, S., Ian, H., 2013. A description logic primer, in: The description logic workshops.

Matijević Gostojić, M., Milosavljević, B., Vuković, Ž., 2024a. Deploying a knowledge-based system for supporting the soundness of digital forensic investigation on a laboratory server, in: Proceedings of the 23th International Conference on WWW/Internet 2024, IADIS.

Matijević Gostojić, M., Slivka, J., Vuković, Ž., Gostojić, S., 2024b. An effectiveness assessment of a knowledge-based system for supporting the soundness of digital forensic investigations, in: Proceedings of the 23th International Conference on WWW/Internet 2024, IADIS.

Matijević, M., Gostojić, S., 2021. Ontology-driven approach for evidence admissibility in network forensics, in: Proceedings of the 11th International Conference on Information Society and Technology (ICIST 2021), In: Zdravković, M., Trajanović, M., Konjović, Z. (Eds.). pp. 11–16.

Matijević Gostojić, M., Vuković, Ž., 2023. A knowledge-based system for supporting the soundness of digital forensic investigations. Forensic Science International: Digital Investigation 46, 301601.

McKemmish, R., 2008. When is digital evidence forensically sound? Springer.

Meyers, M., Rogers, M., 2005. Digital forensics: Meeting the challenges of scientific evidence, in: Advances in Digital Forensics: IFIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, February 13–16, 2005 1, Springer. pp. 43–50.

Mohammed, H., Clarke, N., Li, F., 2016. An automated approach for digital forensic analysis of heterogeneous big data. Journal of Digital Forensics, Security and Law 11, 9.

Mussmann, A., Brunner, M., Breu, R., 2020. Mapping the state of security standards mappings., in: Wirtschaftsinformatik (zentrale tracks), pp. 1309–1324.

Noblett, M.G., Pollitt, M.M., Presley, L.A., 2000. Recovering and examining computer forensic evidence. Forensic Science Communications 2.

Normurod o'g'li, T.B., cap., 2023. The statistics of cyber-crime among the world. JOURNAL OF INNOVATIONS IN SCIENTIFIC AND EDUCATIONAL RESEARCH 6, 812–814.

Obradović, S., Sentić, M., 1959. Osnovi statističke analize. Naučna knjiga.

Office of the Director of National Intelligence, 2015. Xml data encoding specification for intelligence document and media exploitation. URL: https://www.dni.gov/index.php/who-we-are/organizations/ic-cio/ic-cio-related-menus/ic-cio-related-links/ic-technical-specifications/document-and-media-exploitation .

Palekar, A., Josefsson, S., Simon, D., Zorn, G., 2004. Protected EAP Protocol (PEAP) Version 2. Internet-Draft draft-josefsson-pppext-eap-tls-eap-10. Internet Engineering Task Force. URL: https://datatracker.ietf.org/doc/draft-josefsson-pppext-eap-tls-eap/10/. work in Progress.

Pallets, 2010. Flask web development, one drop at a time. URL: https://flask.palletsprojects.com/en/2.0.x/.

Palmer, G., 2001. A road map for digital forensics research-report from the first digital forensics research workshop (dfrws). Utica, New York .

Pereira, T., Santos, H., 2009. An ontology based approach to information security, in: Research Conference on Metadata and Semantic Research, Springer. pp. 183–192.

Petrović, S.R., 2001. Kompjuterski kriminal. Ministarstvo unutrašnjih poslova Republike Srbije.

Pfeifer, B., Krzyzinski, M., Baniecki, H., Saranti, A., Holzinger, A., Biecek, P., 2023. Explainable ai with counterfactual paths. arXiv preprint arXiv:2307.07764 .

Ramanauskaite, S., Shein, A., Čenys, A., Rastenis, J., 2022. Security ontology structure for formalization of security document knowledge. Electronics 11, 1103.

Rudolph, S., 2011. Foundations of description logics, in: Reasoning Web International Summer School. Springer, pp. 76–136.

Saad, S., Traore, I., 2010. Method ontology for intelligent network forensics analysis, in: 2010 Eighth International Conference on Privacy, Security and Trust, IEEE. pp. 7–14.

Šarkić, N., Nikolić, M., 2011. Priručnik o veštačenju: Veštačenje kao dokazno sredstvo. IP „Glosarijum" Beograd.

Schatz, B., Mohay, G., Clark, A., 2004a. Generalising event forensics across multiple domains, in: 2nd Australian Computer Networks Information and Forensics Conference, School of Computer and Information Science, Edith Cowan University. pp. 136–144.

Schatz, B., Mohay, G., Clark, A., 2004b. Rich event representation for computer forensics, in: Proceedings of the Fifth Asia-Pacific Industrial Engineering and Management Systems Conference (APIEMS 2004), Queensland University of Technology Publications Brisbane, Australia. pp. 1–16.

Sikos, L.F., 2021. Ai in digital forensics: Ontology engineering for cybercrime investigations. Wiley Interdisciplinary Reviews: Forensic Science 3, e1394.

Slay, J., Schulz, F., 2014. Development of an ontology based forensic search mechanism: Proof of concept. arXiv preprint arXiv:1407.8258 .

Smith, A.H., Zorn, G., Roese, J., Aboba, D.B.D., Congdon, P., 2003. IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines. RFC 3580. URL: https://www.rfc-editor.org/info/rfc3580, doi:10.17487/RFC3580.

Solanke, A.A., 2022. Explainable digital forensics ai: Towards mitigating distrust in ai-based digital forensics analysis using interpretable models. Forensic science international: digital investigation 42, 301403.

Suchanek, F.M., Kasneci, G., Weikum, G., 2008. Yago: A large ontology from wikipedia and wordnet. Journal of Web Semantics 6, 203–217.

Sunde, N., 2021. What does a digital forensics opinion look like? a comparative study of digital forensics and forensic science reporting practices. Science & justice 61, 586–596.

Syed, Z., Padia, A., Finin, T., Mathews, L., Joshi, A., 2016. Uco: A unified cybersecurity ontology, in: Workshops at the thirtieth AAAI conference on artificial intelligence.

Talib, A.M., Alomary, F.O., 2015. Towards a comprehensive ontology based-investigation for digital forensics cybercrime. Int J Commun Antenna Propag 5, 263–268.

Turnbull, B., Randhawa, S., 2015. Automated event and social network extraction from digital evidence sources with ontological mapping. Digital Investigation 13, 94–106.

Turvey, B.E., 2011. Criminal profiling: An introduction to behavioral evidence analysis. Academic press.

United States Department of Homeland Security, Office of Cybersecurity and Communications, 2007. Common attack pattern enumeration and classification. URL: https://capec.mitre.org/about/index.html .

Valjarevic, A., Venter, H.S., Ingles, M., 2014. Towards a prototype for guidance and implementation of a standardized digital forensic investigation process, in: 2014 Information Security for South Africa, IEEE. pp. 1–8.

Van Eijk, E., 2014. Digital forensics as a service: A game changer. Digital Investigation 11, S54–S62.

Whitcomb, C.M., 2002. An historical perspective of digital evidence: A forensic scientist's view. International Journal of Digital Evidence 1, 7–15.

Xian, Y., Schiele, B., Akata, Z., 2017. Zero-shot learning-the good, the bad and the ugly, in: Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 4582–4591.

Yeboah-Ofori, A., Brown, A.D., 2020. Digital forensics investigation jurisprudence: issues of admissibility of digital evidence. Journal of Forensic, Legal & Investigative Sciences 6, 1–8.

Zorn, G., Aboba, D.B.D., 1999. RADIUS Authentication Server MIB. RFC 2619. URL: https://www.rfc-editor.org/info/rfc2619, doi:10.17487/RFC2619.

Årnes, A., 2023. Cyber Investigations: A Research Based Introduction for Advanced Studies. Wiley. URL: http://gen.lib.rus.ec/book/index.php?md5=74EB034CC085FAF9FAD3F8F0904C7F90.

Биографија

Милица Матијевић Гостојић рођена је 10. 10. 1996. године у Сомбору, Република Србија. Основне академске студије Рачунарства и аутоматике на Факултету техничких наука Универзитета у Новом Саду завршила је 2019. године. Мастер академске студије Рачунарства и аутоматике на Факултету техничких наука Универзитета у Новом Саду завршила је 2021. године.

Од 2019. до 2021. године радила је као сарадник у настави на Катедри за информатику Факултета техничких наука Универзитета у Новом Саду, а од 2021. године на истој катедри ради као асистент. Држи вежбе на предметима Увод у дигиталну форензику, Интернет мреже, Напредна Интернет инфраструктура, Безбедност рачунарских мрежа и Инжењеринг знања. Упоредо ради као сарадник Лабораторије за дигиталну форензику Факултета техничких наука Универзитета у Новом Саду.

Објавила је пет научних радова у међународним часописима и на конференцијама, при чему је један рад објављен у часопису са SCI листе.

Прилог 1: Тест експеримента

Име и презиме: _____

Група: К / Е Време почетка: _____ Време завршетка: _____

ТЕСТ

Извори доказа: **свич 1**, **рутер 1**, **веб-сервер**

ИДЕНТИФИКАЦИЈА

1. Произвођач свича 1 је _____
2. Модел свича 1 је _____
3. Додатна форензичка опрема потребна за истрагу свича 1 је _____ _____
4. Произвођач рутера 1 је _____
5. Модел рутера 1 је _____
6. Додатна форензичка опрема потребна за истрагу рутера 1 је _____ _____
7. Повезивање са рутером 1 могуће је _____каблом путем порта _____
8. Назив веб-сервера је _____
9. Верзија веб-сервера је _____

ПРИКУПЉАЊЕ

1. Да би се сав мрежни саобраћај из приватне мреже 10.10.10.0 преусмерио на форензичку машину, на свичу 1 је конфигурисан _____ _____
2. Алат за прислушкивање мрежног саобраћаја, који мора бити инсталиран на форензичкој машини је _____
3. Алат за прислушкивање мрежног саобраћаја слуша на интерфејсу _____
4. Време почетка прислушкивања мрежног саобраћаја је _____
5. Време завршетка прислушкивања мрежног саобраћаја је _____
6. Формат датотеке у којој се чува снимак мрежног саобраћаја је _____
7. Приступ интерфејсу командне линије на рутеру 1 добијен је повезивањем форензичке машине са рутером 1 путем порта _____

ПРЕГЛЕДАЊЕ

1. Филтрирање мрежних пакета унутар снимка мрежног саобраћаја урађено је употребом филтара _____
2. Дошло је до губљења мрежних пакета услед преусмеравања мрежног саобраћаја на форензичку машину ДА НЕ
3. Начин на који је могуће проверити да ли је дошло до губљења мрежних пакета услед преусмеравања мрежног саобраћаја је _____
4. Команда којом се добија увид у лог сервиса NAT конфигурисаног на рутеру 1 је _____ _____
5. Путања лога приступања веб-серверу је _____
6. Лог приступања веб-серверу бележи приватне IP адресе клијената ДА НЕ

7. Формат лога приступања веб-серверу је _____
   _____

АНАЛИЗА

1. Јавна IP адреса мреже предузећа је _____
2. Приватна IP адреса рачунара са кога је приступано веб-сајту domen.com је
   _____
3. Приватне IP адресе рачунара са којих је приступано Apache2 HTTP веб-серверу су
   _____
4. Ресурс (датотека) коју Apache2 HTTP сервер шаље клијентима на захтев је
   _____
5. Веб-претраживач који је користио малициозни запослени приликом приступања Apache2 HTTP веб-серверу је _____

Прилог 2: Анкета експеримента

УПИТНИК

* Попуњавање упитника је анонимно, а прикупљени подаци ће бити коришћени у сврхе истраживања ефикасности софтвера за вођење форензичке истраге

	апсолутно се не слажем				апсолутно се слажем
Упознавање са начином употребе софтвера је једноставно	1	2	3	4	5
Коришћење софтвера је једноставно	1	2	3	4	5
Кориснички интерфејс је интуитиван	1	2	3	4	5
Олакшана ми је фаза идентификације у задатку	1	2	3	4	5
Олакшана ми је фаза прикупљања у задатку	1	2	3	4	5
Олакшана ми је фаза прегледања у задатку	1	2	3	4	5
Олакшана ми је фаза анализе у задатку	1	2	3	4	5
Препоручио/ла бих овај софтвер	1	2	3	4	5

Недостаци софтвера:

_____

_____

_____

Предности софтвера:

_____

_____

_____

Предлози за унапређење софтвера:

_____

_____

_____

План третмана података

Назив пројекта/истраживања
Обезбеђивање ваљаности форензичке истраге применом дескриптивне логике
Назив институције/институција у оквиру којих се спроводи истраживање
Лабораторија за дигиталну форензику, Факултет техничких наука, Универзитет у Новом Саду
Назив програма у оквиру ког се реализује истраживање
Рачунарство и аутоматика – докторска дисертација

1. Опис података

1.1 Врста студије

Укратко описати тип студије у оквиру које се подаци прикупљају

У оквиру докторске дисертације спроведен је експеримент којим су се прикупили подаци за верификацију система за вођење кроз ваљану форензичку истрагу.

1.2 Врсте података

а) **квантитативни**

б) **квалитативни**

1.3. Начин прикупљања података

а) **анкете, упитници, тестови**

б) клиничке процене, медицински записи, електронски здравствени записи

в) генотипови: навести врсту _____

г) административни подаци: навести врсту _____

д) узорци ткива: навести врсту_____

ђ) снимци, фотографије: навести врсту_____

е) текст, навести врсту _____

ж) мапа, навести врсту _____

з) остало: описати _____

1.3 Формат података, употребљене скале, количина података

1.3.1 Употребљени софтвер и формат датотеке:

a) Excel фајл, датотека _____

b) SPSS фајл, датотека _____

c) PDF фајл, датотека _____

d) Текст фајл, датотека _____

e) JPG фајл, датотека _____

f) **Остало, датотека .ods**

1.3.2. Број записа (код квантитативних података)

а) број варијабли **2 зависне варијабле**

б) број мерења (испитаника, процена, снимака и сл.) **60 испитаника**

1.3.3. Поновљена мерења

а) да

б) **не**

Уколико је одговор да, одговорити на следећа питања:

а) временски размак између поновљених мера је _____

б) варијабле које се више пута мере односе се на _____

в) нове верзије фајлова који садрже поновљена мерења су именоване као _____

Напомене: _____

Да ли формати и софтвер омогућавају дељење и дугорочну валидност података?

а) ***Да***

б) Не

Ако је одговор не, образложити _____

_____

2. Прикупљање података

2.1 Методологија за прикупљање/генерисање података

2.1.1. У оквиру ког истраживачког нацрта су подаци прикупљени?

а) **експеримент**, навести тип **пост-тест са контролном групом**

б) корелационо истраживање, навести тип _____

ц) анализа текста, навести тип _____

д) остало, навести шта _____

2.1.2 Навести врсте мерних инструмената или стандарде података специфичних за одређену научну дисциплину (ако постоје).

тест, анкетни упитник

2.2 Квалитет података и стандарди

2.2.1. Третман недостајућих података

а) Да ли матрица садржи недостајуће податке? Да **Не**

Ако је одговор да, одговорити на следећа питања:

а) Колики је број недостајућих података? _____

б) Да ли се кориснику матрице препоручује замена недостајућих података? Да Не

в) Ако је одговор да, навести сугестије за третман замене недостајућих података

_____

2.2.2. На који начин је контролисан квалитет података? Описати

Сви испитаници имали су предзнање потребно за одговарање на питања теста. Одговори испитаника потом су евалуирани од стране експерта у области.

2.2.3. На који начин је извршена контрола уноса података у матрицу?

Резултат евалуације одговора испитаника на питања теста је 0 или 1. Уколико испитаник није одговорио на питање теста или је дао нетачан одговор, забележена вредност је 0. Уколико је испитаник дао тачан одговор, забележена вредност је 1.

3. Третман података и пратећа документација

3.1. Третман и чување података

*3.1.1. Подаци ће бити депоновани у **Zenodo** репозиторијум.*

3.1.2. URL адреса ***https://zenodo.org/records/16961228***

3.1.3. DOI ***10.23728/b2share.bd0ebebfcae54e4fa34c9a6585d67d0c***

3.1.4. Да ли ће подаци бити у отвореном приступу?

а) ***Да***

б) *Да, али после ембарга који ће трајати до _____*

в) *Не*

Ако је одговор не, навести разлог _____

3.1.5. Подаци неће бити депоновани у репозиторијум, али ће бити чувани.

Образложење

_____

_____

3.2 Метаподаци и документација података

3.2.1. Који стандард за метаподатке ће бити примењен?

Стандард за метаподатке који користи репозиторијум *Zenodo* за складиштење истраживачких резултата.

3.2.1. Навести метаподатке на основу којих су подаци депоновани у репозиторијум.

author: Matijević Gostojić, Milica; title: An Effectiveness Assessment of a Knowledge-Based System for Supporting the Soundness of Digital Forensic Investigations; year: 2025; subjects: digital forensics, evidence admissibility, knowledge representation, evaluation.

Ако је потребно, навести методе које се користе за преузимање података, аналитичке и процедуралне информације, њихово кодирање, детаљне описе варијабли, записа итд.

_____

_____

_____

_____

3.3 Стратегија и стандарди за чување података

3.3.1. До ког периода ће подаци бити чувани у репозиторијуму? _____

3.3.2. Да ли ће подаци бити депоновани под шифром? Да **Не**

3.3.3. Да ли ће шифра бити доступна одређеном кругу истраживача? Да **Не**

3.3.4. Да ли се подаци морају уклонити из отвореног приступа после извесног времена?

Да **Не**

Образложити

_____

_____

4. Безбедност података и заштита поверљивих информација

Овај одељак МОРА бити попуњен ако ваши подаци укључују личне податке који се односе на учеснике у истраживању. За друга истраживања треба такође размотрити заштиту и сигурност података.

4.1 Формални стандарди за сигурност информација/података

Истраживачи који спроводе испитивања с људима морају да се придржавају Закона о заштити података о личности *(https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html)* и одговарајућег институционалног кодекса о академском интегритету.

4.1.2. Да ли је истраживање одобрено од стране етичке комисије? **Да** Не

Ако је одговор Да, навести датум и назив етичке комисије која је одобрила истраживање

22. 5. 2024. Етичка комисија Факултета техничких наука Универзитета у Новом Саду

4.1.2. Да ли подаци укључују личне податке учесника у истраживању? **Да** Не

Ако је одговор да, наведите на који начин сте осигурали поверљивост и сигурност информација везаних за испитанике:

а) Подаци нису у отвореном приступу

б) **Подаци су анонимизирани**

ц) Остало, навести шта

_____

_____

5. Доступност података

5.1. Подаци ће бити

а) ***јавно доступни***

б) доступни само уском кругу истраживача у одређеној научној области

ц) затворени

Ако су подаци доступни само уском кругу истраживача, навести под којим условима могу да их користе:

_____

_____

Ако су подаци доступни само уском кругу истраживача, навести на који начин могу приступити подацима:

_____

_____

5.4. Навести лиценцу под којом ће прикупљени подаци бити архивирани.

Creative Commons Attribution-NonCommercial-NoDerivs (CC-BY-NC-ND)

6. Улоге и одговорност

6.1. Навести име и презиме и мејл адресу власника (аутора) података

Милица Матијевић Гостојић, matijevicmilica@uns.ac.rs

6.2. Навести име и презиме и мејл адресу особе која одржава матрицу с подацима

Милица Матијевић Гостојић, matijevicmilica@uns.ac.rs

6.3. Навести име и презиме и мејл адресу особе која омогућује приступ подацима другим

истраживачима

Милица Матијевић Гостојић, matijevicmilica@uns.ac.rs