Izgradnja otvorenog okvira za uspostavu i očuvanje lanca dokaza u forenzičkoj analizi digitalnih dokaza

Ćosić, Jasmin

Sveučilište u Zagrebu

Fakultet organizacije i informatike

Jasmin Ćosić

IZGRADNJA OTVORENOG OKVIRA ZA USPOSTAVU I OČUVANJE LANCA DOKAZA U FORENZIČKOJ ANALIZI DIGITALNIH DOKAZA

DOKTORSKI RAD

Varaždin, 2014.

PODACI O DOKTORSKOM RADU

I. AUTOR

Ime i prezime	Jasmin Ćosić
Datum i mjesto rođenja	26.07.1970.godine, Bosanska Krupa, Bosna i Hercegovina
Naziv fakulteta i datum diplomiranja na VII/I stupnju	Fakultet informacionih tehnologija, FIT Mostar, 15.10.2006.godine
Sadašnje zaposlenje	Ministarstvo unutarnjih poslova Unsko-sanske županije, BiH

II. DOKTORSKI RAD

Naslov	Izgradnja otvorenog okvira za uspostavu i očuvanje lanca dokaza u forenzičkoj analizi digitalnih dokaza
Broj stranica, slika, tabela, priloga, bibliografskih podataka	185 stranica, 48 slika, 12 tablica, 20 kodova, 5 priloga, 128 bibliografskih podataka
Znanstveno područje i polje iz kojeg je postignut doktorat znanosti	Društvene znanosti, informacijske i komunikacijske znanosti
Mentori ili voditelji rada	Prof.dr.sc. Miroslav Bača, mentor Doc.dr.sc. Markus Schatten, mentor 2
Fakultet na kojem je obranjen doktorski rad	Fakultet organizacije i informatike
Oznaka i redni broj rada	

III. OCJENA I OBRANA

Datum sjednice Fakultetskog vijeća na kojoj je prihvaćena tema	17.07.2012. godine
Datum predaje rada	24.01.2014. godine
Datum sjednice Fakultetskog vijeća na kojoj je prihvaćena pozitivna ocjena rada	23.04.2014. godine
Sastav povjerenstva koje je rad ocijenilo	Prof.dr.sc. Mirko Maleković, predsjednik Prof.dr.sc. Diana Šimić, članica Prof.dr.sc. Miroslav Bača, mentor i član Doc.dr.sc. Markus Schatten, mentor 2 i član Prof.dr.sc. Bernadin Ibrahimpašić, član
Datum obrane doktorskog rada	16.05.2014. godine
Sastav povjerenstva pred kojim je rad obranjen	Prof.dr.sc. Mirko Maleković, predsjednik Prof.dr.sc. Diana Šimić, članica Prof.dr.sc. Miroslav Bača, mentor i član Doc.dr.sc. Markus Schatten, mentor 2 i član Prof.dr.sc. Bernadin Ibrahimpašić, član
Datum promocije	

Sveučilište u Zagrebu

Fakultet organizacije i informatike

Jasmin Ćosić

IZGRADNJA OTVORENOG OKVIRA ZA USPOSTAVU I OČUVANJE LANCA DOKAZA U FORENZIČKOJ ANALIZI DIGITALNIH DOKAZA

DOKTORSKI RAD

Varaždin, 2014.

Sveučilište u Zagrebu

Fakultet organizacije i informatike

JASMIN ĆOSIĆ

IZGRADNJA OTVORENOG OKVIRA ZA USPOSTAVU I OČUVANJE LANCA DOKAZA U FORENZIČKOJ ANALIZI DIGITALNIH DOKAZA

DOKTORSKI RAD

Mentor(i):

Prof.dr.sc. Miroslav Bača
Doc.dr.sc. Markus Schatten

Varaždin, 2014.

University of Zagreb

Faculty of Organization and Informatics

Jasmin Ćosić

BUILDING AN OPEN FRAMEWORK FOR ESTABLISHING AND MAINTAINING THE CHAIN OF CUSTODY IN FORENSIC ANALYSIS OF DIGITAL EVIDENCE

DOCTORAL THESIS

Varaždin, 2014.

Mojoj porodici

ZAHVALE:

Zahvaljujem se svom mentoru prof.dr.sc. Bača Miroslavu na intenzivnoj pomoći tijekom pisanja ovog rada. Bez njegove riznice znanja o domeni digitalne forenzike, rad vjerojatno nikada ne vidio svjetlo dana u ovakvom obliku. Neformalni razgovor uz kavu na temu lanca dokaza, 2009. godine u Dugom selu kraj Zagreba, rezultirao je ovim radom. Veliko Hvala i ko-mentoru doc.dr.sc. Markus Schatten koji mi je nesebično pomogao u domeni formalizama i ontologija. Vrijeme koje je odvajao od svog sinčića kako bi testirao moja „pravila" i logiku funkcioniranja okvira, nikako mu neću moći nadomjestiti. Spoj ontologija i digitalne forenzike koji je napravljen s njima sasvim sigurno će biti vrijedan spomena u znanstvenoj zajednici.

Specijalne zahvale i prof.dr.sc. Mirku Malekoviću, profesoru koji mi je tijekom doktorskog studija pomogao da sva dešavanja i procese promatram kroz prizmu koncepata, atributa i relacija, te da shvatim bitnost baza znanja, deskripcijskih logika i rezoniranja, te sve to ukomponiram u digitalnu forenziku. Zahvaljujem se i prof.dr.sc. Diani Šimić na „terabajtima" znanja iz temelja znanstveno-istraživačkog rada, koje je nesebično podijelila sa mnom, te pomoći oko ideje provedenog istraživanja predstavljenog u radu. Zahvaljujem se prof.dr.sci. Bernadinu Ibrahimpašiću čiji su prijedlozi iz domena kriptografije doprinijeli tomu da rad bude još bolji. Specijalna zahvala i za kolegu i prijatelja mr.sci. Zorana Ćosića, sa kojim sam napisao i objavio veliki broj znanstvenih radova u domeni digitalne forenzike i biometrije.

Hvala mojim roditeljima - mome ocu i mojoj majci koji su me odgajali u duhu i svjetonazoru u kom su knjiga, znanje i učenje temeljne vrijednosti jednog društva.

Posljednje ali i najveće zahvale, i posveta rada u cijelosti, idu mojoj dragoj supruzi Edisi i voljenim kćerkama – Lejli i Zani na potpori i strpljenju, ohrabrenju, razumijevanju te bezuvjetnoj podršci, koje su imale sve vrijeme dok je trajala moja naobrazba i školovanje, a naročito posljednjih godinu dana pisanja doktorskog rada. Vrijeme koje sam mogao provesti sa njima, a proveo sam ga pišući ovaj rad svakako nije bilo provedeno uzaludno. Snagu i inspiraciju za istraživanje i pisanje crpio sam iz njihove ljubavi i strpljenja koje su imale za mene.

SAŽETAK

Krajnji cilj svake digitalne forenzičke istrage je zakonito pribavljen digitalni dokaz i prihvaćen od strane suda. To znači da svaki dokaz mora biti prikupljen kroz proces digitalne forenzičke istrage, a koji ne može početi bez naredbe suda, tužiteljstva ili uprave ukoliko se radi o internim istragama u poduzećima. U samom procesu digitalne forenzičke istrage mora se sačuvati i dokazati nepovredivost digitalnog dokaza kroz dokazivanje nepovredivosti lanca dokaza. To znači da se mora znati svakog trenutka, tko je, što, kada, kako, zašto i gdje dolazio u kontakt sa digitalnim dokazima. Ukoliko dođe do prekida lanca dokaza sud takve dokaze neće prihvatiti. Osnovni cilj ovoga rada je znanstveno istraživanje koje će dati uvid u pregled metoda održanja lanca digitalnih dokaza i metoda zaštite integriteta digitalnih dokaza, te pojašnjenje pojma životnog ciklusa digitalnih dokaza. Cilj je ukazati na nedostatke postojećih metoda i definiranja novih pravaca istraživanja u rješavanju problema lanca digitalnih dokaza primjenom ontologija digitalnih dokaza putem „DEMF“ (engl. *Digital Evidence Management Framework*) kroz koji bi se u svakom trenutku digitalne istrage točno znao odgovor na sva bitna pitanja sudionika u procesu digitalne istrage, ali bi se i održavao lanac dokaza. Krajnji cilj je formalno opisati pojmove koji se javljaju u procesu upravljanja digitalnim dokazima, te izgraditi okvir koji bi pomogao sudcima i drugim osobama koje se bave prihvatljivošću digitalnih dokaza.

U radu je izgrađena ontologija digitalnih dokaza i lanca dokaza, definirana su osnovna poslovna pravila (engl. *if-then rules*) a koja su glavni pokretač okvira koji omogućuje da se odredi koji je dokaz formalno prihvatljiv a koji ne. Urađena je i provjera valjanosti i vrednovanje izrađene ontologije, te su kreirane i instance koje su poslužile za testiranje okvira.

U radu je pored toga po prvi puta prezentirano stanje u sudovima u Bosni i Hercegovini, gdje je urađeno preliminarno istraživanje uz pomoć metode anketiranja, a vezano za digitalne dokaze, dokazivanje nepovredivosti lanca dokaza, te konstrukt prihvatljivosti digitalnih dokaza.

Ključne riječi: digitalna forenzika, digitalni dokazi, lanac digitalnih dokaza, prihvatljivost digitalnih dokaza, ontologije, modeliranje znanja

EXTENDED ABSTRACT

The ultimate goal of every digital forensic investigation is lawfully acquired and by the court accepted digital evidence. This means that all the evidence must be collected through the process of digital forensic investigation, which cannot begin without the order of the court, prosecution or administrative case of internal investigations in enterprises. The integrity of digital evidence must be preserved and prove, on the way proving the inviolability of the chain of evidence. This means that we anytime must: know, who, what, when, how, why and where they come into contact with digital evidence. If there is an interruption of the chain, the court will not accept the evidence. The main aim of this thesis is scientific research that will give insight into the methods of maintaining the chain of digital evidence, methods to prove the integrity of digital evidence and clarification of the life cycle of digital evidence. The goal is to address the shortcomings of existing methods, and defining new directions of research in solving chain of digital evidence problems using the ontology of digital evidence through " DEMF "- Digital Evidence Management Framework. The reason is to exactly know answer all the important questions participants in the digital investigation, but would also maintain the chain of evidence. The ultimate goal is to formally describe concepts that occur in the process of managing digital evidence, and build a framework to help judges and other persons engaged in the admissibility of digital evidence.

Ontology of digital evidence and the chain of evidence are developed, basic business rules (if-then rules) are defined, which are the main driver framework that allows determining which evidence is formally acceptable and which is not. Validation and evaluation of ontology are constructed, and few instances created, that were used for the framework testing.

In addition, in this paper is presented, a preliminary research conducted at the courts in Bosnia and Herzegovina, related to digital evidence, proving the inviolability of the chain of evidence, and construct the admissibility of digital evidence.

Keywords: digital forensic, digital evidence, chain of custody, acceptability of digital evidence, ontology, knowledge modeling

SADRŽAJ

POPIS SLIKA

POPIS TABLICA

POPIS KODOVA

POPIS SWRL PRAVILA

POGLAVLJE I

1 UVOD

Razvojem informacijsko-komunikacijskih tehnologija (engl. *Information Communication Technology - ICT*) krajem sedamdesetih godina ovoga stoljeća dolazi do nastanka računalnog kriminala. Računari su se počeli zloupotrebljavati od strane kriminalaca na način da se koriste kao sredstvo ali i cilj izvršenja kaznenih djela kao što su upadi u računarske sisteme, računarske prijevare, krađa ili uništenje podataka, krađe identiteta, ometanje rada informacijskih sustava i sl. Nastankom Interneta 90-tih godina situacija je postala još ozbiljnija te su podaci kako običnih građana, tako i firmi, organizacija, banaka ali i državnih institucija postali meta raznih organiziranih skupina. Prema podacima [1] 2006. godine šteta prouzročena „*cyber*“ kriminalom je iznosila 1.45 milijardi USD i po prvi puta je bila veća od vrijednosti ukupnog ilegalnog tržišta droga, dok je 2010. godine iznosila čak 114 milijardi direktne, a 274 milijarde USD indirektne materijalne štete.

Zbog svega ovoga javila se potreba za razvojem nove znanstvene discipline – digitalna forenzika, koja će se baviti problemom legalnog i zakonitog prikupljanja dokaza kako u pravosudnim (državne, međudržavne), tako i u korporativnim internim istragama [2]. Krajnji cilj svake digitalne forenzičke istrage je zakonito pribavljen dokaz i prihvaćen od strane suda. To znači da svaki dokaz mora biti prikupljen kroz proces digitalne forenzičke istrage, a koji ne može početi bez naredbe suda, tužiteljstva ili uprave ukoliko se radi o internim istragama u poduzećima. U samom procesu digitalne forenzičke istrage mora se sačuvati i dokazati nepovredivost digitalnog dokaza kroz dokazivanje nepovredivosti lanca dokaza. To znači da se mora znati svakog trenutka, tko je, što, kada, kako, zašto i gdje dolazio u kontakt sa digitalnim dokazima. Ukoliko dođe do prekida lanca dokaza sud takve dokaze neće prihvatiti.

1.1 Predmet istraživanja

Uspostava i očuvanje lanca digitalnih dokaza (digitalnog lanca dokaza)[1] i integriteta digitalnih dokaza u forenzičkoj analizi digitalnih uređaja predstavlja veliki problem za osobe koje provode digitalne istrage unutar neke korporacije, banke, osiguravajućeg društva ili institucije. Razlog je taj što potencijalni digitalni dokaz neće postati dokaz sve dok isti ne bude prihvaćen od strane suda kao krajnje institucije, a u praksi je veoma teško očuvati njegov integritet [3].

Znanstvenici su do danas razvili desetine modela i okvira digitalne forenzičke istrage kako bi osobama koje se bave digitalnom forenzikom pomogli da se forenzička istraga provede u okvirima zakona, te da digitalni dokazi budu prikupljeni na zakonit način i sukladno pravilima struke. Neki od tih modela se više temelje na prvim fazama u samom procesu istraživanja digitalnih dokaza (prepoznavanje, identifikacija), dok neki naglasak stavljaju na faze prikupljanja, analize i rekonstrukcije [4-12].
Najpoznatiji modeli su Leejev model, Caseyev model, DFRW (engl. Digital Forensic Research Workgroup) okvir, USDOJ (engl. United States Departmet Of Justice) model, Reith, Carr and Gunshev model, dok je najkompletniji Ciardhuaianev model koji se sastoji od 13 faza [8]. Faze zajedničke svim nabrojanim modelima su:

- Identifikacija ili prepoznavanje, prikupljanje i čuvanje
- Pretraga i analiza
- Prezentacija i izvještavanje [10].

Ono što je također zajedničko svim fazama forenzičke istrage je i činjenica da je digitalni dokaz osjetljiv na vanjske utjecaje, te da dolazi u kontakt s brojnim faktorima koji ga mogu izmijeniti ili uništiti. Pored ljudskog faktora koji može lako narušiti integritet digitalnog dokaza, tu je i tehnički faktor (oprema), te različite nesreće i nepogode (vatra, voda,

[1]Originalni naziv koncepta je „chain of custody of digital evidence“ ili „chain of evidence“ i kao takav je prepoznatljiv u literaturi.

zemljotres i sl.) [13]. Kako bi digitalni dokaz bio prihvaćen od strane suda tijekom cijelog procesa digitalne istrage, mora se održati lanac dokaza odnosno u svakom trenutku se mora znati tko je, kada, zašto, gdje, na koji način dolazio u kontakt s digitalnim dokazima [14,15]. Koncept lanca očuvanja ili lanac čuvanja se odnosi na potpunu reviziju i kontrolu originalnog dokaznog materijala koji bi potencijalno mogao biti upotrijebljen u sudskome procesu [15]. U literaturi se često može sresti naziv lanac dokaza umjesto lanac čuvanja. Svrha svjedočenja o lancu dokaza je da se dokaže da digitalni dokaz nije bio promijenjen u bilo kojoj fazi forenzičke istrage i da mora uključiti dokumentiranje kako je dokaz prikupljen, gdje je prikupljen, kako je transportiran, analiziran i čuvan [16]. Za sud nije dovoljno poznavati samo točnu lokaciju digitalnog dokaza gdje se nalazi, nego se mora bilježiti cijeli put kojim se kretao sve vrijeme svoga životnog ciklusa. Isto tako se mora strogo voditi evidencija i kontrola pristupa digitalnim dokazima.

Opisane osobine su važne zbog činjenice da sud ne prihvaća digitalne dokaze kao validne ukoliko se u kontaktu s njima nije postupalo sukladno pravilima i propisanim procedurama. U svijetu se danas lanac dokaza vodi na tradicionalan način, kao što se vodio prije 50tak godina. Sa digitalnim dokazima se postupa slično kao u radu s drugim materijalnim dokazima. Pohranjuju se u „posebno pripremljenim prostorijama“ (engl. *Evidence room*), a pristup istima se bilježi kroz tipski obrazac ili formular u koji se upisuje datum, vrijeme, mjesto, ime i prezime osobe koja je pristupala i dolazila u kontakt s digitalnim dokazima. Vrlo rijetko se upotrebljavaju računala i IKT kako bi se bilježio pristup, štitio integritet ili pratio ciklus digitalnog dokaza. U razvijenijim zemljama danas prevladava upotreba hibridnog sustava u kojem se računala koriste kao sredstvo za manualni unos podataka ili upotrebu bar-koda [14]. U radu je dan opširniji pregled i opis koncepta lanca dokaza, te njegove bitnosti u procesu forenzičke istrage digitalnih uređaja.

1.2 Ciljevi istraživanja

Obzirom da se radi o nedovoljno pokrivenom znanstvenom području u dostupnoj literaturi je vrlo malo objavljenih radova koji se bave istraživanjima na ovu temu. Koncept lanca dokaza (engl. *„Chain of Custody"*) postoji relativno dugo, ali vezano za digitalne dokaze pojavljuje se unazad tek nekoliko godina. Razlog je intenzivnije primjenjivanje tzv. „*Daubert princip"* prilikom svjedočenja IT stručnjaka na sudu i prezentiranja digitalnih dokaza. Daubertov princip je zamijenio dugo godina korišteni „*Frye test*"[2], a prema njemu se sve više uvodi znanost i znanstvene metode kao obavezne kod vještačenja i prezentiranja digitalnih dokaza. Sud je mogao prihvatiti samo dokaze koji zadovoljavaju određene uvjete:

- da su procedure ponovljive,
- da je poznat stupanja pogreške korištenih procedura,
- da su procedure objavljene u priznatim časopisima s recenzijom, te
- da su procedure znanstveno prihvaćene.

Primjenjivanjem Daubertovog principa broj isključivanja sudskih vještaka i kvazi eksperata je rapidno povećan, ali je i prema nekim istraživanjima poremećena ravnoteža strana u procesu [17].

Sukladno predmetu istraživanja osnovna svrha ovoga rada je znanstveno istraživanje koje će dati uvid u pregled metoda održanja lanca digitalnih dokaza i metoda zaštite integriteta digitalnih dokaza, te pojašnjenje pojma životnog ciklusa digitalnih dokaza [18]. Cilj je ukazati na nedostatke postojećih metoda i definiranja novih pravaca istraživanja u rješavanju problema lanca digitalnih dokaza primjenom ontologija digitalnih dokaza putem „DEMF"

[2] Fryev test ili Fryev standard, ili test općeg prihvaćanja je test za utvrđivanje prihvatljivosti znanstvenih dokaza. Prema testu je stručno mišljenje temeljeno na znanstvenim tehnikama dopušteno samo ako su tehnike općenito prihvaćene kao pouzdane u relevantnim znanstvenim zajednicama. U slučaju „Daubert protiv Merrell Dow Pharmaceuticals, 509 US 579 (1993)", Vrhovni sud je presudio da „Federalna pravila za dokaze" zamjenjuju Fryev kao standard za dopustivost stručnih dokaza u Federalnim sudovima.

(engl. *Digital Evidence Management Framework*)[3] kroz koji bi se u svakom trenutku digitalne istrage točno znao odgovor na sva bitna pitanja sudionika u procesu digitalne istrage, ali bi se i održavao lanac dokaza. Krajnji cilj je formalno opisati pojmove koji se javljaju u procesu upravljanja digitalnim dokazima, te pomoću izrađene ontologije digitalnih dokaza i odgovarajućeg modela, stvoriti temelje za učinkovitiji pristup izgradnji sustava u kojem bi se mogao uspostaviti i održati lanac dokaza [19].

1.3 Motivacija za istraživanje

Danas je općeprihvaćeno mišljenje i činjenica da je domena digitalne forenzike tzv. crne kutije (engl. *Blackbox*) kako za istražitelje, tako i za tužilaštvo i sudce. Nepoznavanje samog pojma digitalnog dokaza, neovisno od straha od novih tehnologija, veoma često je uzrok nesporazuma, nerazumijevanja, nepoznavanja pa u konačnici i pogrešno donošenih zaključaka koji su utjecali i na same presude. Ovo je bio osnovni motiv za pisanje ove teze, sa ciljem da se situacija promjeni, te da se vrši diseminacija znanja u domeni digitalne forenzike. Nakon prvih istraživanja i objavljenih radova koji opisuju DEMF prve povratne informacije od znanstvene zajednice su stigle u vidu radova autora [6,20-26] koji su potvrda samog koncepta ali i snažna motivacija za daljnje istraživanje i nakon pisanja ovog rada.

1.4 Istraživačka pitanja i hipoteze

Istraživačka pitanja na koja će rad pokušati dati odgovor su:

- Koji su to činitelji koji utječu na lanac digitalnih dokaza ?

[3] „DEMF“ – Digital Evidence Management Framework predstavlja konceptualni okvir za poboljšanje (uspostavu i održanje) lanca dokaza u kom se u svakom trenutku zna tko je , kada, gdje na koji način dolazio u kontakt sa digitalnim dokazima .

- Na koji način je moguće uspostaviti i sačuvati lanac dokaza u forenzičkoj analizi digitalnih uređaja, te očuvati integritet digitalnih dokaza?
- Opisati prijedlog modela koji bi omogućio da se u svim fazama istraživanje digitalnih dokaza zna odgovor na bitna pitanja: tko je, kada, zašto, gdje i na koji način dolazio u kontakt sa digitalnim dokazima ?

Atributi koje utječu i determiniraju digitalne dokaze su:

- Funkcija sažetka digitalnog dokaza,
- Biometrijska karakteristika ili digitalni potpis osobe,
- Vrijeme (vremenski žig),
- Mjesto (zemljopisna lokacija),
- Razlog za istragu i
- Skup procedura kojih se osoblje koje provodi forenzičke istrage mora pridržavati tijekom cijelog procesa istrage.

Pretpostavljeni konstrukti su :

- Prihvatljivost (engl. *Acceptability/Admissible*), kao ključni-temeljni konstrukt, te
    - Autentičnost (engl. *Authenticity*),
    - Cjelovitost (engl. *Completeness*),
    - Pouzdanost (engl. *Reliable*),
    - Vjerodostojnost ili Uvjerljivost (engl. *Believable*) [27], te
    - Relevantnost (engl. *Relevancy*),
    - Točnost (engl. *Accuracy*), kao njegovi pod konstrukti.

Prihvatljivost je pojam koji generalno u konačnici određuje digitalni dokaz, a koji subjektivno ovisi od odluke sudaca ukoliko se radi o službenim istragama, odnosno od odluke Uprave (Odbora) ukoliko se radi o privatnim korporacijskim istragama. U literaturi postoji veoma

malo ili skoro nikako radova koji opisuju na koji način se donosi ta odluka [28,29]. Ne postoji mjera (mjerljivost) za prihvatljivost u kontekstu digitalnih dokaza, nego je to isključiva subjektivna odluka. Digitalni dokaz mora biti u skladu sa određenim pravnim pravilima prije nego dođe do suda, te se moraju poštovati sljedeći principi:

Integritet je zaštita protiv neautorizirane i neopažene promjene podataka. Vanstone [30] definira digitalni integritet kao "svojstvo pri čemu digitalni podaci nisu mijenjani na neovlašten način u vrijeme kad su nastali, prenosili se ili pohranjivali od strane ovlaštenog izvora.“ Glavni uvjet je da dokazi moraju biti zaštićeni od izmjene bilo kakvih parametara podataka i da se to ne može dogoditi neotkriveno.

Autentičnost je višedimenzionalan pojam u kontekstu digitalne forenzike. Najvažnija je kombinacija s integritetom podataka jer je potrebno autentično povezivanje mjernih podataka za određeni uređaj sa svim relevantnim parametrima [31]. Mora biti moguće sa sigurnošću vezati digitalni dokaz sa incidentom koji se desio. Pitanje na koje se mora znati odgovor je da li je digitalni dokaz stigao odakle se to tvrdi (izvor dokaza) ?

Cjelovitost predstavlja pojam kojim se dokazuje da je digitalni dokaz sveobuhvatan, te da potpuno dokazuje postavljenu hipotezu, te da ne postoje drugi dijelovi koji upotpunjuju originalni digitalni dokaz [32]. Digitalni dokaz mora „ispričati cijelu priču, a ne samo jedan njen dio“ [27].

Pouzdanost predstavlja svojstvo digitalnog dokaza koje dokazuje da ne smije biti nikakvih dvojbi oko toga da je digitalni dokaz prikupljan i da se njime rukovalo na zakonit način (autentičnost i istinitost).

Vjerodostojnost – digitalni dokaz mora biti uvjerljiv i razumljiv za članove ocjenjivačkog suda.

Relevantnost predstavlja pojam koji pojašnjava da je digitalni dokaz bitan za određeni slučaj, te da ima tendenciju da izgrađuje nepobitnu činjenicu.
Točnost – digitalni dokaz mora biti istinit, točan, slobodan od pogreške ili greške, precizan ili korektan.
Ključni hipotetski konstrukt je integritet digitalnog dokaza i u najvećoj mjeri on određuje prihvatljivost digitalnih dokaza od strane suda.

Hipoteze koje proizlaze iz istraživačkih pitanja su:

H1: Uspostavom ontologije lanca digitalnih dokaza dobit će se referentni okvir za odlučivanje o formalnoj prihvatljivosti digitalnog dokaza.

H2: Temeljem ontologije digitalnog dokaza i meta podataka o konkretnom digitalnom dokazu, moguće je definirati pravila pomoću kojih će se moći zaključiti da li je taj dokaz formalno prihvatljiv.

1.5 Metodološki okvir

Istraživanje će dati pregled trenutnih spoznaja o nastojanju uspostave i održanja lanca digitalnih dokaza, postojeća rješenja, kao i prijedlog novog pristupa rješenju problema koji se ogleda u analiziranju lanca digitalnih dokaza kroz ontologije u digitalnoj forenzici, skladišta za pohranu digitalnih dokaza kao i okvire za upravljanje lancem dokaza. Kako bi se uopće mogao razumjeti i formalno opisati lanac dokaza potrebno je detaljno poznavanje procesa digitalne forenzičke istrage i koncepta životnog ciklusa digitalnog dokaza, zbog identificiranja različitih varijabli koje imaju utjecaj na digitalne dokaze u različitim fazama istrage.

Prilikom analize trenutnih saznanja koristit će se odabrana literatura iz domena rada i to: referentne knjige iz domene digitalne forenzike, znanstveni članci iz časopisa indeksirani u referentnim bazama podataka (IEEE, ACM, SCOPUS i sl.), zbornici radova s konferencija s međunarodnom recenzijom, dostupni članci s Web stranica autora koji se bave domenom digitalne forenzike.

Ponuđeno rješenje problema i provjera postavljenih hipoteza zahtijevati će korištenje kombinirano - primarno i sekundarno kvalitativne i kvantitativne znanstvene metode [33-35].

U teorijskom dijelu, prilikom opisa osnovnih koncepata iz domene digitalne forenzike i digitalnih dokaza sprovest će se temeljita kvalitativna analiza, za što će se koristiti opće znanstvene metode [35]. Primarna svrha kvalitativnog pristupa je pružanje detaljnog opisa koncepata koji determiniraju domenu lanca digitalnih dokaza, a u cilju stvaranja osnove za produbljenje znanja, te osnove za izgradnju nove teorije.

U empirijskom dijelu, metoda klasifikacije, kao najstarija znanstvena metoda (sistematska, dosljedna i potpuna podjela općeg pojma na posebne) [35] će se koristiti u cilju razvrstavanja osnovnih pojmova, te postavljanja u hijerarhiju osnovnih koncepata koji determiniraju ciljanu domenu lanca digitalnih dokaza. Ovim će se dobiti dijagram taksonomije kao prvi korak za izgradnju otvorene ontologije. Pridjev otvorena, u istraživanju, se može promatrati kroz paradigmu otvorenog koda (engl. *Open source*), ali i kao garancija da će se ponuđena ontologija moći nadograđivati i mijenjati, te ponovno koristiti (engl. *Reusability*). Kako bi se prikazale sve aktivnosti i dinamički procesi koji se događaju unutar samog procesa istraživanje digitalnih dokaza i lanca digitalnih dokaza - DEMF, koristit će se dijagramske tehnike modeliranja i jezik UML (engl. *Unified Modeling Language*) i to dijagram aktivnosti (engl. *Activity diagram*), dijagram slučajeva upotrebe (engl. *Use-case diagram*), te sekvencijalni dijagram (engl. *Sequence diagram*). Ovi modeli će omogućiti lakše shvaćanje samog procesa digitalne forenzičke istrage ali i razumijevanje faktora koji utječu na digitalne dokaze (životni ciklus digitalnog dokaza). U kontekstu opisanog područja istraživanja, od ključnog značaja je informacija (digitalni dokaz), a razumijevanje razmjene informacija (digitalnih dokaza) od krucijalnog je značaja za izgradnju okvira.

Sam proces izgradnje ontologije lanca digitalnih dokaza podrazumijevat će definiranje potrebnih koncepata, relacija među konceptima, instanci ili individua i pravila unutar domene lanca digitalnih dokaza. Ontologija koja će se razvijati je domenska, pri čemu je aplikacijska domena područje forenzičkih znanosti, grana digitalna forenzika koje se odnosi na digitalne dokaze odnosno lanac upravljanja digitalnim dokazima.

Formalna specifikacija termina u domenu lanca digitalnih dokaza, biti će rađena kroz proces razvoja o*ntologije* za što će se koristiti Protége. Jezik koji će se koristiti pri izgradnji ontologije je OWL DL (engl. *Ontology Web Language Description Language*) iz razloga što je baziran na opisnoj logici (engl. *Description logic*) i što omogućuje zaključivanje (engl. *reasoning*). Jezik SWRL (engl. *Semantic Web Rule Language*) će se koristiti za modeliranje pravila u danoj ontologiji koja će omogućiti zaključivanje na osnovu formalnog opisa definicije prihvatljivosti digitalnih dokaza, a koje će se koristiti u provjeri postavljenih hipoteza[4].

Kako bi se postigli definirani ciljevi, potrebno je provesti određeni broj aktivnosti od kojih su najvažniji sljedeći:

- Određivanje i definiranje domene i opsega ontologije, a to je lanac digitalnih dokaza,
- Definiranje pojma lanca dokaza, životnog ciklusa, te prihvatljivosti digitalnog dokaza,
- Modeliranje životnog ciklusa digitalnog dokaza sa ciljem da se pobliže pojasne koncepti koji determiniraju danu domenu,
- Semantički opis identificiranih varijabli neophodnih za izradu ontologije,
- Definiranje klasa, postavljanje hijerarhije među klasama, definiranje relacija te svojstava klasa, postavljanje ograničenja na tim svojstvima, definiranje instanci,
- Razvoj ontologije u *Protégé*-u koristeći OWL DL jezik,
- Formalno definiranje prihvatljivosti digitalnog dokaza,
- Definiranje pravila u SWRL-u koja će se koristiti pri odlučivanju o formalnoj prihvatljivosti digitalnih dokaza,
- Izgradnja otvorenog okvira koji će pomoću izrađene ontologije omogućiti zaključivanje o formalnoj prihvatljivosti digitalnih dokaza,
- Anketiranje sudaca sa ciljem prikupljanja podataka o tomu na koji način se prihvaćaju digitalni dokazi u sudovima u Bosni i Hercegovini,

[4] Lanac dokaza mora omogućiti da se svakog trenutka u svim fazama životnog ciklusa digitalnog dokaza zna tko je, kada, gdje, kako i zašto dolazio u dodir sa digitalnim dokazom. Ukoliko je lanac dokaza prekinut, digitani dokaz neće biti prihvaćen, jer postoji sumnja da je dokaz zamjenjen, falsificiran ili krivotvoren.

- Testiranje okvira studijom slučaja (engl. *Case study*),
- Razvoj i konkretizacija sustava temeljenog na otvorenoj-ontologiji (buduća istraživanja).

Kada je u pitanju istraživanje koje je provedeno i čiji su rezultati predstavljeni u radu, cilj je bio da se da uvid na koji način Sudovi u Bosni i Hercegovini formalno prihvaćaju digitalne dokaze, da li se vrši nadzor nad lancem dokaza, te kakvo je generalno stanje u Sudovima u Bosni i Hercegovini kada su u pitanju digitalni dokazi i prihvatljivost digitalnih dokaza sa aspekta lanca dokaza. Dodatni cilj koji se želio postići je da se skrene pozornost na ovaj problem, te ponudi model za buduća istraživanja, te edukacije koje su neophodne u ovoj domeni.

Metoda koje je korištena u istraživanju je metoda anketiranja, jer se pokazala kao najprikladnija metoda za ovo istraživanje. Testiranje korelacije između određenih rezultata istraživanja provjeravat će se izračunom *Pearsonovog* koeficijenta korelacije (r).

Sastavljen je upitnik sa pitanjima, pri čemu se prilikom sastavljanja pitanja naročito pazilo da se pitanje odnose na sam istraživački problem. Ciljana skupina su bili Sudovi u Bosni i Hercegovini. Cilj je bio prikupiti oko 25-30 popunjenih anketnih obrazaca isključivo sudaca koji dolaze u doticaj sa digitalnim dokazima. Zbog te činjenice se anketa i slanje anketnih obrazaca baziralo na kontaktu samo sa sudcima koji rade u kaznenom postupku, i koji svakodnevno dolaze u kontakt sa digitalnim dokazima. Zbog zakonske regulative, a naročito Direktive o zaštiti privatnosti EU[5], te eksplicitnog zahtjeva sudaca koji su učestvovali u anketi da se zaštite njihovi osobni podaci i onemogući bilo kakva identifikacija, nazivi sudova su kodirani.

[5] Direktiva 95/46/EZ Europskog parlamenta i Vijeća (http://www.azop.hr/page.aspx?PageID=10)

1.6 Znanstveni i društveni doprinos

Društveni doprinos rada se očituje u primjeni rezultata znanstvenih istraživanja u rješavanju konkretnog problema u radu s digitalnim dokazima i prihvaćanju digitalnih dokaza kao takvih u korporacijama, vladinim institucijama, te organizacijama u kojima se provode digitalne forenzičke istrage, kako u intranet okružju, tako i u globalnoj mreži. Rezultati istraživanja se mogu koristiti kako za diseminaciju znanja iz područja digitalne forenzike, tako i za implementaciju konkretnog sustava temeljenog na predloženom okviru (DEMF).

Analiza slučajeva iz prakse, pokazuje da je danas skoro pa nemoguće održati lanac digitalnih dokaza i integritet digitalnog dokaza, te da se zbog toga sve češće digitalni dokazi ne prihvaćaju kao validni i takvi slučajevi se uopće ne procesuiraju ili se dokazi ne prihvaćaju kao relevantni. Istraživanjem i radom se akcent stavio na eventualne propuste koji se čine, te koji su znanstveno manje pokriveni. Izgrađeni okvir omogućuje da se u svakoj fazi životnog ciklusa digitalnog dokaza ne samo održava njegov lanac nego i očuva njegov integritet, čime digitalni dokaz ne bi bio upitan. Za razliku od dosadašnjih istraživanja, primjenom znanstvenih metoda i izrađenom ontologijom digitalnih dokaza identificirani su, definirani i klasificirani osnovni pojmovi, te nakon izrađen model, i dat prijedlog rješenja moguće implementacije. Sveobuhvatni doprinos rada ogleda se u pregledu i analizi postojećih spoznaja iz područja istraživanja – digitalne forenzike odnosno lanca digitalnih dokaza, obuhvatu istraživanja, metodološkom pristupu kao i pojmovnim razgraničenjima. Razvijena ontologija digitalnih dokaza je samo prva faza u lancu narednih aktivnosti koje podrazumijevaju definiranje okvira te u konačnici izgradnju funkcionalnog sustava.

Znanstveni doprinos istraživanja se može odrediti kao:

- Identifikacija činitelja koji imaju presudan značaj na digitalne dokaze,
- Ontološki opis činitelja koji će se upotrebljavati u okviru za postupanje lancem dokaza,

- Izgradnja otvorenog okvira kao osnova za izgradnju sustava temeljenog na DEMF-u u kojem se može uspostaviti i očuvati lanac dokaza,
- Razvoj nove metodologije, preporuke i smjernice za poboljšanje postojećih metoda i okvira za postupanje sa digitalnim dokazima, te
- Sistematizacija i diseminacija znanja iz područja digitalne forenzike.

1.7 Struktura disertacije

Disertacija je strukturirana tako da se sastoji iz devet poglavlja koja su logički povezana i nadovezuju se. U prvom poglavlju je dan prikaz same disertacije, predmet i ciljeva istraživanja, istraživačka pitanja i hipoteze, metodološki okvir te očekivani doprinos. U drugom poglavlju su, u cilju pojašnjenja same domene, dane definicije osnovnih pojmova iz domena digitalne forenzike, a koji su relevantni za samu disertaciju. Poglavlje broj tri daje pregled trenutnog stanja u domeni lanca digitalnih dokaza, dok je u poglavlju broj četiri obrađeni modeli digitalne forenzičke istrage, pojam životnog ciklusa digitalnih dokaza, te okvir za upravljanje digitalnim dokazima. Nastavak je dan u poglavlju broj pet, u kojem je obrađena prihvatljivost digitalnih dokaza i prikazani su rezultati provedenog istraživanja na temu prihvatljivosti digitalnih dokaza u Bosni i Hercegovini. Poglavlje broj šest se odnosi na ontološki pristup rješavanju problema lanca dokaza, dok je poglavlju broj sedam opisan predloženi okvir baziran na ontologiji lanca dokaza. U osmom poglavlju opisana je evaluacija i vrednovanje ontologije. U devetom poglavlju dan je zaključak i otvorena istraživačka pitanja.

POGLAVLJE II

2 DEFINIRANJE OSNOVNIH POJMOVA RELEVANTNIH ZA DISERTACIJU

U ovom poglavlju su definirani osnovni pojmovi relevantni za disertaciju. Dana je definicija digitalne forenzike kao krovne znanstvene discipline koja pokriva interesnu domenu. Nakon toga je definiran pojam digitalnog dokaza, lanca digitalnih dokaza i prihvatljivosti digitalnih dokaza kao ključnih za razumijevanje domenskog problema.

2.1 Pojam digitalne forenzike (engl. *Digital forensic*)

Danas prevladava mišljenje da je digitalna forenzika isključivo vezana za policiju, računarski kriminal i kaznena djela, što je pogrešno, digitalna forenzika je danas potrebna svakoj organizaciji koja je umrežena i ima bilo kakvu ICT infrastrukturu. Ona stupa na snagu nakon što se desi incident, ona je novi bazni element „*obrane u dubini*“ kao sastavni dio računalne sigurnosti [36]. Digitalna forenzika je potrebna tužiteljima u kaznenom zakonodavstvu, advokatima i pravnicima u civilnom zakonodavstvu, osiguravajućim društvima, korporacijama pri provođenju internih (unutarnjih) istraga, agencijama za provođenje zakona, pojedincima [37].

Postoje različite definicije digitalne forenzike i digitalnih dokaza. Prema [38] “Digitalna forenzika se može definisati kao primjena nauke i inženjerstva ka rješavanju legalnih problema digitalnih dokaza”. Pollit i Whiteledge [39] su digitalnu forenziku definirali kao “nauku o prikupljanju, čuvanju, ispitivanju, analiziranju i prezentiranju relevantnih digitalnih dokaza za upotrebu u sudskom procesiranju“. Prema US CERT[6] digitalna forenzika je

[6]US CERT - (United States Computer Emergency Readiness Team) je stručno tijelo ustanovljeno sa ciljem zaštite internet infrastrukture u SAD.

znanstvena disciplina koja kombinira elemente zakona i digitalne znanosti radi prikupljanja i analize podataka iz digitalnih sustava, mreže, bežičnih komunikacija i medija za pohranu podataka u cilju prezentiranja pred sudom.

Sam pojam „forenzika“ je nastao od latinske riječi „*forēnsis“* što znači „*na otvorenom prostoru ili javno*“, a što dolazi od riječi „*forum*“ koja upućuje na lokaciju (javne površine koje su se upotrebljavale za suđenja ili neke druge javne poslove) [40]. Značenje je kasnije preraslo u „znanstveni testovi i tehnike koje se upotrebljavaju za otkrivanje kriminala“ [41]. Kada govorima sa aspekta današnjice, govorit ćemo o „*cyber forenzici“*, i „*digitalnoj forenzici*“ jer se mjesto izvršenja krivičnog djela ne može više vezati za računar i stol na kom se taj računar nalazio u momentu izvršenja toga djela. Istrage se proširuju u virtualni svijet, u svijet Interneta, mreža, i dalje na ostale digitalne uređaje (gsm, gps, digitalne fotoaparate, digitalne kamere, tzv. pametne telefone, PDA uređaje, razne mp3/mp4 „*playere*“, igraće konzole i sl.) [2,38,42,43].

2.2 Pojam digitalnih dokaza (engl. *Digital evidence*)

Pojam digitalni dokaz podrazumjeva bilo kakav relevantan podatak dovoljan da dokaže kazneno djelo na kompjuterskom ili mrežnom mediju za pohranu podataka, uključujući uzorke teksta, slike, videa i glasa.

Digitalni kompjuterski dokaz čini skupina posrednih stvarnih dokaza, od kojih se ni jedan ne smije isključiti iz bilo kog razloga. Dokazi moraju biti potpuni, da se međusobno dopunjuju (da su isprepleteni) i da nemaju tzv. pukotina za donošenje zaključaka, odnosno za utvrđivanje čvrstog dokaza [38,43,44].

Prema SWGDE[7] termin „dokaz“ se upotrebljava za „nešto materijalno“ što će biti priznato od strane suda. Ono mora biti prikupljeno na legalan i zakonit način. Neki objekt (podataka ili materijalna stvar) postaje dokazom jedino, kada u njega povjeruje službena provedba zakona. Prema standardima i procedurama SWGDE-a i IOCE-a[8] pojam digitalnog dokaza predstavlja svaka informacija ili vrijednost koja je smještena ili transmitirana u digitalnom obliku [45,46].

Proces forenzičke istrage započinje davanjem suglasnosti menadžmenta korporacije (upravnog odbora) ukoliko se radi o privatnim unutarnjim istragama ili naredbom za provođenje istrage koju izdaje sud ili odvjetništvo ukoliko se radi o zvaničnim državnim ili međudržavnim istragama. Postoji desetine razvijenih modela i okvira digitalne forenzičke istrage. Svim modelima su zajedničke tri sljedeće faze:

- Identifikacija ili prepoznavanje, prikupljanje i čuvanje
- Pretraga i analiza
- Prezentacija i izvještavanje [8,10].

Najpoznatiji modeli su Leejev model, Caseyev model, DFRW okvir, USDOJ model, Reith, Carr i Gunshev model, [4-6,9,11,12] dok je najcjelovitiji Ciardhuaianov model sa čak 13 faza [8]. Neki od njih se više baziraju na prve faze u samom procesu (prepoznavanje, identifikacija), dok neki akcent stavljaju na faze prikupljanja, analize i rekonstrukcije.

2.3 Pojam lanca digitalnih dokaza (engl. *Chain of digital evidence*)

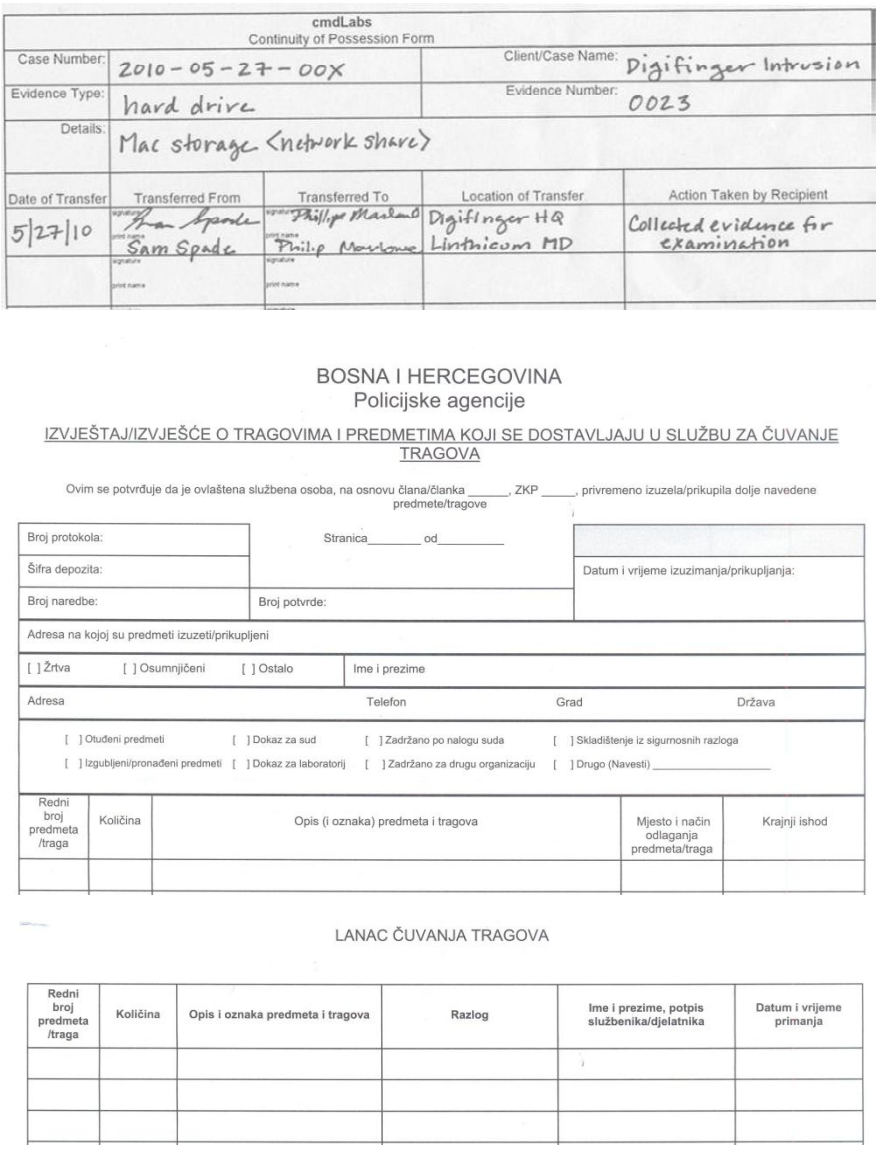
Ono što je zajedničko svim fazama digitalne forenzičke istrage je činjenica da je digitalni dokaz osjetljiv na vanjske utjecaje, te da dolazi u kontakt sa mnogo faktora [47]. Kako bi

[7] SWGDE - *The* Scientific Working Group on Digital Evidence je znanstvena radna skupina za digitalne dokaze ustanovljena 1998.godine od strane saveznih kriminalistički laboratorija u SAD. Jedna je od najstarijih organizacija koja se bavi tehničkim aspektima digitalnim dokazima.

[8] IOCE – International Organization on Digital Evidence je najstarija međunarodna organizacija koja se bavi digitalnim dokazima – zadužena je za razvoj standarda i smjernica.

digitalni dokaz bio prihvaćen od strane suda tijekom cijelog procesa digitalne istrage mora se održati „lanac dokaza“[9] odnosno u svakom trenutku se mora znati tko je, kada, zbog čega, na koji način i gdje dolazio u kontakt sa digitalnim dokazima [14,47–50].

Termin “lanac očuvanja” ili “lanac čuvanja” prema [50] se odnosi na potpunu reviziju i kontrolu originalnog dokaznog materijala koji bi potencijalno mogao biti upotrijebljen u legalne svrhe.



cmdLabs
Continuity of Possession Form

Case Number:	2010-05-27-00X		Client/Case Name:	Digifinger Intrusion
Evidence Type:	hard drive		Evidence Number:	0023
Details:	Mac storage <network share>			
Date of Transfer	Transferred From	Transferred To	Location of Transfer	Action Taken by Recipient
5/27/10	Sam Spade	Philip Marlowe	Digifinger HQ Linthicum MD	Collected evidence for examination

BOSNA I HERCEGOVINA
Policijske agencije

IZVJEŠTAJ/IZVJEŠĆE O TRAGOVIMA I PREDMETIMA KOJI SE DOSTAVLJAJU U SLUŽBU ZA ČUVANJE TRAGOVA

Ovim se potvrđuje da je ovlaštena službena osoba, na osnovu člana/članka _____, ZKP _____, privremeno izuzela/prikupila dolje navedene predmete/tragove

Broj protokola:	Stranica_____ od_____	
Šifra depozita:		Datum i vrijeme izuzimanja/prikupljanja:
Broj naredbe:	Broj potvrde:	

Adresa na kojoj su predmeti izuzeti/prikupljeni

[ ] Žrtva [ ] Osumnjičeni [ ] Ostalo — Ime i prezime

Adresa | Telefon | Grad | Država

[ ] Otuđeni predmeti [ ] Dokaz za sud [ ] Zadržano po nalogu suda [ ] Skladištenje iz sigurnosnih razloga
[ ] Izgubljeni/pronađeni predmeti [ ] Dokaz za laboratorij [ ] Zadržano za drugu organizaciju [ ] Drugo (Navesti) _____

Redni broj predmeta /traga	Količina	Opis (i oznaka) predmeta i tragova	Mjesto i način odlaganja predmeta/traga	Krajnji ishod

LANAC ČUVANJA TRAGOVA

Redni broj predmeta /traga	Količina	Opis i oznaka predmeta i tragova	Razlog	Ime i prezime, potpis službenika/djelatnika	Datum i vrijeme primanja

Slika 1. Pojednostavljena inačica forme za dokumentiranje lanca dokaza [3], te forma za čuvanje lanca dokaza koja se koristi u policijskim agencijama u Bosni i Hercegovini

[9] Originalni izraz je „chain of custody“, iako se u literaturi često može sresti i izraz „chain of evidence“

Prema NIJ[10] [51] lanac čuvanja je proces koji održava i dokumentira kronološki historiju dokaza (Dokument mora da uključuje ime ili inicijale osobe koja je prikupila dokaze, svake osobe ili entiteta koji su imali pristup dokazima, datum kada su dokazi prikupljeni ili im je mijenjana lokacija, naziv agencije i broj slučaja, ime žrtve ili osumnjičenog, detaljan opis svega). Neki autori upotrebljavaju termin „lanac dokaza“ umjesto „lanac čuvanja“. Svrha svjedočenja o lancu dokaza je da se dokaže da digitalni dokaz nije bio promijenjen u bilo kojoj fazi forenzičke istrage i on mora uključiti dokumentiranje kako je dokaz prikupljen, gdje je prikupljen, kako je transportiran, analiziran i čuvan. Prekid lanca čuvanja navodi na sumnju da je dokaz promijenjen, falsificiran ili zamijenjen. Za sud nije dovoljno poznavati točnu lokaciju digitalnog dokaza nego se mora bilježiti cijeli put kojim se kretao sve vrijeme. Isto tako se mora strogo voditi evidencija i stroga kontrola pristupa digitalnim dokazima [2,13,16,20,37,47,52-54]. Ovo su faktori koji su veoma bitni, a kojih se u velikom broju istraga ne pridržava, te zbog kojih najčešće sud ne prihvaća digitalne dokaze kao validne.

2.4 Pojam prihvatljivosti digitalnih dokaza (engl. *Acceptability of digital evidence*)

Prihvatljivost (engl. *Acceptability*) digitalnih dokaza je pojam koji determinira da li će potencijalni digitalni dokaz uistinu i postati dokaz u konačnici, koja obično dobiva sudski epilog ukoliko se radi o zvaničnim, državnim istragama, ili prilikom prezentiranja pred upravom firme (poduzeća) ukoliko se radi o internim istragama. Sudac odlučuje koji dokazi će biti ili ne prihvaćeni u sudnici u kojoj predsjedava. Veoma često se angažira sudski vještak u cilju pojašnjenja tehničkih i znanstvenih aspekata vezano za konkretni digitalni dokaz [55,56]. Danas je malo objavljenih radova na ovu temu [28,57].

[10] NIJ - National Institute of Justice (Nacionalni Institut Pravde SAD)

POGLAVLJE III

3 DOSADAŠNJA - POVEZANA ISTRAŽIVANJA

U ranijim fazama predstavljanja digitalnih dokaza pred sudom, te dokazivanja lanca dokaza, bilo je dovoljno dokazati integritet digitalnog dokaza, te se u te funkcije najčešće koristila jedna od dostupnih funkcija za izračun sažetka MD-5 [58] ili SHA-1 [59]. Računala bi se vrijednost sažetka preslike diska, te potencijalnog digitalnog dokaza, te bi se kasnije isti uspoređivao sa vrijednošću sažetka preslike originalnog diska kako bi se potvrdilo da nije dolazilo do bilo kakvih modifikacija i promjena na originalnom dokazu. Ukoliko se vrijednosti sažetka ne poklapaju sumnja se da je lanac dokaza prekinut, te da se digitalni dokaz mora isključiti. Posljednjih nekoliko godina je otkriveno više ranjivosti MD5 algoritma što je kulminiralo sa MD5 kolizijom [60], nakon čega su znanstvenici uvidjeli da MD5 više nije dobar izbor za očuvanje integriteta digitalnih dokaza [6]. Slična situacija je bila i sa SHA-1 i „*preimage"* napadom. Javila se potreba za jačim algoritmima koji će generirati duže vrijednosti sažetka ali i kompleksnijim metodama za zaštitu integriteta digitalnih dokaza [6,48,61]. Koncept „*lanac dokaza*" vezan za digitalne dokaze, intenzivnije se spominje unazad nekoliko godina, od kada su sudovi počeli da primjenjuju tzv. Daubertov princip prilikom svjedočenja IT stručnjaka (engl. *Infomation Technology*) na sudu i prezentiranja digitalnih dokaza. Daubertov standard (princip) je zamijenio dugo godina korišteni „Frye test", a prema njemu se sve više uvodi znanost i znanstvene metode kao obavezne kod vještačenja i prezentiranja digitalnih dokaza. Samo dokazi koji su pouzdani i relevantni, gdje su primjenjivane metode gdje je poznata mjerljivost pogreške, te koje su obavljene u tzv. peer časopisima, su mogli biti prihvaćeni od strane suda. U nastavku rada će se dati prikaz trenutnog stanja u domeni istraživanja digitalnog lanca dokaza. Korišteni su objavljeni radovi unazad 5-6 godina jer se u tom periodu (od 2006. godine) počelo intenzivnije naglašavati problem očuvanja lanca digitalnih dokaza.

3.1 Primjena ontologija u forenzici

Veoma mali broj radova je objavljenih na temu primjene ontologija u digitalnoj forenzici, te se veoma mali broj autora bavi ovim problemom [62,63]. Postavlja se pitanje zašto su nam ontologije potrebne i što bismo dobili primjenom ontološkog pristupa u rješavanju određenog problema? Danas je veoma čest slučaj da se ne koriste koncizne definicije, te da se često upotrebljavaju fraze i frazeologizmi kod pokušaja pojašnjenja nekih pojmova iz aspekta forenzike. Isto tako se često dešava da pojmovna klasifikacija nije dobro postavljena, te da pojedini izrazi dobivaju posve drugo značenje od onoga stvarnog. Izradom taksonomije i ontologije digitalnih dokaza pojmovna klasifikacija bi bila mnogo jasnija.

Harill i Mislan [64] su se bavili ontologijama u forenzici tzv. „malih uređaja". U svojim istraživanjima [64] su postavili ontologiju „*uređaja malih razmjera*" u cilju predstavljanja znanja o SSDD (engl. *Small Scale Digital Devices*) domeni forenzičkim stručnjacima koji rade analizu podataka tih uređaja. U radu su kategorizirani SSD uređaji prema određenim kriterijima, te je dati iscrpan opis istih. Cilj je bio napraviti okvir u koji bi se smjestili SSD uređaji. Prema autorima ontologija bi se mogla upotrijebiti kao metoda za budući eventualni razvoj standarda i procedura u radu sa SSD uređajima.

Heum Park i dr. [65] u svojim istraživanjima su predstavili ontologiju za istrage u „kibernetičkom[11] prostoru". Kibernetički kriminal je klasificiran u dvije klase - kibernetički teror i kibernetički kriminal. Ove dvije klase su povezane jedna drugom. Autori su definirali koncepte i relacije među njima. Ograničenja ovog ontološkog modela su da je manje baziran na digitalne dokaze i druge faze bitne za proces analize podataka. Jedina faza procesa forenzičke analize koja ima veze sa digitalnim dokazima je faza prikupljanja, dok sve ostale faze ignoriraju.

[11] Pojam Cyber je preveden kao „kiberntički" iako u pravom smislu riječi to nije (Budimpeštanska konvencija). Pojam cyber se danas u literaturi često koristi kao „sajber" jer kibernetički ima sasvim drugo značenje.

Ashley Brinson i ostali u svojim istraživanjima [66] su 2007.godine predstavili ontologiju cyber forenzike u cilju pronalaženja i predstavljanja točnog okvira za specijalizaciju, certifikaciju i edukaciju u domeni cyber forenzike. Prema njima cyber forenzika je sastavljena od tehnologije i profesije. Tehnologija je dalje podijeljena na podklase - hardver i softver, dok je profesija podijeljena na zakon, akademiju, vojsku i privatni sektor. Ontologija je koncipirana „odozgo prema dolje“ a model je eventualno primjenjiv u svrhe razvoja nastavnih planova.

Hoss i Carver [67] su u radu diskutirali o potrebi primjene ontologije kao podrške digitalnoj forenzici ali nikakva konkretna ontologija nije preporučena. Naglašeno je nepostojanje otvorenih ontologija u digitalnoj forenzici, te potreba za stvaranjem baza znanja i uniformnih formalnih reprezentacija. [68] Hoss i Carver su predložili ontologiju koja bi podržala digitalnu forenziku ali nisu preporučili ništa konkretno što bi se moglo upotrijebiti [68].

Ontologija *malware-a* preporučena od strane [69] predstavlja osnovu ontologije malware-a koja se sastoji od svojstava i karakteristika. Ontologija je osmišljena kao polazna osnova za daljnja istraživanja koja bi omogućila računalima da mogu odlučivati o daljnjim postupcima prilikom detektiranja malicioznog koda.

Ćosić i Bača [19] su u ranijim istraživanjima pokušali ontološkim pristupom pomoći boljem razumijevanju i decidnom definiranju pojmova koncepta lanca digitalnih dokaza. Cilj je bio postaviti dijagram taksonomija lanca digitalnih dokaza u svim fazama forenzičke istrage. Razloga za to je mnogo, načini izvršenja kaznenih djela se mijenjaju iz godine u godinu, svakodnevno se pojavljuju novi nosioci podataka koji mogu sadržavati digitalne dokaze, sve ih je teže i teže pronaći, očuvanje lanca dokaza postalo je skoro pa nemoguće bez eksplicitnog poznavanja ove domene. Autori su ovim radom pokušali omogućiti ponovnu upotrebu znanja iz domena digitalne forenzike i lanca čuvanja digitalnih dokaza ali je učinjen i prvi korak ka kreiranju otvorenog okvira za upravljanje digitalnim dokazima.

Prema [62] nije moguće izgraditi jednu ontologiju koja bi bila dovoljno „velika“ da uključi sve koncepte koji se javljaju i koji su interesantni za osobe koji provode forenzičke istrage, dok autori [70] nude okvir za apstrahiranje izvora digitalnih dokaza i formata za pohranu digitalnih dokaza kojim bi se identificirale informacije o digitalnim dokazima koji se prikupljaju iz više izvora.

3.2 Okviri za očuvanje lanca dokaza

“DIALOG” autora Kahvedzic i Kechadi [71] daje generalni vokabular, neovisan od aplikacije, koji se može upotrijebiti za opis digitalne forenzičke istrage na različitoj razini detalja. Okvir je definiran na način da grupira sve koncepte sa polja digitalne forenzike i relacije među njima.

U disertaciji obranjenoj na West Virginia Sveučilištu u SAD 2009. godine Bartlow [72] je predstavio sustav za uspostavu i očuvanje digitalnog lanca dokaza u biometrijskim sustavima. Kroz sigurnosni mehanizam aplikacije kroz kriptografiju, funkciju sažetka, biometrijsku autentifikaciju, biometrijski vodeni žig i hardverski digitalni uređaj za uzimanje otisaka prstiju u radu su date preporuke za konceptualni okvir koji omogućava otkrivanje i prevenciju prijetnji povjerljivosti i integritetu digitalnog lanca dokaza. U prvoj fazi su istražene i razrađene teme sigurnosnih mehanizama kao što su biometrijski vodeni žig, uređaji za uzimanje otisaka prstiju i ponašanje dinamičnosti tipkanja. Nakon toga razvijen je okvir koji se oslanja na ova tri sigurnosna mehanizma i kriptografiju koja je upotrijebljena iz razloga rukovanja sa sigurnosnim prijetnjama presretanja podataka, promjene podataka, kreiranja podataka i povrede porijekla podatka. U kontekstu rada sve tri biometrijske metode kao i digitalni uređaj za uzimanje otisaka se upotrebljavaju za prevenciju neautoriziranog pristupa i prevenciju promjene podataka .

Kuntze i Carsten [73] sa Fraunhofer Instituta za sigurnost informacijskih tehnologija iz Njemačke, su se u svojim istraživanjima bavili sigurnosnim aspektima digitalnog lanca dokaza. U istraživanjima [31,73] je predstavljena ideja „sigurnog digitalnog lanca dokaza“ i preporučena je arhitektura na visokom nivou za sustave kojima je neophodan lanac dokaza. U biti radi se o „osiguranju“ digitalnih zapisa na razini kompletnog informacijsko-komunikacijskog sustava koji je baziran na „sustavima kojima se vjeruje“. Rad nije dao rješenje problema lanca dokaza u svim fazama digitalne istrage nego samo u prvoj fazi prikupljanja i pohranjivanja.

3.3 „Skladišta“ i formati za pohranu digitalnih dokaza

Jedan od načina na koji su znanstvenici pokušali riješiti problem očuvanja lanca dokaza bio je i kroz izradu različitih formata za pohranu digitalnih dokaza. Jedan od napora autora koji se aktivno bave problemom standardizacije formata za pohranu digitalnih dokaza kao preduvjeta za razmjenu digitalnih dokaza, forenzičkih alata i sl. je bio i pokušaj poznatih znanstvenika - članova radne skupine DFRWF[12]. Preporučeni okvir je izgrađen upotrebljavajući RDF (engl. *Resource Description Framework*), kao najčešći i najprihvatljiviji format za predstavljanje podataka i ontologiju za opis vokabulara relevantnih za ove podatke. Metode koje autori koriste u radu su ontološki pristup (ontologije), modeliranja, te jezici UML (engl. *Uniform Modelling Language*), XML (engl. *eXtendable Modelling Language*, RDF (engl. *Resources Description Framework*) [63]. Naglašena je činjenica da je primijenjena ontologija koncepta DEB-a (engl. *Digital Evidence Bag*) Philip Turner-a, te da ne postoji mnogo radova gdje je primijenjena ontologija u području digitalne forenzike i kompjuterskog kriminala. Rad nije dao rješenje problema digitalnog lanca dokaza, a ontologija je upotrijebljena samo za definiranje vokabulara koji se koristi u definiranju ovog formata.

[12] DFRWS – (Digital Forensics Research WorkShop) je međunarodna radna skupina formirana sa ciljem definiranja standardiziranog formata za pohranu digitalnih dokaza (CDESF).

DEB (engl. *Digital Evidence Bag*) [37,74] predstavlja univerzalni „kontejner“ za pohranu digitalnih dokaza koji su prikupljeni iz bilo kojeg izvora. Osigurava da se može pohraniti ne samo podatak (potencijalni digitalni dokaz) nego i samo porijeklo - izvor dokaza, te održati kontinuitet tijekom procesa istrage. Drugim riječima, DEB je dio softvera koji može pohraniti podatke iz bilo kojeg forenzičkog alata koji je pokrenut. DEB se sastoji od *datoteke oznake*, datoteke *indeksa* i *datoteke sadržaja* datoteke. Datoteka oznake sadrži meta podatke o digitalnom dokazu (naziv organizacije i ime i prezime osobe koja je prikupila dokaz, datum i vrijeme prikupljanja, ID broj, izračun funkcije sažetka), indeks datoteka sadrži podatke o pripadajućem fajlu sadržaja (putanju na nosiocu podataka, ime datoteke, vremenski žig), dok datoteka sadržaja predstavlja stvarni digitalni dokaz (sliku, video, tekstualnu datoteku i što drugo). Ne postoji detaljna razrada ovoga koncepta, te prema nekim autorima [63] DEB može biti bilo kakav arhiv (*tar, zip*, i sl.) koji sadrži ove datoteke. Najčešći i javno objavljeni formati za pohranu digitalnih dokaza su *AFF, Raw, DEB, Expert Witness, Gfzip, ProDiscovery, EnCase i SMART Expert Witness* [75]. Neki od ovih alata imaju ugrađene mehanizme zaštite integriteta digitalnog dokaza kroz kombinaciju MD5 i CRC sažetaka dok samo *SMART default* format ima podršku za kriptografski potpis. U tablici 1. su prikazani najpoznatiji formati za pohranu digitalnih dokaza s osnovnim karakteristikama bitnim za lanac dokaza i zaštitu integriteta digitalnog dokaza. Evidentno je da niti jedan format ne sadrži metapodatke koji bi dali odgovor na pitanje 5Ws i 1 H, te način na koji bi se održao digitalni lanac dokaza.

Tablica 1. Matrica postojećih formata az pohranu digitalnih dokaza

Naziv formata	**Podržan od strane forenzičkih alata**	**Da li format sadrži meta-podatke?**	**Koji meta-podaci mogu biti pohranjeni ?**	**Zaštita integriteta digitalnih dokaza**	**Meta-podaci digitalnog lanca dokaza**
Raw[75]	Svaki forenzički alat može čitati raw format	NE	-	-	-

Tablica 1. Matrica postojećih formata az pohranu digitalnih dokaza (nastavak)

AFF[61,76,77]	AFF Tools	DA	Broj slučaja, Istražitelja, Broj dokaza, Serijski broj, Trenutno vrijeme, zabilješke i sl.	MD5	Korisnički definirano (bilo koji broj parova imena/vrijednosti)
AFF4[76]	LibAFF4 (AFF4 tools)	DA	Broj slučaja, Istražitelj, Broj dokaza, Serijski broj, Trenutno vrijeme, zabilješke i sl.	MD5	Korisnički definirano (bilo koji broj parova imena/vrijednosti)
DEB[77,78]	DEB preglednik, DEB imager, DEM cmd wrrapper	DA	Naziv agencije, Istražitelj, Opis, Lokacija, Datum i vrijeme, ID host-a, Opis host-a i sl.	Hash – enkripcija	Datum i vrijeme, ID aplikacije, Potpis aplikacije, Funkcije aplikacije, ID host-a, Pristup DEB komponentama
EnCase[79]	EnCase, FTK, SMART,X-Ways, AFF	DA	Broj slučaja, Istražitelj,Broj dokaza, Opis, Trenutno vrijeme, Zabilješke	MD5, CRC -32	-
GfZip[80]	GFZ Tools (library)	DA	Kao kod AFF	SHA1, MD5, SHA256, X509 i kriptografski potpis	Kriptografski potpisani meta-podaci

Tablica 1. Matrica postojećih formata za pohranu digitalnih dokaza (nastavak)

ProDiscover [81]	ProDiscover	DA	Broj imidža diska, Istražitelj, Vrijeme kreiranja imidža,sistemsko vrijeme,	MD5, SHA1, SHA256, digitalni potpis	NE
SMART default[82]	SMART	DA	Broj slučaja, Istražitelj, Broj dokaza, Opis, Trenutno vrijeme, Bilješke	MD5, CRC -32	NE
SMART Expert Witness Compressed [83]	SMART, FTK imager	DA	Broj slučaja, Istražitelj, Broj dokaza, Opis, Trenutno vrijeme, Bilješke	MD5, CRC -32	NE

Danas ne postoji usvojen međunarodni standard koji daje preporuke za upravljanje lancem dokaza, niti postoje preporuke prihvaćene od strane ISO/IEC organizacije (na svjetskoj razini), postoje samo preporuke i standardi na razini država ili grupa država. Pokušaj standardizacije i postupanja sa digitalnim dokazima na međunarodnoj razini kroz CDESF[13] je propao, a DFRWS je raspustio radnu skupinu za CDESF koncem 2007. godine.

Digitalnoj forenzičkom zajednici je neophodan jedinstveni okvir pomoću kojeg bi se lanac digitalnih dokaza mogao tretirati na isti način u cijelom svijetu. Danas je čest slučaj (naročito kod terorističkih napada), da se neke kriminalne aktivnosti dogovore u jednoj državi na jednoj strani svijeta, počine se u drugoj državi na drugoj strani svijeta, a sredstvo izvršenja (neki digitalni uređaj) se nalazi na sasvim trećem kraju svijeta. Pitanje koje su tu postavlja je gdje je tu digitalni dokaz, te tko je, kada, gdje, zašto i kako rukovao sa njim, da li je dokaz ostao nepromijenjen tijekom ovoga procesa ?

[13] Common Digital Evidence Storage Format

POGLAVLJE IV

4 MODELI DIGITALNE FORENZIČKE ISTRAGE I ŽIVOTNI CIKLUS DIGITALNIH DOKAZA

U ovom poglavlju je dan pregled modela digitalne forenzičke istrage. Modeli su bitni osobama koje vode digitalne forenzičke istrage kako bi se pravilno razumio sam proces digitalne forenzičke istrage, te u konačnici definirao i razumio pojam životnog ciklusa digitalnog dokaza.

Proces prikupljanja digitalnih dokaza mora uvijek započeti na zakonit način. To drugim riječima znači, ukoliko postoji potreba za digitalnom forenzičkom istragom, postupajući tužilac ili sudac (sudac za prethodni postupak) mora dati pismeni nalog da istraga može započeti. S druge strane ukoliko se radi o korporativnim istragama, menadžment poduzeća ili Upravni odbor se mora složiti sa činjenicom da se vodi interna istraga u stegovnom postupku. U svakom slučaju mora postojati pisani dokument, u smislu odobrenja, naredbe ili rješenja o početku istrage.

U kontekstu doticaja s digitalnim dokazima, situacija se razlikuje od zemlje do zemlje. U nekim razvijenim Europskim zemljama i USA [3,84] postoje specijalizirane policijske jedinice (engl. *First Response Forces*) koje su obučene i trenirane da rukuju s bilo kojim tipom digitalnih dokaza. S druge strane, u nekim zemljama taj posao obavljaju policijski službenici koji nisu specijalizirani za taj dio posla.[14]

Prema Međunarodnoj Organizaciji za Digitalne Dokaze (engl. *International Organization on Computer Evidence – IOCE*) [45,85], kada je potrebno da osoblje dolazi u doticaj s digitalnim

[14] Na primjer u Hrvatskoj, Bosni i Hercegovini, ali i Srbiji[128] prikupljanje digitalnih dokaza obavljaju istražitelji koji vode kompletan slučaj, te se tek naknadno, tijekom daljnje istrage angažira sudski vještak u cilju prezentiranja digitalnih dokaza pred sudom.

dokazima, to osoblje mora biti obučeno i educirano za taj posao. U mnogim slučajevima to nije moguće, jer je digitalna forenzika veoma kompleksna znanstvena disciplina i zahtjeva visok nivo ekspertize u više znanstvenih polja, kao što su kriminalistika, pravo, informatika, telekomunikacije i računalne znanosti.

U većini slučajeva se pojavljuje sljedeće osoblje koje dolazi u doticaj sa digitalnim dokazima:

- Osoblje koje prvo dolazi na mjesto događaja (engl. *First responders*);
- Forenzički istražitelji (engl. *Forensic investigators*);
- Sudski vještaci (engl. *Court expert witness*);
- Osoblje za provedbu zakona (engl. *Law enforcement personnel*);
- Policijski službenici (engl. *Police officers*);
- Žrtva (engl. *Victim*);
- Osumnjičeni (engl. *Suspect*);
- Slučajni prolaznici (engl. *Passerby*).

Svatko od spomenutih može narušiti integritet digitalnog dokaza u različitim situacijama, i u svakom trenutku je potrebno znati odgovor na pitanja: "Tko je dolazio u kontakt s digitalnim dokazima" ?

Kako bi se lakše razumio utjecaj ljudskog faktora na digitalne dokaze, te utjecaj na lanac dokaza potrebno je dodatno opisati modele digitalne forenzičke istrage i životni ciklus digitalnog dokaza.

4.1 Modeli i okviri digitalne forenzičke istrage

Kako bi digitalne forenzičke istrage bile što učinkovitije, te u konačnici rezultirale pronađenim i prihvaćenim digitalnim dokazima, bitno je imati funkcionalan model. S takvim

modelom se sam proces digitalne forenzičke istrage može generalizirati, te se može napraviti okvir za razumijevanje svih tehnika i tehnologija koje je neophodno upotrijebiti u samom procesu digitalne forenzičke istrage. U mnogim situacijama istrage neće voditi ka uspješnom procesuiranju počinilaca kaznenih djela, veoma često zbog toga jer je loša priprema i zbog nekompletnost i nepoštivanja propisanih procedura. Istražitelji obično nemaju dovoljno znanja, alata i drugih potrebnih stvari za uspješan rad s digitalnim dokazima. Veoma čest problem je prikupljanje dokaza. U digitalnoj forenzičkoj praksi postoji preko stotinu procedura, preporuka i dokumenata koji opisuju rukovanje sa digitalnim dokazima. Zbog toga je veoma bitno znati pravilno koristiti alate i metode, te upravljati životnim ciklusom digitalnog dokaza.

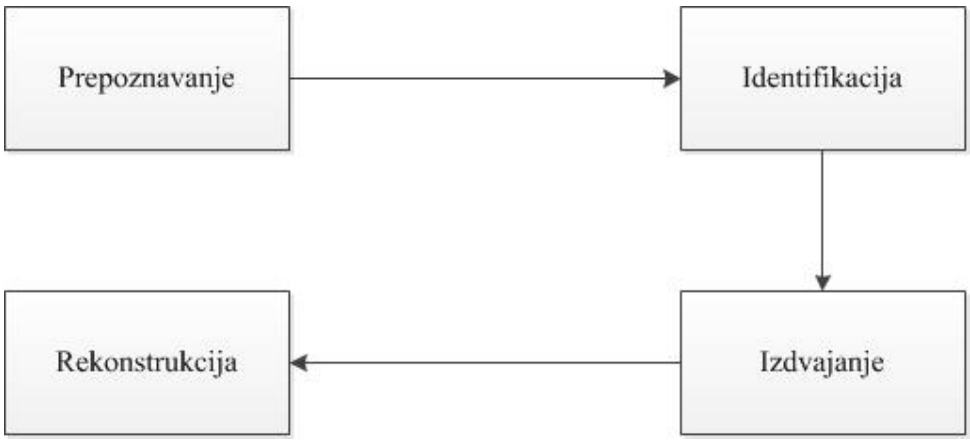
Analizom relevantne i recentne literature evidentno je da neki autori preporučuju model, a neki okvir. U čemu je razlika između modela i okvira? Prema „Oxford riječnik“ okvir je "*a supporting or underlying structure*" [40]. Neki drugi relevantni rječnici definiraju okvir (engl. *framework*) kao "*a skeletal structure designed to support or enclose something*" [86]. Može se reći da je okvir struktura dizajnirana da podrži neku akciju. U forenzički istragama, akcije uključuju faze, korake ili nivoe.

S druge strane isti izvori definiraju model kao "*a standard or example for imitation or comparison and a representation, generally in miniature, to show the construction or appearance of something*". U računarskom svijetu može se reći da model predstavlja apstrakciju nečega što se sastoji od dovoljno detalja da se može upotrijebiti kao formula. Na osnovu navedenog se može utvrditi da postoji razlika između modela i okvira. Model je nešto što ćemo primijeniti na određenu situaciju, a okvir ćemo koristili na mjestu aspekta. Model generalizira proces kako bi se izgradio okvir koji bi pomogao ljudima da shvate što proces može a što ne [41].

Kratak opis najrelevantnijih modela koji se upotrebljavaju u računalnim (digitalnim) istragama je dan u nastavku.

4.1.1 Leejev model

Leejev model (2001) je baziran na znanstvenom CSI procesu poznatom po nazivu engl. *„Scientific Crime Scene Investigation Process*“ [87]. Model identificiraju četiri koraka: prepoznavanje, identifikacija, izdvajanje i rekonstrukcija. Na slici 2. je prikazan Lee znanstveni CSI model (engl. *Lee Scientific Crime Scene Investigation Model*). Model je fokusiran na sistematičan i metodičan pristup istragama koji se može primijeniti u bilo kom kriminalnom slučaju. Ograničenje modela je što analizira samo jedan dio procesa, a ne sve procese, više je fokusiran na prikupljanje podataka a ne pripremu i prezentiranje tih podataka [8].

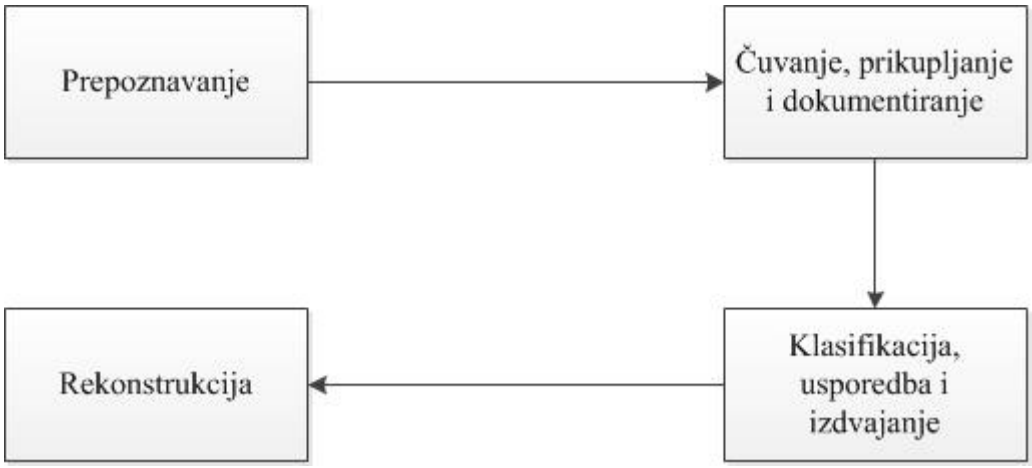


Slika 2. Leejev S CSI model [3][8]

4.1.2 Caseyev model

Casey [2] je preporučio model koji je fokusiran na obradu i ispitivanje digitalnih dokaza. Model je usmjeren na obradu i ispitivanje digitalnih dokaza kao najvažnije faze digitalne forenzičke istrage, te je veoma sličan Leejevom modelu. Prva i posljednja faza – prepoznavanje i rekonstrukcija su identične kao kod Leejevog modela. Ovaj model je također baziran samo na dijelu procesa digitalne forenzičke istrage.

Posljednja faza u samom modelu je proces rekonstrukcije, dok samo prezentiranje i arhiviranje digitalnih dokaza nije jasno predstavljeno.

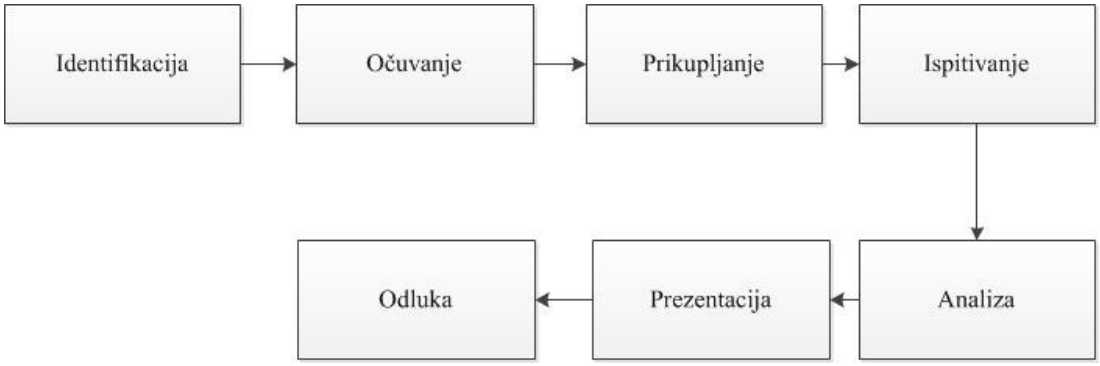


Slika 3. Caseyev model [2]

4.1.3 Okvir DFRW

Radna skupina za digitalne forenzičke istrage (engl. *The Digital Forensic Research Working Group, DFRW*) je razvila okvir koji se sastoji od sedam faza nazvanih „klase“ (slika 4.). Ove klase koje definiraju okvir služe da kategoriziraju aktivnosti istraga u određene grupe.

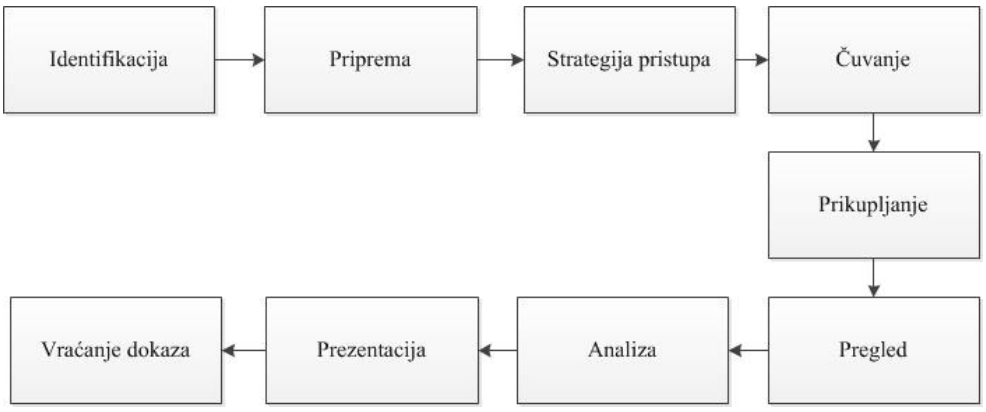
Specifičnosti okvira moraju biti u velikoj mjeri redefinirane za svaku pojedinu istragu ponaosob [88]. Ovaj okvir nije namijenjen da bude konačan i sveobuhvatan, nego kao temelj za daljnji rad koji će definirati puni model i okvir za buduća istraživanja. Model je predstavljen linearno [8].



Slika 4. Okvir DFRW

4.1.4 Reith, Carr i Gunchev model

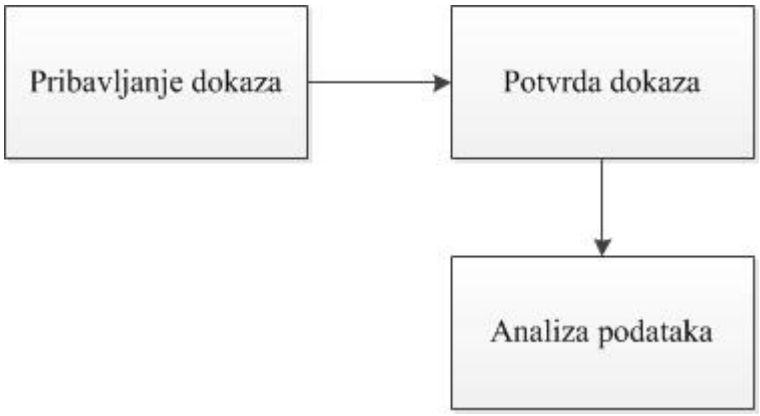
Ovaj model, koji je predstavljen 2002. godine uključuje neke nove komponente koje su nedostajale u prethodnim modelima. Model se fokusira na procedure digitalne istrage i ima devet faza [9]. Model je jako sličan okviru DFRWS.



Slika 5. Reith, Carr & Gunchev model

4.1.5 Kruss & Heisserev model

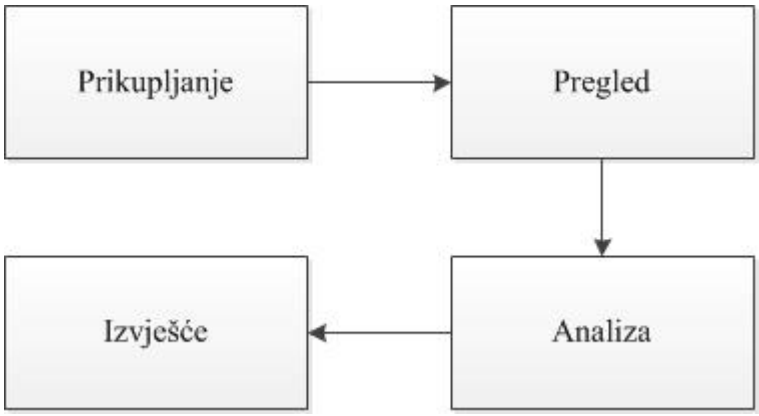
Prema modelu koji su osmislili Kruse i Heisser, proces digitalne forenzičke istrage se sastoji od tri bazne komponente: pribavljanja dokaza, provjeru autentičnosti i analizu [11]. Ove komponente su predstavljene na slici 6.



Slika 6. Kruss i Heisserev model [11]

4.1.6 Model USDOJ

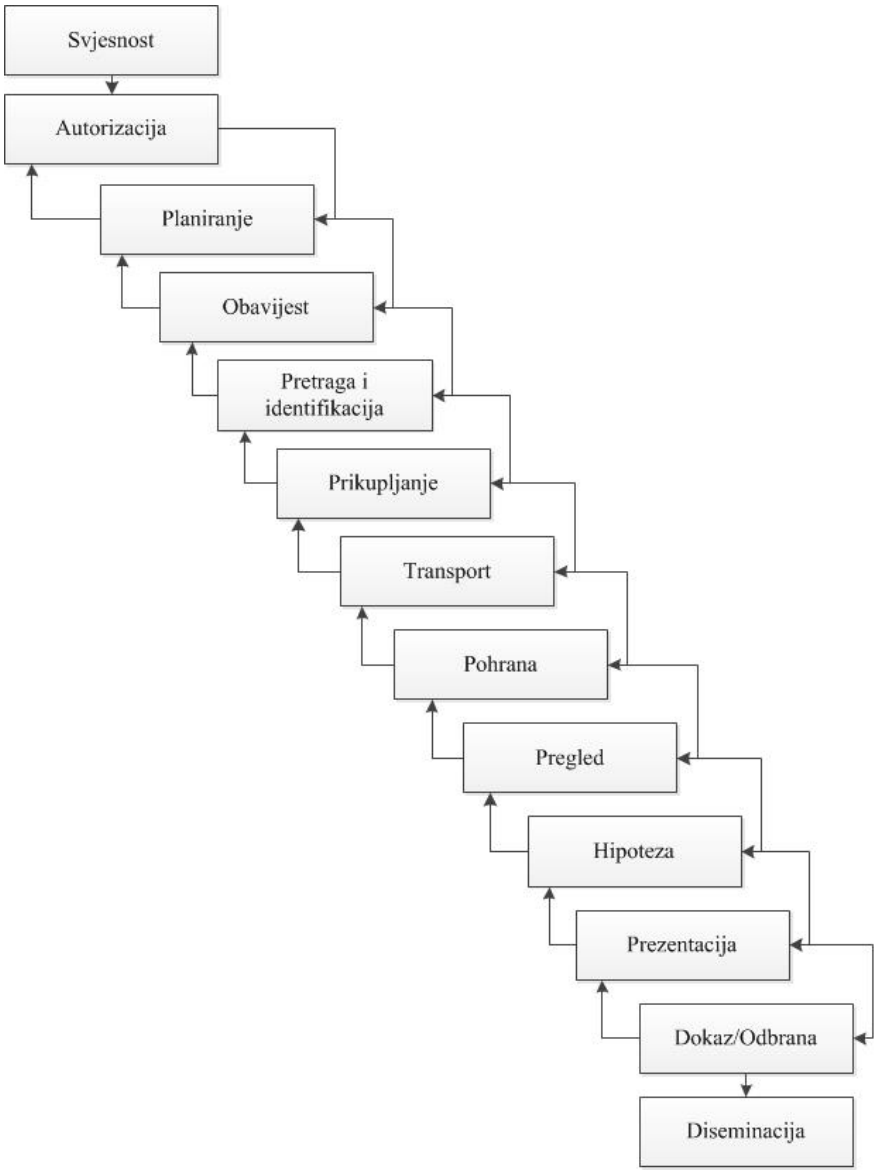
Model USDOJ (engl. *The United States of America`s Department of Justice*) se sastoji od četiri faze: prikupljanje, pregled, analizu i izradu izvještaja i apstrahiran je iz tehnologije [11]. Model je baziran tako da znatno bolje prepoznaje osnovne aspekte forenzičkih procesa, a zatim omogućuje izgradnju metodologije korak po korak. Ovo omogućava da se tradicionalno fizičko forenzičko znanje primjenjuje i na elektroničke dokaze.



Slika 7. Model USDOJ [11]

4.1.7 Prošireni Ciardhuainev model

Model koji preporučuje Ciardhuain [8] je najcjelovitiji model koji se može pronaći u literaturi. Faze ovoga modela se nazivaju aktivnosti i ukupno ih je trinaest. Za razliku od svih dosadašnjih modela, Ciardhuainev model eksplicitno predstavlja slijed informacija u istragama, te obuhvaća puni opseg istraga, a ne samo procesiranje dokaza. Inkluzija slijeda informacija u modelu, kao i aktivnosti istraga, čini ovaj model obuhvatnijim od drugih modela. On pruža osnovu za razvoj tehnika i alata za potporu u istragama [8]. Model je predstavljen na slici 8.



Slika 8. Ciardhuainev model koji se sastoji od 13 aktivnosti

4.1.8 Nekoliko novijih modela

Model forenzičkih procesa, preporučen od [89] se sastoji od četiri faze: prikupljanje, pregled, analiza i izvješćivanje. Model je veoma sličan ranije opisanim modelima [39].

Kohn, Eloff i Oliver (2006) su preporučili okvir koji je baziran na iskustvima drugih autora [11]. Prema [90] , okvir za procese istraga uključuje sve kombinacije odgovora na incident i računalne forenzike, a u cilju poboljšanja postojećih procesa.

Svi preporučeni okviri su upotrebljivi i imaju svoju kvalitetu. Činjenica je da je veoma teško razviti jedan okvir koji bi se mogao upotrijebiti u svim procesima istraga. Neki autori preporučuju mapiranje procesa naspram aktivnosti, a u cilju poboljšanja, te kreiranja novog okvira. Takav primjer je i „*Digital Forensic Investigation Framework*“ koji je uspostavljen kako bi ponudio jasan vodič koji bi trebalo slijediti u forenzičkim procesima [10].

4.1.9 DEMF okvir (Digital Evidence Management Framework)

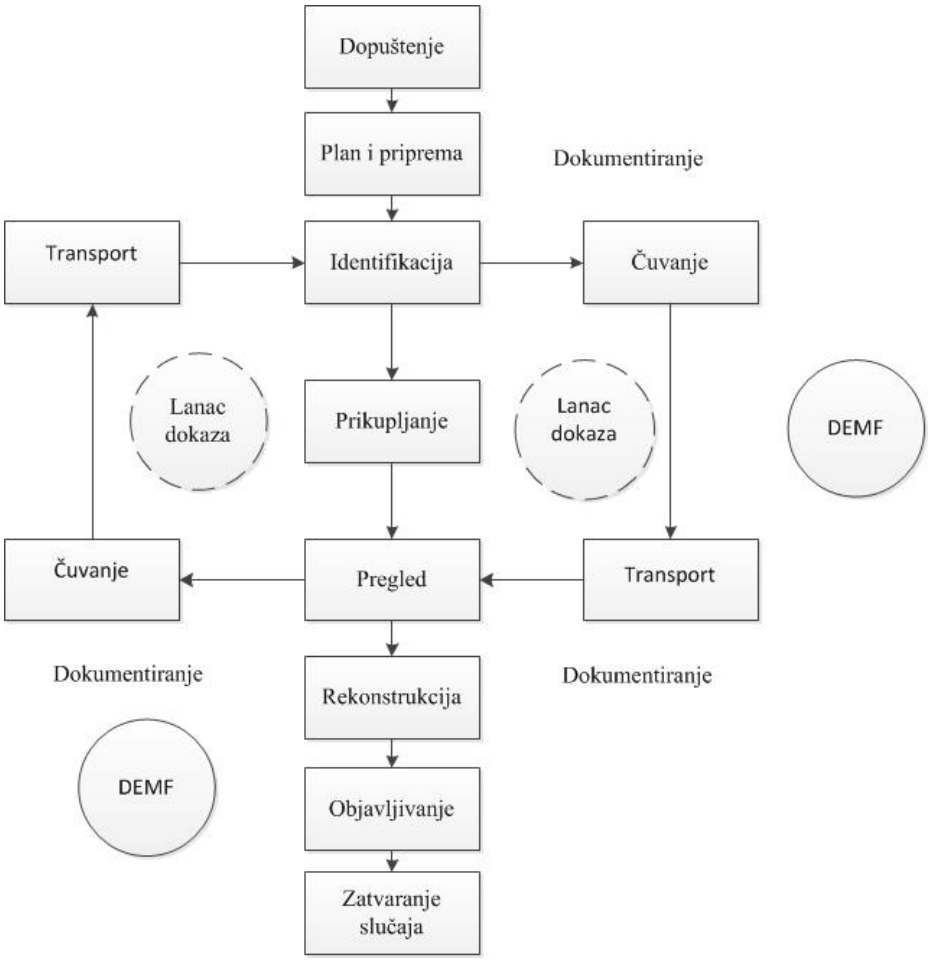
U poglavlju je predstavljeno nekoliko najčešće spominjanih modela koji se mogu pronaći u dostupnoj literaturi. Neki od modela se baziraju samo na određenim fazama digitalne istrage, dok je najcjelovitiji Ciardhuaianev model, koji obuhvata sve faze digitalne forenzičke istrage. Problem koji se pojavljuje u praksi je da u svakoj državi ne postoje iste standardne operativne procedure i zbog toga se ne može svaki model primijeniti u svakoj zemlji. U nekim Evropskim zemljama (npr. Hrvatska, Bosna i Hercegovina i Srbija) ne postoji dovoljno forenzičkih eksperata koji se mogu nositi sa digitalnim dokazima u svim fazama istrage. Najčešće su policijski službenici ili istražitelji ujedno i osoblje koje prikuplja pa i analizira digitalne dokaze. Drugi problem je taj da niti jedan od pobrojanih modela ne pridaje važnost pojmu „lanca dokaza“ i dokumentiranju lanca dokaza u forenzičkim istragama. Svrha svjedočenja o lancu dokaza je dokazati da dokaz nije primijenjen niti mijenjan kroz sve faze, i mora sadržavati dokumentaciju o tome kako se prikupljaju dokazi, kako su transportirani, analizirani i prezentirani. Pristup dokazima mora biti pod kontrolom i revizijom [47].

Cjelovitost lanca digitalnih dokaza igra vrlo važnu ulogu u digitalnom procesu forenzičke istrage, s obzirom na činjenicu da u svakoj fazi istrage istražitelji moraju znati gdje, kada i kako se otkrio i pronašao digitalni dokaz, kada je, tko dolazio u kontakt s dokazima, i sl.

Pravilno vođenje lanca dokaza mora uključivati dokumentaciju s odgovorima na sva ova pitanja. Ako jedna od tih pitanja ostane bez odgovora, lanac dokaza je ugrožen i prekinut [48].

Bitnost dokumentacije i vođenja lanca dokaza su središnja točka predloženog okvira autora Ćosić i Bača [12]. Glavne aktivnosti dane su u nastavku:

- Dopuštenje ili dozvola
- Planiranje i priprema
- Faze lanca dokaza
    - Identifikacija
    - Prikupljanje
    - Pregled
    - Transport i čuvanje
- Rekonstrukcija (hipoteza)
- Objavljivanje (dokaz/obrana)
- Zatvaranje slučaja
- Arhiviranje dokaza



Slika 9. Okvir DEMF [12]

Slika 9. prikazuje kompletan slijed i faze u preporučenom okviru. Pojašnjenje svake faze je dano u nastavku:

Dopuštenje/Dozvola

Svaka istraga mora započeti na zakonit način, a to podrazumijeva pribavljanje pismenog dopuštenja. Proces prikupljanja digitalnih dokaza mora započeti uz pismeno dopuštenje, naredbu suda ili državnog odvjetništva ako se radi o zvaničnim istragama ili dopuštenjem za vođenje internih istraga ukoliko se radi o internim istragama unutar poduzeća ili korporacije. U oba slučaja dopuštenje mora biti pisani dokument [47].

Planiranje i priprema

U ovim fazama istražitelji ili drugo osoblje koje vrši istragu još uvijek ne dolazi u kontakt sa digitalnim dokazima. Ovaj proces podrazumijeva izradu plana za istragu i autorizaciju od strane lokalne institucije koja će istragu i voditi. Autorizacija nije samo pribavljanje dozvole, odnosno naredbe za provođenje istrage, neophodna je za dobivanje naloga za pretres za korištenje bilo kojeg predmeta koji su pronađeni tijekom istražnog postupka. To znači, ako nemamo dozvolu, pronađeni dokaz ne može biti prihvaćen od strane suda[15]. Otvaranje dokaza i dokaznog materijala propisano je Kaznenim zakonom države, te veoma često se određene istrage i obustavljaju zbog nepridržavanja ovog propisa i propisanih procedura. Zbog toga je ova faza veoma bitna i ona determinira cijeli daljnji tok istrage. Također svi procesi u ovoj fazi moraju biti zakoniti i dokumentirani na adekvatan način.

Faze lanca dokaza

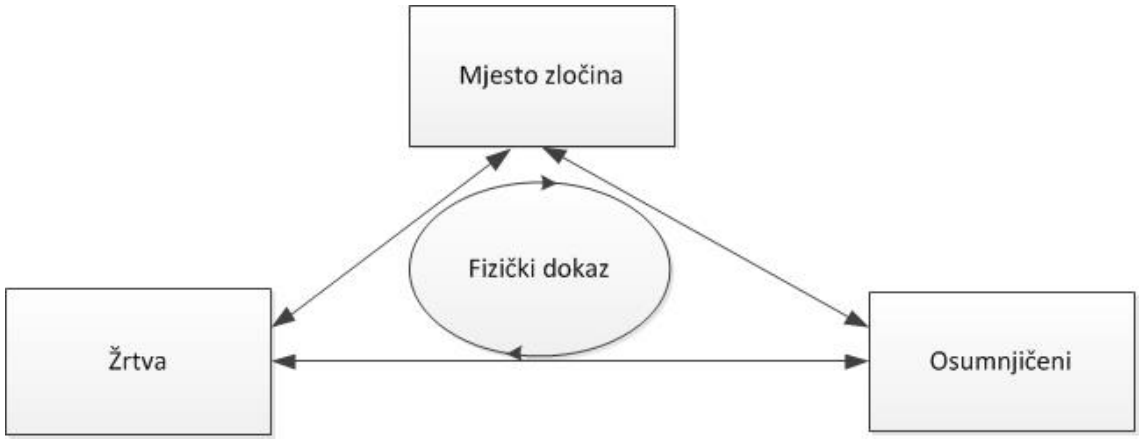
Identifikacija

Faza identifikacije u preporučenom radnom okviru bazirana je na lokaciji i identifikaciji opreme gdje je digitalni dokaz izvorno pohranjen. Radi se obično o računalima, nosiocima podataka, mreži, ugrađenim sistemima, mobilnim telefonima i sl. Okruženje može biti manje kompleksno npr. računalo na kom se radi tzv. „*post-mortem*“ analiza, a može biti veoma kompleksno, npr. računarstvo u oblacima (engl. „*Clouding*“), gdje je potrebno uključiti i davatelje Internet usluga, druge agencije, korporacije i sl. Ništa od toga se ne može započeti bez tzv. „*posebnih istražnih radnji*“ koje može odobriti isključivo sud uz adekvatnu naredbu. U svakom slučaju potrebno je identificirati digitalni dokaz i izdvojiti ga iz gomile datoteka. U specijalnim slučajevima kada se do dokaza mora doći „u letu“ (engl. „*On the fly*“) neophodno je također poduzimanje posebnih istražnih radnji, a pomoću kojih se vrši tzv. „*presretanje komunikacija*“ u cilju pribavljanja ovih dokaza. Veoma čest slučaj je kada se izvršitelji nekog

[15] Radi se o „nezakonito prikupljenom dokazu“ kojeg sud neće prihvatiti

kaznenog djela nalaze na teritoriji više država, te razmjenjuju elektroničku poštu putem raznih servisa za razmjenu informacija. Obzirom da je poznat samo digitalnih identitet tih lica, a ne stvarni, obično se vrši presretanje svog prometa između tih lica, a sve u cilju identifikacije i pronalaska digitalnih dokaza koji mogu upućivati na neko kazneno djelo.

U ovoj fazi potrebno je pridržavati se Lokardovog principa razmjene (engl. *Locard Exchange Principle*), koji pretpostavlja da uvijek dolazi do razmjene materije između dva objekta koji dolaze u kontakt na mjestu zločina. To znači da na mjestu zločina uvijek ostaju tragovi koje je potrebno pronaći [43]. Lokardov princip razmjene se primjenjuje i u digitalnim istragama, npr. kada dva računara komuniciraju na mreži između njih se razmjenjuju određene informacije (TCP/IP komunicira između ta dva računara). Bilo kakva komunikacija s nekim računalom, putem mreže, USB diska, CD/DVD ROM-a i sl. ostat će zabilježena u nekim *.log* datotekama ili barem u privremenoj memoriji računala dok je računalo uključeno.



Slika 10. Lokardov princip razmjene [2]

Cijelo vrijeme se mora imati na umu da digitalni dokaz može biti u privremenom stanju (npr. u RAM memoriji ili SWAP datoteci), i u tom slučaju se mora raditi tzv. „živa akvizicija“ (engl. *Live aqusition*). Živom akvizicijom se pored datoteke vrši povrat i *vremenskog žiga, datoteka registara, swap datoteka* i ostali detalji iz memorije [7]. Stoga se prije započinjanja samog procesa digitalne istrage – faze prikupljanja mora identificirati o kakvoj će se akviziciji raditi.

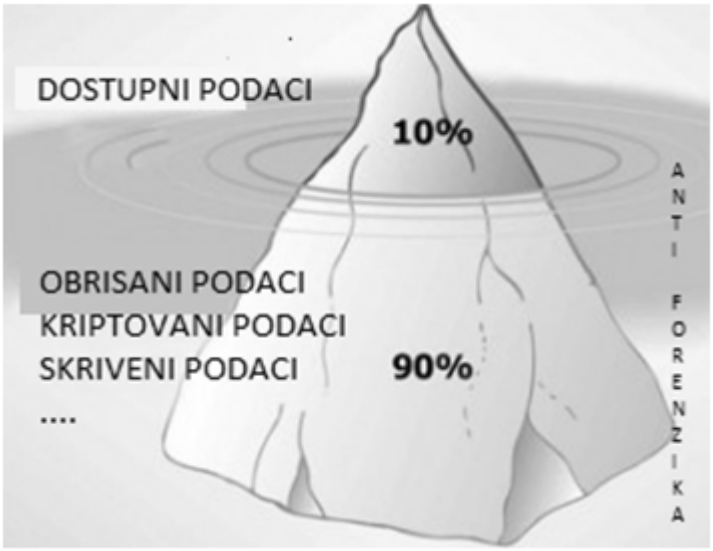
Prikupljanje

Proces prikupljanja digitalnih dokaza je najosjetljivija faza, jer u većini slučajeva je ovo prvi kontakt s fizičkim medijem na kom se dokazi nalaze-hardverom. U ovoj fazi osoblje mora biti veoma pažljivo, jer digitalni dokaz se nalazi u digitalnom formatu (niz nula i jedinica), i veoma lako se može uništiti ili promijeniti. Sva oprema (hardver) na kojoj se eventualnom mogu nalaziti dokazi se izuzima, radi se akvizicija i priprema za kasniju analizu. Ova faza je u fokusu mnogih znanstvenih istraživanja, jer svaka, pa i najmanja greška u ovoj fazi, može biti pogubna za daljnji tijek istrage. Ćosić i Bača su u već spomenutim istraživanjima upozoravali na rizike iz ove faze.

Pregled

Sve ono što je napisano i rečeno za fazu prikupljanja vrijedi i za fazu pregleda. Pregled digitalnih dokaza zahtjeva visok nivo znanja i ekspertize iz više različitih domena – poznavanje forenzičkih znanosti, tehničkih i informacijskih znanosti, poznavanje procesa kriminalističke istrage te prava. U ovoj fazi je veoma bitno imati kontrolu nad integritetom digitalnih dokaza. Svaki korak mora biti dokumentiran, a lanac dokaza se mora moći dokazati u ovoj fazi. Proces pregleda (analizu podataka) obično rade računalni forenzički eksperti, ali u nekim slučajevima u nekim zemljama, sud može zahtijevati angažiranje vještaka Informacijsko-komunikacijske struke. Ova vanjska ekspertiza mora biti neovisna i mora se bazirati na znanstvenim metodama koje vještak koristi. Ovisno od veličine ulaznih podataka, koji danas mogu biti reda *terabajta*, na izlazu može biti veoma mnogo, malo ili nikako podataka koje treba analizirati. Ovdje vrijedi princip ledenog brijega (slika 11.). Naime, veoma malo podataka se može pronaći regularnim pregledom izuzete opreme. Većina informacija je kodirana, kriptirana, skrivena, obrisana, i na neki od načina zaštićena kako je istražitelji ne bi mogli pronaći. Danas postoje posebne anti-forenzičke tehnike čija je osnovna namjena skrivanje, brisanje, mijenjanje podataka u cilju onemogućavanja regularnih forenzičkih alata [91,92]. Ukoliko digitalnu antiforenziku promatramo s aspekta primarne

namjene, i poštujući činjenicu da se radi o tehnologiji, može se reći da je to skup metoda i tehnika čija je primarna namjena kompromitiranje procesa digitalne forenzičke istrage, manipuliranjem sustava i narušavanjem integriteta digitalnog dokaza [92]. Stoga se ova činjenica nikako ne smije zanemarivati tijekom cijelog procesa.



Slika 11. Princip ledenog brijega koji vrijedi kod pretrage digitalnih dokaza

Transport i čuvanje

Transport i čuvanje digitalnih dokaza su faze koje se periodično ponavljaju. U ovim fazama digitalni dokazi su posebno osjetljivi, jer su pod utjecajem raznovrsnih faktora (osoblje, tehnički faktori, različite nepogode).

Rekonstrukcija

Tijekom cijelog procesa digitalne forenzičke istrage, osoblje koje vodi istrage mora imati postavljenu polaznu hipotezu koju treba dokazati ili pobiti. U nekim složenijim slučajevima obično se postavi više hipoteza, jedna glavna i nekoliko pomoćnih. Na ovaj način se

pokušava dokazati što se uistinu dogodilo. Proces rekonstrukcije je proces u kom se slažu kockice, cjelina se sastavlja iz dijelova koji su disperzirani, koji se moraju prepoznati, prikupiti. Ova faza se mora dokumentirati.

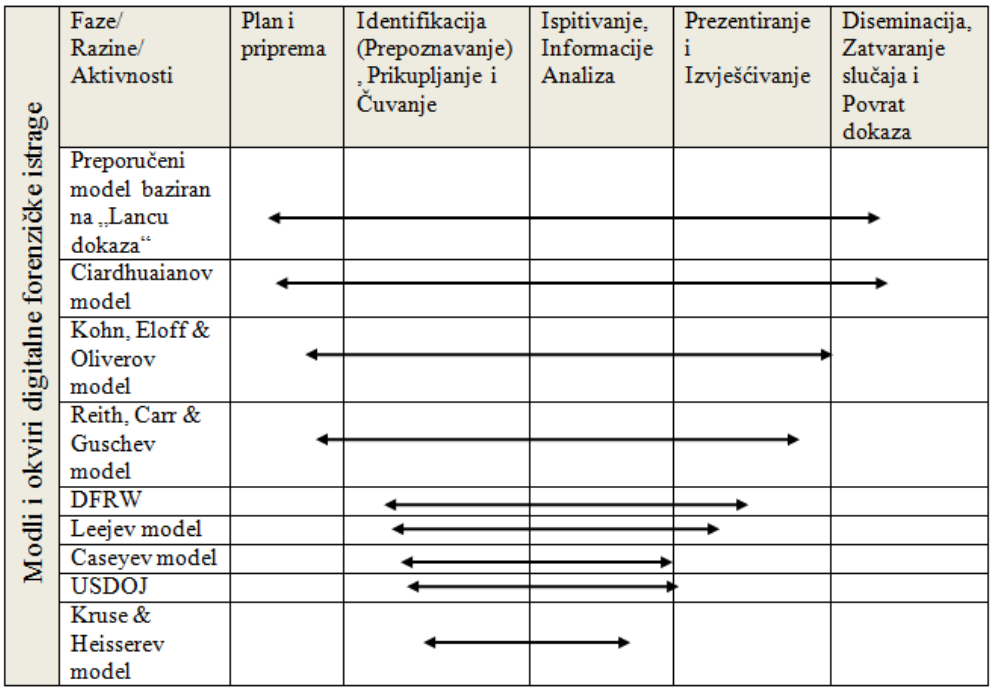
Objavljivanje rezultata

Proces objavljivanja rezultata digitalne istrage podrazumijeva prezentaciju rezultata na samom suđenju ukoliko se radi o zvaničnim istragama, ili ukoliko se radi o internim istragama unutar korporacija, na sastanku uprave. Objavljivanje rezultata također podrazumijeva dokazivanje i obranu i na kraju diseminaciju rezultata kroz baze znanja. Svaka korporacija, pa i sam sud, ima svoj vlastiti sustav baza znanja u koji pohranjuje ove rezultate za buduće korištenje.

Zatvaranje slučaja

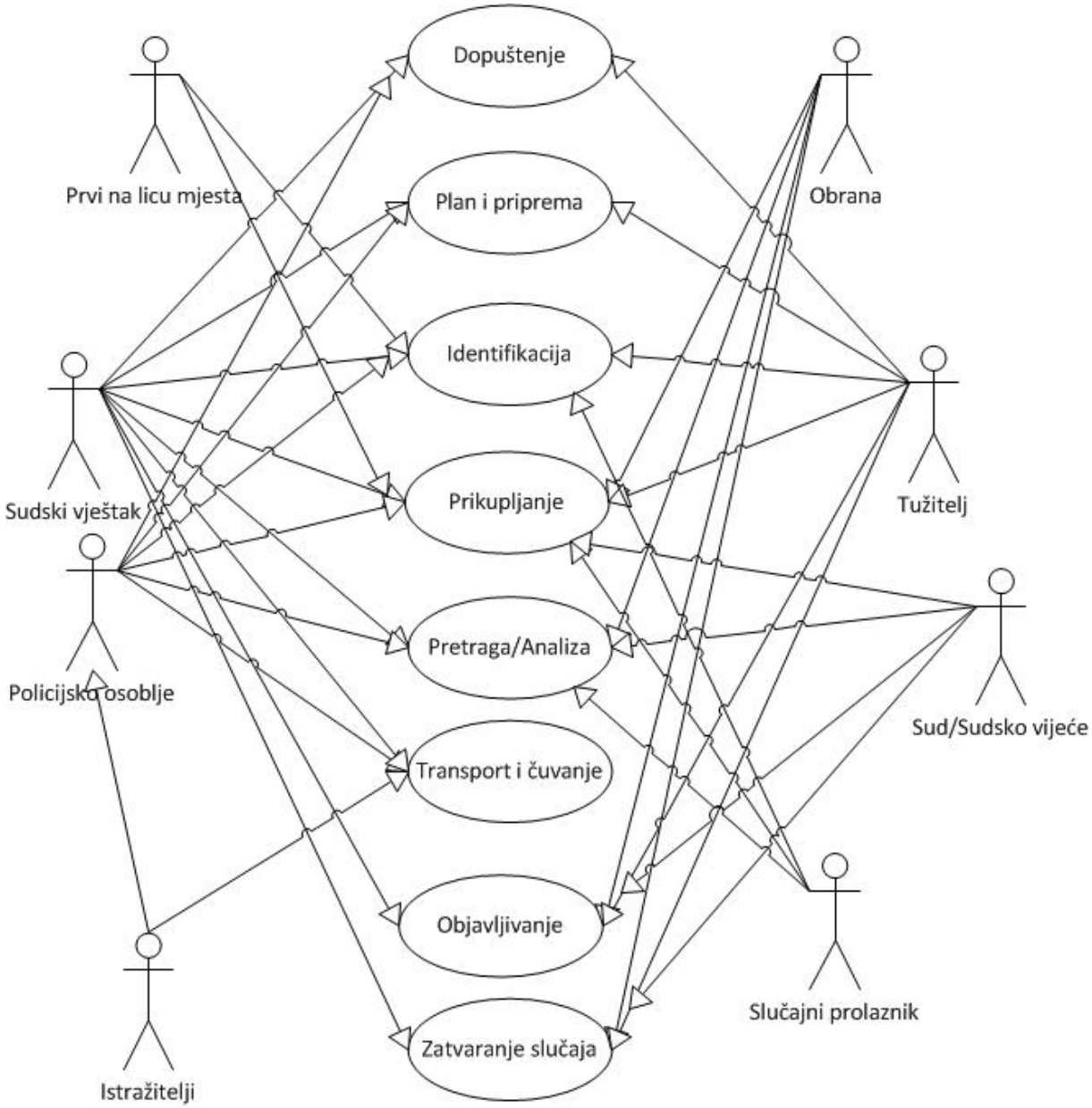
Posljednja faza u procesu digitalne forenzičke istrage nije predstavljanje digitalnih dokaza pred sudom. U nekim slučajevima postoji potreba da se rukuje s originalnim dokazima, a u toj fazi dolazimo u direktni kontakt , te se strogo mora voditi evidencija i očuvati lanac dokaza. Digitalni dokazi prolaze kroz svoj životni ciklus i na kraju tog ciklusa se moraju pohraniti i arhivirati (zatvaranje slučaja).

Tablica 2. Usporedba najčešće korištenih modela [12]



Modli i okviri digitalne forenzičke istrage	Faze/ Razine/ Aktivnosti	Plan i priprema	Identifikacija (Prepoznavanje) , Prikupljanje i Čuvanje	Ispitivanje, Informacije Analiza	Prezentiranje i Izvješćivanje	Diseminacija, Zatvaranje slučaja i Povrat dokaza
	Preporučeni model baziran na „Lancu dokaza“					
	Ciardhuaianov model					
	Kohn, Eloff & Oliverov model					
	Reith, Carr & Guschev model					
	DFRW					
	Leejev model					
	Caseyev model					
	USDOJ					
	Kruse & Heisserev model					

U tablici broj 2. je dana usporedba pobrojanih modela. Postoji veliki broj faza/razina/aktivnosti koje su slične od modela do modela. U nekim su aktivnosti iste ali su nazivi različiti. Kao što se može primijetiti neki modeli su nekompletni i baziraju se samo na nekim fazama, dok su neki cjelovitiji i obuhvatniji od drugih (Ciardhuainev model). Preporučeni model baziran na lancu dokaza (engl. *„Chain of Evidence“ model*) autora Cosic i Baca također pokriva sve faze digitalne forenzičke istrage.



Slika 12. Dijagram slučajeva upotrebe preporučenog modela

Na slici 12. je prikazan UML dijagram slučajeva upotrebe preporučenog okvira baziranog na lancu dokaza. Evidentno je da u okviru korespondira nekoliko glavnih aktera: Policijsko osoblje (*Osoblje prvo na licu mjesta, istražitelji*), Slučajni prolaznici, Sudski vještaci, Obrana, Odvjetništvo i Sud. Svaki od učesnika ima svoju ulogu.

4.2 Životni ciklus digitalnog dokaza

Ne postoji eksplicitna definicija životnog ciklusa digitalnog dokaza, ali se može upotrijebiti definicija digitalne datoteke u kontekstu digitalnog arhiviranja i informacije. Prema Hodgeu [93], u "*Best Practices for Digital Archiving—An Information Life Cycle Approach*", postoji nekoliko faza u životnom ciklusu informacije:

- Kreiranje (engl. *Creation*),
- Akvizija i prikupljanje (engl. *Acquisition and collection*),
- Identifikacija i katalogizacija (engl. *Identification and cataloguing*),
- Pohranjivanje (engl. *Storage*),
- Očuvanje (engl. *Preservation*), te
- Pristup (engl. *Access*).

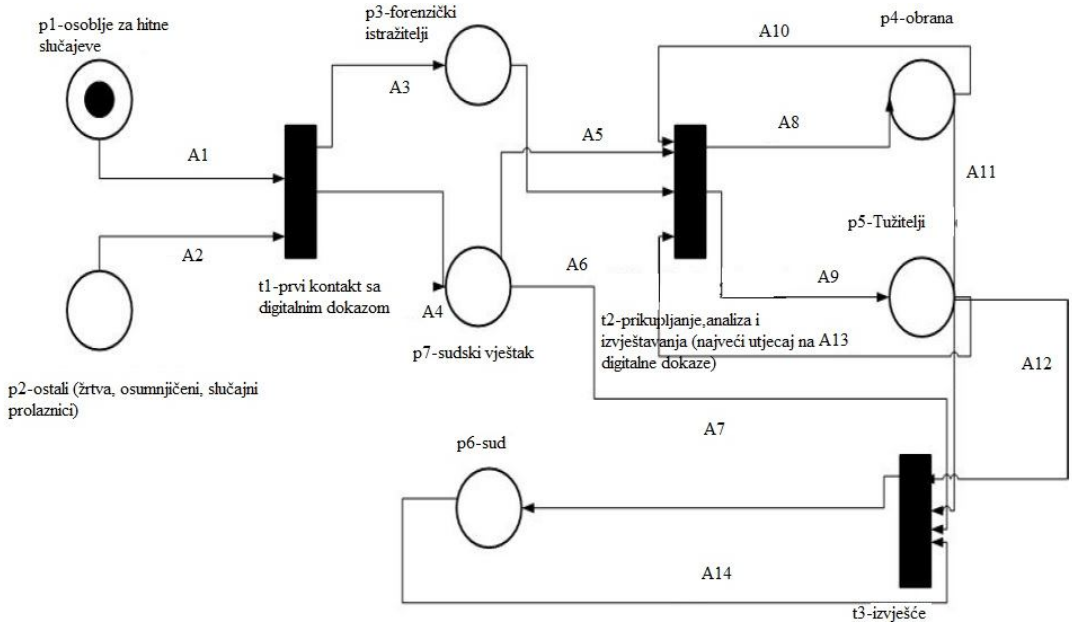
Postoje sličnosti u životnom ciklusu digitalnog dokaza. Prva faza u životnom ciklusu digitalnog dokaza nije faza kreiranja, jer u procesu digitalne forenzičke istrage već imamo digitalnu datoteku koja je kreirana u nekom ranijem periodu. Ova datoteka će postati digitalni dokaz tek u budućnosti u nekoj sljedećoj fazi.

Prva faza u životnom ciklusu digitalnog dokaza je identifikacija i prikupljanje. U ovoj fazi, istražitelji koji vode forenzičke istrage moraju pregledati ogromne količine podataka kako bi pronašli nešto što se može dovesti u vezu sa dokazima. Ova faza je veoma kompleksna i postoji mnogo utjecaja koji mogu narušiti lanac dokaza.
Sljedeća faza životnog ciklusa je pregled ili ispitivanje. U ovoj fazi kontakt s digitalnim dokazima imaju istražitelji i sudski vještaci. Faza ispitivanja podrazumijeva identifikaciju potencijalnih digitalne dokaze i odvajanje od druge velike količine digitalnih datoteka.
Proces pohrane i transporta su faze koje su neizostavne u ovom krugu. Sve vrijeme, tijekom cijelog procesa, mora se očuvati i održati lanac dokaza.

Faza izvješćivanja i objave rezultata podrazumijeva prezentiranje digitalnih dokaza pred odvjetništvom/sudom. U ovoj fazi kontakt sa digitalnim dokazima pored istražitelja, sudskih vještaka imaju i obrana i odvjetništvo.

Prezentiraju se rezultati forenzičke istrage, na kraju se slučaj zatvara, digitalni dokazi se pohranjuju i arhiviraju.

Kada uzmemo u obzir sve ove aspekte i činjenice, može se reći da životni ciklus digitalnih dokaza može početi s identifikacijom i prikupljanjem, nastavlja s ispitivanjem i izvještavanjem, i završava pohranom i arhiviranjem.



Slika 13. Životni ciklus digitalnog dokaza modeliran Petri mrežama [18]

Na slici 13. je prikazan životni ciklus digitalnog dokaza modeliran Petrijevim mrežama (engl. *Petri nets*). U svim fazama životnog ciklusa različito osoblje dolazi u kontakt s digitalnim dokazima, te postoji opasnost od narušavanja integriteta dokaza što u konačnici može utjecati na odluku sudca.

Proces prikupljanja digitalni dokaza nije tako jednostavan jer istražitelji i osoblje koje provodi digitalne istrage moraju točno znati sa čime se susreću i što ih očekuje kada prvi puta dođu u kontakt sa digitalnim dokazima [43]. Ova tvrdnja nije trivijalna ako uzmemo u obzir da samo jedan pogrešan korak može biti fatalan za cijeli tijek istrage. Na primjer, ukoliko osoblje koje provodi forenzičke istrage ugasi „*živo*“ računalo s Windows XP operativnim sustavom preko 50 datoteka će biti promijenjeno i 5 novih datoteka će biti kreirano pri prvom sljedećem

pokretanju sustava [13]. Ovo praktički znači da samo jedan neoprezan korak može uzročiti da se dokazi nepovratno izgube i naruši njegov integritet.

Postoji više preporuka i pokušaja standardizacije u ovom polju. Prva organizacija koja je uspostavljena sredinom 90tih sa ciljem da „osigura harmonizaciju metoda i prakse na međunarodnoj razini i garantira upotrebu digitalnih dokaza u sudovima drugih država“ [94] je bila međunarodna organizacija za digitalne dokaza (engl. *International Organization of Computer Evidence - IOCE*). IOCE je dala preporuku za nekoliko principa povezanih s digitalnim dokazima. Direkcija Federalnog Kriminalističkog Laboratorija[16] je 1998. godine formirala Znanstvenu radnu skupinu za digitalne dokaze (engl. - *Science Working Group on Digital Evidence* - SWGDE). Ova radna skupina je objavila više dokumenata najbolje prakse, vodiča, preporuka i tehničkih izvještaja. Ovi tehnički dokumenti nisu imali tehničkih detalja, ali su se mogli upotrijebiti kao okvir za razvoj određenih modela.

Radno tijelo za digitalnu forenziku SAD-a[17] (engl. *Digital Forensic Research Workshop - DFRWS*) je 2001.godine započela kao radionica, i nastavila je s radom i nastojanjima da u okruženje unese akademskom i praktično znanje. Svaka od ovih organizacija je imala principe i procedura ali ne i tehničke detalje kako implementirati ove preporuke.

4.3 Osiguranje integriteta digitalnih dokaza

Postoji više metoda i preporuka za digitalno potpisivanje digitalnih dokaza od strane ljudskog faktora koji dolazi u dodir sa njima. Najčešći način je digitalni potpis. Ova metoda podrazumijeva upotrebu asimetrične kriptografije. Osoba koja potpisuje upotrebljava tajni ključ da generira digitalni potpis, i bilo tko može provjeriti potpis upotrebljavajući objavljeni javni ključ u vidu certifikata potpisnika. Ova metoda ima mnogo nedostataka kao što su složenost, sporost, ključevi mogu biti ugroženi, certifikat može isteći, privatni ključ uvijek mora biti zaštićen. Integritet digitalnog dokaza osigurava da je informacija kompletna i nepromijenjena od vremena akvizicije (izuzimanja) pa do kraja procesa.

[16] Direkcija Federalne Kriminalističke Laboratorije je djelovala kao dio Federalnog ureda za istrage (engl. Federal Bureau of Investigation-FBI) SAD-a. Cilj je bio da SWGDE bude Američka komponenta IOCE-a.

[17] Prva radionica DFRWS je održana 2001.g. u Utica, New York u SAD-u. Okupila je preko 50 sveučilišnih istraživača, računalnih forenzičkih istražitelja i analitičara. Ovaj događaj je sponzoriran od strane Air Force Research Laboratory (AFRL).

Prema preporukama SWGIT [95] postoji više metoda za osiguranje integriteta dokaza: funkcija sažetka, vizualna verifikacija, digitalni potpis, pisana dokumentacija, CRC (engl. *Cyclic redundancy check*) funkcija, enkripcija, vodeni žig i metode vlasništva. U tablici 3. je dan pregled metoda za osiguranje integriteta digitalnih dokaza.

Tablica 3. Pregled metoda za osiguranje integriteta digitalnog dokaza [48]

Metoda	**Dužina**	**Opis**	**Prednosti**	**Nedostatci**
Ciklična provjera redundancije (engl. *Cyclic redundancy checks,* CRC): CRC 16 CRC 32 CRC 64	 16 bit 32 bit 64 bit	CRC često korištena metoda prilikom transfera datoteka – provjera uspješnosti samog transfera.	Veoma jednostavno za upotrebu, veoma brza, malo podataka na izlazu	Slaba sigurnost i osiguranje sažetka funkcije, problem s „analizom poruke“, veoma lako generirati drugu poruku koja rezultira istim CRC-om
Kriptografska funkcija sažetka (engl. *Cryptographic hash function*): MD2 MD4 MD5 SHA1 SHA224/256 SHA384/512	 128 bit 128 bit 128 bit 160 bit 224/256 bit 384/512 bit	Funkcija sažetka – matematički izračun koji rezultira generiranjem brojčane vrijednosti ovisno od ulaznih podatka. Ova vrijednost predstavlja vrijednost sažetka (engl. *hash value*).	Veoma lako je izračunati vrijednost sažetka za bilo koju poruku, relativna sigurnost funkcije, kriptografija funkcije	tzv. „*Collision and Preimage attack*“, osim SHA 224/256 i SHA 384/512

Tablica 3. Pregled metoda za osiguranje integriteta digitalnog dokaza (nastavak) [48]

Digitalni potpis (engl. *Digital signature*)	Ovisno o funkcije sažetka koja se upotrebljava	Rezultat je sažetak koji je kriptiran sa specifičnim privatnim ključem. Integritet datoteke može biti verificiran upotrebom funkcije sažetka i javnog ključa.	Povezanost identititeta s integritetom.	Sporost, kompliciranost implementacije
Vremenski žig (engl.*Time Stamp*)	Ovisno od funkcije sažetka koja se upotrebljava	Obično se upotrebljava za zapisivanje dešavanja, u kom slučaju je događaj obilježen s vremenskim pečatom. U datotečnom sustavu vremenski žig ukazuje na datum i vrijeme kreiranja ili modifikacije datoteke. Vremensko označavanje s povjerenjem je proces sigurnog čuvanja vremena kreiranja i modifikacije	Povezuje datum i vrijeme sa integritetom	Kompliciranost implementacije, ovisnost od „trećih strana“.

Tablica 3. Pregled metoda za osiguranje integriteta digitalnog dokaza (nastavak) [48]

Kodirnaje (engl. *Encryption*)	Ovisno od algoritma koji se upotrebljava	Kodiranje je proces prijenosa informacija (*plaintext*) upotrebljavajući algoritam (*cypher*) kako bi se učinio „nečitak“ za bilo koga tko nema specifično znanje (obično je to ključ). Rezultat procesa je kodirana informacija. Kodiranjem se štiti integritet i povjerljivost informacije.	Visoka sigurnost	Sporost, kompleksnost implementacije i održavanje

Prema Hosmeru [94,96] preporučene metode su metoda ciklične kontrole pogreške s CRC16, CRC32, jednosmjernim algoritmom sažetka, SHA-1, MD5, MD4, MD2 i digitalni potpis RSA, SA i PGP .

Danas najveći broj dostupnih forenzičkih aplikacija upotrebljava neki od dostupnih algoritama za provjeru sažetka (engl. *Hashing ili Checksum*) za verifikaciju integriteta digitalnog dokaza. Najviše zastupljeni su MD5 (*Message Diggest 5*) i SHA1 (*Secure Hash Algorithm 1*). Zbog prijavljenih slabosti ovih algoritama (MD5 i SHA0) [39], NIST[18] i druge organizacije za osiguranje integriteta digitalnih dokaza preporučuju da se upotrebljavaju

[18] NIST - Natinal Institute of Standard and Technology je nacionalni institut za standardizaciju i tehnologije SAD-a.

višestruki algoritmi kako bi se reducirao rizik od napada i slabosti koje su se pojavile u korištenju ovih algoritama.

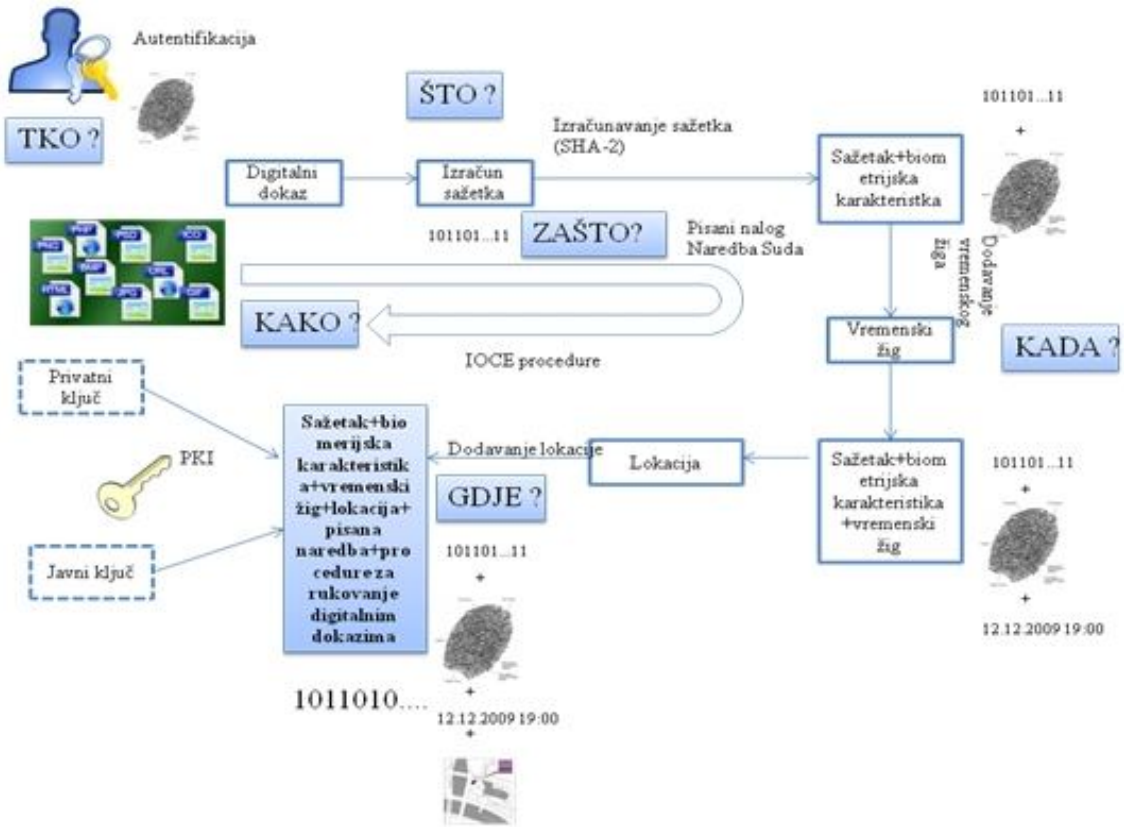
Neke aplikacije upotrebljavaju seriju SHA 2 algoritama: SHA-224, SHA-256, SHA-384 i SHA-512, algoritme koji generiraju duže sažetke.

4.4 Okvir za upravljanje digitalnim dokazima (engl. *Digital Evidence Managemet Framework*)

U ranijim radovima autori [19,47,49] su dali preporuke za okvir, koji bi mogao služiti kao osnova za izgradnju sustava u kom bi se mogao očuvati integritet digitalnih dokaza, dokazati očuvanost lanca dokaza, te imati kontrola nad dokazima tijekom cijelog procesa digitalne istrage. Istraživanja je financiralo Ministarstvo znanosti, obrazovanja i športa, Republike Hrvatske, kroz znanstvene projekte „Metodologija vrednovanja biometrijskih karakteristika“ (016-0161199-1721) i praktični projekt „Višestruka biometrijska autentifikacije pomoću pametne kartice“ (2008-043).

Okvir bi omogućavao da se svakog trenutka zna odgovor na pitanja 5W`s & 1 H. Slika 14. pokazuje izgled preporučenog okvira na visokoj razini apstrakcije. Okvir pokazuje životni ciklus digitalnog dokaza u svim fazama istrage, te potencijalne ranjivosti koje mogu biti iskorištene kako bi se narušio integritet digitalnog dokaza, a samim time narušio i lanac dokaza. Autentifikacija na sustav bi se vršila nekom biometrijskom karakteristikom korisnika sustava (otiska prsta, zjenica oka i sl.). Korisnici bi mogli biti istražitelji, sudski vještaci, tužitelji ili neko drugo zvanično osoblje. Odmah nakon autentifikacije na sustav izračunavao bi se sažetak nekom od dostupnih funkcija za izračun koje generiraju dulji sažetak (SHA512 ili MD5), te bi se vršila provjera da li osoba ima pravo pristupa na sustav. U bazi podataka korisnika sustava morali bi uzorci biometrijskih karakteristika sa vrijednostima sažetka.[19]

[19] Danas većina zemalja u EU ali van EU (Bosna i Hercegovina i Srbija npr.) već imaju baze podataka svojih građana u kojima su za svaku osobu pohranjene biometrijske karakteristike. To je jedan od uvjeta iz mape puta EU a kako bi svi građani u EU imali biomerijska osobna dokumenta.



Slika 14. Pogled na DEMF - visoka razina konceptualizacije

U prvoj fazi životnog ciklusa digitalnog dokaza pristup dokazu imaju osumnjičeni, svjedoci, slučajni prolaznici (npr. Internet cafee), te osoblje koje prvo dolazi na lice mjesta (engl. *first responders*). Njihov utjecaj na digitalne dokaze u ovoj fazi je jako velik. U ovoj fazi se mora pridržavati IOCE[20] principa, jer mala nepažnja znači nepovratno izgubljene dokaze[21]. Nakon što je korisnik sustava izvršio prijavljivanje, ukoliko se radi o istražitelju, sudskom vještaku, ili nekom drugom tko je ovlašten za rukovanje digitalnim dokazima izvršio bi se izračun sažetka digitalnog dokaza ponovno korištenjem MD5 i SHA512 funkcije. Nakon toga bi se dodavao sažetak razloga pristupu digitalnim dokazima, ovo bi obično bila naredba suda, naredba nadležnog tužilaštva i sl., te sažetak IOCE procedure ili nekog Pravilnika o rukovanju digitalnim dokazima. Sljedeće što je jako bitno je dodavanje vremenskog žiga. On naime

[20] Principi koje je propisala međunarodna organizacija za digitalne dokaze

[21] Računalo koje je uključeno nikako se ne smije ugasiti jer se može desiti da se dokazi nalaze u tzv. latentnom stanju, ili ukoliko je pokrenut program za kriptiranje sadržaja diska, usb-a i sl. nakon što se računalo ugasi šifra koja je bila rezidentna u memoriji računala nepovratno se gubi.

pokazuje (dokazuje) točan datum i vrijeme kada se pristupalo dokazima. Za ovu funkcionalnost se može koristiti interni sustav za vremensko označavanje ukoliko ga institucije imaju, ili se može koristiti usluga tzv. trećih lica (vremensko označavanje sa povjerenjem) gdje ključnu ulogu igra TSA (engl. *Time Stamp Authority*) od koje dobivamo vremenski pečat [48,94]. Prilikom dobivanja vremenskog pečata digitalni dokaz neće biti ugrožen jer se ne potpisuje on nego isključivo njegov sažetak (*hash vrijednost*). Sljedeće što se u sustavu dešava je dodavanje lokacije odnosno mjesta gdje je pristupano digitalnom dokazu.

Danas većina tzv. ugrađenih sustava i digitalnih uređaja u sebi ima ugrađen gps-om (eng. *Global positioning system*) ili a-gps (eng. *Assisted gps*) koji je podržan od strane davatelja mobilnih usluga a koji može služiti za tzv. geo-označavanje. Ukoliko se radi o zvaničnim institucijama svaki gps uređaj koji može odrediti točnu lokaciju, može se upotrijebiti u ove svrhe. Čuvanjem ovih podataka uvijek bi se znalo točno mjesto gdje se rukovalo sa digitalnim dokazima. Ovaj skup podataka dodatno bi se mogao osigurati implementiranjem infrastrukture javnog ključa (engl. *Public Key Infrastructure, PKI*) potpisivanjem ove skupine podataka sa tajnim ključem. Generalno okvir bi se mogao predstaviti kao sljedeća funkcija[1]:

```
CoDe = f {  fingerprint _of _file,          //what
            biometrics_characteristic,      //who
            time_stamp,                     //when
            gps_location,                   //where        [1]
            reason,                         //why
            set_of_procedures};             //how
```

U posljednje dvije godine nekoliko autora iz Velike Britanije, Španjolske, Omana, Brazila i Malezije, se bavilo pokušajima izgradnje sličnih okvira ili pokušajima implementacije ili čak formaliziranja DEMF-a [6][20][21][22][23][24][25][26].

POGLAVLJE V

5 PRIHVATLJIVOST DIGITALNIH DOKAZA

U ovom poglavlju je pojašnjen koncept prihvatljivosti digitalnih dokaza, te su predstavljeni rezultati istraživanja na temu prihvatljivosti digitalnih dokaza u sudovima u Bosni i Hercegovini. Cilj je da se stekne uvid u način na koji sudci rezoniraju kada trebaju donijeti odluku o prihvatljivosti digitalnih dokaza, te da se istraži trenutna situacija u sudovima u Bosni i Hercegovini kada je u pitanju prihvatljivost i očuvanje lanca dokaza. Unutar poglavlja će biti prezentirani i rezultati preliminarnog istraživanje koje je provedeno u sudovima u Bosni i Hercegovini, a na temu prihvatljivosti digitalnih dokaza u kaznenom postupku.

Prihvatljivost (engl. *Acceptability*) digitalnih dokaza je pojam koji determinira da li će potencijalni digitalni dokaz uistinu i postati dokaz u konačnici, koja obično dobiva sudski epilog ukoliko se radi o zvaničnim, državnim istragama. Suci odlučuju koji će dokaz biti prezentiran ili ne u njihovoj sudnici. Isto tako, suci odlučuju o angažiranju sudskih vještaka za oblast informatike koji će svjedočiti o znanstvenim aspektima potencijalnih digitalnih dokaza. Danas postoji veoma malo objavljenih radova koji opisuju kako suci donose tu odluku [55,56,97]. U okruženju (zemlje Balkana ali i šire) nije bilo javno objavljivanih rezultata ovakvih ili sličnih znanstvenih istraživanja.

Bitno za razumijevanje prihvatljivosti digitalnih dokaza je razumijevanje dva osnovna principa koji se spominju kod prihvatljivosti digitalnih dokaza na sudovima. To su Daubertov princip i Fryeov test. Daubertov princip je, kako je već spomenuto, zamijenio dugo godina korišteni „*Fryev test*“, a prema njemu se sve više uvodi znanost i znanstvene metode kao obavezne kod vještačenja i prezentiranja digitalnih dokaza. O ovome je detaljnije pisano u trećem poglavlju.

Američko Pravilo 702 kao dio Federalnog zakona o dokazima (engl. *Federal Rules of Evidence*) daje smjernice za kvalifikacije vještaka i umanjuju mogućnosti pristranosti u vještačenju. Pravilo 702 Američkog zakonodavstva se koristi kao preventiva mogućim nagađanjima od strane vještaka, a koje bi sudac mogao koristiti [97].

5.1 Provedeno istraživanje na temu prihvatljivosti digitalnih dokaza u sudovima u Bosni i Hercegovini

U cilju ustanovljenja na koji način se digitalni dokazi prihvaćaju u sudovima u Bosni i Hercegovini, urađeno je preliminarno istraživanje u nekoliko sudova u različitim dijelovima Bosne i Hercegovine, različite razine, općinski, županijski i državni Sud BiH. Obuhvaćeni su isključivo suci koji odlučuju u „kaznenom postupku" (tzv. „*krivičari*") koji se svakodnevno susreću sa digitalnim dokazima. Istraživanjem nisu obuhvaćeni suci koji odlučuju u građanskim parnicama – parničnom postupku, jer se tu digitalni dokazi pojavljuju veoma rijetko ili u skoro zanemarljivo malom procentu.

5.1.1 Uvod

Kako bi bili pravilno informirani i mogli donositi odluke o prihvatljivosti digitalnih dokaza u sudnici, te razumjeti svjedočenje sudskih vještaka, suci i porota moraju imati određeno znanje o informacijsko-komunikacijskim tehnologijama [3,57,98].

Veoma često to znanje nije bazirano na formalnim obukama i edukaciji, nego na osobnom iskustvu i znanju koje je stečeno upotrebom računala i interneta [28,99]. Mason [100] je u svojim istraživanjima predstavio nekoliko kompleksnih situacija sa kojima se suci susreću i sa kojima se moraju nositi u sudnici sa kojom predsjedavaju:

- Sucu je prezentirana tzv. „log datoteka"[22] s mrežnog servera, koja pokazuje da je upad u server došao sa posebne IP adrese. Zapisi davatelja Internet usluga (engl. *Internet Service Provider - ISP*) pokazuju da je IP adresa pripadala računaru s posebnim prebivalištem u vrijeme incidenta. Ova informacija bi trebala biti upotrijebljena da „nepropisno" identificira osobu kao prijestupnika.
- Sucu je prezentirana povijest poziva i zapisi davatelja telefonskih usluga koji pokazuju da je jedan mobilni telefon upotrijebljen za poziv prema drugom mobilnom telefonu. Sudac i porota možda pogrešno vjeruju da ovaj dokaz dokazuje da su vlasnici ova dva telefona imali konverzaciju.

[22] Datoteka koja se nalazi na mrežnom poslužitelju a u kojoj su zabilježana sva dešavanja kako na sistemskom dijelu, tako i na mrežnom i aplikacijskom dijelu poslužitelja.

- Meta podaci Microsoft Word dokumenta uključuju ime osobe koja je registrirala softver. Osim u slučaju da se ta informacija namjero izbriše, ona ostaje u svakom dokumentu koji je generiran s Office aplikacijom. Sudac koji vodi slučaj obično zaključuje da meta podaci koji su uključeni u dokument dokazuju da ime te osobe identificira autora dokumenta.
- Digitalni potpis na elektroničkom dokumentu može biti prihvaćen od strane suda kao dokaz da je vlasnik potpisa ujedno i tvorac elektroničkog dokumenta. Ukoliko je elektronički potpis kompromitiran funkcija elektronskog potpisivanja se može zloupotrijebiti. Ukoliko to sudac ili porota ne razumije, krivotvoren dokument može biti prihvaćen kao legitiman u procesu [100].

Jedna od situacija s kojima se suci susreću u kaznenom postupku, a u kojoj moraju znati donijeti ispravnu odluku je i sljedeća:

- Od administratora jednog web portala i davatelja Internet usluga (engl. *Internet Service Provider*) dobiveni su podaci o licu koje je činilo DDoS napad (engl. *Distributed Denial of Service*) na jedan web portal. Podaci su sadržavali IP adresu s datumom i vremenom kada je davalac Internet usluga tu adresu dodijelio licu. Izuzimanjem i pregledom računala ustanovljeno je da računalo koristi osoba koja nema nikakvog znanja niti motiva da uradi ovakve napade, te da je najvjerojatnije njegovo računalo bilo tzv. „*zombie*“ i dio mreže *botova* kojima je upravljano iz daljine s potpuno druge lokacije.

Druga situacija u kojoj se suci susreću s kompleksnošću problema prihvatljivosti digitalnih dokaza je sljedeća:

- Lice osumnjičeno da je učinilo kazneno djelo snimljeno je video-nadzorom iz banke koja se nalazila u blizini počinjenja kaznenog djela. Policija je izuzela video-zapis sa snimkom te izdvojila dio na kom je zabilježeno izvršenje djela. Integritet digitalnog snimka je osiguran SHA-256 funkcijom. Obzirom da je bio mrak te loše osvjetljenje u blizini kamere lice se nije moglo prepoznati, te je vještak posebnim metodama izdvojio fotografiju licu te istu „retuširao“ a kako bi se dobila kvalitetnija slika. Ovom metodom je potpuno promijenjen originalni digitalni dokaz te sljedeće uzimanje SHA-256 sažetka dalo je potpuno drugi rezultat !

Uloga suca je ključna i on igra ulogu „vratara“ u odlučivanju koji će se dokaz prihvatiti u njegovoj sudnici [99,101,102]. Pravilo 702 Federalnih pravila o dokazima[23] osigurava vodič za sudove o kvalificiranju sudskog vještačenja i osiguranju znanstveno temeljenog svjedočenja. „*Daubert vs. Merrel „Dow Pharmaceuticals Inc*„ 1993.godine opisuje test sa 4 koraka koji determiniraju koji dokazi mogu biti prihvaćeni u sudovima u USA [3,17,57]:

- Testiranje: Mogu li i jesu li znanstvene procedure neovisno testirane?
- Objavljivanje: Jesu li znanstvene procedure objavljene i da li su prošle znanstvenu recenziju?
- Učestalost pogreške: Da li je poznata učestalost pogreške, te da li se potencijalno može u primjeni znanstvenih procedura?
- Prihvaćanje: Da li su znanstvene procedure generalno prihvaćene od strane relevantne znanstvene zajednice?

Prije Daubertovog principa prihvaćanja, suci su odlučivali prema „*Fry v. United States*“, a koji je zahtijevao da su znanstveni dokazi prezentirani pred sudom produkt generalno prihvaćenih metoda od strane znanstvene zajednice, ali su dopuštali sudcu da sam donosi odluku o generalnom prihvaćanju. Daubertov princip ili test je osigurao sucima vodič za prihvaćanje dokaza.

Kao što je već ranije konstatirano danas je veoma malo literature koja opisuje kako sudci prihvaćaju digitalne dokaze [28,29,57]. U okruženju u Bosni i Hercegovini, Hrvatskoj, Srbiji nema objavljenih radova na ovu temu. Pretraživanje relevantnih baza podataka, korištenje pretraživača na internetu pojma „prihvatljivost digitalnih dokaza“ nije dalo ili je dalo veoma malo rezultata.

5.1.2 Ciljevi istraživanja

Cilj istraživanja je bio da se da uvid u trenutno stanje, primarno, na koji način sudovi u Bosni i Hercegovini formalno prihvaćaju digitalne dokaze, da li se vrši nadzor nad lancem dokaza, te kakvo je generalno stanje u sudovima u Bosni i Hercegovini kada su u pitanju digitalni dokazi, prihvatljivost digitalnih dokaza s aspekta lanca dokaza. Dodatni cilj koji se želi postići

[23] FRE – Federal Rule of Evidence je Federalni zakon o dokazima SAD

je da se skrene pozornost na ovaj problem, te ponudi model za buduća istraživanja, te edukacije koje su neophodne u ovoj domeni.

5.1.3 Metodologija istraživanja

Metoda anketiranja se pokazala kao najprikladnija metoda za ovo istraživanje. Sastavljen je upitnik, pri čemu se prilikom sastavljanja pitanja naročito pazilo „da se svako pitanje odnosi na indikator, indikator na varijablu, a varijabla na hipotezu, a hipoteza na problem“ [103]. Ciljana skupina su bila sudovi različitih razina (od razine općine, preko županije pa do države). Cilj je bio prikupiti oko 25-30 popunjenih anketnih obrazaca. Potrebno je napomenuti da su sudovi organizirani tako da su suci u njima podijeljeni na suce koji vode „građanske parnice“ i suce koji vode „krivični postupak“. Digitalni dokazi se u Bosni i Hercegovini (slična situacija je i sa Hrvatskom i Srbijom)[24] u parničnom postupku ne koriste ili se koriste u jako malom omjeru naspram kaznenog postupka. Zbog te činjenice se anketa i slanje anketnih obrazaca baziralo na kontaktu samo sa sucima koji rade u kaznenom postupku, i koji svakodnevno dolaze u kontakt sa digitalnim dokazima.

5.1.4 Prikupljanje podataka i karakteristika uzorka

Istraživanje je provedeno na uzorku od 80 sudaca koji rade u krivičnim sudovima na različitim razinama u različitim dijelovima Bosne i Hercegovine. Upitnik je urađen on-line i u svibnju 2013. godine je poslan na adrese ciljanih sudaca (80 sudaca).

Adrese elektroničke pošte sudaca su pronađene na web stranici Visokog sudskog i tužilačkog vijeća[25], svaka adresa je bila tipa *ime.prezime@pravosudje.ba*. Nakon mjesec dana upitnik (anketu) koja je napravljena kao web forma, su popunila samo 4 sudca, što je značilo da je bilo potrebno da ih se dodatno animira kako bi procent bio veći. Isto je urađeno telefonski, posredstvom predsjednika i sekretara sudova koji su na sebe preuzeli obavezu iniciranja popunjavanja ankete od strane ciljanih sudaca. Samo jedan predsjednik suda je inzistirao da se anketa izvrši slanjem štampanih obrazaca koje će se naknadno popuniti i vratiti popunjeni.

[24] Povrda ove konstatacije stoji i u izlaganjima sa konferencije o digitalnim dokazima koju organizira MUP HR i tvrtka INSIG2 (http://www.mup.hr/main.aspx?id=121965)

[25] Neovisni i samostalni organ koji ima zadatak da osigura nezavisno, nepristrano i profesionalno pravosuđe u Bosni I Hercegovini (www.hjpc.ba)

Nakon četiri mjeseca rezultat je bio 30 popunjenih anketnih obrazaca što je prema [104] činilo stopu povrata od 37.5 % , koja se smatra prihvatljivom u ovakvom istraživanju [104]. Potrebno je napomenuti da u svim anketnim obrascima nisu bila popunjena sva polja jer pojedini sudci nisu odgovarali na pitanja koja bi se mogla dovesti u direktnu vezu sa njihovim identitetom. Iako je u dopisu koji je slat sudovima bilo jasno naznačeno i dana je izjava o čuvanju tajnosti i osobnih podataka, želja za anonimnosti je bila velika, te je inzistirano da nazivi sudova budu kodirani. Odnos spola ispitanika je 60% muški naspram 40% ženski (tablica 4.). Najveći broj sudaca ispitanika je u starosnoj dobi od 41-50 godina (36,6%), zatim 31 do 40 godina 23%, a slijede sudci starosti između 51 i 60 godina (20%), te preko 60 godina (20% ili 6 sudaca).

Tablica 4. Tablica frekvencija modaliteta demografskih karakteristika ispitanika

	Broj ispitanika	**Procentualni iznos**
Spol ispitanika		
Muški	18	60%
Ženski	12	40%
Ukupno:	30	100%
Dob ispitanika		
31-40	7	23%
41-50	11	36,6%
51-60	6	20%
Preko 60 godina	6	20%
Ukupno:	30	100%*
Radno iskustvo kao sudac		
Do 10 godina	9	31%
10-15 godina	5	17%
16-20 godina	5	17%
21-30 godina	3	10%
Preko 30 godina	7	24%
Ukupno:	29	100%*

*Zbroj postotaka pojedinih modaliteta zbroj nije 100% zbog zaokruživanja.

Radnog iskustva kao sudac do 10 godina starosti ima najviše sudaca (31%), nakon čega slijede sudci sa radnim iskustvom preko 30 godina (24%), 10-15 godina (17%) i 16-20 godina (17%). Radnog iskustva od 21-30 godina je 10% sudaca (3 sudca), dok jedan sudac nije odgovorio na ovo pitanje.

Tablica 5. Tablica frekvencija modaliteta demografskih karakteristika ispitanika br.2

	Broj ispitanika	**Procentualni iznos**
Razina suda		
Općinski	17	59%
Županijski	5	17%
Državni	7	24%
Ukupno:	29	100%
Populacija stanovništva koje pokriva sud		
Do 20.000	1	3,3%
20.001-50.000	1	3,3%
50.001-100.000	10	33,3%
Preko 100.000	18	60%
Ukupno:	30	100%*

*Zbroj postotaka pojedinih modaliteta zbroj nije 100% zbog zaokruživanja

Što se tiče razine suda najviše sudaca ispitanika je s općinske razine suda koji rješava kaznena djela po osnovu mjesne nadležnosti iz oblasti računalnog kriminala (kaznena djela za koja je propisana manja kazna ili je načinjena manja šteta) i to 17 što čini 59%, nakon čega slijedi državni sud sa 7 sudaca (24%) te Županijski sud sa 5 ispitanika (17%). Jedan sudac nije popunio ovo polje u anketi. Najviše sudova pokriva područja sa populacijom preko 100.000 stanovnika i to 18, što čini 60% uzorka. Rezultati su prikazan u tablici 5.

5.1.5 Rezultati istraživanja

U nastavku će biti prikazani rezultati istraživanja, odnosno pokušat će se dobiti odgovori na sljedeća pitanja:

- Na kojoj razini je poznavanje IKT-a od strane sudaca,

- Na kojoj razini je poznavanje procesa digitalne istrage i digitalnih dokaza,
- Koji faktori su bili ključni za poznavanje digitalnih dokaza,
- Da li se prilikom prihvaćanja digitalnih dokaza slijede određena pravila ili standardi,
- Da li se angažira sudski vještak kao pomoć pri pojašnjenju digitalnih dokaza,
- Da li je sucima poznat pojam „lanac očuvanja dokaza“ i metode očuvanja integriteta digitalnog dokaza,
- Da li suci u predmetima u kojima predsjedavaju Vijećem inzistiraju na dokazivanju nepovredivosti lanca digitalnih dokaza, te
- Koji faktori najviše doprinose efikasnom prezentiranju digitalnih dokaza kao ključnih za određeni slučaj.

Kao što je već ranije rečeno, anketa je poslana elektronskom poštom na 80 različitih adresa sudaca u različitim dijelovima Bosne i Hercegovine, ali se vratila samo od 4 suca. To čini svega 0.05%. Slična je i situacija s doktorskom disertacijom [57] gdje se od 10.000 poslanih elektroničkih poruka vratilo svega 18 (0.0018%). Ovo je značilo da je bilo potrebno na neki način inicirati i motivirati suce da popune anketu. Nakon dodatno učinjenih napora i dobivenih podataka rezultati su sumirani u tablici 6. u kojoj su prikazani anominizirani rezultati istraživanja. Podaci koji bi eventualno mogli identificirati sud ili konkretnog sudca u tom sudu nisu prikazani jer je to izričito traženo od sudaca prilikom objave rezultata istraživanja.

Tablica 6. Anominizirani rezultati ankete

ID	HS	IN	WE	DF	DD	Isk	DDD	Standard	Vještak	5ws&1h	Starost	Spol	Pop
I1	5.0	5.0	5.0	5.0	5.0	>	DA	DAUBERT	DA	DA	45	M	>100K
I2	3.0	3.0	3.0	3.0	3.0	<	DA	FRY	DA	DA	37	Ž	>20K
I3	4.0	4.0	4.0	3.0	3.0	<	DA	FRY	DA	NE	42	M	>100K
I4	5.0	5.0	5.0	5.0	5.0	<	DA	NEZNAM	DA	NE	43	M	>100K
I5	3.0	4.0	4.0	2.0	2.0	>	DA	NEZNAM	DA	NE	50	Ž	>100K
I6	3.0	3.0	3.0	1.0	2.0	=	DA	NEZNAM	DA	DA	55	Ž	>100K
I7	5.0	5.0	5.0	4.0	4.0	<	DA	NEZNAM	DA	DA	32	M	>100K
I8	3.0	2.0	2.0	2.0	3.0	=	DA	NEZNAM	DA	NE	62	M	>100K
I9	2.0	3.0	2.0	3.0	2.0	>	DA	NEZNAM	DA	NE	55	Ž	<100K
I10	4.0	4.0	4.0	3.0	3.0	<	DA	FRY	DA	DA	56	M	<100K
I11	2.0	2.0	2.0	1.0	1.0	=	DA	NEZNAM	DA	NE	63	M	<300K
I12	4.0	4.0	4.0	1.0	2.0	=	DA	NEZNAM	DA	NE	49	Ž	<100K

Tablica 6. Parcijalni rezultati ankete (nastavak)

I13	1.0	3.0	4.0	1.0	1.0	=	DA	NEZNAM	DA	NE	64	M	<100K
I14	1.0	2.0	2.0	2.0	3.0	=	DA	NEZNAM	DA	NE	47	M	<100K
I15	2.0	3.0	2.0	2.0	3.0	<	DA	NEZNAM	DA	NE	48	M	<100K
I16	2.0	2.0	2.0	2.0	1.0	>	DA	NEZNAM	DA	NE	59	Ž	<100K
I17	2.0	2.0	2.0	2.0	2.0	=	DA	NEZNAM	DA	NE	64	M	<100K
I18	5.0	4.0	3.0	3.0	3.0	>	DA	NEZNAM	DA	DA	37	Ž	>50K
I19	1.0	3.0	4.0	2.0	2.0	=	DA	NEZNAM	DA	NE	31	Ž	>100K
I20	5.0	5.0	4.0	4.0	4.0	<	DA	FRY	DA	DA	33	Ž	>100K
I21	3.0	2.0	3.0	2.0	2.0	=	DA	FRY	DA	DA	51	Ž	<100K
I22	1.0	1.0	1.0	1.0	1.0	=	DA	NEZNAM	DA	DA	59	M	<100K
I23	4.0	4.0	4.0	1.0	3.0	=	DA	FRY	DA	NE	44	M	<100K
I24	3.0	3.0	3.0	4.0	3.0	=	DA	DAUBERT	DA	NE	43	Ž	<100K
I25	4.0	5.0	5.0	4.0	4.0	<	DA	NEZNAM	DA	DA	37	M	<100K
I26	4.0	3.0	3.0	3.0	3.0	=	DA	NEZNAM	DA	NE	39	M	<100K
I27	3.0	2.0	1.0	1.0	1.0	=	DA	FRY	DA	DA	61	M	<100K
I28	1.0	1.0	1.0	1.0	1.0	=	DA	NEZNAM	DA	DA	65	M	<100K
I29	2.0	4.0	2.0	3.0	2.0	=	DA	NEZNAM	DA	DA	48	Ž	<100K
I30	2.0	3.0	2.0	2.0	2.0	=	DA	NEZNAM	DA	NE	50	M	<300K

Pojašnjenje: HS=Poznavanje hardvera i softvera; IN=Poznavanje interneta i mreža; WE=poznavanje web tehnologija i e-mail komunikacije; DF=Poznavanje digitalne forenzike, DD=Poznavanje digitalnih dokaza; ISK: Iskustvo i znanje u odnosu na druge sudce; DDD= Slaganje sa definicijom digitalnih dokaza; Standard=Standard ili pravilo slijeđeno prilikom prihvaćanja digitalnih dokaza; Vještak=Angažiranje sudskog vještaka u predmetima; 5ws&1h=Poznavanje lanca dokaza i dokazivanje 5ws&1h u sudnici; Starost=Starost ispitanika; Spol=Spol ispitanika; Pop=Populacija stanovništva koje sud pokriva izražena u tisućama (1K=1.000 stanovnika).

Obzirom da je bilo potrebno ustanoviti da li postoji povezanost dvaju varijabli, ovdje se kao najbolja metoda javio statistički test korelacije. Izračunom faktora korelacije se pokušao izračunati stupanj povezanosti dvaju različitih brojčanih pokazatelja.

Na osnovu rezultata iz tablice broj 6 izračunate su potrebne relevantne korelacije. Za 30 ispitanika (podataka) df=28, alpha=0.5 (two tailed), i kritična Pearsonova vrijednost je =0.361.

1. Stavljanjem u korelaciju vrijednosti Starost i DD (starost sudaca i poznavanje digitalnih dokaza) dobit će se faktor korelacije r = - 0.6779,
2. Stavljanjem u korelaciju vrijednosti Starost i DF (starost sudaca i poznavanje procesa digitalne forenzike) dobit će se vrijednost faktora korelacije r = - 0.6223,
3. Stavljanjem u korelaciju vrijednosti Starost i WE (starost sudaca i poznavanje tehnologija i e-mail komunikacije) dobit će se vrijednost faktora korelacije r = - 0.6202,
4. Stavljanjem u korelaciju vrijednosti Starost i HS (starost sudaca i poznavanje hardvera i softvera) dobit će se vrijednost faktora korelacije r = - 0.4482.

Kako je r negativan ovo indicira da mlađi sudci imaju višu razinu znanja o ovim tehnologijama.

- ✓ Kada se u odnos stave vrijednosti Starost i 5ws&1h (starost sudaca i poznavanje lanca dokaza i dokazivanje 5ws&1h u sudnici) dobit će se r = - 0.1358, gdje r konvergira prema 0, što znači da postoji slaba veza, odnosno da ne postoji veza između ove dvije varijable. Ovo znači da poznavanje ovih koncepata nema nikakve veze sa godinama starosti sudaca.

- ✓ Na pitanje koji standard slijede prilikom prihvaćanja digitalnih dokaza u sudnici kojom predsjedavaju:
    - 7 sudaca je odgovorilo da slijede „FRY“ princip ili standard,
    - 2 da slijede „DAUBERT“ princip,
    - dok je najviše sudaca, čak 21 (što čini 70% ispitanika) odgovorilo da ne zna (nije znalo odgovor na ovo pitanje).

- ✓ Svi ispitanici (100%) su se složili sa ponuđenom definicijom digitalnih dokaza i nisu imali ništa za dodati.

- ✓ Svi ispitanici (100%) su se također izjasnili da koriste usluge sudskog vještaka u sudskim procesima u kojima su involvirani digitalni dokazi:
    - 63% je smatralo da taj vještak mora biti na zvaničnoj listi vještaka Ministarstva pravde dok je
    - 37% smatralo da taj vještak ne mora biti na zvaničnoj listi vještaka Ministarstva pravde, te da može biti i prijatelj suda.

- ✓ 12 sudaca (40%) je upoznato s pojmom lanca dokaza i insistira na dokazivanju istog u sudnici kojom predsjedavaju, dok 18 (60%) sudaca nije upoznato sa pojmom niti traži da se dokaže nepromjenjivost digitalnog dokaza.

- ✓ Kao odgovor na pitanje: "koji faktori su bili ključni za Vaše poznavanje digitalnih dokaza iz pitanja br.1 (osobna edukacija, edukacija putem visokog sudskog i tužilačkog vijeća, osobno iskustvo, treninzi):
    - 18 sudaca se izjasnilo da je to bila „osobna edukacija",
    - 10 da je to bila edukacija putem visokog sudskog i tužilačkog vijeća,
    - 2 da je to bila edukacija putem sudskih vještaka.

- ✓ 17 sudaca (57%) smatra da ima isto iskustva u poznavanju digitalnih dokaza u odnosu na druge kolege sudce, dok 5 (17%) smatra da ima manje iskustva. 8 sudaca (26%) smatra da ima više iskustva od drugih kolega sudaca u poznavanju digitalnih dokaza.

- ✓ Veoma interesantni odgovori su bili na pitanje: "da li postoji standard tehničkih kompetencija koje moraju imati tužitelji (državni odvjetnici) ili odvjetnici? Na koji način tehničko (ne)razumijevanje digitalnih dokaza na raspravama utiče na Vašu odluku?":
    - 6 sudaca je smatralo da su bitne kompetencije sudskog vještaka te da se očekuje od njega da „poznaje slučaj",
    - 3 su smatrala „*da mihi factum dabo tibi jus"* (lat. dajte mi činjenice i ja ću vama pravo),
    - 3 su smatrala da je najvažnije da oni poznaju digitalne dokaze,
    - 3 smatrala da ne postoji nikakav standard.
    - Ostali 15 sudaca (50%) nisu dali odgovor na ovo pitanje!

- ✓ Na pitanje: "gledajući s aspekta prezentiranja digitalnih dokaza u sudnici kojom predsjedavate, koji faktori su odlučujući i najviše doprinose efikasnom prezentiranju digitalnih dokaza kao ključnih faktora vezanih za određeni slučaj":
    - 10 sudaca (33%) je odgovorilo da je najvažnije vještačenje vještaka IT(IKT) struke i ono što on pojasni,

- 5 (17%) ih se izjasnilo sa „ne znam“,
- dok se ostali 15 (50%) nisu dali odgovor na ovo pitanje.

5.1.6 Zaključak

U poglavlju je dat prikaz preliminarnog istraživanja na temu prihvatljivosti digitalnih dokaza u sudovima u BiH. Slična istraživanja nisu vršena u okruženju, dok je u USA 2010.godine na Sveučilištu *Nova Southeaeasten* obranjena doktorska disertacija na sličnu temu [57].

Rezultati istraživanja provedenog u BiH se mogu ukratko rezimirati na sljedeći način:

- Postoji inverzna korelacija i stvarna značajna povezanost između starosti sudaca i njihovog poznavanja hardvera i softvera, interneta i e-mail komunikacije, digitalnih dokaza i digitalne forenzike, što ukazuje na činjenicu da je domena IKT-a i digitalne forenzike više bliska sudcima mlađe životne dobi (r je od ± 0.4 i ± 0.7).
- Postoji neznatna ili skoro nikakva korelacija između starosti sudaca i poznavanja pojma lanca dokaza, te dokazivanja 5ws&1h (r je od ± 0.00 i ± 0.20), što indicira na činjenicu da je (ne)poznavanje ovog procesa generalno neovisno od godina starosti sudaca.
- Sudci su najviše oslonjeni za sudske vještake i vjeruju onome što im oni prenesu i što im pojasne, a to je Nalaz i mišljenje Sudskog vještaka IKT struke.
- Evidentno je nepoznavanje od strane sudaca „Fry“ i “Daubert“ principa, te način na koji se eventualno prihvaćaju digitalni dokazi, koje pravilo slijede. I u ovom dijelu presudnu ulogu igraju sudski vještaci.

Istraživanje je pokazalo da se suci svakodnevno susreću s digitalnim dokazima u sudnicama u kojima predsjedavaju, u vidu elektroničkih poruka, tekstualnih dokumenata, fotografija, video uradaka (video-nadzori i sl.), web stranice, kratkih pisanih poruka sa mobilnih telefona, ali da su im najčešće ti dokazi prezentirani u materijalnom obliku, na papiru. Samim time oni te dokaze poistovjećuju sa materijalnim dokazima i ne prave distinkciju. Većina ih smatra da dokazi trebaju biti tretirani kao svaki drugi dokazi, te da je dužnost i obaveza vještaka IT / IKT struke da im dokaze pojasni. Isto tako zabrinjavajuća je činjenica da suci (a ni tužitelji) ne znaju gdje granica obaveza vještaka, te Naredbe koje donose su obično površne, nejasne, nestručno napisane, čime već u startu dolazi do problema i nesuglasica. Ovakvoj situaciji je u

cijelosti posvećen „*Rule 702 Američkog Saveznog Zakona o dokazima*“, dok zemlje u okruženju (ali i mnoge EU zemlje) takav zakon nemaju. Rezultati ankete su pokazali da suci nisu svjesni činjenice da su digitalni dokazi latentni, da se lako mijenjaju i/ili uništavaju.

Ovo pokazuje da je sucima potrebna ozbiljna i sveobuhvatna obuka koja će obuhvatiti prvo osnove IT-a, Internet i mreže, hardver i softver, te nakon toga sam proces digitalne forenzičke istrage, te u konačnici digitalne dokaze, njihove osnovne karakteristike i principe prihvatljivosti.

POGLAVLJE VI

6 ONTOLOŠKI PRISTUP RJEŠAVANJU PROBLEMA LANCA DOKAZA

U ovom poglavlju dat će se pregled pojma ontologije, izrađenih ontologija u domeni digitalne forenzike i digitalnih dokaza, te preporučena ontologija digitalnog lanca dokaza. Izrađena ontologija uz pomoć postavljenih SWRL (engl. *Semantic Web Rule Language*) pravila, predstavljat će okvir preporučenog modela pomoću kog bi se moglo dokazati da li je očuvan ili ne lanac digitalnih dokaza u procesu digitalne forenzičke istrage, te na osnovu toga donijeti zaključak da li je uopće takav digitalni dokaz i prihvatljiv.

6.1 Uvod u ontologije

Danas, više nego ikada ranije, digitalna forenzika se oslanja na znanje i sustave za upravljanje znanjem kao veoma važne resurse. Razlog za to leži u činjenici da se digitalne tehnologije razvijaju eksponencijalnom brzinom, a znanje pohranjeno u sustave znanja omogućava lakše razvijanje modela, standarda i procedura. Veoma često je potrebno stvoriti nove koncepte i ideje iz postojećih informacija koje su pohranjene u računalu u čitljivom obliku u tzv. sustave znanja. Ovdje značajnu ulogu igraju ontologije, koje nam pomažu u procesu kreiranja novog znanja i definicija u ciljanoj domeni.

Ukoliko promatramo ontologiju u kontekstu filozofije ona čini dio metafizike koji se bavi fenomenom bivanja odnosno postojanja. Pojam ontologija je grčkog porijekla i predstavlja spoj dvije riječi "*onto*" što znači "biće, stvarnost, postojanje", i "*logos*" što znači „znanost"[26]. Dakle, ontologija predstavlja znanost o biću - znanost o postojanju [105].

Ontologije danas imaju veoma veliku primjenu u računarstvu i informatici u umjetnoj inteligenciji, sustavima za upravljanje, sustavima za potporu odlučivanju, bazama znanja,

[26] 'Ontology', ili bolje rečeno 'ontologia', pojavljuje se kao kovanica – spoj dva filozofa koji su pisali neovisno jedan od drugo 1613.godine: Jacob Lorhard u njegovom djelu Theatrum Philosophicum i Rudolf Göckel u njegovom Lexicon Philosophicum. Prvo pojavljivanje u Engleskoj je u "Bailey's Dictionary" 1721 godine , gdje je ontologija definirana kao 'an account of being in the abstract'.

semantičkom webu, bioinformatici i softverskom inženjerstvu. Ontologije u kontekstu IKT-a predstavljaju formaliziranje znanja, odnosno formalno definiranje sustava od pojmova (koncepata) i odnosa između tih koncepata. Najbolju definiciju ontologije u istraživanjima umjetne inteligencije i predstavljanja znanja dao je Grubor [106] - Ontologija je eksplicitna specifikacija konceptualizacije. Prema autoru Nicola Guarinou [107] postoji distinkcija između ontologije sa velikim „O“ i malim „o“. Ontologija sa „O“ je povezana sa filozofijom i pojmom „bivanja postojanja“ i Aristotelovim teorijama postojanja. Ontologija sa malim “o“ je i dalje vezana za filozofiju i sustavni prikaz postojanja, te opisuje situaciju u kojoj je znanje stečeno u svrhu organiziranja i klasifikacije [66,108].

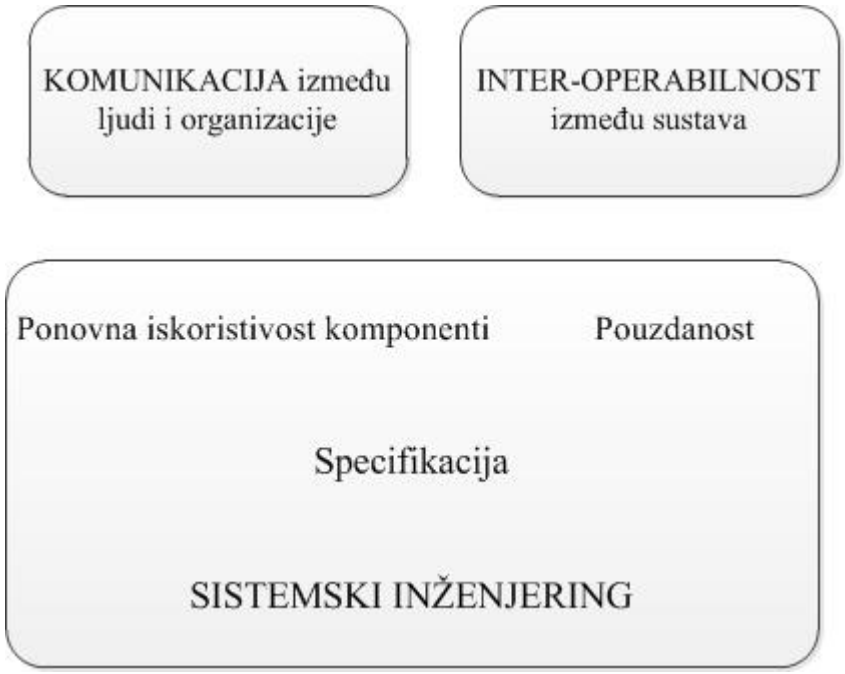
Još neke definicije (kroz povijest) naglašavaju karakteristike ontologije, njenu formalnu primjenu i njen značaj:

- Borst [109]: „Ontologija je formalna, eksplicitna specifikacija zajedničke konceptualizacije“.
- Guarino i Giaretta [110]: „Ontologija je logička teorija koja daje eksplicitni, nepotpuni prikaz konceptualizacije...“.
- Jasper i Uschold daju definiciju koja popularizira ontologije na druge discipline [111]: „Ontologije mogu pružiti različite forme, ali će nužno uključivati rječnik pojmova i neke specifikacije njihovog značenja; to uključuje i definiciju koncepta i njihovog međusobnog odnosa što u cijelosti nameće strukturu domene i ograničava moguće prikaze pojmova“.

Tako se do danas ontologije koriste za različite namjene: procesiranje prirodnog jezika, upravljanje znanjem, e-trgovinu, inteligentna integracija informacija, semantički web, itd. i u različitim područjima:

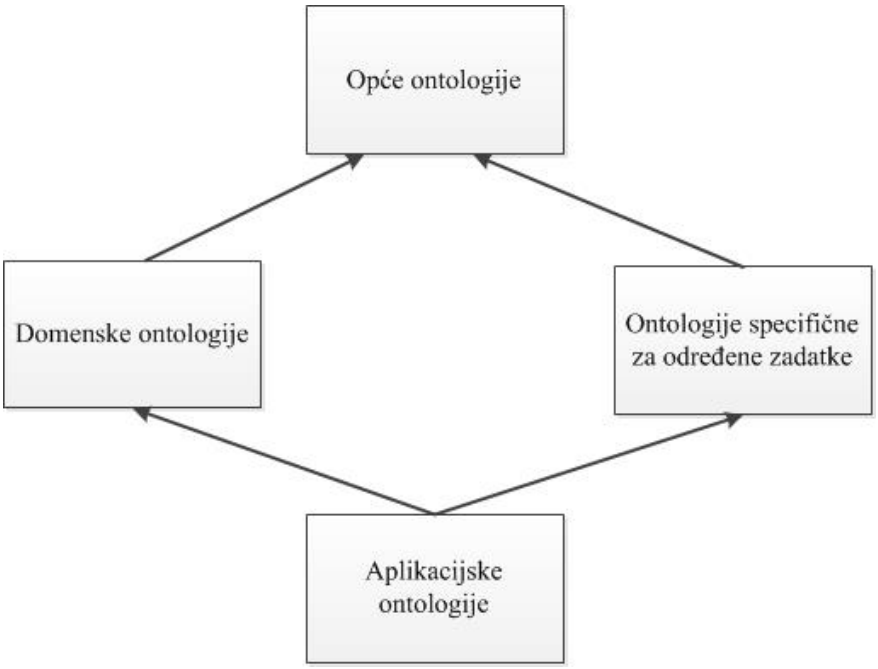
- inženjerstvo znanja,
- softversko inženjerstvo,
- inženjerstvo baza podataka i
- inteligentni agenti i višeagentni sustavi.

Ontologije stvaraju rječnik ciljane domene opisujući koncepte, atribute i relacije među tim konceptima unutar domene. Ontologije igraju veoma veliku ulogu i prihvaćene su u mnogim poslovnim i znanstvenim sustavima, kao metode za ponovno korištenje, dijeljenje i obradu znanja u ciljanoj domeni, te interoperabilnosti sustava. (slika 15.).



Slika 15. Glavne kategorije upotrebe ontologija prema [112]

U kontekstu ovog rada koristit će se izraz *otvorena ontologija* [113] u cilju omogućavanja daljnjeg proširenja izrađene ontologije, kao i u kontekstu pojma otvorenog koda u softverskom inženjerstvu (engl. *open source*). Naime, digitalna forenzika kao znanstvena disciplina se konstantno mijenja i evaluira, te je stoga nemoguće napraviti zatvoreni sustav koji nije podložan promjenama. Stoga je cilj izraditi potpuno funkcionalnu ontologiju koje će se vremenom, pojavom novih metoda, alata ili novih koncepata veoma lako moći promijeniti (u smislu dodavanja novih funkcionalnosti).



Slika 16. Podjela ontologija i njihova hijerarhija [107]

Prema Guarinou [107] postoje tri tipa ontologija prema razini generaliziranja i stupnju ovisnosti o zadatku (slika 16.) i to:

- Opće ontologije (eng. *Top level general ontology*) koje opisuju generalne koncepte kao što su svemir, vrijeme, objekti, događaji, akcije i sl.
- Domenske ontologije (engl.*Domain ontology*) i ontologije za specifične zadatke (engl. *task*) koje opisuju rječnik iz neke generičke domene (npr. medicina, automobilska industrija i sl.) ili neki generički zadatak (dijagnoza, prodaja i sl.), a koje specijaliziraju koncepte iz top-level ontologija, i
- Aplikacijske ontologije (engl. *Application ontology*) koje opisuju koncepte koji su ovisni od specifične domene i zadataka, a koje su obično specijalizirane od strane obje vrste ontologija.

Ontologija koja će se izraditi predstavlja domensku ontologiju jer opisuje koncepte, instance, atribute i relacije unutar jednog užeg područja (područje lanca digitalnih dokaza). Ovdje je potrebno pojasniti činjenicu da postoji distinkcija između ontologije digitalnih dokaza i ontologije lanca digitalnih dokaza. Ontologija digitalnih dokaza predstavlja generalizaciju odnosno uopćenu ontologiju s pobrojanih mnogo koncepata koji se mogu javiti, a vezani su za sam pojam digitalnog dokaza, dok je njena specijalizacija ontologija lanca dokaza u kojoj su pobrojani koncepti koji karakteriziraju dokazivanje lanca dokaza. Prva ontologija je neophodna radi provjere hipoteze H1, a druga radi provjere hipoteze H2.

Ontologija digitalnih dokaza i lanca digitalnih dokaza će se realizirati u OWL-u (*engl. Web Ontology Language*) kao standardiziranom jeziku za ontologije. Ontologija izgrađena za potrebe ovog rada će biti metoda (alat) koja će pomoći da se definiraju pojmovi, jasnije shvate koncepti, te u konačnici u prvoj fazi definira dijagram taksonomije lanca dokaza, a koji će biti osnova za izradu funkcionalne ontologije koja će biti osnova za okvir u kojem će se moći dokazati lanac dokaza. Postoji mnogo razloga za izgradnju ovakve ontologije. Digitalni dokazi se mijenjaju i evaluiraju. Početkom nastanka pojma digitalne forenzike (prije 25 godina) digitalni dokazi su se nalazili u računalima, vanjskim nosiocima podataka (CD,FDD, JAZZ,itd), nastanak mreža i Interneta je preselio digitalnu forenziku u oblake (engl. *Cloud*), a danas digitalne dokaze možemo pronaći na mobilnim telefonima, multimedijalnim sviračima, konzolama za video igre, pa čak i satovima i drugim tzv. „ugrađenim sustavima“ (engl. *Embedded systems*). Digitalne dokaze je sve teže i teže pronaći, te na zakonit način prikupiti. Drugi razlog je integritet digitalnog dokaza, te očuvanje lanca dokaza što iz dana u dan postaje sve kompleksnije i teže. Svaka i najmanja promjena medija na kom se nalaze digitalni dokazi izmijenit će ili potpuno uništiti digitalne dokaze [19].

6.2 Slična istraživanja na temu ontologija u domeni digitalne forenzike

Veoma malo je objavljenih znanstvenih radova i javno objavljenih funkcionalnih ontologija u domeni digitalne forenzike. Više je razloga za to, a jedan od njih je svakako multidisciplinarnost znanstvenog polja digitalne forenzike. Pored dobrog poznavanja tehničkih aspekata (informatika, računarstvo i telekomunikacije), neophodno je dobro poznavanje i kriminalistike i mjesta zločina, kao i prava - zakonske regulative u domeni forenzike, prezentiranja digitalnih dokaza pred sudom. Svi pokušaji izrade ontologije se završava u fazi definiranja koncepata te izrade dijagrama taksonomije [64-67,69,71,114] a što je opisano u trećem poglavlju. Prema Huang, Yasinsac i Hayes [62] nije moguće izraditi jednu krovnu ontologiju koja će biti dovoljno velika da uključi sve koncepte koji se pojavljuju u ciljanoj domeni. Stoga će izgrađena ontologija digitalnih dokaza u dijagram taksonomije uključiti sve koncepte relevantne za sam pojam, ali će se prilikom izgradnje okvira specijalizirati na lanac dokaza, koncepte, atribute, relacije među konceptima, individue, te pravila a koji se pojavljuju u procesu dokazivanja lanca dokaza.

6.3 Ontološki pristup problemu lanca dokaza

Kao što je već ranije spomenuto, ontologija je eksplicitna specifikacija konceptualizacije u stvarnom svijetu. Ontologijom se:

- definira najčešće korišteni rječnik podataka za istraživače koji žele dijeliti informacije u određenoj domeni,
- omogućava se ponovna upotrebljivost domenskog znanja,
- čini pretpostavke domene jasnijim,
- izdvaja domensko znanje iz operativnog znanja,
- analizira domensko znanje [115].

Metoda razvoja ontologije koja će se koristiti u radu je „Ontology Development 101“ [115] razvijena na Sveučilištu Stanford, California, USA. U dijelu rada u kom je opisana metodologija, detaljno je pojašnjena metoda izrade same ontologije.

6.3.1 Definiranje domene i obuhvat ontologije

Krovna domena za koju će se razvijati ontologija je znanstvena disciplina digitalna forenzika. Cilj je razviti ontologiju digitalnih dokaza, aplikaciju lanca dokaza koja će biti osnova za izgradnju okvira u kom će se moći održati i dokazati očuvanje digitalnog lanca dokaza. Osnovu za razvoj ontologije čini DEMF (engl. *Digital Evidence Management Framework*), okvir koji je razvijen u ranijim fazama istraživanja a u kom se svakog trenutka mora znati tko je, kada, gdje, kako i zašto dolazio u kontakt s digitalnim dokazima [48-49].

Izrađena ontologija će omogućiti korištenje znanja pohranjenog u vidu rječnika podataka domene digitalne forenzike, omogućit će ponovnu upotrebljivost (engl. *Reusability*) domenskog znanja, te će, obzirom da će ontologija biti formalizirana u OWL-u i SWRL-u omogućiti korištenje iste od strane računalnih programa i drugih agenata. Ontologija će biti otvorena, te će imati veze na sve slične i kompatibilne ontologije koje su već ranije izrađene a upotrebljive su. Pored diseminacije znanja o nužnosti vođenja lanca dokaza, ontologiju će pored sudaca, odvjetnika, istražitelja koji vode digitalne istrage moći koristiti i inženjeri pri kreiranju softvera za rad s digitalnim dokazima u smislu vođenja lanca dokaza i dokazivanja očuvanja integriteta digitalnog dokaza.

6.3.2 Ponovno korištenje postojećih ontologija

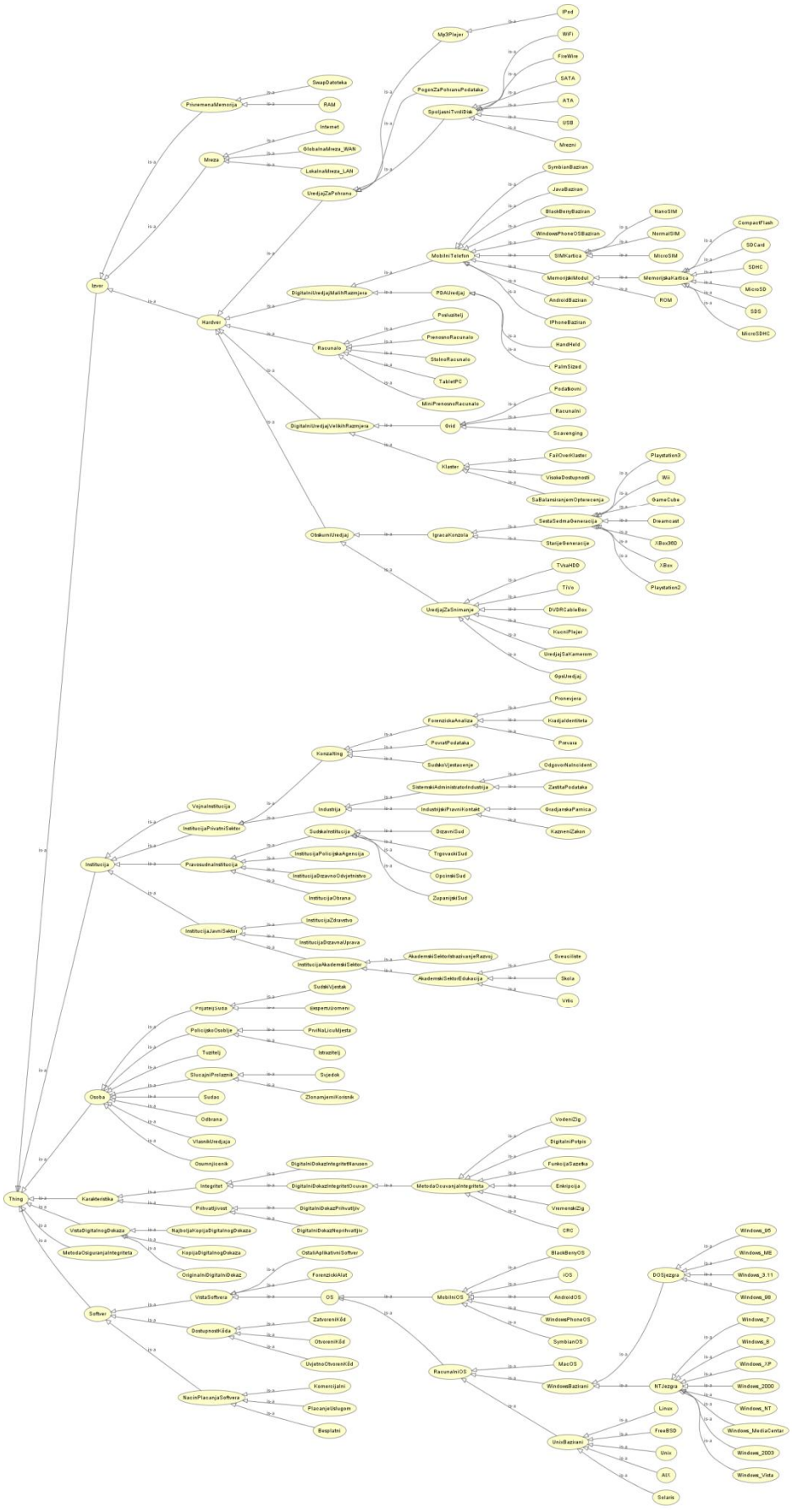
Pretraživanjem relevantnih baza podataka, te analizom dostupnih radova a koji su spominjati u ranijim dijelovima rada ustanovljeno je da nema mnogo izrađenih ontologija u domeni digitalne forenzike. *Ontoligua* biblioteka ontologija (http://www.ksl.stanford.edu/software/ontolingua/) ili *DAML* biblioteka ontologija (http://www.daml.org/ontologies/) su pokazale da nema dostupnih, izrađenih ontologija iz ove domene[27]. Jedna od ontologija koja postoji i koja je javno objavljena [64] bila je kandidat za importiranje u ontologiju lanca dokaza. Obzirom da je u radu predstavljen samo dijagram taksonomije, kao prva faza izrade ontologije, kontaktirao sam autora kako bih eventualno došao do iste u nekom računalu čitljivom obliku, međutim nisam dobio odgovor. Ista je iskorištena u dijelu prilikom kreiranja koncepata i relacija u domeni (uređaji malih razmjera). Slična situacija je bila i sa ontologijama predstavljenim u radovima [19,66] koje su urađene samo na razini dijagrama taksonomije. Iste, obzirom da nisu javno objavljene u obliku čitljivom za računala ili agente, korištene su na razini definiranja koncepata i relacija među konceptima u jednom dijelu digitalnih dokaza (tehnologija i profesija). Izrađena ontologija će se javno objaviti u nekom od repozitorija (*Open Ontology Reposotory, Swoogle, Protege Ontology Library*), te će biti javno dostupna za korištenje.

6.3.3 Definiranje klasa i hijerarhije klasa u domeni lanca digitalnih dokaza

Postoji više mogućih pristupa u razvoju hijerarhije klasa, odozgo prema dole (engl. *Top-down*), odozdo prema gore (engl. *Bottom-up*) i kombinirana metoda (engl. *Combination*) [112]. Pristup koji će se koristiti u razvoju ontologije u disertaciji je odozgo prema dole (eng. *Top-down*). Ključni koncept (klasa) je digitalni dokaz. Ovaj koncept je dalje podijeljen na Instituciju, Izvor, Karakteristiku, Osobu, Softver i Vrstu digitalnog dokaza.

Na slici 17. prikazan je dijagram taksonomije digitalnog dokaza, a koji će zbog kompleksnosti biti podijeljen na nekoliko dijelova i detaljnije pojašnjen.

[27] Pretraga je vršena prema ključnim riječima (chain of custody, digital evidence, digital forensic), kao i po ciljanoj domeni (digitalna forenzika)



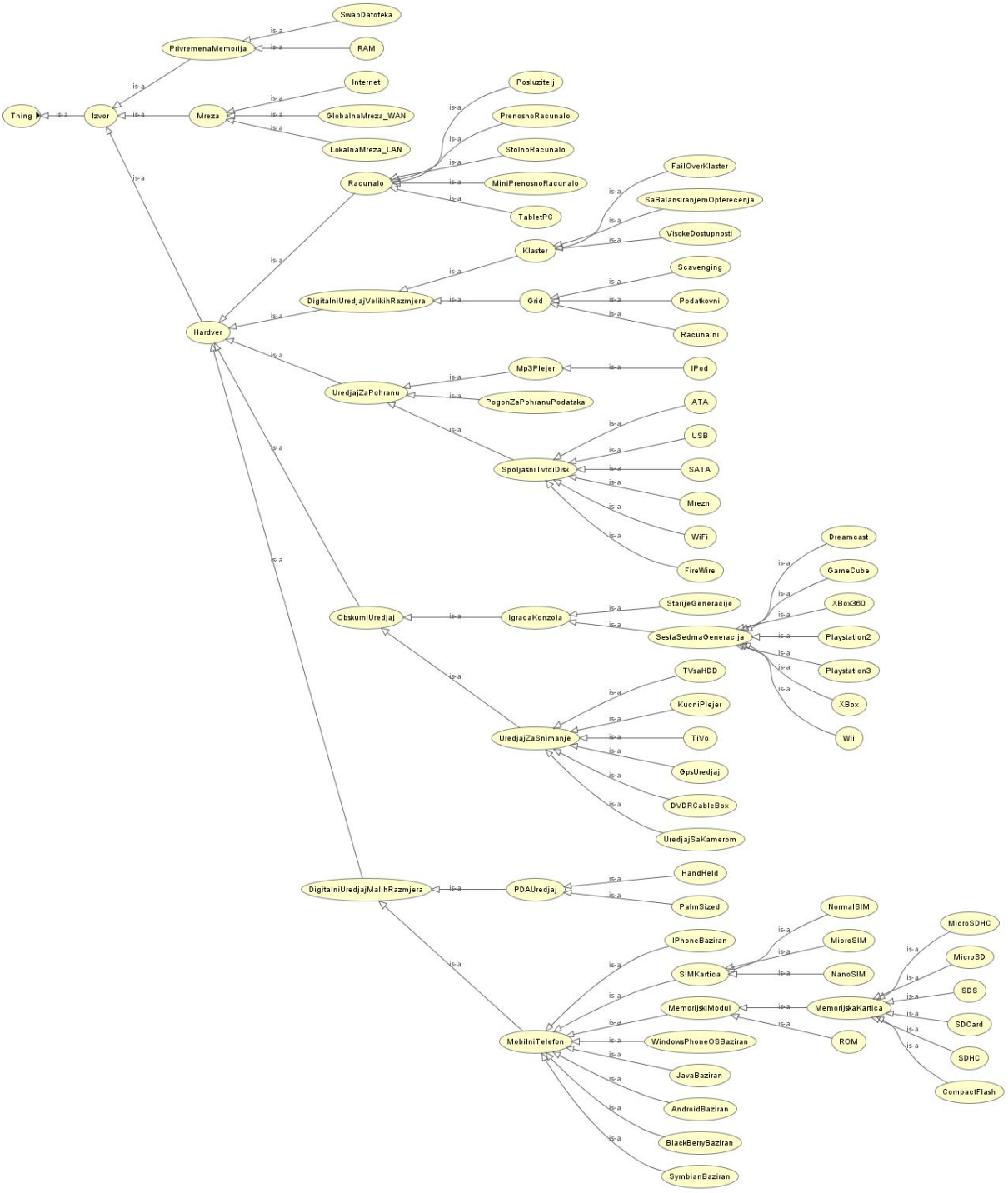
Slika 17. Dijagram taksonomije koncepta „digitalni dokaz“

Ontologija koncepta *„Institucija“* je ponovno iskorištena (engl. *reusability*) iz rada [66] sa manjim modifikacijama i dodavanjem novih klasa. Modifikacije se odnose na izmjene u domenu Javnog sektora, gdje su dodate nove klase i relacije među klasama. Klasa *Institucija* se sastoji od poklasa je *VojnaInstitucija, InstitucijaJavniSektor, InstitucijaPrivatniSektor i PravosudnaInstitucija*. Podklase *PravosudneInstitucije su InstitucijaPolicijskeAgencije, InstitucijaDrzavnoOdvjetništvo, InstitucijaObrana i SudskaInstitucija. Podklase SudskeInstitucije* su *TrgovackiSud, ZupanijskiSud, OpcinskiSud i DrzavniSud*. Podklase klase *InstitucijaPrivatniSektor* su *Industrija (IndustrijskiPravniKontakt i SistemskiAdministrator),* dok su podklase klase *Konzalting (PovratPodataka, SudskaVjestačenja i ForenzickaAnaliza)*. Podklase klase *InstitucijaJavniSektor* su *InstitucijaDrzavnUprava, InstitucijaZdravstvo i InstitucijaAkademskiSektor*. Podklase klase *InstitucijaAkademskiSektor* su *AkademskiSektorIstraživanjeRazvoj i AkademskiSektorEdukacija (Vrtic, Sveuciliste i Skola*). Dijagram taksonomije je prikazan na slici 18.

Slika 18. Dijagram taksonomije koncepta „Institucije“

Sljedeći koncept *„Izvor“* je i najkompleksniji i sadrži najveći broj podklasa. Ovaj koncept je i najviše sklon promjenama, te je kreiran od dvije urađene ontologije proširene s još mnogo novih koncepata [19,64,66]. Razloga za to je mnogo, a jedan od osnovnih je ekspanzija

mobilnih telefona, tzv. pametnih uređaja, ugrađenih sustava, igraćih konzola, te drugih uređaja malih razmjera koji u sebi mogu sadržavati digitalne dokaze. Ontologija ovog koncepta je dana na slici 19.[28].



Slika 19. Dijagram taksonomije koncepta „Izvor digitalnog dokaza”

[28] U ranijim klasifikacijama su se neki koncepti npr. „igraće konzole“ ili „uređaji za snimanje“ svrstavali u tzv. Obskurne uređaje, dok je danas situacija drugačija, te bi se u tu klasu mogli svrstati neki drugi uređaji - ekspanzija proizvoda sa Dalekog Istoka (Kina, Japan, Tajvan).

Koncept *„Izvor“* se sastoji od podklase *Hardver, Mreza (Globalna_WAN, Lokalna_LAN i Internet) i PrivremenaMemorija (RAM i SWAP datoteke)*. Podklasa *Mreza* predstavlja izvor digitalnih dokaza bilo gdje na mreži (na serveru u lokalnoj mreži, u globalnoj WAN mreži ili na internetu – „clouding“). Podklase klase *Hardver* su *DigitalniUredjajiMalihRazmjera, DigitalniUredjajiVelikihRazmjera, ObskurniUredjaji*[29], *Racunala i UredjajiZaPohranu*. *DigitalniUredjajMalihRazmjera* su *MobilniTelefoni (AndroidBazirani, BlackBarryBazirani, IPhoneBazirani, JavaBazirani, WindowsOSBazirani i SymbianBazirani*[30]*), MemorijskiModuli (MemorijskeKartice i ROMMemorija), SIM kartice (Micro, Nano, Normal), PDAUredjaji (HandHeld i PalmSized)*. Podklase klase *UredjajVelikihRazmjera* su *Grid (Podatkovni, Racunalni i Scavening) i Klaster*[31] *(FailOver, SaBalansomOpterecenja, VisokeDostupnosti). Klasa ObskurniUredjaji* je sastavljena od podklasa *IgracaKonzola*[32] *(SestaSedmaGeneracija i StarijaGeneracija), te UredjajZaSnimanje (DVDRCCable box, GPSUredjaj, KucniPlajeri, TiVo, TVSaHDD, UredjajSaKamerom*). Podklase *Računala* su *MiniPrenosnaRacunala, Posluzitelji, PrenosnaRacunala, StolnaRacunala, Tableti*. *UredjajiZaPohranu* mogu biti *DrajvovZaPohranuPodataka, MP3Plejer, SpoljasnDisk (ATA, FireWire, Mrezni, SATA, USB, WIFI).*

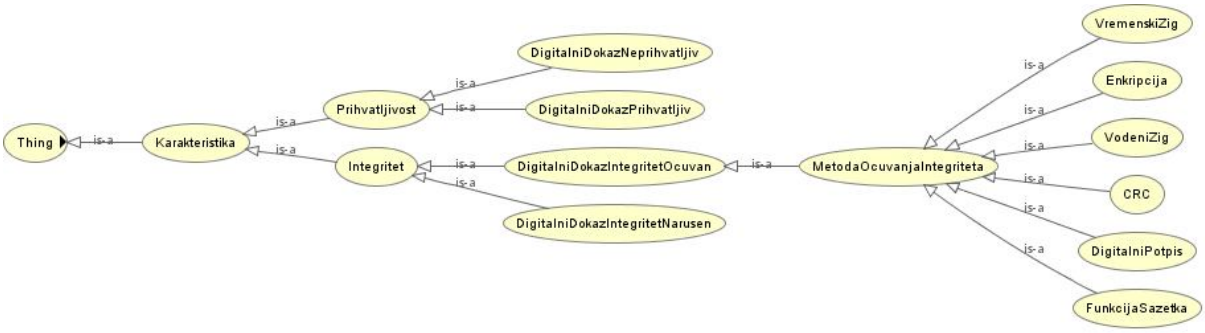
Podklase klase *“Karakteristike”* su *Integritet i Prihvatljivost*. Podklase klase *Integritet* su *DigitalniDokazIntegritetNarusen i DigitalniDokazIntegritetOcuvan,* a podklase klase *Prihvatljivost* (*DigitalniDokazPrihvatljiv i DigitalniDokazNeprihvatljiv*). Podklasa klase *DigitalniDokazInegritetOcuvan* je *MetodaOcuvanjaIntegriteta* čije su podklase *VodeniZig, DigitalniPotpis, CRC, VremenskiZig, Enkripcija i FunkcijaSazetka*. Dijagram taksonomije ovog koncepta je prikazan na slici 20.

[29] Pojam “Obscure devices” je preuzet u originalom nazivu i u to vrijeme je predstavljao “nejasne” uređaje (uređaje za konzole, uređaje za snimanje i sl.).

[30] Klasifikacija mobilnih telefona, kao podklasa digitalnih uređaja malih razmjera, rađena je na način da se vodi računa o ovisnosti o operativnom sustavu koji pogoni iste, a iz razloga što operativni sustav mobilnih telefona determinira i upotrebu različitih forenzičkih alata koji se upotrebljavaju u analizi istih.

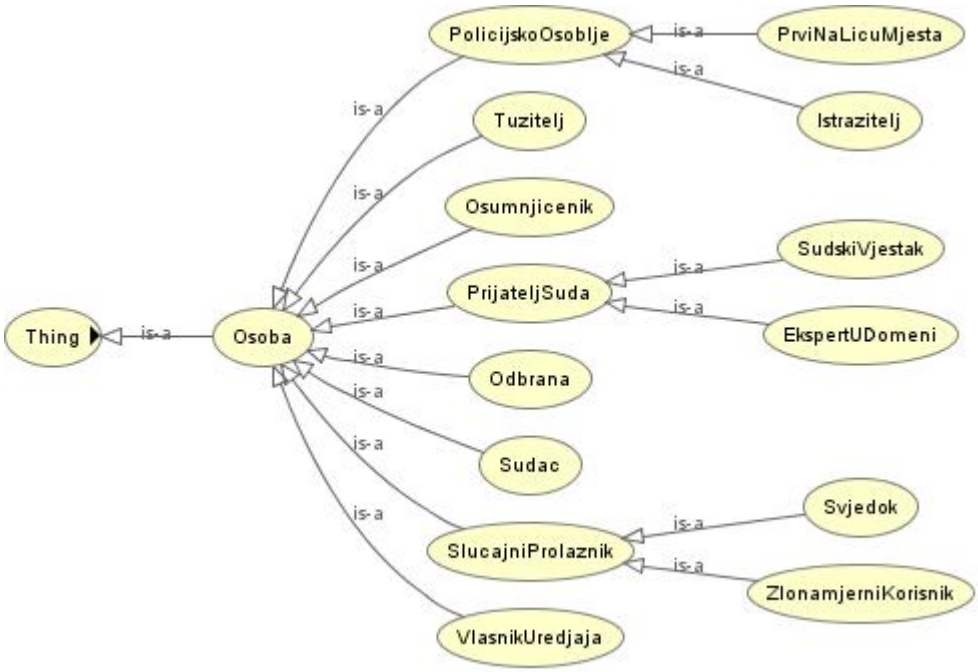
[31] Upotrijebljeni su originalni nazivi za Grids i Klasters jer bi uporaba Hrvatskih izraza promijenila smisao i značenje ovih izraza.

[32] Igraće konzole.



Slika 20. Karakteristike digitalnog dokaza u kontekstu prihvatljivosti

Podklase klase *"Osoba"* su *PolicijskoOsoblje (PrviNaLicuMjesta i Istrazitelj), Tuzitelj, Osumnjicenik, PrijateljSuda (SudskiVjestak i ExpertUDomeni), Odbrana, Sudac, SlucajniProlaznik (Svjedok i ZlonamjerniKorisnik)* te *VlasnikUredjaja.* Slika 21. ilustrira dijagram taksonomije klase *Osoba*.

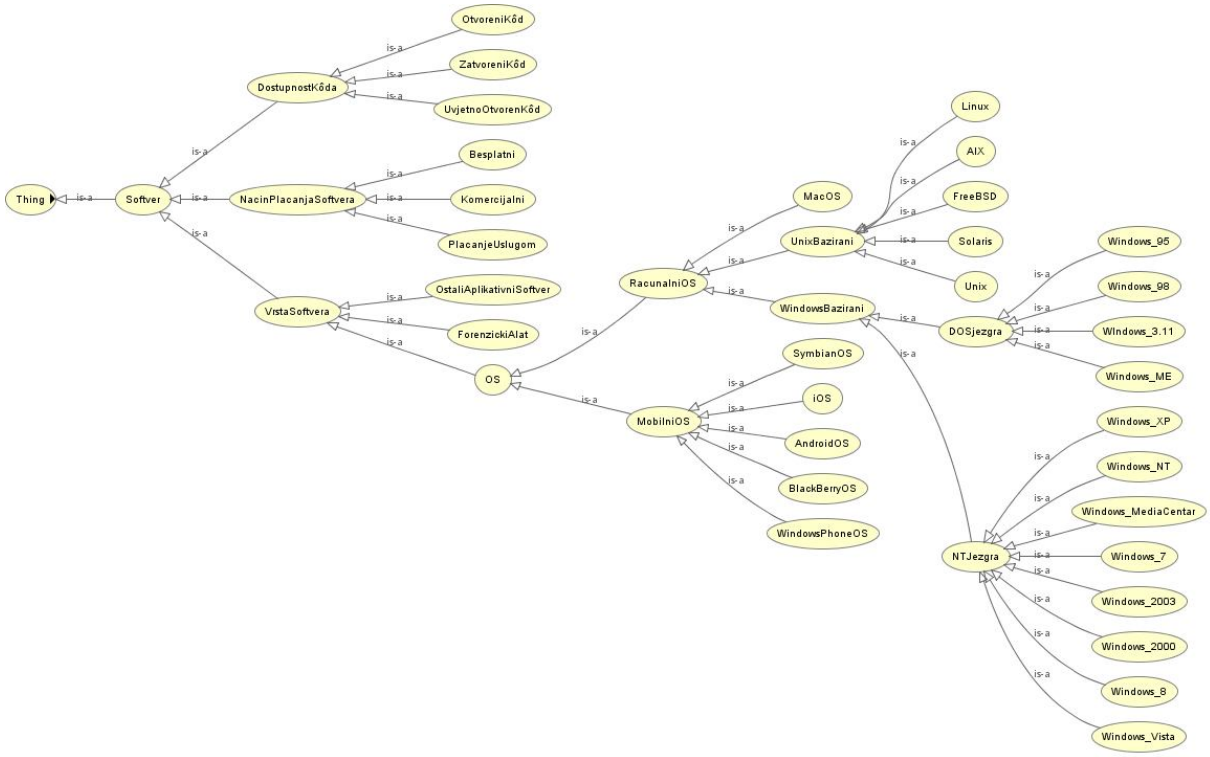


Slika 21. Dijagram taksonomije koncepta "Osoba"

Podklase klase *"Softver"* se mogu promatrati s razine *NacinPlacanja (Besplatni, Komercijalni i PlacanjeUslugom)*, *DostupnostKôda (OtvoreniKôd, ZatvoreniKôd te UvjetnoOtvoreniKôd)* te *VrsteSoftvera (OS, ForenzickiAlat i OstaliAplikativniSoftver)*. *OS* može biti *MobilniOS i RacunalniOS*. Podklase klase Mobilni*OS* su *AndroidOS, BlackBerryOS, IOS, Symbian i WindowsPhoneOS*, dok su podklase klase *RacunalniOS*, *MacOS, WindowsBazirani i UnixBazirani (AIX, FreeBSD, Linux, Solaris, Unix*). *WindowsBazirani* je *DOSJezgra* (*Windows_3.11*, *Windows_95, Windows_98 i Windows_ME*)

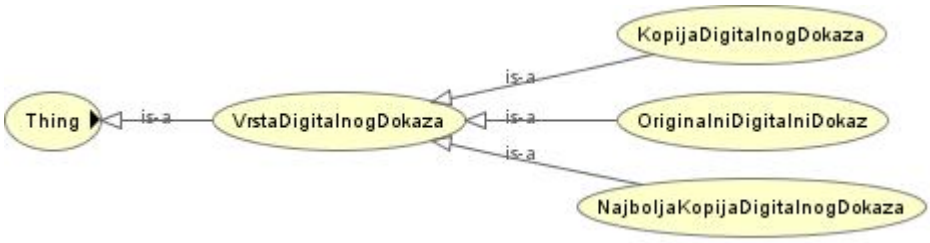
dok je *NTJezgra* (*Windows_NT, Windows_2000, Windows_2003,Windows_XP, WindowsMediaCentar, Windows_Vista, Windows_7 i Windows_8*)

Ilustracija dijagrama taksonomije je dana na slici 22.



Slika 22. Dijagram taksonomije koncepta „Softver“

Posljednji u nizu glavnih koncepata je koncept nazvan *„VrstaDigitalnogDokaza“* čije su podklase *KopijaDigitalnogDokaza, NajboljaKopijaDigitalnogDokaza i OriginalniDigitalniDokaz*. Prema IOCE [45] nikada se ne smije rukovati s originalnim digitalnim dokazima nego se moraju napraviti dvije identične kopije - kopija (engl. *copy*) i najbolja kopija (engl. *best copy*) koje moraju biti identične originalu i sa kojima se rukuje tijekom procesa digitalne forenzičke istrage (slika 23.). Vrijednost funkcije sažetka uvijek se mora čuvati, te mora biti nepromjenjena kopija u odnosu na originalni digitalni dokaz.



Slika 23. Dijagram taksonomije koncepta „Vrste digitalnog dokaza"

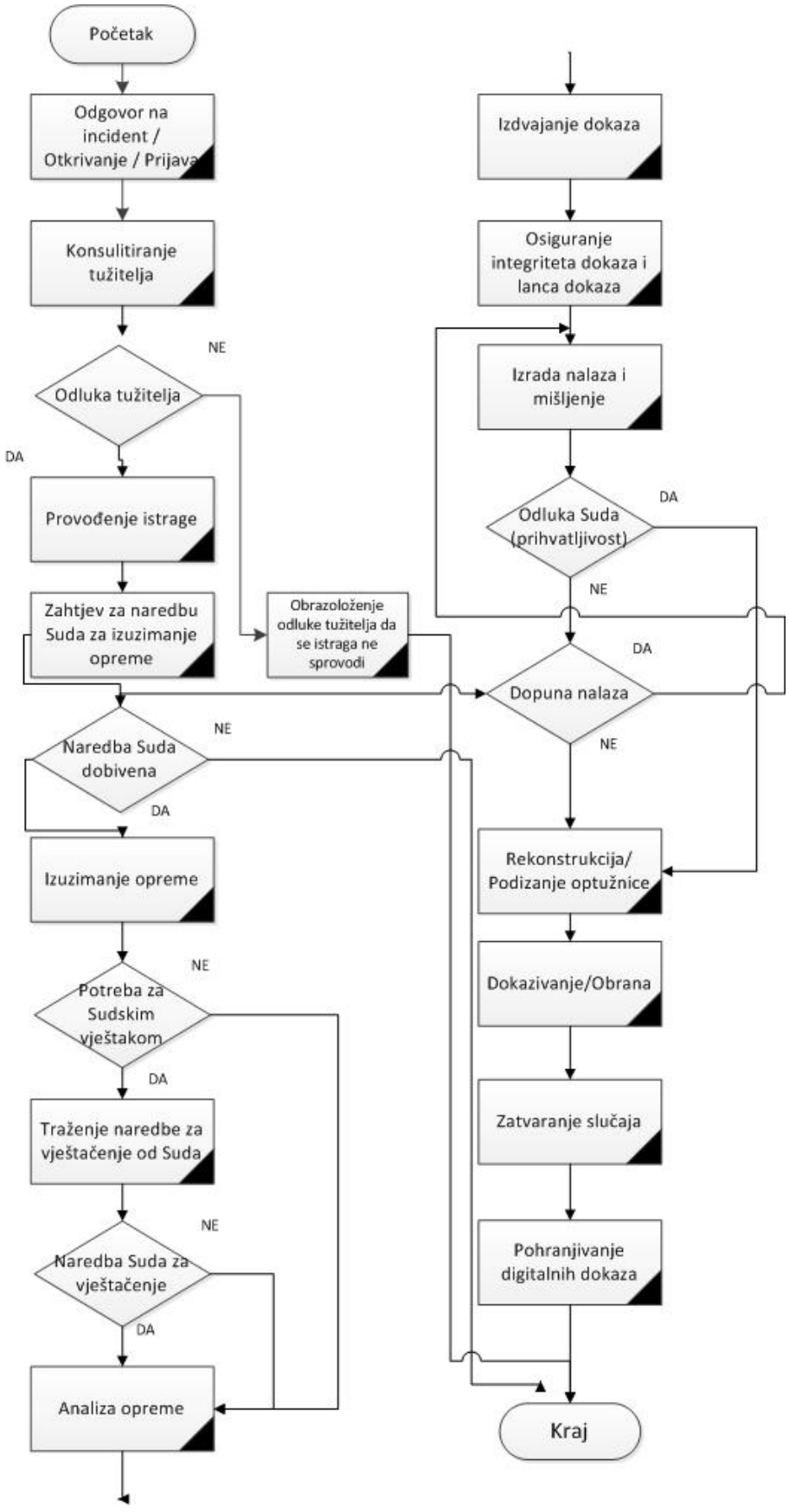
Obzirom da je tema rada - izgradnja otvorenog okvira za očuvanje lanca dokaza i prihvatljivost digitalnih dokaza prilikom izrade okvira će se broj promatranih koncepata značajno smanjiti i uzeti u obzir samo oni koncepti koji su neophodni kako bi se izgradio spomenuti okvir.

6.3.4 Definiranje svojstava-atributa klasa i relacija među klasama

Definiranje i postavljene u dijagram taksonomije klasa ne nude mnogo informacija o samim konceptima i promatranoj domeni. Nakon što su definirane klase potrebno ih je opisati, odnosno opisati njihovu strukturu. Kao što je ranije spomenuto biti će korišteni samo koncepti koji su neophodni za definiranje otvorenog okvira i pravila koji će omogućiti zaključivanje o formalnoj prihvatljivosti digitalnih dokaza.

Svojstva mogu biti objektna – svojstva koja entitete povezuju s entitetima (individue, klase svojstva ili tip podataka), te podatkovna – svojstva koja entitetu pridružuju tzv. „literal" (podatkovnu vrijednost).

Pri opisu će se koristiti Manchester notacija, jer je ista mnogo čitljivija za ljude od OWL ili RDF notacije koja se koristi kao najčešća notacija za zapisivanje ontologija za računala. Obzirom da relacija i svojstava ima jako mnogo, te uzevši u obzir činjenicu da je za izradu okvira potrebna samo specijalizirana ontologija lanca dokaza, u nastavku će se spominjati samo relacije, atributi i individue koje se javljaju u samom životnom ciklusu digitalnih dokaza a što se može vidjeti na slici 24.



Slika 24. Dijagram aktivnosti koje se obavljaju u procesu digitalne forenzičke istrage

Opis svojstava objekata (relacija):

```
ObjectProperty: analizira

    Characteristics:
        Functional

    Domain:
        PolicijskiIstrazitelj,
        SudskiVjestak,

    Range:
        Izvor
```

Kôd 6.1 Zapis u manchester notaciji svojstva "analizira"

Kôd prikazan u 6.1 pokazuje svojstvo analizira koje subjektu koji je individua klase SudskiVjestak i PolicijskiIstrazitelj pridružuje individuu klase Izvor.

```
ObjectProperty: donosiOdluke

    Characteristics:
        Functional

    Domain:
        Sudac

    Range:
        Prihvatljivost
```

Kôd 6.2 Zapis u manchester notaciji svojstva "donosiOdluke"

Kôd prikazan u 6.2 pokazuje svojstvo donosiOdluke koje subjektu koji je individua klase Sudac pridružuje individuu klase Prihvatljivost.

```
ObjectProperty: ocuvanIntegritet

    Characteristics:
        Functional

    Domain:
        Integritet
```

```
    Range:
        MetodaOsiguranjaIntegriteta

    InverseOf:
        DigitalniDokazIntegritetNarusen,
        DigitalniDokazNeprihvatljiv
```

Kôd 6.3 Zapis u manchester notaciji svojstva "ocuvanIntegritet"

Kôd prikazan u 6.3 pokazuje svojstvo ocuvanIntegritet koje subjektu koji je individua klase Inegritet pridružuje individuu klase MetodaOsiguranjaIntegriteta. Vidljivo je da je ovo svojstvo inverzno svojstvima DigitalniDokazIntegritetNarusen i DigitalniDokazNeprihvaljiv.

```
ObjectProperty: jeIzuzetOd

        Characteristics:
        Functional

    Domain:
        jeIzuzetOd some Osoba,
        Hardver

    Range:
        Osoba
```

Kôd 6.4 Zapis u manchester notaciji svojstva "jeIzuzetOd"

Kôd prikazan u 6.4 pokazuje svojstvo jeIzuzetOd koje subjektu koji je individua klase Hardver pridružuje individuu klase Osoba. Karakteristika svojstva je funkcionalna.

```
ObjectProperty: jeVlasnik

    Characteristics:
        InverseFunctional

    Domain:
        Osoba,
        jeVlasnik

    Range:
        Hardver
```

Kôd 6.5 Zapis u manchester notaciji svojstva "jeVlasnik"

Kôd prikazan u 6.5 pokazuje svojstvo jeVlasnik koje subjektu koji je individua klase Osoba pridružuje individuu klase Hardver. Karakteristika ovog svojstva je inverzna funkcionalnost.

```
ObjectProperty: koristeAlate

        Characteristics:
        Functional

    Domain:
        PrijateljSuda,
        PolicijskiIstrazitelj,
        SudskiVjestak

    Range:
        ForenzickiAlat
```

Kôd 6.6 Zapis u manchester notaciji svojstva "koristeAlate"

Kôd prikazan u 6.6 pokazuje svojstvo koristeAlate koje subjektu koji je individua klasa SudskiVjestak, PolicijskiIstrazitelj i PrijateljSuda pridružuje individuu klase ForenzickiAlat

```
ObjectProperty: seNalazi

    Characteristics:
        Functional

    Domain:
        OriginalniDigitalniDokaz,
        seNalazi

    Range:
        Izvor
```

Kôd 6.7 Zapis u manchester notaciji svojstva "seNalazi"

Kôd prikazan u 6.7 pokazuje svojstvo seNalazi koje subjektu koji je individua klase OriginalniDigitalniDokaz pridružuje individuu klase Izvor.

```
ObjectProperty: predsjedavaVijecem

    Domain:
        predsjedavaVijecem min 3 Sudac,
        Sudac

    Range:
        Sud
```

Kôd 6.8 Zapis svojstva "predsjedavaVijecem"

Kôd prikazan u 6.8 pokazuje svojstvo presjedavaVijecem koje subjektu koji je individua klase Sudac pridružuje individuu klase Sud.

```
ObjectProperty: jePronadjen

    Characteristics:
        Functional

    Domain:
        jePronadjen min 0 OriginalniDigitalniDokaz

    InverseOf:
        nijePronadjen
```

Kôd 6.9 Zapis svojstva "jePronadjen"

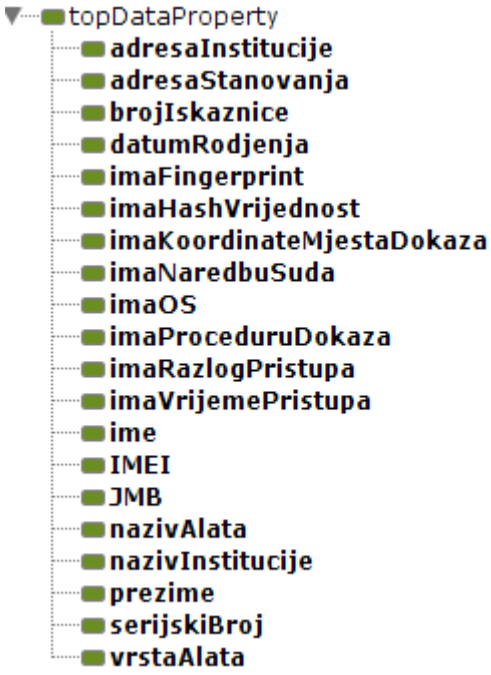
Kôd prikazan u 6.9 pokazuje svojstvo jePronadjen.

```
ObjectProperty: vodiIstragu

    Characteristics:
        Functional

    Domain:
        vodiIstragu min 1 Osoba

    InverseOf:
        jePodIstragom
```

Kôd 6.10 Zapis svojstva "vodiIstragu"

Kôd prikazan u 6.10 pokazuje svojstvo vodiIstragu. Istragu vodi minimalno 1 Osoba, a svojstvo je inverzno od svojstva jePodIstragom.

U nastavku su pobrojani zapisi osnovnih svojstava podataka i objekata koji su neophodni da se opišu digitalni dokazi i sam lanac dokaza.



Slika 25. Atributi koji opisuju svojstva podataka digitalnih dokaza

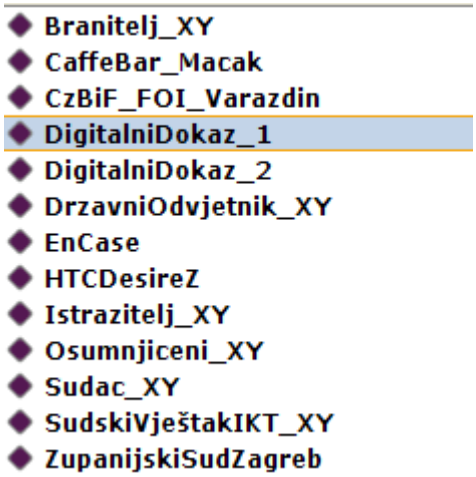
Slika 26. Atributi koji opisuju svojstva objekata digitalnih dokaza

6.3.5 Kreiranje instanci

Instanca u ontologijama predstavlja konkretizaciju klase odnosno entiteta. Tako na primjer sljedeći kôd predstavlja opis individue CzBiF_FOI_Varazdin koja je tip klase AkademskiSektor i pripada toj klasi.

```
Individual: CzBiF_FOI_Varazdin
  Types: AkademskiSektor
        Facts: jeuSklopuInstitucije
```

Kôd 6.8 Zapis u manchester notaciji kreiranja individue "*CzBiF_FOI_Varazdin*"



Slika 27. Popis individua kreiranih u ontologiji

Slika br. 27 prikazuje popis individua kreiranih za potrebe ontologije (okvira) dok je u nastavku dan opis i formalizacija istih u OWL-u:

```
Individual:Osumnjiceni_XY
    Types:
          Osoba
    Facts:
       jeUposlenU     CaffeBar_Macak,
       jeVlasnik     HTCDesireZ ,
       ime    "Miroslav"^^xsd:string,
       prezime    "Barković"^^xsd:string,
      JMB „1212957111130"^^xsd:string
```

Kôd 6.8 Zapis u manchester notaciji kreiranja individue "Osumnjiceni_XY"

Kôd prikazan u 6.8 opisuje kreiranje individue Osumnjiceni_XY koja pripada klasi Osoba, uposlena je u individui CaffeBar_Macak , vlasnik je mobilnog telefona HTCDesireZ, zove se Miroslav, prezima Barković i ima JMBG 1212957111130.

```
Individual:   Istrazitelj_XY
    Types:
          Osoba
   Facts:
       jeUposlenU     CzBiF_FOI_Varazdin ,
       prezime   "Petronijević"^^xsd:string,
       ime   "Saša"^^xsd:string,
       JMB   "0507970125000"^^xsd:string
```

Kôd 6.9 Zapis u manchester notaciji kreiranja individue "Istrazitelj_XY"

Kôd prikazan u 6.9 opisuje kreiranje individue Istrazitelj_XY koja je tip klase Osoba, ima svojstva da je uposlena u CzBiF_FOI_Varazdin, preziva se Petronijević, zove Saša i ima JMB 0507970125000.

```
Individual:   CzBiF_FOI_Varazdin
    Types:

          Institucija
   Facts:
       adresaInstitucije   "Pavlinska 2, 42000 Varaždin,
Hrvatska"^^xsd:string
```

Kôd 6.10 Zapis u manchester notaciji kreiranja individue "CzBiF_FOI_Varazdin"

Kôd prikazan u 6.10 opisuje kreiranje individue CzBiF_FOI_Varazdin koja pripada klasi Institucija, ima adresu Pavlinska 2, 42000 Varaždin, Hrvatska.

```
Individual:   CaffeBar_Macak
    Types:
          Institucija
    Facts:
       adresaInstitucije   "Pavlinska 45, 42000
Varaždin"^^xsd:string
```

Kôd 6.11 Zapis u manchester notaciji kreiranja individue "CaffeBar_Macak"

Kôd prikazan u 6.11 opisuje kreiranje individue CaffeBar_Macak koja pripada klasi Institucija, i ima adresu Pavlinska 45, 42000 Varaždin.

```
Individual:   EnCase
    Types:
          Komercijalni ,
          Softver ,
          ForenzickiAlat
```

Kôd 6.12 Zapis u manchester notaciji kreiranja individue "EnCase"

Kôd prikazan u 6.12 opisuje kreiranje individue EnCase, koja je softver, komercijalni i pripada klasi ForenzickiAlat.

```
Individual:   SudskiVjestakIKT_XY
    Types:
          Osoblje ,
          PrijateljSuda ,
          PolicijskiIstrazitelj ,
          SudskiVjestak ,

    Facts:
       koristeAlate     EnCase ,
       imaLicencu EnCase,
       jeUposlenU     CzBiF_FOI_Varazdin ,
       analizira     HTCDesireZ ,
       ime   "Jasmin"^^xsd:string,
       prezime   "Ćosić"^^xsd:string,
       JMB   "2607970111130"^^xsd:string
```

Kôd 6.13 Zapis u manchester notaciji kreiranja individue "SudskiVjestakIKT_XY"

```
Individual:   HTCDesireZ
    Types:
          Izvor ,
          MobilniTelefon ,
          DigitalniUredjajMalihRazmjera ,
          OriginalniDigitalniDokaz ,
          Hardver ,

    Facts:
       jeIzuzetOd     Osumnjiceni_XY ,
       IMEI   "35-209900-176148-23"^^xsd:string,
       imaOS   „Android 4.0“,
       serijskiBroj „S/N:321543SBK32"^^xsd:string
```

Kôd 6.14 Zapis u manchester notaciji kreiranja individue "HTCDesireZ"

Kôd prikazan u 6.14 opisuje kreiranje individue HTCDesireZ koja pripada klasi Izvor, DigitalniUredjajMalihRazmjena, Hardver, koji je izuzet od individue Osumnjiceni_XY, ima IMEI, imaOS i serijski broj.

```
Individual:   DigitalniDokaz_1
    Types:

          KopijaDigitalnogDokaza ,
          OriginalniDigitalniDokaz ,
          NajboljaKopijaDigitalnogDokaza ,

   Facts:
       seNalazi     HTCDesireZ ,
       imaKoordinateMjestaDokaza   "44°53′N 16°09′E"^^xsd:string,
       imaProceduruDokaza   "Pravilnik o rukovanju digitalnim
       dokazima"^^xsd:string,
       imaHashVrijednost
"cb8d50487ca35f064a16471a0ca0722e898def84cb076c40903916a6223b3fdc"^^
xsd:string,
       imaRazlogPristupa   "Naredba Županijskog Suda 0013456/13
"^^xsd:string,
       imaFingerprint
"09c68b804cb3eb5bef7ca31806b274adccad147533341cab4e677c61b004f6c"^^x
sd:string,
       imaVrijemePristupa   "24.12.2012. 16:00 sati 24
sekunde"^^xsd:string
```

Kôd 6.15 Zapis u manchester notaciji kreiranja individue "DigitalniDokaz_1"

Kôd prikazan u 6.15 opisuje kreiranje individue DigitalniDokaz_1 koja pripada klasama KopijaDigitalnogDokaza, OriginalniDigitalniDokaz,NajboljaKopijaDigitalnogDokaza. Isti ima svojstva da se nalazi u HTCDesireZ, ima KoordinateMjestaDokaza, ima VrijemePristupa, ima ProceduruDokaza, ima HashVrijednosti, ima RazlogPristupa i ima Fingerprint.

```
Individual:   DigitalniDokaz_2
    Types:
          KopijaDigitalnogDokaza ,
          OriginalniDigitalniDokaz ,
          NajboljaKopijaDigitalnogDokaza

   Facts:
       seNalazi     HTCDesireZ ,
       imaVrijemePristupa   "21.12.2012. 16:45:55 SATI"^^xsd:string,
       imaProceduruDokaza   "Pravilnik o prikupljanju digitalnih
dokaza "^^xsd:string,
       imaRazlogPristupa   "Naredba Suda broj 01 000456 KT
/13"^^xsd:string
```

Kôd 6.16 Zapis u manchester notaciji kreiranja individue "DigitalniDokaz_2"

Kôd prikazan u 6.16 opisuje kreiranje individue DigitalniDokaz_2 koja pripada klasama KopijaDigitalnogDokaza, OriginalniDigitalniDokaz,NajboljaKopijaDigitalnogDokaza. Isti ima svojstva da se nalazi u HTCDesireZ, ima VrijemePristupa, ima ProceduruDokaza, ima RazlogPristupa.

```
Individual:   DrzavniOdvjetnik_XY
    Types:
          Osoba

    Facts:
       prezime   "Bogunović"^^xsd:string,
       ime   "Miroslav"^^xsd:string,
       JMB   "0101970124543"^^xsd:string,
       podizeOptuznicu   Osumnjiceni_XY
```

Kôd 6.17 Zapis u manchester notaciji kreiranja individue "DrzavniOdvjetnik_XY"

Kôd prikazan u 6.17 opisuje kreiranje individue DrzavniOdvjetnik_XY koja pripada klasi Osoblje. Ista ima prezime, ime i JMBG i svojstvo da podizeOptuznicu.

```
Individual:   Sudac_XY
    Types:
          Osoba

    Facts:
       prezime   "Madić"^^xsd:string,
       ime   "Neven"^^xsd:string,
       JMB   "3112958121513"^^xsd:string,
       donosiOdluke   Osumnjiceni_XY,
       donosiOdluke   DigitalniDokaz_1,
       donosiOdluke   DigitalniDokaz_2,
       jeUposlen    ZupanijskiSudZagreb
```

Kôd 6.18 zapis u Mančester notaciji individue Sudac_XY

Kôd prikazan u 6.18 opisuje kreiranje individue Sudac_XY. Isti pripada klasi Osoblje, ima prezime, ime, JMB, ima svojstvo da donosiOdluke, te jeUposlen u ZupanijskiSudZagreb.

```
Individual:   ZupanijskiSudZagreb
    Types:
          Sud
```

```
    Facts:
       adresaInstitucije:  "Trg Nikole Šubića Zrinskog 5,10000
Zagreb,
       Hrvatska"^^xsd:string
```

Kôd 6.19 Zapis u Mančester notaciji individue Županijski sud u Zagrebu

Kôd prikazan u 6.19 opisuje kreiranje individue ZupanijskiSudZagreb. Ista pripada klasi Sud te ima adresu Trg Nikole Šubića Zrinskog 5, 10000 Zagreb.

```
Individual: Branitelj_XY

    Facts:
     zastupa>  Osumnjiceni_XY,
     ime>  "Branislav"^^xsd:string,
     prezime>  "Mišić"^^xsd:string,
    JMB>  "0101967123221"^^xsd:string
```

Kôd 6.20 Zapis u Mančester notaciji individue Branitelj_XY

Kôd prikazan u 6.19 opisuje kreiranje individue Branitelj_XY. Ista pripada klasi Osoba te ima svoje ime Branislav, prezime Mišić, te JMB 0101967123221, te isti zastupa individuu Osumnjiceni_XY.

POGLAVLJE VII

7 KONCEPTUALNI OKVIR ZA IZGRADNJU SUSTAVA ZA PRIHVATLJIVOST DIGITALNOG DOKAZA

U prethodnom poglavlju opisana je ontologija digitalnih dokaza, s naglaskom na lanac dokaza. Pobrojani su osnovni koncepti, njihove karakteristike i svojstva, te su kreirane i individue s osnovnim svojstvima (atributima), a koje se javljaju u životnom ciklusu digitalnog dokaza, te determiniraju lanac dokaza, a samim time i prihvatljivost digitalnog dokaza.

U nastavku rada, u ovom poglavlju definirat će se formalna prihvatljivost digitalnih dokaza, te postaviti određena pravila koja moraju biti slijeđena kako bi digitalni dokaz bio formalno prihvaćen od strane suda. Pravila će se i formalizirati kroz SWRL te integrirati u ontologiju, što će u konačnici predstavljati okvir uz pomoć kojeg će se moći odlučivati o formalnoj prihvatljivosti digitalnih dokaza.

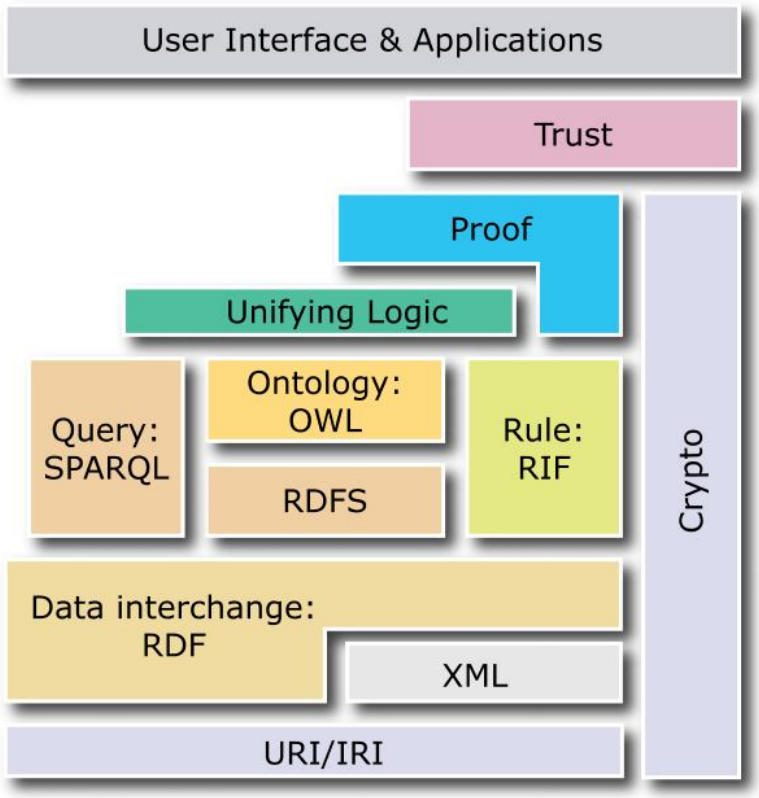
7.1 Semantičko modeliranje definicije formalne prihvatljivosti digitalnih dokaza uz pomoć SWRL-a

Jezik pravila za semantički web (eng. *Semantic Web Rule Language, SWRL*) razvio se iz RuleML jezika koji je prvenstveno namijenjen modeliranju poslovnih pravila. SWRL objedinjuje porodicu XML serijaliziranih jezika pravila koja se proteže kroz sve industrijski standardizirane oblike web pravila [116].

SWRL posjeduje moć konceptualizacije i razvoja modela OWL-a i izražajnost koju nudi RuleML u kombinaciji sa OWL-om. W3C ga je predstavio 2004. godine kao jezik koji sadrži punu snagu OWL DL jezika, ali kompleksniju odlučivost i praktičnu implementaciju. SWRL je osmišljen kao jezik za izražavanje pravila temeljenih na konceptima OWL-a. Samim time SWRL omogućava u svojim izrazima potpuno korištenje koncepata iz OWL-a kako bi osigurao naprednije mogućnosti zaključivanja od onih koje ima sam OWL. Semantički je

SWRL izgrađen korištenjem deskriptivne logike (engl. *Description Logic,DL*), iste osnove kakvu ima OWL DL [117,118].

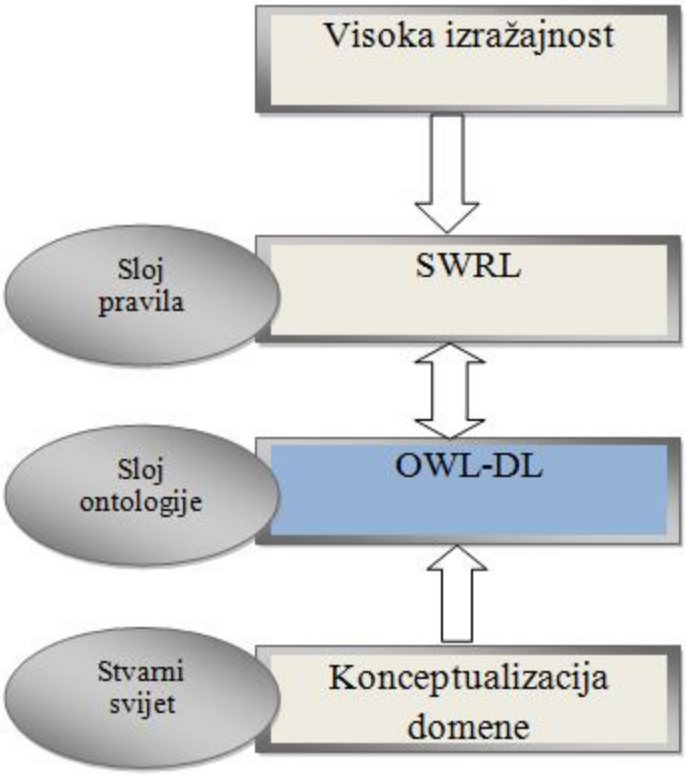
Osnovna namjena SWRL-a je postavljanje poslovnih pravila u cilju zaključivanja – donošenja određenih zaključaka na osnovu ranije formaliziranih pravila.



Slika 28. Posljednja inačica W3C Sematic Web "Layer Cake" u izvornom obliku (http://www.w3.org/2007/03/layerCake.png)

Na početku Projekta semantičkog web-a , W3C je definirao stog tehnologije (nazvan *„Layer Cake*“ - http://www.w3.org/2007/03/layerCake.png). Vremenom ste stog mijenjao, evaluirao, a posljednja inačica je prikazana u izvornom obliku na slici 28. Ova specifikacija je prerasla u 4 glavne grupe jezika: RDF (modeliranje podataka), OWL/RDFS (ontologije), SPARQ (upiti) i SWRL (uloge) (Slika 27. i 28.) SWRL je postao *de-facto* standard za pravila u semantičkom web-u. Obzirom da kombiniranje OWL-a i SWRL-a ne nudi dovoljno funkcionalnosti (definiranih u specifikaciji jezika) , upotreba u definiranju poslovnih pravila bi bila nemoguća bez tzv. pogona (engl. „*Engine*“) u kojima su integrirane te funkcionalnosti

[119]. Najpoznatiji su iz obitelji KAON2 (http://kaon2.semanticweb.org/), FaCT++ (http://owl.man.ac.uk/factplusplus/), HermiT (http://hermit-reasoner.com/), RacerPro (http://semanticweb.org/wiki/RacerPro) i Pellet (http://clarkparsia.com/pellet/). Za potrebe ovog rada upotrjebljavat će se Pellet reasoner [120]. Slika pokazuje mjesto SWRL-a u slojevima ontologije.



Slika 29. Slojevi ontologije

SWRL pravila sastoje se od dva dijela: premisa (*antecedent*) i zaključak (*konsekvent*). Premisa predstavlja tijelo SWRL pravila, dok zaključak predstavlja tzv. glavu SWRL pravila [117]. Svako pravilo u svojoj suštini sastoji se od atoma, pa tako i premisa i zaključak, kako slijedi:

$$atom \wedge atom \wedge atom \rightarrow atom \wedge atom$$

$$premisa \rightarrow zaključak$$

pri čemu se zaključak ispunjava u slučaju kad su svi atomi premise zadovoljeni.

Svaki atom je sljedećeg oblika:

$$p(arg_1, arg_2, \dots arg_n)$$

gdje je p simbol predikata iz OWL-a, dok su $arg_1, \dots, arg_n$ argumenti tog predikata. Pri tome simbol predikata može predstavljati OWL klasu, svojstvo ili tip podatka. Argumenti mogu biti OWL individue, podatkovne vrijednosti ili varijable koje se na njih odnose [116,117].

U nastavku je dan kôd u kom je prikazano korištenje atoma za prikaz jedne OWL individue iz izgrađene ontologije digitalnih dokaza.

```
NajboljaKopijaDigitalnogDokaza(?x)
```

SWRL 7.1 Varijabla ?x postaje individua OWL klase "NajboljaKopijaDigitalnogDokaza"

NajboljaKopijaDigitalnogDokaza je OWL klasa, dok je ?x varijabla koja predstavlja individuu klase *NajboljaKopijaDigitalnogDokaza*. Umjesto varijable ?x moguće je umetnuti i konkretnu OWL individuu, a što je prikazano u sljedećem kôdu:

```
NajboljaKopijaDigitalnogDokaza(Pictures001.jpg)
```

SWRL 7.2 Kôd provjerava da li je OWL individua koja se zove *Pictures001.jpg* član ekstenzije OWL klase *NajboljaKopijaDigitalnogDokaza*

DEFINIRANJE FORMALNE PRIHVATLJIVOSTI DIGITALNOG DOKAZA

Kako bi proces digitalne istrage bio potpun, te digitalni dokaz bio formalno prihvatljiv moraju biti ispunjeni određeni uvjeti:

7.1 Hardver koji je izuzet od neke osobe (osumnjičenog, žrtve) mora sadržavati originalni digitalni dokaz.
7.2 Osoba koja je vlasnik tog hardvera može biti osumnjičeni.
7.3 Prijatelji suda koji imaju naredbu suda za vještačenje su sudski vještaci u tom predmetu.

7.4 Kopija digitalnog dokaza koja ima izračunatu funkciju sažetka („hash vrijednost“) je najbolja kopija digitalnog dokaza.

7.5 Najbolja kopija digitalnog dokaza koja ima izračunatu funkciju sažetka („hash vrijednost“) je originalni digitalni dokaz.

7.6 Za takvu kopiju se kaže da ima očuvan integritet.

7.7 Originalni digitalni dokaz koji ima *fingerprint osobe, tzv. hash vrijednost, koordinate mjesta, procedure, razlog pristupa, vrijeme pristupa*, smatra se formalno prihvatljivim dokazom.

Formalizirajmo sada ove uvjete redoslijedom:

Definicija 7.1 *Hardver koji je izuzet od osumnjičenog mora sadržavati originalni digitalni dokaz.*

$$\text{ORIGINALNIDD} \equiv \text{DIGITALNIDOKAZ} \sqcap \exists \text{IZUZET.OSUMNJICENI}$$

```
Hardver(?x), jeIzuzetOd(?x, ?osum),Osumnjiceni(?osum) ->
                OriginalniDigitalniDokaz(?x)
```

SWRL 7.3 SWRL iskaz koji definira kada je dokaz OriginalniDigitalniDokaz

U SWRL iskazu br. 7.1 je definirano sljedeće: Individua ?x koja pripada klasi *hardver*, i koja je izuzeta od individue *?osum* a koja pripada klasi *Osumnjiceni* , je originalni digitalni dokaz. Znači dokaz će biti originalan samo ukoliko su zadovoljena ova dva uvjeta.

Definicija 7.2 *Osoba koja je vlasnik tog hardvera može biti osumnjičeni.*

$$\textit{OSUMNJICENI} \equiv \textit{POJEDINAC} \sqcap \exists \textit{ JEVLASNIK.HARDVER}$$

```
Pojedinci(?x) ^ Uredjaj(?ur) ^ jeVlasnik(?x, ?ur) → Osumnjiceni(?x)
```

SWRL 7.4 SWRL iskaz koji definira kada je osoba osumnjičenik u slučaju

SWRL iskaz br.7.2 definira da ukoliko indvidua ?x pripada klasi *Pojedinci*, te ukoliko je vlasnik nekog uređaja *?ur* a koji pripada klasi *Uredjaj*, onda je ta osoba *Osumnjiceni*.

Definicija 7.3 *Prijatelji suda koji imaju naredbu suda za vještačenje su sudski vještaci u tom predmetu.*

$$SUDSKIVJESTACI \equiv PRIJATELJSUDA \sqcap \exists\ IMANAREDBU.SUDA$$

```
PrijateljiSuda(?x) ^  imaNaredbuSuda(?x, ?naredba) →
                    SudskiVjestaci(?x)
```

SWRL 7.5 Definiranje pojma Sudski vještaci u SWRL-u

U SWRL iskazu br. 7.3 je rečeno da individua ?x koja pripada klasi *PrijateljiSuda*, ukoliko ima naredbu suda pripada klasi *Sudski vještak*. To znači da će ta osoba i formalno biti uključena u slučaj kao „ključna“ osoba koja će prezentirati digitalne dokaze sudu.

Definicija 7.4 i 7.5 *Najbolja kopija digitalnog dokaza koja ima „hash vrijednost“ je originalni digitalni dokaz.*

$$ODD \equiv DD \sqcap \exists\ IMAHASHVRIJEDNOST.KOPIJADD$$

```
KopijaDigitalnogDokaza(?x) ^ imaHashVrijednost(?x, ?sha2) →
                    NajboljaKopijaDigitalnogDokaza(?x)
```

SWRL 7.6 SWRL pravilo koje definira Najbolju kopiju digitalnog dokaza

SWRL pravilo br.7.4 7.5 kaže da bi digitalni dokaz bio najbolja kopija digitalnog dokaza[33] , on mora da ima osiguran integritet kroz ne izmijenjenu „hash vrijednost“.

Definicija 7.6 *Kopija digitalnog dokaza koja ima „hash vrijednost“ je najbolja kopija digitalnog dokaza.*

$$NKDD \equiv KDD \sqcap \exists\ IMAHASHVRIJEDNOST.KOPIJADD$$

```
OriginalniDigitalniDokaz(?x) ^ imaHashVrijednost(?x,?hash) ^
                        swrlb:Equal(?hash,
"cb8d50487ca35f064a16471a0ca0722e898def84cb076c40903916a6223b3fdc")
                → DigitalniDokazIntegritetOcuvan(?x)
```

SWRL 7.7 SWRL pravilo koje osigurava integritet digitalnog dokaza

SWRL pravilo br. 7.6 kaže da ukoliko originalni digitalni dokaz ima izračun funkcije sažetka (hash vrijednost), tada je očuvan integritet tog dokaza

Definicija 7.7 *Originalni digitalni dokaz koji ima fingerprint, hash vrijednost, koordinate mjesta, procedure, razlog pristupa, vrijeme pristupa, smatra se formalno prihvatljivim dokazom.*

$$DDPRIHVATLJIV \equiv DIGITALNIDOKAZ \sqcap \exists IMAFINGERPRINT.DD \wedge DIGITALNIDOKAZ \sqcap \exists IMAHASH.DD \wedge DIGITALNIDOKAZ \sqcap \exists IMAKOORDINATE.DD \wedge DIGITALNIDOKAZ \sqcap \exists IMAPROCEDURU.DD \wedge DIGITALNIDOKAZ \sqcap \exists IMARAZLOG.DD \wedge DIGITALNIDOKAZ \sqcap \exists IMAVRIJEME.DD$$

[33] Prema IOCE standardima, nikada se ne rukuje originalnim digitalnim dokazima. Uvijek se naprave dvije identične kopije-kopija i najbolja kopija (engl.copy and best copy) te se rukuje kopijom digitalnog dokaza.

```
OriginalniDigitalniDokaz(?x) ^ imaFingerprint(?x, ?fp) ^
imaHashVrijednost(?x, ?sha2) ^ imaKoordinateMjestaDokaza(?x, ?gps) ^
imaProceduruDokaza(?x, ?proc) ^ imaRazlogPristupa(?x, ?razl) ^
imaVrijemePristupa(?x, ?ts) → DigitalniDokazPrihvatljiv(?x)
```

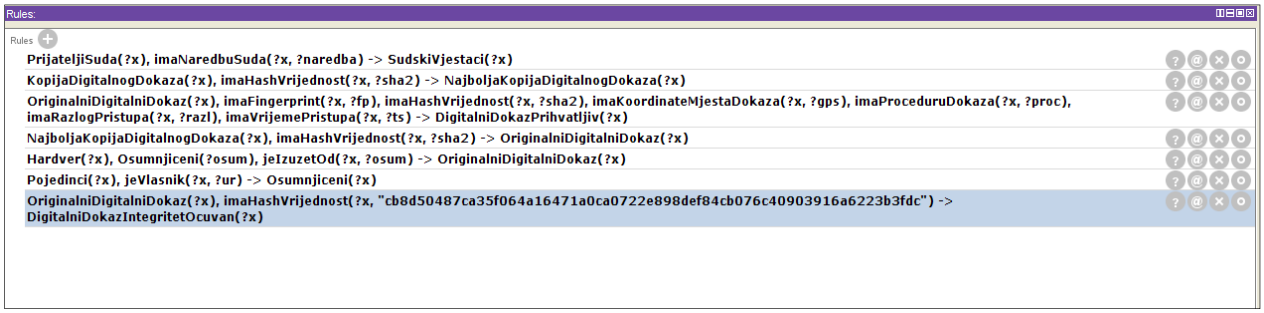
SWRL 7.8 Definiranje pravila za formalnu prihvatljivost digitalnih dokaza

Iskaz SWRL 7.8 definira formalnu prihvatljivost digitalnog dokaza i kaže:

„Digitalni dokaz je formalno prihvatljiv ako je zadovoljen „5w`s & 1 h“, odnosno ukoliko se zna:

- Tko je rukovao s digitalnim dokazima ?
- Što je digitalni dokaz ?
- Kada je rukovano s digitalnim dokazima ?
- Kako je rukovano s digitalnim dokazima ?
- Gdje je rukovano s digitalnim dokazima ?
- Zašto je rukovano s digitalnim dokazima ? „

To znači da će sud formalno prihvatiti digitalni dokaz ukoliko on ima: *fingerprint osobe* koja je rukovala sa njim - to može biti digitalni potpis, biometrijska karakteristika (otisak prsta, iris zjenica i sl.), *vrijednost funkcije sažetka* odnosno „hash vrijednost“ kojim će se osigurati integritet dokaza, *vremenski žig* koji će potvrditi kada se rukovalo sa digitalnim dokazima, SOP (engl. Standardne operativne procedure) *način* na koji je rukovano sa digitalnim dokazima (*procedure*), *koordinate mjesta* koje će potvrditi gdje je rukovano sa digitalnim dokazima, te *razlog zbog čega* je sve rađeno a to je obično naredba Suda ili Tužiteljstva i sl.).



Slika 30. Popis pravila implementiranih u Protége-u

7.2 Testiranje funkcionalnosti okvira

Za testiranje funkcionalnosti samog okvira kreirane su konkretne individue klasa izrađene ontologije sa konkretnim atributima. Slijeđena su pravila definirana u SWRL-u. Cilj je bio da se vidi da li će okvir moći prepoznati kada je digitalni dokaz formalno prihvatljiv a kada ne. Tablice broj 7. i 8. prikazuju interpretaciju osnovnih koncepata i svojstava iz studije slučaja.

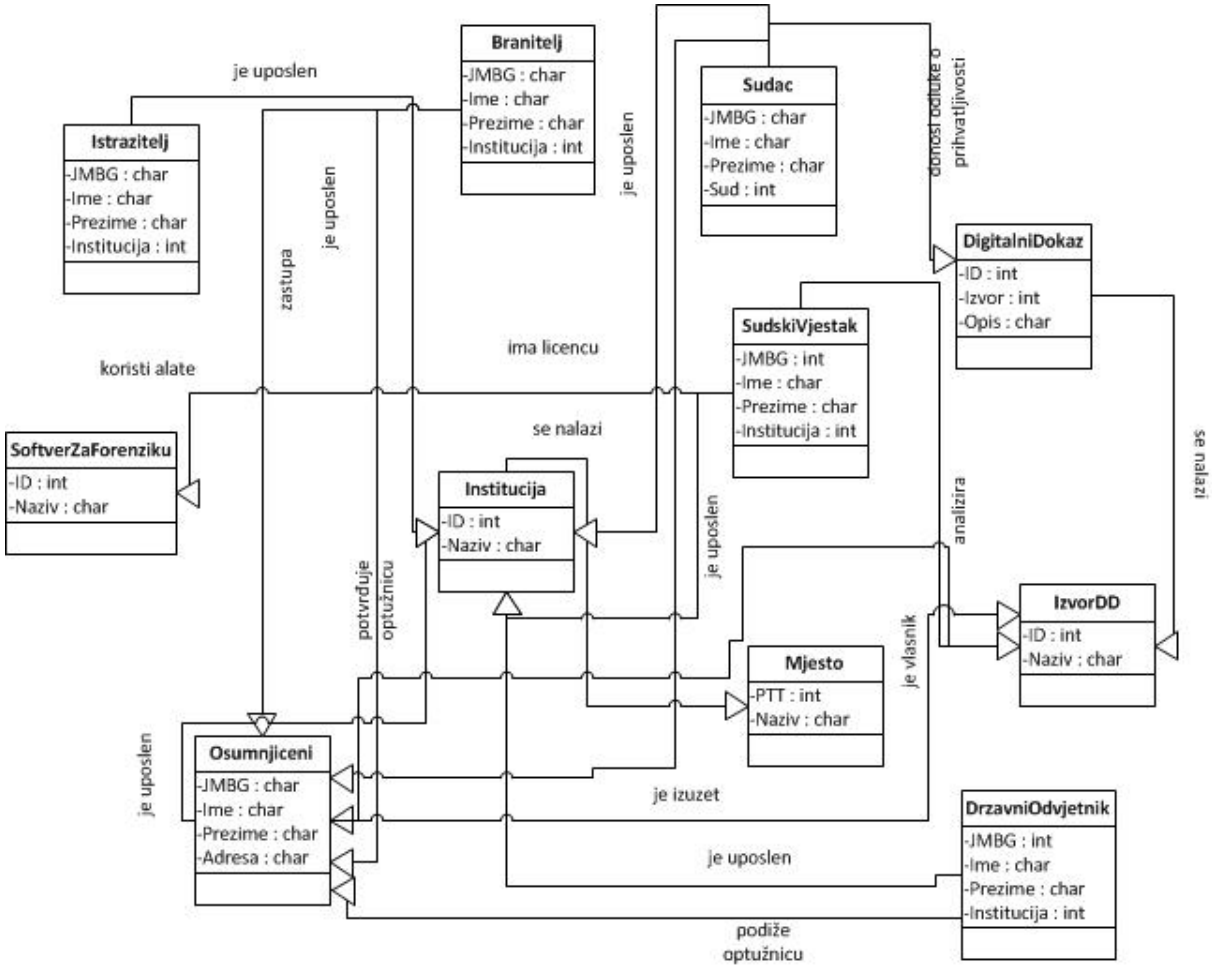
Tablica 7. Interpretacija koncepata iz studije slučaja

Koncept (A)	**Skup u kojeg se koncept preslikava u interpretaciji I (A`)**
Osoblje	{Sudac_XY,Osumnjiceni_XY,SudskiVjestakIKT_XY,Branitelj_XY, DrzavniOdvjetnik_XY}
IzvorDigitalnogDokaza	{MobilniTelefon_HTCDesereZ}
Institutucija	{CaffeBar_Macak,CZBiF_FOI_Varazdin,ZupanijskiSudZagreb}
DigitalniDokaz	{DigitalniDokaz_1,DigitalniDokaz_2}
Softver	{Encase}
Prihvatljivost	{DigitalniDokazPrihvatljiv,DigitalniDokazNeprihvatljiv}

Tablica 8. Interpretacija svojstava iz studije slučaja

Relacija (R)	**Skup u kojeg se relacija preslikava u intepretaciji I (R`)**
jeUposlen	{(Sudac_XY,ZupanijskiSudZagreb),(Osumnjiceni_XY,CaffeBar_Macak),(SudskiVjestakIKT_XY,CZBiF_FOI_Varazdin),(Branitelj_XY,Advokatura_Zagreb),(DrzavniOdvjetnik_XY,DrzavnoOdvjetnistvo_RH)
donosiOdluke	{(Sudac_XY, DigitalniDokazPrihvatljiv), (Sudac_XY, DigitalniDokazNeprihvatljiv }
jeIzuzet	{(DigitalniDokaz,Osumnjiceni_XY)}
seNalazi	{(DigitalniDokaz, MobilniTelefon_HTCDesereZ)}
zastupa	{(Branitelj_XY,Osumnjiceni_XY)}
podizeOptuznicu	{(DrzavniOdvjetnik_XY,Osumnjiceni_XY)}
potvrđujeOptuznicu	{(Sudac_XY,Osumnjiceni_XY)}
jeVlasnik	{(Osumnjiceni_XY, MobilniTelefon_HTCDesereZ)}
imaLicencu	{(SudskiVjestakIKT_XY,Encase)}
analizira	{(SudskiVjestakIKT_XY, MobilniTelefon_HTCDesereZ)}
koristiAlat	{(SudskiVjestakIKT_XY,Encase)}

Generalno UML dijagram klasa s atributima i relacijama modeliran za DBMS (engl. *Database Management System*) je prikazan kako slijedi (slika 31.):

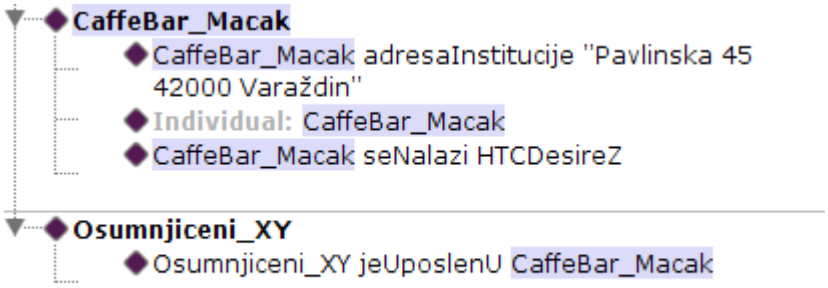


Slika 31. UML dijagram klasa sa pridruživanjem glavnih aktivnosti u procesu lanca dokaza

Opisani su osnovni koncepti, njihovi osnovni atributi, te relacije između koncepata koji se pojavljuju u procesu digitalne forenzičke istrage u svim njenim fazama.

Slika 32. Implementacija individue Osumnjiceni_XY

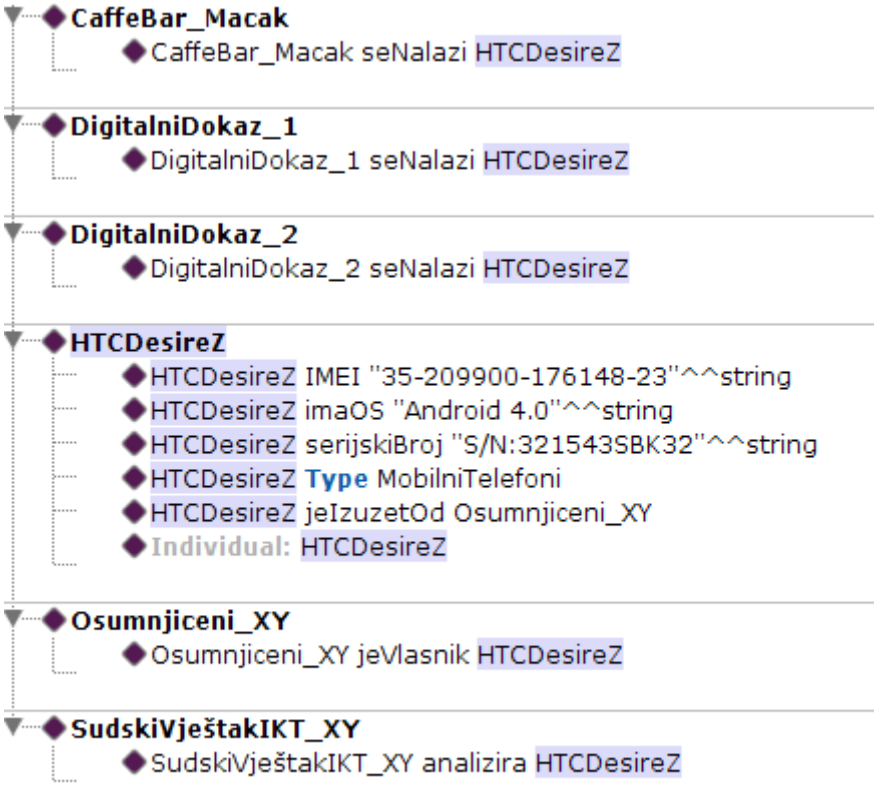
Slika 32. pokazuje implementaciju individua u programu Protége. Cafee Bar Mačak u kojem je uposlen osumnjičeni se nalazi na adresi Pavlinska 45, 42000 Varaždin (slika br. 33).



Slika 33. Implementacija individue CaffeBar Macak

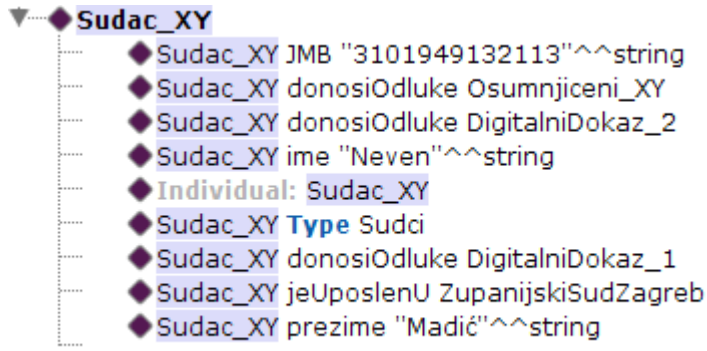
Slika 34. Implementacija individue SudskiVještakIKT_XY u Protége-u

Na slici 34. je prikazana implementacija individue SudskiVjestakIKT_XY i to kako slijedi: ime je Jasmin, prezime Ćosić, ima JMBG 2607970111130, uposlen je u CzBiF FOI-a Varaždin, koristi alat EnCase, te analizira mobilni telefon HTC Desire Z u kom su pronađeni digitalni dokazi.



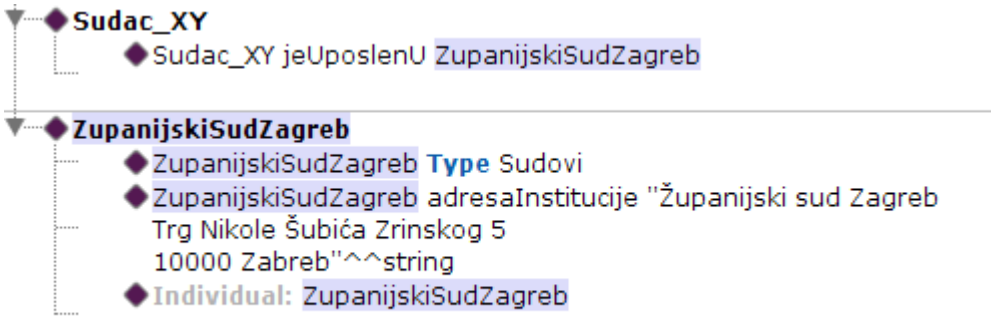
Slika 35. Implementacija uređaja HTC Desire Z u kom se nalaze digitalni dokazi

Na slici 35. je dan formalni opis uređaja *HTC Desire Z* u kom se nalazi *DigitalniDokaz_1* i *DigitalniDokaz_2*, a koji su izuzeti od *Osumnjicenog_XY*, te koje analizira *SudskiVjestakIKT_XY*. Uređaj karakterizira *IMEI* i *serijskiBroj* , isti je podtip klase *MobilniTelefoni*.



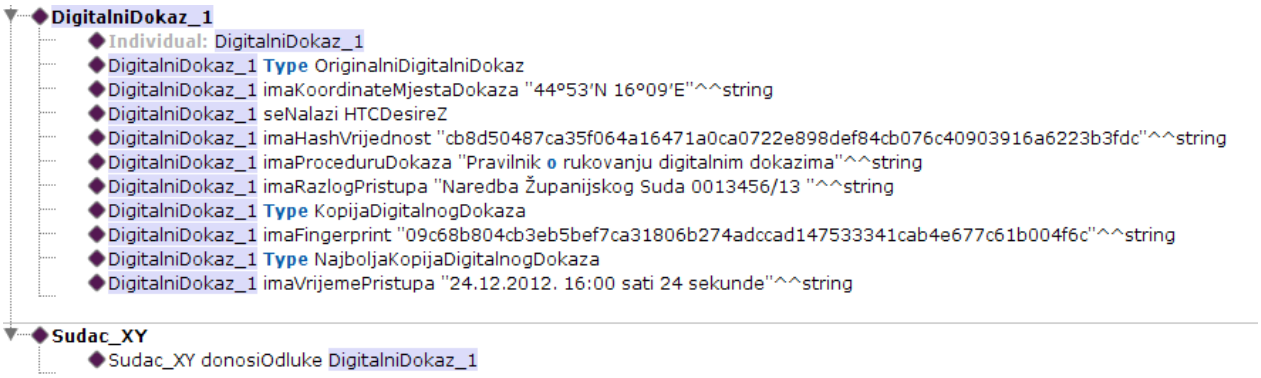
Slika 36. Implementacija individue Sudac_XY

Slike 36. i 37. prikazuju formalni opis individua *Sudac_XY* i *ZupanijskiSudZagreb*

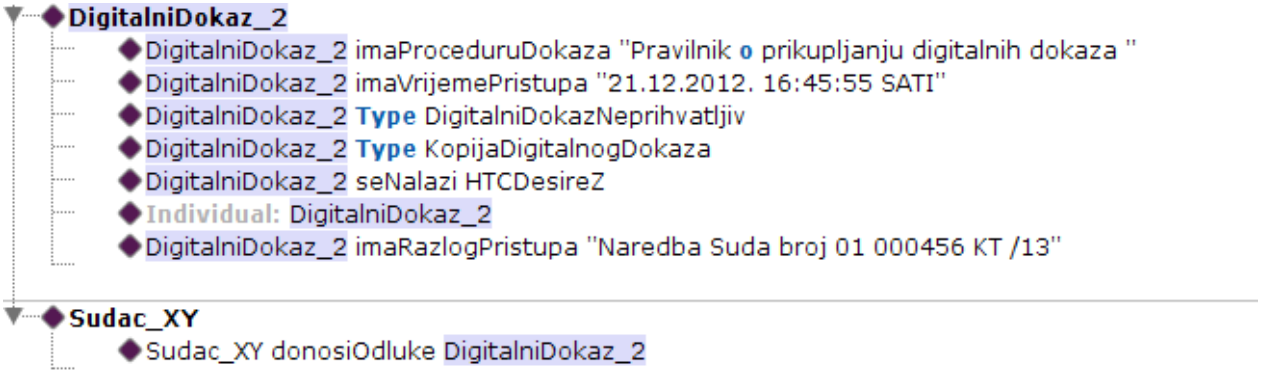


Slika 37. Implementacija individue Županijski Sud u kojoj je uposlen Suda_XY

U uređaju su pronađena 2 digitalna dokaza, *DigitalniDokaz_1* i *DigitalniDokaz_2*. Individua *DigitalniDokaz_1* je potpuna , sadrži sve atribute koji su potrebni i koje treba da ima, dok je individua *DigitalniDokaz_2* nepotpuna, nedostaju joj ključni atributi hash vrijednost i fingerprint osobe (slike 38. i 39.).

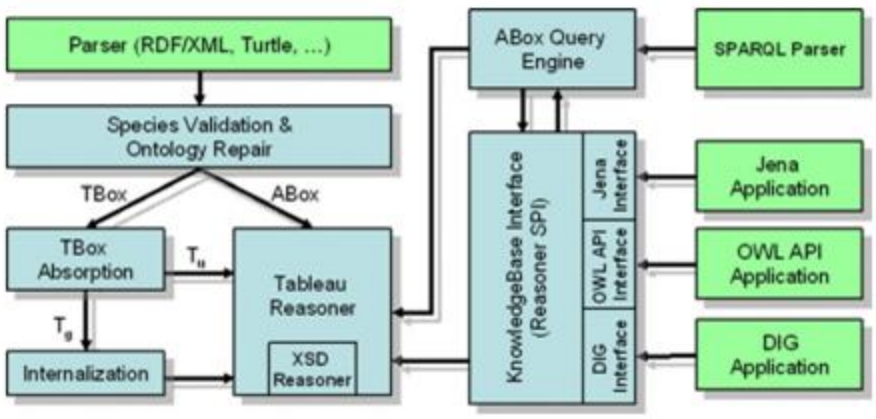


Slika 38. Atributi individue digitalnog dokaza nazvane DigitalniDokaz_1



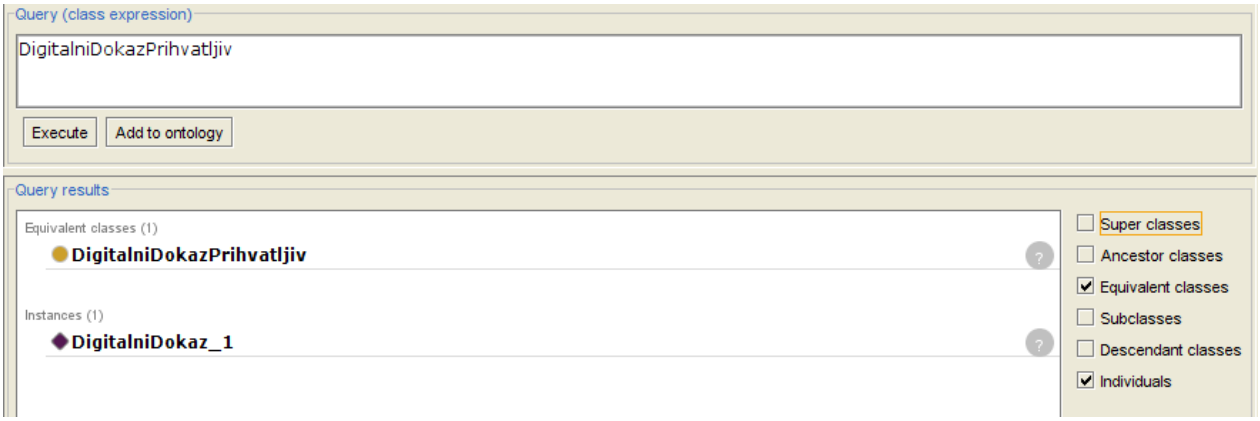
Slika 39. Atributi individue digitalnog dokaza nazvane DigitalniDokaz_2

Sada kada posjedujemo sve neophodne elemente (individue, atribute, relacije i pravila), možemo kroz Protége izvršiti testiranje okvira. Ovdje ključnu ulogu igra „*reasoner*“ ili deduktivni dodatak Protége-u koji omogućava rasuđivanje nad ontologijom. Korišten je Pellet reasoner [120]. Pellet je namijenjen za aplikacije u kojima je potrebno predstaviti informacije i omogućiti rezoniranje nad njima korištenjem OWL-a. Postao je neizostavan alat koji se koristi sa OWL-om, a koji ima punu potporu za OWL-DL. Implementiran u Java-i, distribuira se pod licencom otvorenog koda [121]. Na slici 40. vidimo njegove glavne komponente.



Slika 40. Glavne komponente Pellet-a [121]

Obzirom da je individua *DigitalniDokaz_1* koncipirana tako da ima sve atribute koji određuju formalnu prihvatljivost, kada smo pokrenuli upit u „DL query TAB-u“, Pellet reasoner je kao rezultat dao Instancu DigitalniDokaz_1 (slika 41.).

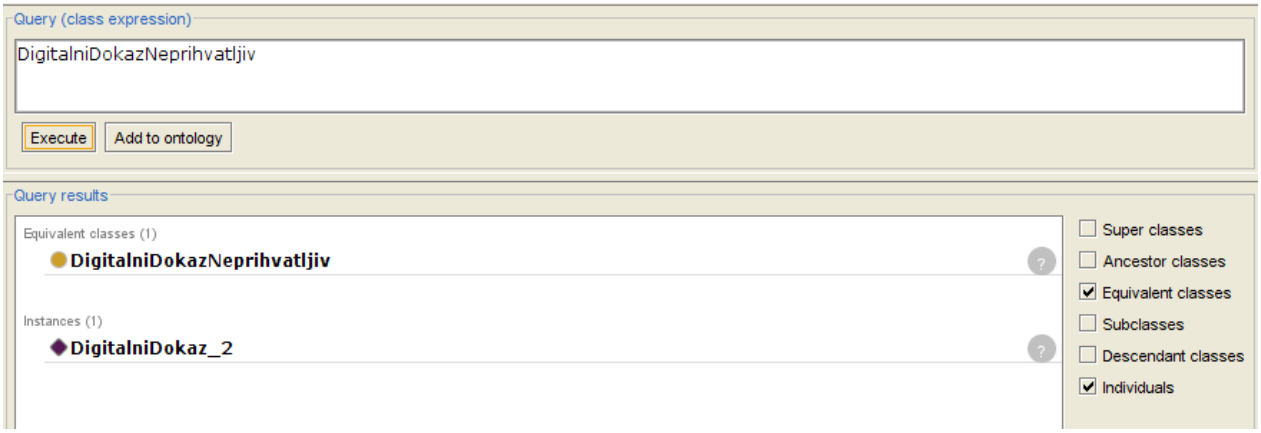


Slika 41. DL upit koji daje odgovor na pitanje koji je digitalni dokaz prihvatljiv

Individua *DigitalniDokaz_2* je koncipirana tako da nema sve potrebne atribute koji determiniraju digitalne dokaze. Kada postavimo upit o *DigitaniDokazNeprihvatljiv* kroz DL Query TAB, Pellet će odgovoriti sa *DigitalniDokaz_2* (slika 42.). Isti odgovor bi dobili korištenjem upita:

NOT DigitalniDokazPrihvatljiv

Što znači negaciju iskaza DigitalniDokazPrihvatljiv.



Slika 42. DL upit koji daje odgovor na pitanje koji je digitalni dokaz neprihvatljiv

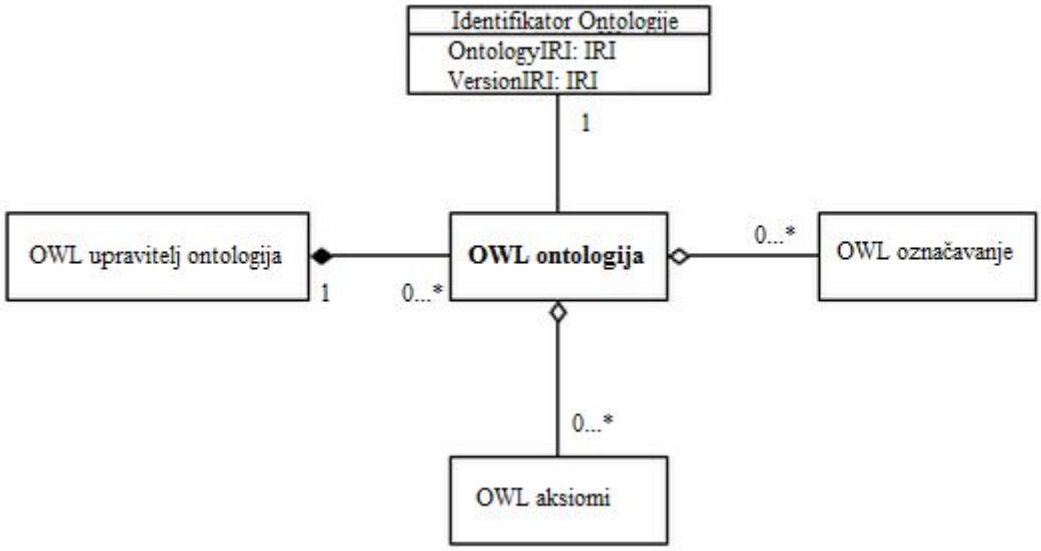
7.3 Mogućnosti korištenja okvira i načini integracije u softverske proizvode

Okvir formaliziran u OWL-u s pravilima postavljenim u SWRL-u biti će postavljen on-line na neki od javno dostupnih i korištenih repozitorija ontologija. Na ovaj način omogućit će se dostupnost i njegovo korištenje. Okvir će biti moguće importirati u druge ontologije putem dostupnih alata ili jednostavno putem korištenja URI-a[34] koji identificira i referencira ontologiju. Danas postoje već gotovi alati razvijeni od strane Akademske zajednice u nekoliko Sveučilišta u svijetu a koji omogućuju razvoj aplikacija u nekom programskom jeziku (npr. Java) koji se oslanjaju na znanje pohranjeno u ontologiju. Takav primjer su Odsjek za računalne znanosti Sveučilišta u Manchesteru, Velika Britanija, te Centar za istraživanje i razvoj IKT-a Sveučilišta u Karlsruhe, Njemačka. Jedno od vodećih na polju ontologija je i Sveučilište Stanford, USA. Razvijeno je nekoliko različitih sučelja (engl. *Interface*) u vidu API-ja (engl. *Application Programming Interface*) i java aplikacija koje omogućavaju izradu aplikacija i manipulaciju ontologijama (pozivanje ontologije, importiranje, dodavanje, brisanja klasa, svojstava, individua, postavljanje pravila nad istom te rasuđivanje na osnovu tih pravila. Neki od njih su OWL API, HP Jena Toolkit, KAON i KAON2, NeOnToolkit, SKOS API i sl. [122].

Danas je u akademskim krugovima u domeni umjetne inteligencije (eng. *Artificial Intelligence, AI*) veoma česta upotreba OWL API sučelja (engl. *Interface*) u kombinaciji sa

[34] URI (engl. Uniform Resource Identifier) predstavlja set karaktera koji identificiraju neki resurs na web-u

Apache Maven[35] projektom, a pomoću kojeg se programiraju aplikacije iz domene baza znanja, a koje crpe znanje pohranjeno u ontologijama [123]. Na slici 43. je prikazana arhitektura OWL API sučelja, gdje se vidi da je u centru repozitorija OWL ontologija na koju se sve oslanja.



Slika 43. Položaj ontologije i upravljanje njome u OWLAPI-u

U nastavku su dana dva primjera kôda za kreiranje ili učitavanje ontologije iz OWL API:

```
OWLOntologyManager m = create();
OWLOntology o =
m.createOntology(http://www.semanticweb.org/jasmin/demf);
assertNotNull(o);
```

Kôd 7.11 Implementacija kreiranja ontologije u Java-i

```
OWLOntologyManager m = create();
OWLOntology o =
m.loadOntologyFromOntologyDocument(://www.semanticweb.org/jasmin/dem
```

[35] Apache Maven je softverski alat namjenjen za upravljanje i razumijevanje programskih projekta.. Na temelju koncepta projekta objekta modela (POM), Maven može upravljati projektom, graditi, izvješćivati i dokumentirati iz središnjeg dijela informacije, npr. ontologije (http://maven.apache.org/)

```
f);
assertNotNull(o);
```

Kôd 7.12 Primjer učitavanja ontologije iz IRI-ja

Na ovaj način je moguće kreirati veoma učinkovite aplikacije u java ili nekom drugom programskom jeziku, a koje će se oslanjati na izrađene ontologije i znanje pohranjeno u njima.

7.4 Ograničenja okvira

Ograničenje okvira proizlazi iz činjenice da se pojam nepromjenjivosti funkcije sažetka nije tretirao kao poseban problem iako to možda i zaslužuje. Kada digitalni dokaz prođe jedan krug u svom životnom ciklusu, računa se vrijednost sažetka (*hash funkcija*). Taj sažetak se pohranjuje i osigurava 5Ws&1H. Problem koji se ovdje pojavljuje je sve veći problem koji istražiteljima stvara tzv. „anti-forenzika“ kojom zlonamjerni korisnici na svaki mogući način pokušavaju kompromitirati forenzičku znanost, metode i alate, a sve u cilju narušavanja integriteta i osporavanja kako lanca dokaza tako i cijele forenzičke istrage. Kako znati da je sažetak koji se nalazi uz originalni digitalni dokaz uistinu originalni sažetak koji je nastao korištenjem okvira ili je krivotvoren ?

Ovo je realan problem kojim se autor planira baviti i u nastavku svoga bavljenja ovom tematikom. Jedan od mogućih rješenja je korištenje ugrađenih funkcija u SWRL iskazima kao što su funkcija:

```
swrlb:stringEqualIgnoreCase (?x1,?x2)
```

ili

```
swrlb:equal (?x1,?x2)
```

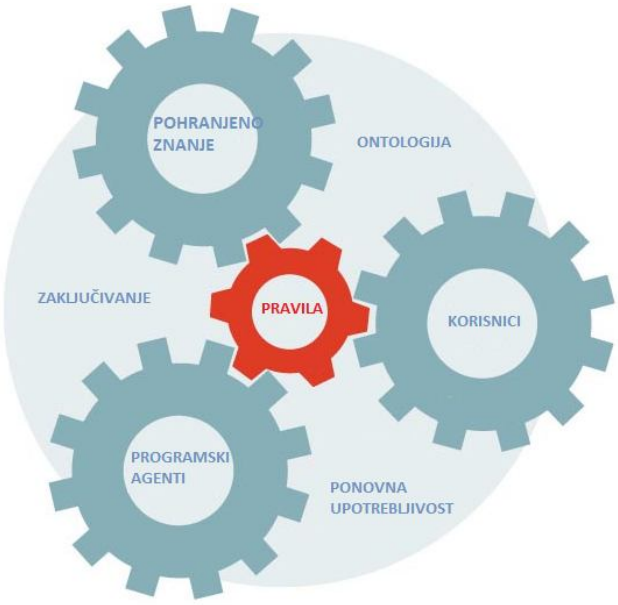
Uporabom ovih funkcija uspoređivala bi se dva niza koji bi predstavljali dva hash sažetka u dva ciklusa digitalnog dokaza - npr. nepromjenjivost hash funkcije, ukoliko nizovi (hash) nisu potpuno isti, neovisno od malih/velikih slova, izraz neće biti točan.

POGLAVLJE VIII

8 PROVJERA VALJANOSTI (ENGL. VALIDATION) I VREDNOVANJE (ENGL. EVALUATION) IZRAĐENE ONTOLOGIJE

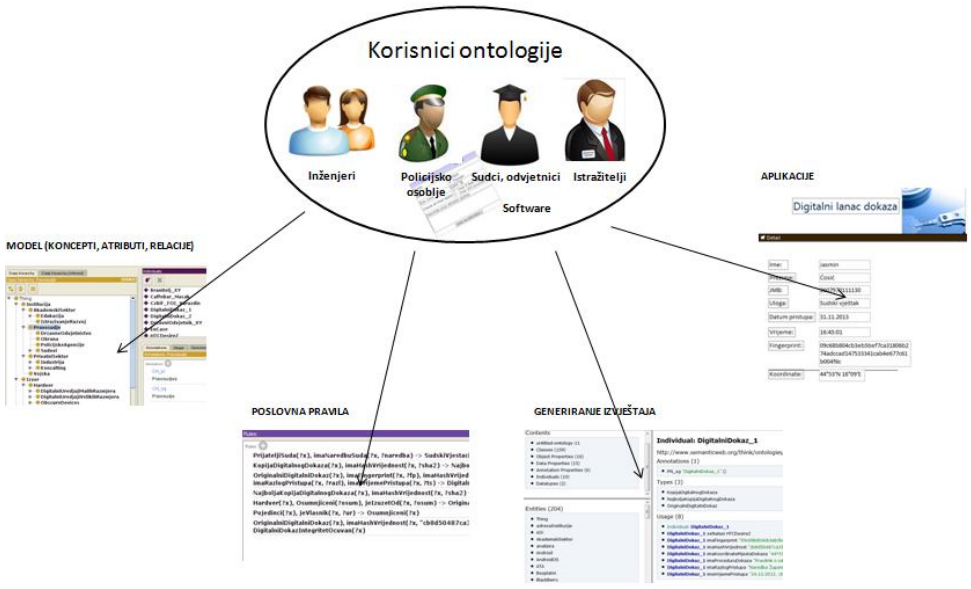
Kao što je ranije naglašeno izrađena ontologija treba da definira najčešće korišteni rječnik podataka za istraživače koji žele dijeliti informacije u određenoj domeni, da omogući ponovnu upotrebljivost domenskog znanja, da učini pretpostavke domene jasnijim, izdvoji, te omogući analizu domenskog znanja nasuprot operativnog [115].

Osnovu za izrađenu ontologiju čini DEMF (engl. *Digital Evidence Management Framework*), okvir koji je razvijen u ranijim fazama istraživanja a u kom se svakog trenutka mora znati tko je, kada, gdje, kako, zašto dolazio u kontakt sa digitalnim dokazima [47-49]. Time će se omogućiti korištenje znanja pohranjenog u vidu rječnika podataka domene digitalne forenzike, omogućit će ponovnu upotrebljivost (engl. *Reusability*) domenskog znanja, te će obzirom da će ontologija biti formalizirana u OWL-u i SWRL-u omogućiti korištenje iste od strane računalnih programa i drugih softverskih agenata. Ontologija je otvorena, uvijek se mogu nadodavati nove klase, atributi, relacije ili instance klasa, te je bitno napomenuti da ima veze na sve slične i kompatibilne ontologije koje su već ranije izrađene, a upotrebljive su. Na slici 44. su prikazane ključne komponente sustava te njihov odnos. Evidentno je da su pravila pokretač sustava te da od njihove implementacije ovisi i sama funkcionalnost sustava.



Slika 44. Pravila kao "pogon" i ključni element sustava

Pored diseminacije znanja o nužnosti vođenja lanca dokaza, ontologiju mogu koristiti sudci, odvjetnici, istražitelji koji se bave digitalnim istragama, ali i inženjeri pri kreiranju softvera za rad s digitalnim dokazima u smislu vođenja lanca dokaza i dokazivanja očuvanja integriteta digitalnog dokaza (slika 45.).



Slika 45. Mogućnosti korištenja izgrađene ontologije

U ovom poglavlju biti će urađena provjera valjanosti (engl. *Consistency check*) i vrednovanje ontologije (engl. *Evaluation*). Vrednovanje i provjera valjanosti ontologije se može provesti na nekoliko različitih načina:

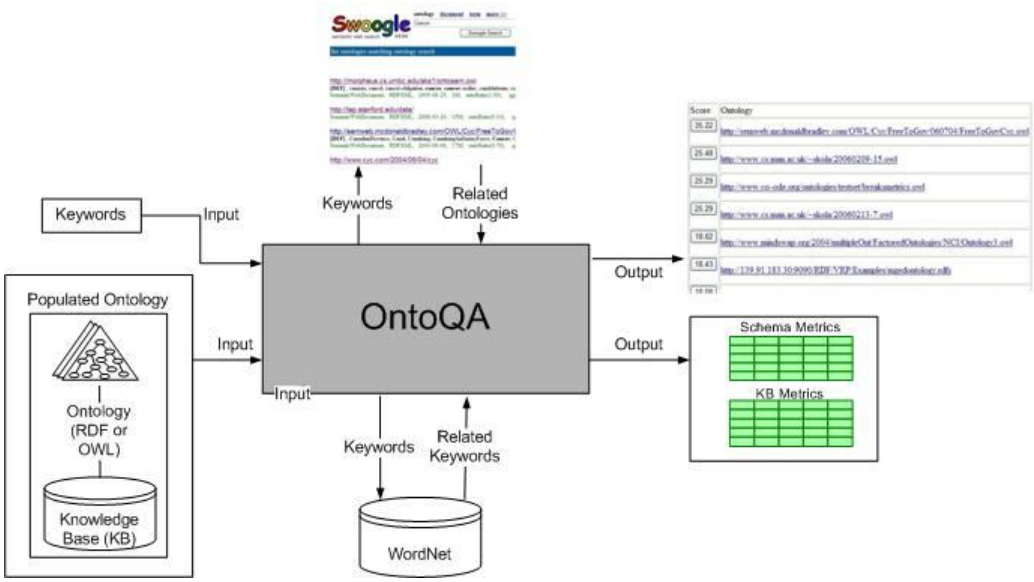
- Kroz sam alat za kreiranje ontologije
- Vrednovanje ontologije u nekom kontekstu
- Vrednovanje unutar nekog programa-aplikacije. To se još naziva i aplikacijski bazirano vrednovanje ontologije (engl. *Application based ontology evaluation*)
- Vrednovanje u kontekstu njene primjene i zadataka koje treba da obavlja. To se još naziva i vrednovanje temeljeno na zadaći (engl. *Taks based evaluation*) [124].

Uzimajući u obzir sve veći interes za razvoj sadržaja za tzv. semantički web, te sukladno tomu razvoj sve većeg broja ontologija iz različitih područja pojavila se potreba za razvoj metodologija i alata za evaluaciju istih. Glavni pravci u procesima razvoja evaluacijskih metoda Ontologija su sljedeći:

1. Evaluacija utemeljena na razvoju ontologije (engl. *Evolution based evaluation*)
   Ova vrsta evaluacija temelji se na praćenju promjena već razvijenih ontologija kroz vrijeme korištenja iste. Ontologija evoluira i mijenja se kroz vrijeme uglavnom iz tri sljedeća razloga:
   - promjene unutar domene Ontologije koje se ogledaju u nadodavanju sadržaja u vidu novih znanja iz predmetne domene
   - promjene u konceptualizaciji koje se ogledaju u promjeni načina ili pogleda na opis određenih koncepata u funkciji domenskih promjena.
   - promjene u eksplicitnim specifikacijama koje se ogledaju u eventualnoj promjeni implementacijskog alata ili jezika implementacije Ontologije
2. Logička evaluacija (engl. *Logical rule-based evaluation*)
   Ova vrsta evaluacija temelji se na validacije logičke strukture Ontologije na temelju ugrađenih (*built-in*) alata ili pravila (npr. *Reasoner*)
3. Evaluacija utemeljena na metrikama performansi (engl. *Metric feature based*)
   Ova vrsta evaluacija temelji se na parametrima performansi Ontologije sukladno domeni i namjeni same Ontologije. Većina tehnika kojima se koriste metodologije za ocjenu ovoga tipa temelje se na objedinjavanju određenih statističkih ovisnosti

parametara koji su definirani unutar same ontologije te koji opisuju znanje predmetne domene.

Za potrebe provjere konzistentnosti i evaluacije izrađene ontologije koristit će se dodatci koji se integriraju u sam Protége (*Pellet, OntoClean, OntoCheck, EvaluationTab*), te metoda OntoQA [125,126] koja će biti opisana u nastavku, a koja će se provjeravati aplikacijom koju su autori napisali u java programskom jeziku i koja se distribuira pod licencom otvorenog koda[36].



Slika 46. Arhitektura OntoQA metode[126][127]

Prema OntoQA metodi, metrika je podijeljena u dvije kategorije: metrika sheme (strukture) i metrika baze znanja (instanci) (slika 46.). Metrike sheme se bavi evaluacijom strukture ontologije, te potencijalom ontologije u predstavljanju specifičnih znanja dok se metrike baze znanja bavi evaluacijom dispozicije instanci podataka unutar ontologije te efektivnog korištenja znanja modeliranog kroz strukturu ontologije.

U nastavku slijedi opis obje kategorije metrike.

[36] http://tartir-ontoqa.googlecode.com/files/OntoQA.zip

8.1 METRIKA SHEME (STRUKTURE)

Metrika sheme (strukture) evaluira strukturu same ontologije. Nepostojanje standardne analize strukture ontologije onemogućava procjenu «korektnosti» strukture ontologije. Ova metrika postavlja temelje za evaluaciju bogatstva podacima, širine, dužine te dosljednost same strukture ontologije.

8.1.1 Bogatstvo vezama (engl. *Relationship Richness*)

Ova metrika reflektira različitost tipova relacija među podacima unutar ontologije. Ontologija koja ima samo vlastite ili strukturne relacije siromašnija je od one koja ima više različitih setova relacija. Parametar se računa pomoću indeksa koji nam pokazuje koliko je blizu ili je udaljena shema strukture od dijagrama taksonomije, te predstavlja raznolikost tipova relacija unutar ontologije i dobar je indikator bogatstva sheme. Ovaj indeks se izražava u postotku.

$$RR = \frac{|P|}{|SC| + |P|} \qquad [2]$$

Gdje je |P|: broj relacija, a |SC|: broj pod klasa

Kada u formulu unesemo podatke iz izrađene ontologije dobit će se vrijednosti:

DD Ontologija digitalnih dokaza	CoC Ontologija lanca dokaza
RR=21.64	RR=37.30

Prema dobivenim rezultatima evidentno je da je RR kod ontologije digitalnih dokaza bliži nuli (0.216) nego kod ontologije lanca dokaza gdje je on 0.37. Ovo indicira da je kod ontologije digitalnih dokaza većina relacija pod klase (IS-A veza).

8.1.2 Bogatstvo atributa (engl. *Attribute Richness*)

Broj atributa (*slots*) koji je definiran za svaku klasu može indicirati i kvalitetu dizajna ontologije i količinu informacija koje se odnose na instance podataka. Ovaj indeks pokazuje koliko informacija sadrže klase. Općeniti se može reći da ontologija koja sadrži više atributa koji su definirani, izražava više znanja.

$$AR = \frac{|att|}{|C|} \qquad [3]$$

Gdje je |att|: broj atributa literal-a , a |C|: broj klasa

Kada u formulu unesemo podatke iz izrađene ontologije dobit će se vrijednosti:

DD Ontologija digitalnih dokaza	CoC Ontologija lanca dokaza
AR=1.09	AR=1.40

Prema dobivenim podacima iz formule [3] evidentno je da je kod ontologije lanca dokaza vrijednost bogatstva atributima veća. Ontologija digitalnih dokaza ima nižu vrijednost (1.09) u odnosu na ontologiju lanca dokaza (1.40), što znači da su klase kod ontologije digitalnih dokaza u prosjeku siromašnije s atributima, te da generiraju manje znanja.

8.1.3 Bogatstvo nasljeđivanja (engl. *Inheritance Richness*)

Metrika bogatstva vlastite strukture (engl. *Inheritance*) opisuje distribuciju informacija među različitim razinama stabla strukture ontologije. Ona je dobar pokazatelj koliko je dobro znanje grupirano u različite kategorije i potkategorije u ontologiji. Ova mjera razlikuje vodoravnu ontologiju u kojoj klase imaju veliki broj direktnih pod klasa, te vertikalnu u kojoj klase imaju mali broj direktnih klasa. Ontologija sa malim indeksom bogatstva nasljeđivanja pokazuje da se radi o dubokoj ili vertikalnoj ontologiji koja pokriva specifičnu domenu, dok ontologija sa visokim indeksom pokazuje da se radi o površnoj ili horizontalnoj ontologiji koja indicira da

se radi o generalnoj ontologiji sa širokim spektrom općenitog znanja s niskom razinom detalja.

Generalno znanje (*spanning various domains*) vs. specifično

$$IR_S = \frac{\sum_{C_i \in C} \left| H^C \left(C_j, C_i \right) \right|}{|C|} \qquad [4]$$

Gdje je $|H^c(c_j, c_i)|$: broj pod-klasa klase C_i, a $|C|$: broj klasa

Kada u formulu unesemo podatke iz izrađene ontologije dobit će se vrijednosti:

DD Ontologija digitalnih dokaza	CoC Ontologija lanca dokaza
IR_S =3.35	IR_S =3.29

Kada se usporede rezultati dobiveni formulom [4] može se zaključiti da ontologija digitalnih dokaza ima nešto veći koeficijent bogatstva nasljeđivanja (3.35) nego ontologija lanca dokaza (3.29) što znači da je horizontalnost izraženija i da predstavlja više općeg generalnog znanja. U odnosu na nju kod Ontologije lanca dokaza vertikalnost je izraženija, ontologija je specifičnija, te izražava više specifičnog znanje.

8.2 METRIKA BAZE ZNANJA

Način na koji su podaci pozicionirani i distribuirani unutar ontologije također je važno mjerilo kvalitete ontologije, jer to može ukazivati na učinkovitost dizajna ontologije, te količine znanja iz stvarnog svijeta koje je pohranjeno u ontologiji. Metrika instance obuhvaća podatke koji opisuju bazu znanja kao cjelinu, i podatke koji opisuju način na koji se svaka klasa shema koristi u bazi znanja.

8.2.1 Bogatstvo klasa (engl. *Class Richness-CR*)

Ova metrika je povezana s time kako su instance distribuirane kroz klase definirane unutar ontologije. Broj klasa koje imaju instance u bazi znanja se usporedi s ukupnim brojem klasa, dajući opću predodžbu o tome koliko se dobro baza znanja koristi znanjem modeliranim shemom klasa. Dakle, ako baza znanja ima mali indeks bogatstva klasa, tada baza znanja nema podatke koji pokazuju sve znanje klasa koje postoji u shemi. S druge strane baza znanja koja ima velik indeks bogatstva klasa (CR) indicira da podaci pohranjeni u bazi znanja predstavljaju većinu znanja u shemi.

$$CR = \frac{|C'|}{|C|} \qquad [5]$$

Gdje je |C'|:broj klasa koje koriste a |C|: broj definiranih klasa

Kada u formulu unesemo podatke iz izrađene ontologije dobit će se vrijednosti:

DD Ontologija digitalnih dokaza	CoC Ontologija lanca dokaza
CR=38.28	CR=46.28

Prema rezultatima dobivenim iz [5] evidentno je da ontologija lanca dokaza (CR je 46.28) reprezentira mnogo više znanja nego ontologija digitalnih dokaza (CR je 38.28).

8.2.2 Prosječna populacija (engl. *Average Population*)

Prosječna populacija ili prosječna distribucija instanci kroz sve klase pokazuje broj instanci naspram broja klasa.

$$P = \frac{|I|}{|C|} \qquad [6]$$

Gdje je |I|: broj instanci, a |C|: broj definiranih klasa

Kada u formulu unesemo podatke iz izrađene ontologije dobit će se vrijednosti:

DD Ontologija digitalnih dokaza	CoC Ontologija lanca dokaza
P=0.12	P=0.25

Prosječna distribucija instanci kroz klase pokazuje da je ovaj koeficijent veći kod ontologije lanca dokaza (P=0.25) što ukazuje na to da je znanje pohranjeno u ovu ontologiju veće nego je to slučaj kod ontologije digitalnih dokaza (P=0.12). Obzirom da su instance izmišljene i kreirane su samo pojedinačne, a u cilju provjere funkcionalnosti same ontologije, vrijednosti dobivene ovom metrikom ne oslikavaju stvarno stanje.

8.3 ANALIZA REZULTATA DOBIVENIH ONTOQA METODOM:

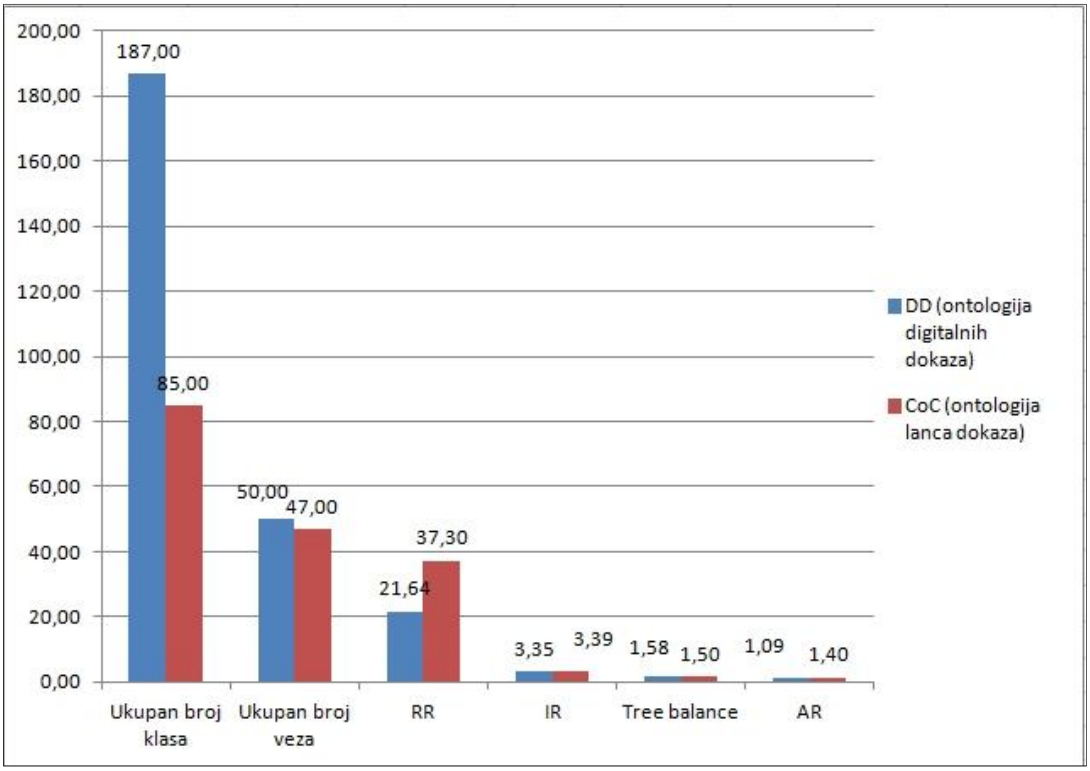
Rezultati dobiveni uz pomoć alata OntoQA predstavljeni su u nastavku u tablicama 8. i 9. i slikama 47. i 48.

Tablica broj 9. prikazuje metriku sheme DD Ontologije digitalnih dokaza i DD Ontologije lanca dokaza. Kratica RR (engl. *Relationship Richness*) predstavlja bogatstvo vezama, IR (engl. *Inheritance Richness*) bogatstvo nasljeđivanjem i AR (engl. *Atributte Richness*) bogatstvo atributa.

Tablica 9. Metrika sheme DD (Ontologije digitalnih dokaza) i CoC (Ontologije lanca dokaza)

Metrika sheme	DD (ontologija digitalnih dokaza)	CoC (ontologija lanca dokaza)
Ukupan broj klasa	187	85
Ukupan broj veza	50	47
RR (bogatsto vezama)	21.64	37.30
IR (bogatstvo nasljeđivanja)	3.35	3.39
Tree balance	1.58	1.50
AR (bogatstvo atributima)	1.09	1.40

Slika 47. predstavlja grafički prikaz poredbe dvije izrađene Ontologije - Ontologije digitalnih dokaza i lanca dokaza u metrici sheme. Evidentno je da se najveća razlika pojavljuje u ukupnom broju klasa, te bogatstvu vezama (RR).



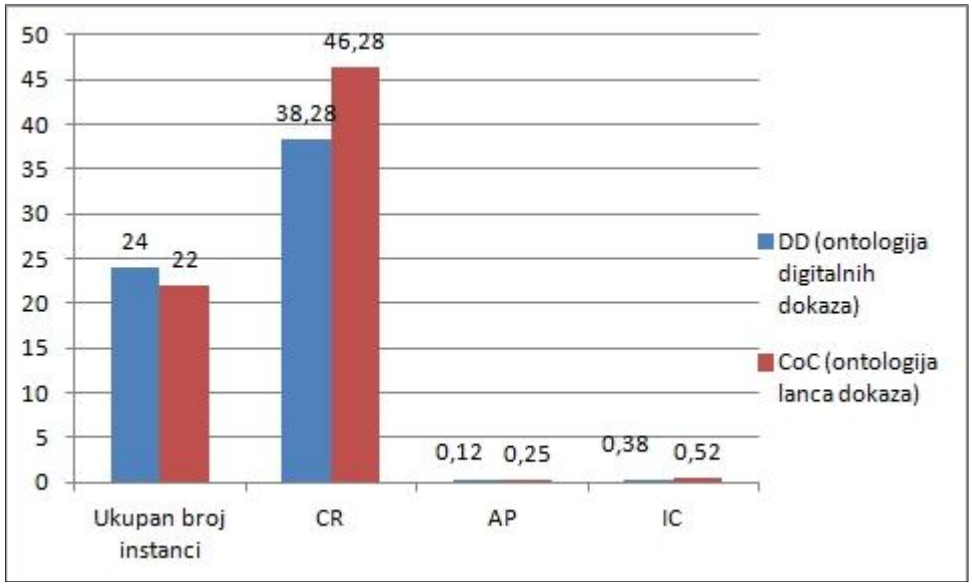
Slika 47. Grafički prikaz poredbe metrike sheme DD (Ontologije digitalnih dokaza) i CoC (Ontologije lanca dokaza)

Tablica broj 10. pokazuje metriku baze znanja, te poredbu dvije izrađene ontologije. Kratica CR (engl. *Class Richness*) predstavlja bogatstvo klasa, AP (engl. *Average Population*) je prosječna populacija i IC (engl. *Inheritance Richness*) pokrivenost instanci ili individua.

Tablica 10. Metrika baze znanja DD (Ontologije digitalnih dokaza) i CoC (Ontologije lanca dokaza)

Metrika baze znanja	DD (ontologija digitalnih dokaza)	CoC (ontologija lanca dokaza)
Ukupan broj instanci	24	22
CR (bogatstvo klasama)	38.28	46.28
AP (prosječna populacija)	0.12	0.25
IC (pokrivenost instanci)	0.38	0.52

Slika 48. predstavlja grafički prikaz poredbe dvije izrađene Ontologije - Ontologije digitalnih dokaza i lanca dokaza u metrici baze znanja. Najveća razlika se pojavljuje u bogatstvu klasama (CR).



Slika 48. Grafički prikaz poredbe metrike baze znanja DD (Ontologije digitalnih dokaza) i CoC (Ontologije lanca dokaza)

Na osnovu rezultata dobivenih proračunima korištenjem OntoQA metode može se zaključiti da je ontologija digitalnih dokaza uopćenija, više generalna, da sadrži veći broj koncepata, većina relacija su pod klase (IS-A veza), sa neznatno većim brojem atributa, ali i većim koeficijentom nasljeđivanja, što znači da je ontologija horizontalnija, sa generalno pohranjenim znanjem.

Suprotno dijametralno ontologija lanca dokaza je vertikalija, specijaliziranija, bogatija, u sebi ima sadržano pohranjeno specifično znanje. Isto tako prosječna distribucija instanci kroz klase pokazuje da je ovaj koeficijent veći kod ontologije lanca dokaza (P=0.25) što ukazuje na to da je znanje pohranjeno u ovu ontologiju veće nego je to slučaj kod ontologije digitalnih dokaza (P=0.15). Obzirom da su instance izmišljene i kreirane su samo pojedinačne, a u cilju provjere funkcionalnosti same ontologije, vrijednosti dobivene ovom metrikom ne oslikavaju stvarno stanje i podložne su promjenama.

8.4 Usporedba sa drugim recentnim i referentnim ontologijama

U nastavku (Tablice broj 11. i 12.) je urađena usporedba sa nekoliko referentnih ontologija. Podaci o metrikama ontologija SWETO, TAP, GlycO, KAOntology su preuzeti iz [126,127], dok su podaci o metrici CameraOntology ontologije preuzeti iz repozitorija Stanforskog Sveučilišta (http://protege.cim3.net/file/pub/ontologies/).

Tablica 11. Poredba izrađenih ontologija sa nekoliko drugih – poredba bogatstva klasama

Ontologija	Klase	Relacije	Instance	Bogatstvo klasama
SWETO[37]	44	101	813,217	59.100
TAP[38]	6.969	25	85.637	0.240
GlycO[39]	361	56	660	48.100
KAOntology[40]	96	0	0	71.420
CameraOntology[41]	10	15	2	25
CoC Ontologija	85	47	22	46.280
DD Ontologija	187	50	24	38.28

Usporedba je vršena sa nekoliko ontologija:

1. SWETO je generalna ontologija opće namjene. Pokriva nekoliko domena, publikacije, zemljopis, terorizam, udruženja.
2. TAP je ontologija izrađena na Stanford Sveučilištu , te je također ontologija opće namjene podijeljena u 43 pod-domene – sport, zemljopis, publikacije i sl.
3. GlycO je ontologija razvijena na Sveučilištu Georgija (Laboratorij za glikan).

[37] LSDIS' ontologija opće namjene – pokriva domenu publikacija, udruženja, zemljopisa i terorizam.

[38] Stanford's ontologija opće namjene. Podjeljena u 43 domene. Neke od domona su publikacije, sport i zemljopis.

[39] LSDIS' ontologija koncepta „Glycan Expression".

[40] Ontologija definira koncepte akademskih istraživanja. Autor je Ian Horrocks . (http://protegewiki.stanford.edu/wiki/Protege_Ontology_Library).

[41] OWL ontologija o dijelovima foto kamere (http://protegewiki.stanford.edu/wiki/Protege_Ontology_Library).

4. KAOntology je Ontologija definira koncepte akademskih istraživanja. Autor je Ian Horrocks
5. CameraOntology je ontologija koja pokriva domenu digitalnih kamera.

Prema rezultatima prikazanim u tablici 11. CR je najveći kod KAOntology ontologije što znači da podaci u bazi znanja ove ontologije predstavljaju najviše znanja u shemi. Ontologija lanca dokaza je prema rezultatima negdje u sredini između spomenutih ontologija.

Tablica 12. Poredba izrađenih ontologija sa nekoliko drugih – ostale metrike

Ontologija	Broj klasa	Broj instanci	Bogatstvo nasljeđivanja	Bogatstvo klasama	Prosječna populacija
SWETO	44	1,003,021	0.9	56.8%	22,795.9
TAP	3,230	71,487	1.2	9.4%	22.1
GlycO	356	387	1.3	18.0%	1.1
KAOntology	96	0	4.0	71.42	0.0
CameraOntology	10	2	2.5	25.0	0.2
DD Ontologija	187	24	3.35	38.28	0.12
CoC Ontologija	85	22	3.29	46.28	0.25

Prema rezultatima prikazanim u tablici 12. najgeneralnija ontologija je KAOntologija, dok su najspecifičnije, vertikalne SWETO, TAP i GlycO ontologije. DD Ontologija i CoC Ontologija također su relativno generalne. Prosječna populacija DD i CoC ontologija su u usporedbi sa ostalim ontologijama u tablici 12. negdje u sredini - vrijednosti su veće od PropreO, KAOntology, CameraOntology ali su manje od GlycO, TAP i SwetO ontologija. Sve vrijednosti izrađenih ontologija su u prihvatljivim granicama. U odnosu na ostale objavljene ontologije obje su ontologije horizontalne.

POGLAVLJE IX

9 ZAKLJUČAK I OTVORENA PITANJA

Predmet rada je uspostava i očuvanje lanca digitalnih dokaza (digitalnog lanca dokaza) i integriteta digitalnih dokaza u forenzičkoj analizi digitalnih uređaja. Ovo je aktivnost koja predstavlja veliki problem za osobe koje provode digitalne istrage unutar neke korporacije, banke, osiguravajućeg društva ili institucije. Razlog je taj što potencijalni digitalni dokaz neće postati dokaz sve dok ne bude prihvaćen od strane suda kao krajnje institucije, a u praksi je veoma teško očuvati njegov integritet. Osnovna svrha rada je bila znanstveno istraživanje koje će dati uvid u pregled samog koncepta digitalnog dokaza, te njegove glavne karakteristike – prihvatljivosti, metoda održanja lanca digitalnih dokaza i metoda zaštite integriteta digitalnih dokaza, te pojašnjenje pojma životnog ciklusa digitalnih dokaz.

Cilj je bio definiranje novih pravaca istraživanja u rješavanju problema dokazivosti lanca digitalnih dokaza primjenom ontologija digitalnih dokaza temeljenih na „DEMF“ (engl. *Digital Evidence Management Framework*) kroz koji bi se u svakom trenutku digitalne istrage točno znao odgovor na sva bitna pitanja sudionika u procesu digitalne istrage, ali bi se i osiguravao lanac dokaza. Krajnji cilj je bio formalni opis koncepata koji se javljaju u procesu upravljanja digitalnim dokazima, te pomoću izrađene ontologije digitalnih dokaza i odgovarajućeg modela, stvaranje temelja za učinkovitiji pristup izgradnji sustava u kojem bi se mogao uspostaviti i održati lanac dokaza te sačuvati integritet. Tematika vezana za realizaciju ciljeva prisutna je u razmatranju tijekom pisanja svih poglavlja rada. Cjelokupni rezultat istraživanja dat je u poglavljima 4,5,6,7 i 8.

Istraživačka pitanja koja je autor postavio i na koja je rad pokušao dati odgovor su:

1. Koji su to činitelji koji utječu na lanac digitalnih dokaza ?
2. Na koji način je moguće uspostaviti i sačuvati lanac dokaza u forenzičkoj analizi digitalnih uređaja, te očuvati integritet digitalnih dokaza ?
3. Opisati prijedlog modela koji bi omogućio da se u svim fazama digitalne forenzičke istrage zna odgovor na bitna pitanja: tko je, kada, zašto, gdje i na koji način dolazio u kontakt sa digitalnim dokazima ?

Odgovor na prvo pitanje je dan u poglavlju 4 gdje su opisivani modeli digitalne forenzičke istrage, modeliran je jedan generalni proces životnog ciklusa digitalnog dokaza u kom su identificirani svi činitelji koji imaju bilo kakav utjecaj na dokaze i dokazivost lanca dokaza. Na pitanje broj dva je dan odgovor u poglavljima 4, 6 i 7, ali se to pitanje provlači i kroz pisanje svih poglavlja disertacije. Uspostava i očuvanje lanca dokaza obaveza je institucije koja provodi digitalne istraga, te prezentiranje istog je obavezno pred Sudom odnosno Sudskim vijećem. To je praksa u razvijenim zemljama svijeta (SAD i EU) dok je situacija u okruženju (BiH) predstavljena u poglavlju broj 5. Prijedlog modela je dan u poglavljima 4, 6 i 7 gdje je formaliziran proces digitalne forenzičke istrage u jeziku ontologija OWL, te definirana i formirana pravila („*if-then rules"*) koja definiraju formalnu prihvatljivost i govore o tomu koji će dokaz biti formalno prihvatljiv a koji ne.

Hipoteze koje proizlaze iz istraživačkih pitanja su bile: **H1:** Uspostavom ontologije lanca digitalnih dokaza dobit će se referentni okvir za odlučivanje o formalnoj prihvatljivosti digitalnog dokaza, te **H2:** Temeljem ontologije digitalnog dokaza i meta podataka o konkretnom digitalnom dokazu, moguće je definirati pravila pomoću kojih će se moći zaključiti da li je taj dokaz formalno prihvatljiv.

Provjera H1 je detaljno elaborirana u poglavlju 6 i dijelom u poglavlju 7. Izgrađena je generalna horizontalna ontologija domene digitalnih dokaza koja je obuhvatila sve koncepte koji se javljaju u samom procesu, njihove odnose i svojstva. Ovim smo dobili okvir (*framework*) koja je osnova za nadogradnju za provjeru H2 koje je obrađena u poglavlju 7. Nakon definiranja glavnih koncepata, njihovih atributa i relacija, kreirane su instance te pravila (*rules*) koja formalno opisuju prihvatljivost digitalnih dokaza. Pravila su testirana, te je samo digitalni dokaz koji je ispunjavao sve uvjete mogao biti prihvatljiv. U teorijskom, prvom dijelu disertacije napravljen je pregled recentne literature iz područja digitalne forenzike i digitalnih dokaza, što je prepoznato kao jedan od značajnijih doprinosa ovog rada.

Društveni doprinos rada se očituje u primjeni rezultata znanstvenih istraživanja u rješavanju konkretnog problema u radu s digitalnim dokazima i prihvaćanju digitalnih dokaza kao takvih u korporacijama, vladinim institucijama, te organizacijama u kojima se provode digitalne forenzičke istrage, kako u intranet okružju, tako i u globalnoj mreži. Rezultati istraživanja će se moći koristiti kako za diseminaciju znanja iz područja digitalne forenzike, tako i za implementaciju konkretnog sustava temeljenog na predloženom okviru (DEMF) a što je već pokušavano u ranije citiranim radovima.

Analiza slučajeva iz prakse pokazuje da je danas skoro nemoguće održati lanac digitalnih dokaza i integritet digitalnog dokaza, te da se zbog toga sve češće digitalni dokazi ne prihvaćaju kao validni i takvi slučajevi se uopće ne procesuiraju ili se dokazi ne prihvaćaju kao relevantni. Istraživanjem i radom se stavio akcent na propuste koji se čine, te koji su znanstveno manje pokriveni u dostupnoj literaturi. Takav slučaj je i istraživanje provedeno u BiH a opisano u poglavlju broj 5. Upotrebom saznanja i izgrađenog okvira omogućeno je da se u svakoj fazi životnog ciklusa digitalnog dokaza ne samo održava njegov lanac nego i očuva njegov integritet, čime digitalni dokaz ne bi bio upitan.

Za razliku od dosadašnjih istraživanja, primjenom znanstvenih metoda i izrađenom ontologijom (lanca) digitalnih dokaza identificirani su, definirati i klasificirati osnovni pojmovi, te nakon toga izrađen model, te dat prijedlog rješenja moguće implementacije. Sveobuhvatni doprinos rada ogleda se u pregledu i analizi postojećih spoznaja iz područja istraživanja – digitalne forenzike odnosno lanca digitalnih dokaza, obuhvatu istraživanja, metodološkom pristupu kao i pojmovnim razgraničenjima. Razvijena ontologija digitalnih dokaza je prva faza u lancu narednih aktivnosti koje podrazumijevaju definiranje okvira te u konačnici izgradnju funkcionalnog sustava.

Znanstveni doprinos istraživanja se može odrediti kao: Identifikacija činitelja koji imaju presudan značaj na digitalne dokaze, ontološki opis činitelja koji će se upotrebljavati u okviru za postupanje lancem dokaza, izgradnja otvorenog okvira kao osnova za izgradnju sustava temeljenog na DEMF-u u kojem se može uspostaviti i očuvati lanac dokaza, razvoj nove metodologije, preporuke i smjernice za poboljšanje postojećih metoda i okvira za postupanje sa digitalnim dokazima, sistematizacija i diseminacija znanja iz područja digitalne forenzike.

9.1 Otvorena pitanja

Pitanje koje ostaje otvoreno je već spomenuto ograničenje okvira. Kada digitalni dokaz prođe jedan krug u svom životnom ciklusu, vrši se izračun sažetka (*hash funkcija*). Taj sažetak se pohranjuje i time osigurava 5Ws&1H. Kako i na koji način riješiti problem koji istražiteljima stvara „anti-forenzika“ kojom zlonamjerni korisnici na svaki mogući način pokušavaju kompromitirati forenzičku znanost, metode i alate a sve u cilju narušavanja integriteta i osporavanja kako lanca dokaza tako i cijele forenzičke istrage. Kako znati da je sažetak koji

se nalazi uz originalni digitalni dokaz uistinu originalni sažetak koji je nastao korištenjem okvira ili je krivotvoren? U daljem radu autor će se baviti proširenjem SWLR-a i uporabom neke od dostupnih funkcija kako bi se ovaj problem riješio, npr. *swrlb:stringEqualIgnoreCase (?x1,?x2)* ili *swrlb:equal (?x1,?x2)* kojima bi se vršila usporedba dva sažetka u dva ciklusa digitalnog dokaza, ukoliko vrijednosti sažetka nisu potpuno iste, neovisno od malih/velikih slova, izraz neće biti točan, te stoga niti digitalni dokaz neće moći biti prihvaćen.

PRILOZI

PRILOG A - popis Sudova u kojima je vršeno istraživanje

- Sud X0X310CY
- Sud X0X8CA1Y
- Sud X0X9155Y
- Sud X0X0FA4Y
- Sud X0X330FY
- Sud X0X3797Y
- Sud X0X66EBY
- Sud X0XEAC7Y
- Sud X0X68C0Y
- Sud X0XEBB4Y

PRILOG B – inicijalni dopis sudovima

Jasmin Ćosić
Doktorand Fakulteta Organizacije i Informatike
Sveučilišta u Zagrebu
Bihać, 25.03.2013.godine

PREDMET: ISTRAŽIVANJE NA TEMU FORMALNE PRIHVATLJIVOSTI DIGITALNIH DOKAZA I LANCA DOKAZA U SUDOVIMA U BIH,-

„Sud 0X310C“

„Adresa 0X61C14F81“

n/r Predsjednik-ca Suda

Poštovani,

Obraćam Vam se ovim putem da mi date odobrenje za provođenje znanstvenog istraživanja o digitalnim dokazima, formalnoj prihvatljivosti digitalnih dokaza i lancu dokaza u sudovima u BiH u Vašoj instituciji. Istraživanje ću vršiti kao Doktorand na Fakultetu Organizacije i Informatike Sveučilišta u Zagrebu, a isto će biti sastavni dio moje doktorske disertacije čije pisanje je odobrio Senat Sveučilišta u Zagrebu na sjednici održanoj dana 18.01.2013.godine (u prilogu).

Uposlen sam u MUP-u USK kao Šef Odjela za IT, a od 2008.godine sam Stalni sudski vještak IKT struke, imenovan od strane Federalnog Ministarstva Pravde BiH. Također sam angažiran kao predavač - asistent na grupi informatičkih predmeta na Pedagoškom fakultetu u Bihaću

(odsjek matematika-fizika). Član sam Asocijacije informatičara BiH, IEEE i ACM ogranka Jugoistočna Europa.

Svrha ovoga istraživanja je da se ustanovi na koji način sudovi u BiH prihvaćaju digitalne dokaze, te da li se vrši revizija "lanca dokaza" pri prihvaćanju, da li se postupa prema *Fry* ili *Daubertovom* principu ili na neki treći način. Odabrani i zamoljeni ste da učestvujete u istraživanju kao dio odabranog uzorka.

Samo popunjavanje ankete neće Vam oduzeti više od 20 minuta vremena, a samo učešće u anketi za Vas nema nikakvog rizika. Prilikom popunjavanja ankete i obrade rezultata pridržavati će se odredaba Zakona o zaštiti osobnih podataka, te ostale zakonske regulative u BiH. Svi podaci će biti korišteni isključivo u znanstvene svrhe i smatrat će se povjerljivim. Rezultati istraživanja biti će objavljeni isključivo u sklopu doktorske disertacije i nikako drugačije.

Učestvovanje u ovoj anketi neće Vam donijeti nikakvu direktnu materijalnu korist ali smatram da će rezultati ankete identificirati potrebe za dodatnom edukacijom, treninzima i obukama iz domena digitalnih dokaza. Ovo će donijeti korist svim Sudovima u BiH.

Rezultati istraživanja, anketni obrasci i ostalo vezano za istraživanje će se biti pohranjeno na mom lap-topu i prijenosnoj memoriji , zaštićeno, kriptirano i van dometa trećih lica i biti će uništeno nakon provedenog istraživanja.

Vaše učestvovanje u istraživanju je jako bitno i doprinijet će znanstvenoj zajednici i istraživanjima na temu digitalnih dokaza. Ukoliko imate bilo kakvih dodatnih pitanja , slobodno me kontaktirajte. Ukoliko imate bilo kakvih dodatnih pitanja vezano za Vaša prava kao sudionika u istraživanju molim kontaktirajte Fakultet Organizacije i Informatike, Sveučilišta u Zagrebu (prof.dr. Bača Miroslav ili doc.dr. Markus Schatten).

U narednih nekoliko dana možete očekivati sljedeći dopis i anketni obrazac koji treba da popune sve sudije iz Vaše institucije i vrate na moju adresu.

Hvala Vam

Pričitao/la sam i razumio/la ovaj dopis i informacije , te se slažem da institucija koju zastupam učestvuje u ovom projektu.
Stavljanjem Vašeg potpisa na ovaj Zahtjev i vraćanjem na adresu autora, dajete suglasnost za učestvovanje u istraživanju i prihvaćate da se slažete sa uvjetima navedenim u dopisu.

POTPIS I DATUM:

_____

Hvala !

S Poštovanjem !

Jasmin Ćosić, dipl.ing. IT
PhD Candidate FOI Varaždin
Adresa: Podgrmečka bb, 77240 Bosanska Krupa, BiH
e-mail: jascosic@gmail.com
gsm: 061/790-484

PRILOG C – dopis Sudovima, on-line anketa

ISTRAŽIVANJE NA TEMU PRIHVATLJIVOSTI DIGITALNIH DOKAZA U SUDOVIMA U BIH

Poštovani,

Ovim putem Vas zamoljavam da učestvujete u znanstvenom istraživanju o digitalnim dokazima i prihvatljivosti digitalnih dokaza u Sudovima u BiH. Istraživanje je prvo sa ovakvom tematikom u regionu, a vršit ću ga kao Doktorand na Fakultetu Organizacije i Informatike Sveučilišta u Zagrebu. Isto će biti sastavni dio moje doktorske disertacije čije pisanje je odobrio Senat Sveučilišta u Zagrebu na sjednici održanoj dana 18.01.2013.godine.

Svrha ovoga istraživanja je da se ustanovi na koji način sudci u BiH formalno prihvaćaju digitalne dokaze, te da li se vrši revizija "lanca dokaza" pri prihvaćanju, da li se postupa prema *Fry* ili *Daubertovom* principu ili na neki treći način. Odabrani i zamoljeni ste da učestvujete u istraživanju kao dio uzorka.

Samo popunjavanje ankete neće Vam oduzeti više od 15 minuta vremena, a samo učešće u anketi za Vas nema nikakvog rizika. Prilikom obrade rezultata istraživanja, pridržavati će se odredaba Zakona o zaštiti osobnih podataka, te ostale zakonske regulative. Svi podaci će biti korišteni isključivo u znanstvene svrhe i smatrat će se povjerljivim. Rezultati istraživanja biti će objavljeni isključivo u sklopu doktorske disertacije i nikako drugačije.

Učestvovanje u ovoj anketi neće Vam donijeti nikakvu direktnu materijalnu korist ali smatram da će rezultati ankete identificirati potrebe za dodatnom edukacijom, treninzima i obukama iz domena digitalnih dokaza. Ovo će donijeti korist svim Sudovima.

Rezultati istraživanja, anketni obrasci i ostalo vezano za istraživanje će se biti pohranjeno na mom lap-topu i prijenosnoj memoriji , zaštićeno, kriptirano i van dometa trećih lica, biti će uništeno nakon provedenog istraživanja.
Vaše učestvovanje u istraživanju je jako bitno i doprinijet će znanstvenoj zajednici i istraživanjima na temu digitalnih dokaza. Ukoliko imate bilo kakvih dodatnih pitanja , slobodno me kontaktirajte. Ukoliko imate bilo kakvih dodatnih pitanja vezano za Vaša prava kao sudionika u istraživanju molim kontaktirajte Fakultet Organizacije i Informatike, Sveučilišta u Zagrebu (prof.dr. Bača Miroslav ili doc.dr. Markus Schatten).

Poveznica na istraživanje je (molim da kliknete mišem na nju):

https://docs.google.com/forms/d/1Dkx3Z8HUTUSTS0ym9pztWkNfoXXqFmsSRFpFAfxPDtc/viewform

Hvala !

S Poštovanjem !

Jasmin Ćosić, dipl.ing. IT
PhD Candidate FOI Varaždin
Adresa: Podgrmečka bb, 77240 Bosanska Krupa, BiH
e-mail: jascosic@gmail.com
gsm: 061/790-484

PRILOG D – anketni obrazac

ISTRAŽIVANJE NA TEMU PRIHVATLJIVOSTI DIGITALNIH DOKAZA

PITANJA:

0. Da li ste se u svom dosadašnjem radu u sudnici susretali sa digitalnim dokazima (dokazi prikupljeni iz računara, mobilnih telefona, prijenosnih memorija, digitalnih foto-aparata kao što su fotografije, audio-video materijali, elektronski dokumenti i sl.)
    a. Da
    b. Ne

AKO JE ODGOVOR NA PITANJE **NE** MOLIM DA PRESKOČITE PITANJA 1-10 I PREĐETE NA POSLJEDNJE PITANJE (pitanje br.11) !

1. Ocijenite ocjenom od 1 do 5 Vaše poznavanje sljedećih tehnologija: (1-loše poznavanje, 5-odlično poznavanja):

    a. Hardware & Software (1,2,3,4,5)
    b. Internet i računarske mreže (1,2,3,4,5)
    c. Web tehnologije i E-mail komunikacija (1,2,3,4,5)
    d. Proces digitalne forenzičke istrage (1,2,3,4,5)
    e. Pojam digitalnih dokaza (1,2,3,4,5)

2. Koji faktori su bili ključni za Vaše poznavanje digitalnih dokaza iz pitanja br. 1e (osobna edukacija, edukacija putem sudskog vijeća, osobno iskustvo, treninzi kojima ste prisustvovao/la):

    _____

    _____

3. Da li smatrate da imate više, isto ili manje znanja, iskustva i/ili poznavanja digitalnih dokaza od Vaših kolega sudaca sa drugih općina :

    a. Više

b. Manje
c. Isto

4. Razmotrite sljedeću definiciju:

   „Digitalni dokazi se odnose na informacije ponuđene u pravnim postupcima za pomoć u procesu odlučivanja, koji proizlazi iz digitalnih izvora i procesa digitalne forenzičke istrage. Izvori digitalnih dokaza uključuju računare, muzičke plejere, kamere, PDA uređaje, mobilne telefone, prijenosne memorije i sl. kao i mrežnu opremu – Ip telefone, broadcasting servise, pružatelje mrežnih i internet usluga."

   Da li se slažete sa ovim definicijom (DA/NE)

   Ako je odgovor NE kako biste je dopunili/promijenili/sami definirali:

   _____
   _____
   _____

5. Da li prilikom odlučivanja i uzimanja u razmatranje digitalnih dokaza slijedite određeni standard (pravilo) ?
   a) DA (Fry/Daubert)
   b) DA (neko drugo pravilo, upisati koje)
      _____
   c) NE (odlučujemo na drugi način – opisati koji)

   _____
   _____
   _____

6. Da li postoji standard tehničkih kompetencija koje moraju imati tužitelj i odvjetnici ? Na koji način tehničko (ne)razumijevanje digitalnih dokaza od strane tužitelja i odvjetnika na raspravama kojima Vi predsjedavate utiče na Vašu odluku:

   _____
   _____
   _____

7. Da li je praksa da angažirate vještaka informacijsko-komunikacijske struke kao pomoć u pojašnjenju digitalnih dokaza u sudnici kojom predsjedavate ?

a) DA
    a. Da li je vještak kojeg angažirate sa službene liste vještaka koju sud objavljuje?
        i. DA
        ii. NE
b) NE

8. Da li Vam je poznat pojam „lanac digitalnih dokaza“ ili „lanac očuvanja digitalnih dokaza“ , odnosno „metode zaštite integriteta digitalnih dokaza“?
    a. DA
    b. NE

9. Da li ste, obzirom na jednostavnost manipulacije digitalnim dokazima u dosadašnjem radu insistirali na proceduri „dokazivanja lanca digitalnih dokaza“ tj. dokazivanju integriteta digitalnih dokaza?

    a. Da
    b. Ne

10. Gledajući sa aspekta prezentiranja digitalnih dokaza u sudnici kojom predsjedavate, koji faktori su odlučujući i najviše doprinose efikasnom prezentiranju digitalnih dokaza kao ključnih faktora vezanih za određeni slučaj ?

    _____

    _____

    _____

11. Opće informacije:
    a. Koliko imate godina ?
    b. Kojeg ste spola ?
    c. Koliko dugo ste sudac ?
    d. Koje je razine sud u kojem ste sudac (općinski/kantonalni/državni i sl.) ?
    e. Kolika je populacija stanovništva u općini/kantonu/regionu u kojoj se nalazi sud u kom radite ?

PRILOG E – dio izvornog kôda ontologije prikazan u manchester notaciji

```
################################################
#ONTOLOGIJA DIGITALNIH DOKAZA V.1.2 (C) 2014
#ZAPIS GLAVNIH KARAKTERISTIKA ONTOLOGIJE
#JE DAN U MANČESTER NOTACIJI
#CJELOKUPAN SOURCE CODE ĆE BITI JAVNO OBJAVLJEN
#U NEKOM OD JAVNO DOSTUPNIH REPOZITORIJA
################################################

Ontology: <http://www.semanticweb.org/DEMF>

Datatype: rdf:PlainLiteral

Datatype: xsd:string

Datatype: xsd:dateTime

##########################
#SVOJSTVA OBJEKATA
##########################

ObjectProperty: <http://www.semanticweb.org/DEMF#vodiIstragu>

    Characteristics:
        Functional

    Domain:
        <http://www.semanticweb.org/DEMF#vodiIstragu> min 0
<http://www.semanticweb.org/DEMF#Tuzitelj>

    InverseOf:
        <http://www.semanticweb.org/DEMF#jePodIstragom>


ObjectProperty: <http://www.semanticweb.org/DEMF#jeLicenciran>


    Characteristics:
        Functional

    Domain:
        <http://www.semanticweb.org/DEMF#Softver>


ObjectProperty: <http://www.semanticweb.org/DEMF#poznaje>


    Characteristics:
        Reflexive

    Domain:
        <http://www.semanticweb.org/DEMF#poznaje> some
<http://www.semanticweb.org/DEMF#Osoba>


ObjectProperty: <http://www.semanticweb.org/DEMF#jeVlasnik>
```

```
    Characteristics:
        InverseFunctional

    Domain:
        <http://www.semanticweb.org/DEMF#jeVlasnik> some
<http://www.semanticweb.org/DEMF#Osoba>,
        <http://www.semanticweb.org/DEMF#Osoba>

    Range:
        <http://www.semanticweb.org/DEMF#Hardver>


ObjectProperty: <http://www.semanticweb.org/DEMF#ocuvanIntegritet>


    Characteristics:
        Functional

    Domain:
        <http://www.semanticweb.org/DEMF#Integritet>

    InverseOf:
        <http://www.semanticweb.org/DEMF#narusenIntegritet>,
        <http://www.semanticweb.org/DEMF#nijePrihvatljiv>


ObjectProperty: <http://www.semanticweb.org/DEMF#nijePrihvatljiv>


    Range:
        <http://www.semanticweb.org/DEMF#DigitalniDokazNeprihvatljiv>

    InverseOf:
        <http://www.semanticweb.org/DEMF#jePrihvatljiv>,
        <http://www.semanticweb.org/DEMF#ocuvanIntegritet>


ObjectProperty: <http://www.semanticweb.org/DEMF#ispituje>


    Characteristics:
        Reflexive

    Domain:
        <http://www.semanticweb.org/DEMF#Osoba>

    Range:
        <http://www.semanticweb.org/DEMF#Osoba>


ObjectProperty: <http://www.semanticweb.org/DEMF#jeUposlenU>


    Characteristics:
        Functional
```

```
    Domain:
        <http://www.semanticweb.org/DEMF#Osoba>,
        <http://www.semanticweb.org/DEMF#jeUposlenU> min 0
<http://www.semanticweb.org/DEMF#Osoba>

    Range:
        <http://www.semanticweb.org/DEMF#Institucija>


ObjectProperty: <http://www.semanticweb.org/DEMF#jePronadjen>


    Characteristics:
        Functional

    Domain:
        <http://www.semanticweb.org/DEMF#jePronadjen> min 0
<http://www.semanticweb.org/DEMF#OriginalniDigitalniDokaz>

    InverseOf:
        <http://www.semanticweb.org/DEMF#nijePronadjen>


ObjectProperty: <http://www.semanticweb.org/DEMF#zastupa>


    Characteristics:
        Functional

    Domain:
        <http://www.semanticweb.org/DEMF#zastupa> min 1
<http://www.semanticweb.org/DEMF#Odbrana>,
        <http://www.semanticweb.org/DEMF#Odbrana>

    Range:
        <http://www.semanticweb.org/DEMF#Osumnjicenik>


ObjectProperty: <http://www.semanticweb.org/DEMF#imaLicencu>


    Characteristics:
        Functional

    Domain:
        <http://www.semanticweb.org/DEMF#Osoba>,
        <http://www.semanticweb.org/DEMF#imaLicencu> min 1
<http://www.semanticweb.org/DEMF#Osoba>

    Range:
        <http://www.semanticweb.org/DEMF#Softver>


ObjectProperty: <http://www.semanticweb.org/DEMF#nijePronadjen>


    InverseOf:
        <http://www.semanticweb.org/DEMF#jePronadjen>
```

```
ObjectProperty: <http://www.semanticweb.org/DEMF#jePrihvatljiv>


    Domain:
        <http://www.semanticweb.org/DEMF#VrstaDigitalnogDokaza>

    InverseOf:
        <http://www.semanticweb.org/DEMF#nijePrihvatljiv>


ObjectProperty: <http://www.semanticweb.org/DEMF#narusenIntegritet>



    InverseOf:
        <http://www.semanticweb.org/DEMF#ocuvanIntegritet>


ObjectProperty: <http://www.semanticweb.org/DEMF#donosiOdluke>


    Characteristics:
        InverseFunctional

    Domain:
        <http://www.semanticweb.org/DEMF#Sudac>

    Range:
        <http://www.semanticweb.org/DEMF#Prihvatljivost>


ObjectProperty: <http://www.semanticweb.org/DEMF#podizeOptuznicu>


    Characteristics:
        Functional

    Domain:
        <http://www.semanticweb.org/DEMF#Sudac>,
        <http://www.semanticweb.org/DEMF#podizeOptuznicu> exactly 1
<http://www.semanticweb.org/DEMF#Sudac>


ObjectProperty: <http://www.semanticweb.org/DEMF#imaOS>


    Domain:
        <http://www.semanticweb.org/DEMF#imaOS> min 1
<http://www.semanticweb.org/DEMF#Hardver>


ObjectProperty: <http://www.semanticweb.org/DEMF#predsjedavaVijecem>


    Characteristics:
        Functional
```

```
    Domain:
        <http://www.semanticweb.org/DEMF#predsjedavaVijecem> min 1
<http://www.semanticweb.org/DEMF#Sudac>,
        <http://www.semanticweb.org/DEMF#Sudac>

    Range:
        <http://www.semanticweb.org/DEMF#SudskaInstitucija>


ObjectProperty: <http://www.semanticweb.org/DEMF#traziIzuzece>

    Characteristics:
        Functional

    Domain:
        <http://www.semanticweb.org/DEMF#traziIzuzece> min 0
<http://www.semanticweb.org/DEMF#Osoba>,
        <http://www.semanticweb.org/DEMF#Osoba>


ObjectProperty: <http://www.semanticweb.org/DEMF#jeDio>


    Characteristics:
        Functional

    Domain:
        <http://www.semanticweb.org/DEMF#PravosudnaInstitucija>,
        <http://www.semanticweb.org/DEMF#VojnaInstitucija>,
        <http://www.semanticweb.org/DEMF#InstitucijaPrivatniSektor>,
        <http://www.semanticweb.org/DEMF#InstitucijaAkademskiSektor>

    Range:
        <http://www.semanticweb.org/DEMF#Institucija>


ObjectProperty: <http://www.semanticweb.org/DEMF#analizira>


    Characteristics:
        Functional

    Domain:
        <http://www.semanticweb.org/DEMF#SudskiVjestak>,
        <http://www.semanticweb.org/DEMF#PolicijskoOsoblje>,
        <http://www.semanticweb.org/DEMF#analizira> some
<http://www.semanticweb.org/DEMF#Osoba>

    Range:
        <http://www.semanticweb.org/DEMF#Izvor>


ObjectProperty: <http://www.semanticweb.org/DEMF#jePodIstragom>


    Domain:
```

```
        <http://www.semanticweb.org/DEMF#jePodIstragom> min 0
<http://www.semanticweb.org/DEMF#Osumnjicenik>

    InverseOf:
        <http://www.semanticweb.org/DEMF#vodiIstragu>


ObjectProperty:
<http://www.semanticweb.org/DEMF#pruzaUslugeKonzaltinga>


    Characteristics:
        Reflexive

    Domain:
        <http://www.semanticweb.org/DEMF#pruzaUslugeKonzaltinga> some
<http://www.semanticweb.org/DEMF#Osoba>,
        <http://www.semanticweb.org/DEMF#Osoba>


ObjectProperty: <http://www.semanticweb.org/DEMF#koristeAlate>

    Characteristics:
        Functional

    Domain:
        <http://www.semanticweb.org/DEMF#SudskiVjestak>,
        <http://www.semanticweb.org/DEMF#PrijateljSuda>,
        <http://www.semanticweb.org/DEMF#PolicijskoOsoblje>

    Range:
        <http://www.semanticweb.org/DEMF#ForenzickiAlat>


ObjectProperty: <http://www.semanticweb.org/DEMF#seNalazi>

    Characteristics:
        Functional

    Domain:
        <http://www.semanticweb.org/DEMF#OriginalniDigitalniDokaz>,
        <http://www.semanticweb.org/DEMF#seNalazi> some
<http://www.semanticweb.org/DEMF#OriginalniDigitalniDokaz>

    Range:
        <http://www.semanticweb.org/DEMF#Izvor>,
        <http://www.semanticweb.org/DEMF#Hardver>


ObjectProperty: <http://www.semanticweb.org/DEMF#jeIzuzetOd>

    Characteristics:
        Functional

    Domain:
        <http://www.semanticweb.org/DEMF#jeIzuzetOd> some
<http://www.semanticweb.org/DEMF#Hardver>,
        <http://www.semanticweb.org/DEMF#Hardver>
```

```
    Range:
        <http://www.semanticweb.org/DEMF#Osoba>


##########################
#SVOJSTVA PODATAKA
##########################


DataProperty: <http://www.semanticweb.org/DEMF#serijskiBroj>

    Domain:
        <http://www.semanticweb.org/DEMF#Hardver>

    Range:
        xsd:string


DataProperty: <http://www.semanticweb.org/DEMF#JMB>

    Domain:
        <http://www.semanticweb.org/DEMF#Osoba>

    Range:
        xsd:string


DataProperty: <http://www.semanticweb.org/DEMF#imaProceduruDokaza>

    Range:
        xsd:string


DataProperty: <http://www.semanticweb.org/DEMF#nazivAlata>

    Domain:
        <http://www.semanticweb.org/DEMF#ForenzickiAlat>

    Range:
        xsd:string


DataProperty: <http://www.semanticweb.org/DEMF#vrstaAlata>

    Domain:
        <http://www.semanticweb.org/DEMF#ForenzickiAlat>

    Range:
        xsd:string


DataProperty: <http://www.semanticweb.org/DEMF#imaFingerprint>

    Domain:
        <http://www.semanticweb.org/DEMF#Osoba>

    Range:
```

```
        xsd:string


DataProperty: <http://www.semanticweb.org/DEMF#IMEI>

    Domain:
        <http://www.semanticweb.org/DEMF#IMEI> exactly 1 xsd:string,
        <http://www.semanticweb.org/DEMF#MobilniTelefon>


DataProperty: <http://www.semanticweb.org/DEMF#datumRodjenja>

    Domain:
        <http://www.semanticweb.org/DEMF#Osoba>,
        <http://www.semanticweb.org/DEMF#datumRodjenja> exactly 1
xsd:dateTime

    Range:
        xsd:dateTime


DataProperty: <http://www.semanticweb.org/DEMF#nazivInstitucije>

    Domain:
        <http://www.semanticweb.org/DEMF#Institucija>

    Range:
        xsd:string


DataProperty: <http://www.semanticweb.org/DEMF#imaHashVrijednost>

    Domain:
        <http://www.semanticweb.org/DEMF#imaHashVrijednost> min 1
xsd:string,
        <http://www.semanticweb.org/DEMF#VrstaDigitalnogDokaza>

    Range:
        xsd:string


DataProperty: <http://www.semanticweb.org/DEMF#imaOS>

    Domain:
        <http://www.semanticweb.org/DEMF#Hardver>

    Range:
        xsd:string


DataProperty: <http://www.semanticweb.org/DEMF#ime>

    Domain:
        <http://www.semanticweb.org/DEMF#Osoba>

    Range:
        xsd:string
```

```
DataProperty: <http://www.semanticweb.org/DEMF#imaNaredbuSuda>

    Domain:
        <http://www.semanticweb.org/DEMF#imaNaredbuSuda> exactly 1
xsd:string,
        <http://www.semanticweb.org/DEMF#Osoba>

    Range:
        xsd:string


DataProperty: <http://www.semanticweb.org/DEMF#imaVrijemePristupa>

    Domain:
        <http://www.semanticweb.org/DEMF#Osoba>

    Range:
        xsd:string


DataProperty: <http://www.semanticweb.org/DEMF#adresaStanovanja>


    Domain:
        <http://www.semanticweb.org/DEMF#Osoba>


DataProperty: <http://www.semanticweb.org/DEMF#prezime>

    Domain:
        <http://www.semanticweb.org/DEMF#Osoba>

    Range:
        xsd:string


DataProperty: <http://www.semanticweb.org/DEMF#adresaInstitucije>

    Domain:
        <http://www.semanticweb.org/DEMF#Institucija>

    Range:
        xsd:string


DataProperty: <http://www.semanticweb.org/DEMF#brojIskaznice>

    Domain:
        <http://www.semanticweb.org/DEMF#brojIskaznice> exactly 1
xsd:string,
        <http://www.semanticweb.org/DEMF#Osoba>


DataProperty: <http://www.semanticweb.org/DEMF#imaRazlogPristupa>

    Domain:
        <http://www.semanticweb.org/DEMF#Osoba>,
```

```
        <http://www.semanticweb.org/DEMF#imaRazlogPristupa> exactly 1
xsd:string

    Range:
        xsd:string


DataProperty:
<http://www.semanticweb.org/DEMF#imaKoordinateMjestaDokaza>

    Domain:
        <http://www.semanticweb.org/DEMF#imaKoordinateMjestaDokaza> min
1 xsd:string,
        <http://www.semanticweb.org/DEMF#VrstaDigitalnogDokaza>

    Range:
        xsd:string


#########################
#KLASE
#########################


Class: <http://www.semanticweb.org/DEMF#ForenzickiAlat>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#koristeAlate> only
<http://www.semanticweb.org/DEMF#Institucija>,
        <http://www.semanticweb.org/DEMF#VrstaSoftvera>


Class: <http://www.semanticweb.org/DEMF#SDS>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MemorijskaKartica>


Class: <http://www.semanticweb.org/DEMF#FailOverKlaster>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Klaster>


Class: <http://www.semanticweb.org/DEMF#IgracaKonzola>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#ObskurniUredjaj>


Class: <http://www.semanticweb.org/DEMF#VojnaInstitucija>


    SubClassOf:
        <http://www.semanticweb.org/DEMF#Institucija>


Class: <http://www.semanticweb.org/DEMF#DigitalniDokazPrihvatljiv>
```

```
    SubClassOf:
        <http://www.semanticweb.org/DEMF#Prihvatljivost>

    DisjointWith:
        <http://www.semanticweb.org/DEMF#DigitalniDokazNeprihvatljiv>


Class: <http://www.semanticweb.org/DEMF#SIMKartica>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MobilniTelefon>


Class: <http://www.semanticweb.org/DEMF#Windows_Vista>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#NTJezgra>


Class: <http://www.semanticweb.org/DEMF#DigitalniDokazNeprihvatljiv>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Prihvatljivost>

    DisjointWith:
        <http://www.semanticweb.org/DEMF#DigitalniDokazPrihvatljiv>


Class: <http://www.semanticweb.org/DEMF#MicroSIM>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SIMKartica>


Class: <http://www.semanticweb.org/DEMF#SlucajniProlaznik>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Osoba>


Class: <http://www.semanticweb.org/DEMF#Windows_2000>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#NTJezgra>


Class: <http://www.semanticweb.org/DEMF#Windows_2003>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#NTJezgra>


Class: <http://www.semanticweb.org/DEMF#Enkripcija>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MetodaOcuvanjaIntegriteta>
```

```
Class: <http://www.semanticweb.org/DEMF#SymbianOS>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MobilniOS>


Class: <http://www.semanticweb.org/DEMF#AkademskiSektorEdukacija>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#InstitucijaAkademskiSektor>


Class: <http://www.semanticweb.org/DEMF#CompactFlash>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MemorijskaKartica>


Class: <http://www.semanticweb.org/DEMF#VisokeDostupnosti>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Klaster>


Class: <http://www.semanticweb.org/DEMF#TVsaHDD>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#UredjajZaSnimanje>


Class: <http://www.semanticweb.org/DEMF#Odbrana>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Osoba>,
        <http://www.semanticweb.org/DEMF#zastupa> min 1
<http://www.semanticweb.org/DEMF#Osumnjicenik>


Class: <http://www.semanticweb.org/DEMF#PravosudnaInstitucija>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Institucija>


Class: <http://www.semanticweb.org/DEMF#Klaster>

    SubClassOf:

<http://www.semanticweb.org/DEMF#DigitalniUredjajVelikihRazmjera>


Class: <http://www.semanticweb.org/DEMF#WindowsPhoneOSBaziran>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MobilniTelefon>
```

```
Class: <http://www.semanticweb.org/DEMF#Osoba>


Class: <http://www.semanticweb.org/DEMF#UredjajZaSnimanje>



    SubClassOf:
        <http://www.semanticweb.org/DEMF#ObskurniUredjaj>


Class: <http://www.semanticweb.org/DEMF#MiniPrenosnoRacunalo>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Racunalo>


Class: <http://www.semanticweb.org/DEMF#Racunalo>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Hardver>


Class:
<http://www.semanticweb.org/DEMF#SistemskiAdministratorIndustrija>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Industrija>


Class: <http://www.semanticweb.org/DEMF#Windows_ME>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#DOSjezgra>


Class: <http://www.semanticweb.org/DEMF#TabletPC>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Racunalo>


Class: <http://www.semanticweb.org/DEMF#KradjaIdentiteta>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#ForenzickaAnaliza>


Class: <http://www.semanticweb.org/DEMF#NajboljaKopijaDigitalnogDokaza>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#jePrihvatljiv> only
<http://www.semanticweb.org/DEMF#VrstaDigitalnogDokaza>,
        <http://www.semanticweb.org/DEMF#VrstaDigitalnogDokaza>


Class:
<http://www.semanticweb.org/DEMF#AkademskiSektorIstrazivanjeRazvoj>
```

```
    SubClassOf:
        <http://www.semanticweb.org/DEMF#InstitucijaAkademskiSektor>


Class: <http://www.semanticweb.org/DEMF#Wii>


    SubClassOf:
        <http://www.semanticweb.org/DEMF#SestaSedmaGeneracija>


Class: <http://www.semanticweb.org/DEMF#DVDRCableBox>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#UredjajZaSnimanje>


Class: <http://www.semanticweb.org/DEMF#DOSjezgra>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#WindowsBazirani>


Class: <http://www.semanticweb.org/DEMF#SudskaInstitucija>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#PravosudnaInstitucija>


Class:
<http://www.semanticweb.org/DEMF#DigitalniUredjajVelikihRazmjera>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Hardver>


Class: <http://www.semanticweb.org/DEMF#IndustrijskiPravniKontakt>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Industrija>


Class: <http://www.semanticweb.org/DEMF#NTJezgra>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#WindowsBazirani>


Class: <http://www.semanticweb.org/DEMF#IPod>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Mp3Plejer>


Class: <http://www.semanticweb.org/DEMF#Prihvatljivost>

    SubClassOf:
```

```
        <http://www.semanticweb.org/DEMF#Karakteristika>


Class: <http://www.semanticweb.org/DEMF#WindowsBazirani>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#RacunalniOS>


Class: <http://www.semanticweb.org/DEMF#Solaris>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#UnixBazirani>


Class: <http://www.semanticweb.org/DEMF#PolicijskoOsoblje>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#jeUposlenU> some
<http://www.semanticweb.org/DEMF#InstitucijaPolicijskaAgencija>,
        <http://www.semanticweb.org/DEMF#Osoba>


Class: <http://www.semanticweb.org/DEMF#Mp3Plejer>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#UredjajZaPohranu>


Class: <http://www.semanticweb.org/DEMF#InstitucijaPolicijskaAgencija>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#PravosudnaInstitucija>


Class: <http://www.semanticweb.org/DEMF#WiFi>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SpoljasniTvrdiDisk>


Class: <http://www.semanticweb.org/DEMF#Sveuciliste>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#AkademskiSektorEdukacija>


Class: <http://www.semanticweb.org/DEMF#MemorijskiModul>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MobilniTelefon>


Class: <http://www.semanticweb.org/DEMF#BlackBerryBaziran>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MobilniTelefon>
```

```
Class: <http://www.semanticweb.org/DEMF#LokalnaMreza_LAN>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Mreza>


Class: <http://www.semanticweb.org/DEMF#ObskurniUredjaj>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Hardver>


Class: <http://www.semanticweb.org/DEMF#MicroSDHC>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MemorijskaKartica>


Class: <http://www.semanticweb.org/DEMF#Unix>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#UnixBazirani>


Class: <http://www.semanticweb.org/DEMF#OtvoreniKôd>


Class: <http://www.semanticweb.org/DEMF#HandHeld>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#PDAUredjaj>


Class: <http://www.semanticweb.org/DEMF#InstitucijaPrivatniSektor>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Institucija>


Class: <http://www.semanticweb.org/DEMF#PrijateljSuda>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Osoba>,
        <http://www.semanticweb.org/DEMF#pruzaUslugeKonzaltinga> min 1
<http://www.semanticweb.org/DEMF#PravosudnaInstitucija>


Class: <http://www.semanticweb.org/DEMF#InstitucijaDrzavnaUprava>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#InstitucijaJavniSektor>


Class: <http://www.semanticweb.org/DEMF#BlackBerryOS>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MobilniOS>
```

```
Class: <http://www.semanticweb.org/DEMF#ZupanijskiSud>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SudskaInstitucija>


Class: <http://www.semanticweb.org/DEMF#Karakteristika>


Class: <http://www.semanticweb.org/DEMF#SaBalansiranjemOpterecenja>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Klaster>


Class: <http://www.semanticweb.org/DEMF#Podatkovni>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Grid>


Class: <http://www.semanticweb.org/DEMF#AndroidBaziran>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MobilniTelefon>


Class: <http://www.semanticweb.org/DEMF#FreeBSD>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#UnixBazirani>


Class: <http://www.semanticweb.org/DEMF#Industrija>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#InstitucijaPrivatniSektor>


Class: <http://www.semanticweb.org/DEMF#KazneniZakon>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#IndustrijskiPravniKontakt>


Class: <http://www.semanticweb.org/DEMF#DigitalniDokazIntegritetOcuvan>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Integritet>

    DisjointWith:

<http://www.semanticweb.org/DEMF#DigitalniDokazIntegritetNarusen>


Class: <http://www.semanticweb.org/DEMF#MobilniTelefon>
```

```
    SubClassOf:
        <http://www.semanticweb.org/DEMF#DigitalniUredjajMalihRazmjera>


Class: <http://www.semanticweb.org/DEMF#VrstaDigitalnogDokaza>


Class: <http://www.semanticweb.org/DEMF#NacinPlacanjaSoftvera>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Softver>


Class: <http://www.semanticweb.org/DEMF#PogonZaPohranuPodataka>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#UredjajZaPohranu>


Class: <http://www.semanticweb.org/DEMF#NanoSIM>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SIMKartica>


Class: <http://www.semanticweb.org/DEMF#PalmSized>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#PDAUredjaj>


Class: <http://www.semanticweb.org/DEMF#SudskoVjestacenje>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Konzalting>


Class: <http://www.semanticweb.org/DEMF#Softver>


Class: <http://www.semanticweb.org/DEMF#GameCube>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SestaSedmaGeneracija>


Class: <http://www.semanticweb.org/DEMF#MetodaOsiguranjaIntegriteta>


Class: <http://www.semanticweb.org/DEMF#Mrezni>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SpoljasniTvrdiDisk>


Class: <http://www.semanticweb.org/DEMF#KucniPlejer>
```

```
    SubClassOf:
        <http://www.semanticweb.org/DEMF#UredjajZaSnimanje>


Class: <http://www.semanticweb.org/DEMF#DigitalniPotpis>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MetodaOcuvanjaIntegriteta>


Class: <http://www.semanticweb.org/DEMF#Hardver>


    SubClassOf:
        <http://www.semanticweb.org/DEMF#Izvor>


Class: <http://www.semanticweb.org/DEMF#StolnoRacunalo>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Racunalo>


Class: <http://www.semanticweb.org/DEMF#MacOS>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#RacunalniOS>


Class: <http://www.semanticweb.org/DEMF#Playstation2>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SestaSedmaGeneracija>


Class: <http://www.semanticweb.org/DEMF#MicroSD>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MemorijskaKartica>


Class: <http://www.semanticweb.org/DEMF#Playstation3>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SestaSedmaGeneracija>


Class: <http://www.semanticweb.org/DEMF#Windows_NT>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#NTJezgra>


Class: <http://www.semanticweb.org/DEMF#UnixBazirani>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#RacunalniOS>
```

```
Class: <http://www.semanticweb.org/DEMF#SDCard>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MemorijskaKartica>


Class: <http://www.semanticweb.org/DEMF#UredjajZaPohranu>


    SubClassOf:
        <http://www.semanticweb.org/DEMF#Hardver>


Class: <http://www.semanticweb.org/DEMF#GlobalnaMreza_WAN>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Mreza>


Class: <http://www.semanticweb.org/DEMF#PrviNaLicuMjesta>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#PolicijskoOsoblje>


Class: <http://www.semanticweb.org/DEMF#USB>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SpoljasniTvrdiDisk>


Class: <http://www.semanticweb.org/DEMF#UredjajSaKamerom>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#UredjajZaSnimanje>


Class: <http://www.semanticweb.org/DEMF#SymbianBaziran>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MobilniTelefon>


Class:
<http://www.semanticweb.org/DEMF#DigitalniDokazIntegritetNarusen>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Integritet>

    DisjointWith:

<http://www.semanticweb.org/DEMF#DigitalniDokazIntegritetOcuvan>


Class: <http://www.semanticweb.org/DEMF#PlacanjeUslugom>

    SubClassOf:
```

```
        <http://www.semanticweb.org/DEMF#NacinPlacanjaSoftvera>


Class: <http://www.semanticweb.org/DEMF#VlasnikUredjaja>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Osoba>


Class: <http://www.semanticweb.org/DEMF#SDHC>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MemorijskaKartica>


Class: <http://www.semanticweb.org/DEMF#XBox360>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SestaSedmaGeneracija>


Class: <http://www.semanticweb.org/DEMF#GpsUredjaj>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#UredjajZaSnimanje>


Class: <http://www.semanticweb.org/DEMF#Konzalting>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#InstitucijaPrivatniSektor>


Class: <http://www.semanticweb.org/DEMF#VrstaSoftvera>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Softver>


Class: <http://www.semanticweb.org/DEMF#Dreamcast>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SestaSedmaGeneracija>


Class: <http://www.semanticweb.org/DEMF#WIndows_3.11>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#DOSjezgra>


Class: <http://www.semanticweb.org/DEMF#UvjetnoOtvorenKôd>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#DostupnostKôda>


Class: <http://www.semanticweb.org/DEMF#OS>
```

```
    SubClassOf:
        <http://www.semanticweb.org/DEMF#VrstaSoftvera>


Class: <http://www.semanticweb.org/DEMF#MobilniOS>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#jeDio> some
<http://www.semanticweb.org/DEMF#MobilniTelefon>,
        <http://www.semanticweb.org/DEMF#OS>


Class: <http://www.semanticweb.org/DEMF#ZatvoreniKôd>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#DostupnostKôda>


Class: <http://www.semanticweb.org/DEMF#OpcinskiSud>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SudskaInstitucija>


Class: <http://www.semanticweb.org/DEMF#FireWire>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SpoljasniTvrdiDisk>


Class: <http://www.semanticweb.org/DEMF#ForenzickaAnaliza>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Konzalting>


Class: <http://www.semanticweb.org/DEMF#Windows_98>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#DOSjezgra>


Class: <http://www.semanticweb.org/DEMF#PovratPodataka>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Konzalting>


Class: <http://www.semanticweb.org/DEMF#VremenskiZig>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MetodaOcuvanjaIntegriteta>


Class: <http://www.semanticweb.org/DEMF#SwapDatoteka>

    SubClassOf:
```

```
        <http://www.semanticweb.org/DEMF#PrivremenaMemorija>


Class: <http://www.semanticweb.org/DEMF#DigitalniUredjajMalihRazmjera>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Hardver>


Class: <http://www.semanticweb.org/DEMF#MemorijskaKartica>


    SubClassOf:
        <http://www.semanticweb.org/DEMF#MemorijskiModul>


Class: <http://www.semanticweb.org/DEMF#Izvor>


Class: <http://www.semanticweb.org/DEMF#ATA>


    SubClassOf:
        <http://www.semanticweb.org/DEMF#SpoljasniTvrdiDisk>


Class: <http://www.semanticweb.org/DEMF#SudskiVjestak>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#imaLicencu> some
<http://www.semanticweb.org/DEMF#ForenzickiAlat>,
        <http://www.semanticweb.org/DEMF#analizira> some
<http://www.semanticweb.org/DEMF#Izvor>,
        <http://www.semanticweb.org/DEMF#PrijateljSuda>,
        <http://www.semanticweb.org/DEMF#pruzaUslugeKonzaltinga> some
<http://www.semanticweb.org/DEMF#Institucija>


Class: <http://www.semanticweb.org/DEMF#PDAUredjaj>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#DigitalniUredjajMalihRazmjera>


Class: <http://www.semanticweb.org/DEMF#OdgovorNaIncident>

    SubClassOf:

<http://www.semanticweb.org/DEMF#SistemskiAdministratorIndustrija>


Class: <http://www.semanticweb.org/DEMF#Svjedok>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SlucajniProlaznik>


Class: <http://www.semanticweb.org/DEMF#RAM>
```

```
    SubClassOf:
        <http://www.semanticweb.org/DEMF#PrivremenaMemorija>


Class: <http://www.semanticweb.org/DEMF#Integritet>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Karakteristika>


Class: <http://www.semanticweb.org/DEMF#Windows_XP>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#NTJezgra>


Class: <http://www.semanticweb.org/DEMF#Vrtic>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#AkademskiSektorEdukacija>


Class: <http://www.semanticweb.org/DEMF#Istrazitelj>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#PolicijskoOsoblje>


Class: <http://www.semanticweb.org/DEMF#InstitucijaZdravstvo>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#InstitucijaJavniSektor>


Class: <http://www.semanticweb.org/DEMF#Linux>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#UnixBazirani>


Class: <http://www.semanticweb.org/DEMF#AndroidOS>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MobilniOS>


Class: <http://www.semanticweb.org/DEMF#Windows_7>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#NTJezgra>


Class: <http://www.semanticweb.org/DEMF#Windows_8>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#NTJezgra>
```

```
Class: <http://www.semanticweb.org/DEMF#Sudac>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Osoba>,
        <http://www.semanticweb.org/DEMF#jeUposlenU> some
<http://www.semanticweb.org/DEMF#SudskaInstitucija>,
        <http://www.semanticweb.org/DEMF#predsjedavaVijecem> min 1
<http://www.semanticweb.org/DEMF#SudskaInstitucija>


Class: <http://www.semanticweb.org/DEMF#Grid>

    SubClassOf:

<http://www.semanticweb.org/DEMF#DigitalniUredjajVelikihRazmjera>


Class: <http://www.semanticweb.org/DEMF#ZlonamjerniKorisnik>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SlucajniProlaznik>


Class: <http://www.semanticweb.org/DEMF#Racunalni>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Grid>


Class: <http://www.semanticweb.org/DEMF#Pronevjera>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#ForenzickaAnaliza>


Class: <http://www.semanticweb.org/DEMF#Prevara>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#ForenzickaAnaliza>


Class: <http://www.semanticweb.org/DEMF#CRC>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MetodaOcuvanjaIntegriteta>


Class: <http://www.semanticweb.org/DEMF#Windows_95>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#DOSjezgra>


Class: <http://www.semanticweb.org/DEMF#EkspertUDomeni>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#PrijateljSuda>
```

```
Class: <http://www.semanticweb.org/DEMF#PrenosnoRacunalo>


    SubClassOf:
        <http://www.semanticweb.org/DEMF#Racunalo>


Class: <http://www.semanticweb.org/DEMF#SestaSedmaGeneracija>


    SubClassOf:
        <http://www.semanticweb.org/DEMF#IgracaKonzola>


Class: <http://www.semanticweb.org/DEMF#SATA>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SpoljasniTvrdiDisk>


Class: <http://www.semanticweb.org/DEMF#InstitucijaObrana>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#PravosudnaInstitucija>


Class: <http://www.semanticweb.org/DEMF#DrzavniSud>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SudskaInstitucija>


Class: <http://www.semanticweb.org/DEMF#MetodaOcuvanjaIntegriteta>

    SubClassOf:

<http://www.semanticweb.org/DEMF#DigitalniDokazIntegritetOcuvan>


Class: <http://www.semanticweb.org/DEMF#InstitucijaJavniSektor>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Institucija>


Class: <http://www.semanticweb.org/DEMF#Scavenging>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Grid>


Class: <http://www.semanticweb.org/DEMF#PrivremenaMemorija>


    SubClassOf:
        <http://www.semanticweb.org/DEMF#Izvor>,
```

```
        <http://www.semanticweb.org/DEMF#jeDio> some
<http://www.semanticweb.org/DEMF#Hardver>


Class: <http://www.semanticweb.org/DEMF#Institucija>


Class: <http://www.semanticweb.org/DEMF#StarijeGeneracije>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#IgracaKonzola>


Class: <http://www.semanticweb.org/DEMF#ROM>


    SubClassOf:
        <http://www.semanticweb.org/DEMF#MemorijskiModul>


Class: <http://www.semanticweb.org/DEMF#DostupnostKôda>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Softver>


Class: <http://www.semanticweb.org/DEMF#NormalSIM>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SIMKartica>


Class: <http://www.semanticweb.org/DEMF#Tuzitelj>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#ispituje> min 1
<http://www.semanticweb.org/DEMF#Osumnjicenik>,
        <http://www.semanticweb.org/DEMF#Osoba>,
        <http://www.semanticweb.org/DEMF#vodiIstragu> some
<http://www.semanticweb.org/DEMF#Tuzitelj>


Class: <http://www.semanticweb.org/DEMF#RacunalniOS>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#jeDio> some
<http://www.semanticweb.org/DEMF#Racunalo>,
        <http://www.semanticweb.org/DEMF#OS>


Class: <http://www.semanticweb.org/DEMF#OstaliAplikativniSoftver>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#VrstaSoftvera>


Class: <http://www.semanticweb.org/DEMF#TrgovackiSud>
```

```
    SubClassOf:
        <http://www.semanticweb.org/DEMF#SudskaInstitucija>


Class: <http://www.semanticweb.org/DEMF#OriginalniDigitalniDokaz>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#jePrihvatljiv> only
<http://www.semanticweb.org/DEMF#VrstaDigitalnogDokaza>,
        <http://www.semanticweb.org/DEMF#VrstaDigitalnogDokaza>


Class: <http://www.semanticweb.org/DEMF#Windows_MediaCentar>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#NTJezgra>


Class: <http://www.semanticweb.org/DEMF#KopijaDigitalnogDokaza>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#jePrihvatljiv> only
<http://www.semanticweb.org/DEMF#VrstaDigitalnogDokaza>,
        <http://www.semanticweb.org/DEMF#VrstaDigitalnogDokaza>


Class: <http://www.semanticweb.org/DEMF#TiVo>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#UredjajZaSnimanje>


Class: <http://www.semanticweb.org/DEMF#SpoljasniTvrdiDisk>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#UredjajZaPohranu>


Class: <http://www.semanticweb.org/DEMF#FunkcijaSazetka>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MetodaOcuvanjaIntegriteta>


Class: <http://www.semanticweb.org/DEMF#Besplatni>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#NacinPlacanjaSoftvera>


Class: <http://www.semanticweb.org/DEMF#ZastitaPodataka>

    SubClassOf:

<http://www.semanticweb.org/DEMF#SistemskiAdministratorIndustrija>


Class: <http://www.semanticweb.org/DEMF#AIX>
```

```
    SubClassOf:
        <http://www.semanticweb.org/DEMF#UnixBazirani>


Class: <http://www.semanticweb.org/DEMF#Osumnjicenik>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#jePodIstragom> some
<http://www.semanticweb.org/DEMF#Osumnjicenik>,
        <http://www.semanticweb.org/DEMF#Osoba>


Class: <http://www.semanticweb.org/DEMF#Komercijalni>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#NacinPlacanjaSoftvera>


Class: <http://www.semanticweb.org/DEMF#VodeniZig>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MetodaOcuvanjaIntegriteta>


Class: <http://www.semanticweb.org/DEMF#XBox>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#SestaSedmaGeneracija>


Class: <http://www.semanticweb.org/DEMF#iOS>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MobilniOS>


Class: <http://www.semanticweb.org/DEMF#Skola>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#AkademskiSektorEdukacija>


Class: <http://www.semanticweb.org/DEMF#Posluzitelj>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Racunalo>


Class: <http://www.semanticweb.org/DEMF#InstitucijaDrzavnoOdvjetnistvo>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#PravosudnaInstitucija>


Class: <http://www.semanticweb.org/DEMF#Mreza>

    SubClassOf:
```

```
        <http://www.semanticweb.org/DEMF#Izvor>


Class: <http://www.semanticweb.org/DEMF#GradjanskaParnica>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#IndustrijskiPravniKontakt>


Class: <http://www.semanticweb.org/DEMF#IPhoneBaziran>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MobilniTelefon>


Class: <http://www.semanticweb.org/DEMF#WindowsPhoneOS>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MobilniOS>


Class: <http://www.semanticweb.org/DEMF#Internet>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#Mreza>


Class: <http://www.semanticweb.org/DEMF#JavaBaziran>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#MobilniTelefon>


Class: <http://www.semanticweb.org/DEMF#InstitucijaAkademskiSektor>

    SubClassOf:
        <http://www.semanticweb.org/DEMF#InstitucijaJavniSektor>


#########################
#INDIVIDUE
#########################


Individual: <http://www.semanticweb.org/DEMF#Istrazitelj_XY>

    Facts:
     <http://www.semanticweb.org/DEMF#prezime>
"Petronijević"^^xsd:string,
     <http://www.semanticweb.org/DEMF#ime>  "Saša"^^xsd:string,
     <http://www.semanticweb.org/DEMF#JMB>  "0507970125000"^^xsd:string


Individual: <http://www.semanticweb.org/DEMF#SudskiVještakIKT_XY>

    Types:
        <http://www.semanticweb.org/DEMF#SudskiVjestak>
```

```
    Facts:
     <http://www.semanticweb.org/DEMF#imaLicencu>
<http://www.semanticweb.org/DEMF#EnCase>,
     <http://www.semanticweb.org/DEMF#koristeAlate>
<http://www.semanticweb.org/DEMF#EnCase>,
     <http://www.semanticweb.org/DEMF#jeUposlenU>
<http://www.semanticweb.org/DEMF#CzBiF_FOI_Varazdin>,
     <http://www.semanticweb.org/DEMF#analizira>
<http://www.semanticweb.org/DEMF#HTCDesireZ>,
     <http://www.semanticweb.org/DEMF#ime>  "Jasmin"^^xsd:string,
     <http://www.semanticweb.org/DEMF#prezime>  "Ćosić"^^xsd:string,
     <http://www.semanticweb.org/DEMF#JMB>  "2607970111130"^^xsd:string


Individual: <http://www.semanticweb.org/DEMF#Sudac_XY>

    Types:
        <http://www.semanticweb.org/DEMF#Sudac>

    Facts:
     <http://www.semanticweb.org/DEMF#donosiOdluke>
<http://www.semanticweb.org/DEMF#DigitalniDokaz_2>,
     <http://www.semanticweb.org/DEMF#donosiOdluke>
<http://www.semanticweb.org/DEMF#Osumnjiceni_XY>,
     <http://www.semanticweb.org/DEMF#donosiOdluke>
<http://www.semanticweb.org/DEMF#DigitalniDokaz_1>,
     <http://www.semanticweb.org/DEMF#jeUposlenU>
<http://www.semanticweb.org/DEMF#ZupanijskiSudZagreb>,
     <http://www.semanticweb.org/DEMF#JMB>
"3101949132113"^^xsd:string,
     <http://www.semanticweb.org/DEMF#ime>  "Neven"^^xsd:string,
     <http://www.semanticweb.org/DEMF#prezime>  "Madić"^^xsd:string


Individual: <http://www.semanticweb.org/DEMF#DrzavniOdvjetnik_XY>

    Facts:
     <http://www.semanticweb.org/DEMF#podizeOptuznicu>
<http://www.semanticweb.org/DEMF#Osumnjiceni_XY>,
     <http://www.semanticweb.org/DEMF#prezime>
"Bogunović"^^xsd:string,
     <http://www.semanticweb.org/DEMF#ime>  "Miroslav"^^xsd:string,
     <http://www.semanticweb.org/DEMF#JMB>  "0101970124543"^^xsd:string


Individual: <http://www.semanticweb.org/DEMF#Branitelj_XY>

    Facts:
     <http://www.semanticweb.org/DEMF#zastupa>
<http://www.semanticweb.org/DEMF#Osumnjiceni_XY>,
     <http://www.semanticweb.org/DEMF#ime>  "Branislav"^^xsd:string,
     <http://www.semanticweb.org/DEMF#prezime>  "Mišić"^^xsd:string,
     <http://www.semanticweb.org/DEMF#JMB>  "0101967123221"^^xsd:string


Individual: <http://www.semanticweb.org/DEMF#ZupanijskiSudZagreb>

    Types:
```

```
        <http://www.semanticweb.org/DEMF#SudskaInstitucija>

    Facts:
     <http://www.semanticweb.org/DEMF#adresaInstitucije>  "Županijski
sud Zagreb
Trg Nikole Šubića Zrinskog 5
10000 Zabreb"^^xsd:string


Individual: <http://www.semanticweb.org/DEMF#Osumnjiceni_XY>

    Facts:
     <http://www.semanticweb.org/DEMF#jeUposlenU>
<http://www.semanticweb.org/DEMF#CaffeBar_Macak>,
     <http://www.semanticweb.org/DEMF#jeVlasnik>
<http://www.semanticweb.org/DEMF#HTCDesireZ>,
     <http://www.semanticweb.org/DEMF#JMB>
"1212957111130"^^xsd:string,
     <http://www.semanticweb.org/DEMF#ime>  "Miroslav",
     <http://www.semanticweb.org/DEMF#prezime>  "Barković"


Individual: <http://www.semanticweb.org/DEMF#CzBiF_FOI_Varazdin>

    Facts:
     <http://www.semanticweb.org/DEMF#adresaInstitucije>  "Pavlinska 2,
42000 Varaždin, Hrvatska"^^xsd:string


Individual: <http://www.semanticweb.org/DEMF#CaffeBar_Macak>

    Facts:
     <http://www.semanticweb.org/DEMF#seNalazi>
<http://www.semanticweb.org/DEMF#HTCDesireZ>,
     <http://www.semanticweb.org/DEMF#adresaInstitucije>  "Pavlinska 45
42000 Varaždin"


Individual: <http://www.semanticweb.org/DEMF#EnCase>

    Facts:
     <http://www.semanticweb.org/DEMF#vrstaAlata>
"komercijalni"^^xsd:string


Individual: <http://www.semanticweb.org/DEMF#HTCDesireZ>

    Types:
        <http://www.semanticweb.org/DEMF#MobilniTelefon>

    Facts:
     <http://www.semanticweb.org/DEMF#jeIzuzetOd>
<http://www.semanticweb.org/DEMF#Osumnjiceni_XY>,
     <http://www.semanticweb.org/DEMF#IMEI>  "35-209900-176148-
23"^^xsd:string,
     <http://www.semanticweb.org/DEMF#imaOS>  "Android
4.0"^^xsd:string,
```

```
     <http://www.semanticweb.org/DEMF#serijskiBroj>
"S/N:321543SBK32"^^xsd:string


Individual: <http://www.semanticweb.org/DEMF#DigitalniDokaz_1>

    Types:
        <http://www.semanticweb.org/DEMF#KopijaDigitalnogDokaza>,
        <http://www.semanticweb.org/DEMF#OriginalniDigitalniDokaz>,

<http://www.semanticweb.org/DEMF#NajboljaKopijaDigitalnogDokaza>

    Facts:
     <http://www.semanticweb.org/DEMF#seNalazi>
<http://www.semanticweb.org/DEMF#HTCDesireZ>,
     <http://www.semanticweb.org/DEMF#imaKoordinateMjestaDokaza>
"44°53′N 16°09′E"^^xsd:string,
     <http://www.semanticweb.org/DEMF#imaHashVrijednost>
"cb8d50487ca35f064a16471a0ca0722e898def84cb076c40903916a6223b3fdc"^^xsd
:string,
     <http://www.semanticweb.org/DEMF#imaProceduruDokaza>  "Pravilnik o
rukovanju digitalnim dokazima"^^xsd:string,
     <http://www.semanticweb.org/DEMF#imaRazlogPristupa>  "Naredba
Županijskog Suda 0013456/13 "^^xsd:string,
     <http://www.semanticweb.org/DEMF#imaFingerprint>
"09c68b804cb3eb5bef7ca31806b274adccad147533341cab4e677c61b004f6c"^^xsd:
string,
     <http://www.semanticweb.org/DEMF#imaVrijemePristupa>  "24.12.2012.
16:00 sati 24 sekunde"^^xsd:string


Individual: <http://www.semanticweb.org/DEMF#DigitalniDokaz_2>

    Types:
        <http://www.semanticweb.org/DEMF#KopijaDigitalnogDokaza>,
        <http://www.semanticweb.org/DEMF#DigitalniDokazNeprihvatljiv>

    Facts:
     <http://www.semanticweb.org/DEMF#seNalazi>
<http://www.semanticweb.org/DEMF#HTCDesireZ>,
     <http://www.semanticweb.org/DEMF#imaProceduruDokaza>  "Pravilnik o
prikupljanju digitalnih dokaza ",
     <http://www.semanticweb.org/DEMF#imaVrijemePristupa>  "21.12.2012.
16:45:55 SATI",
     <http://www.semanticweb.org/DEMF#imaRazlogPristupa>  "Naredba Suda
broj 01 000456 KT /13"

##########################
#PRAVILA
##########################

Rule:

<http://www.semanticweb.org/DEMF#KopijaDigitalnogDokaza>(?<urn:swrl#x>)
, <http://www.semanticweb.org/DEMF#imaHashVrijednost>(?<urn:swrl#x>,
?<urn:swrl#sha2>) ->
<http://www.semanticweb.org/DEMF#NajboljaKopijaDigitalnogDokaza>(?<urn:
swrl#x>)
```

```
Rule:

<http://www.semanticweb.org/DEMF#OriginalniDigitalniDokaz>(?<urn:swrl#x
>), <http://www.semanticweb.org/DEMF#imaFingerprint>(?<urn:swrl#x>,
?<urn:swrl#fp>),
<http://www.semanticweb.org/DEMF#imaHashVrijednost>(?<urn:swrl#x>,
?<urn:swrl#sha2>),
<http://www.semanticweb.org/DEMF#imaKoordinateMjestaDokaza>(?<urn:swrl#
x>, ?<urn:swrl#gps>),
<http://www.semanticweb.org/DEMF#imaProceduruDokaza>(?<urn:swrl#x>,
?<urn:swrl#proc>),
<http://www.semanticweb.org/DEMF#imaRazlogPristupa>(?<urn:swrl#x>,
?<urn:swrl#razl>),
<http://www.semanticweb.org/DEMF#imaVrijemePristupa>(?<urn:swrl#x>,
?<urn:swrl#ts>) ->
<http://www.semanticweb.org/DEMF#DigitalniDokazPrihvatljiv>(?<urn:swrl#
x>)

Rule:

<http://www.semanticweb.org/DEMF#NajboljaKopijaDigitalnogDokaza>(?<urn:
swrl#x>),
<http://www.semanticweb.org/DEMF#imaHashVrijednost>(?<urn:swrl#x>,
?<urn:swrl#sha2>) ->
<http://www.semanticweb.org/DEMF#OriginalniDigitalniDokaz>(?<urn:swrl#x
>)

Rule:

    <http://www.semanticweb.org/DEMF#Hardver>(?<urn:swrl#x>),
<http://www.semanticweb.org/DEMF#Osumnjicenik>(?<urn:swrl#osum>),
<http://www.semanticweb.org/DEMF#jeIzuzetOd>(?<urn:swrl#x>,
?<urn:swrl#osum>) ->
<http://www.semanticweb.org/DEMF#OriginalniDigitalniDokaz>(?<urn:swrl#x
>)

Rule:
    <http://www.semanticweb.org/DEMF#PrijateljSuda>(?<urn:swrl#x>),
<http://www.semanticweb.org/DEMF#imaNaredbuSuda>(?<urn:swrl#x>,
?<urn:swrl#naredba>) ->
<http://www.semanticweb.org/DEMF#SudskiVjestak>(?<urn:swrl#x>)

Rule:

<http://www.semanticweb.org/DEMF#OriginalniDigitalniDokaz>(?<urn:swrl#x
>), <http://www.semanticweb.org/DEMF#imaHashVrijednost>(?<urn:swrl#x>,
"cb8d50487ca35f064a16471a0ca0722e898def84cb076c40903916a6223b3fdc") ->
<http://www.semanticweb.org/DEMF#DigitalniDokazIntegritetOcuvan>(?<urn:
swrl#x>)
```

REFERENCE

[1] Symantec, “Cyber Crime Report 2011,” *Cyber Crime Report 2011"*, 2011. [Online]. Dostupno: http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/. [Pristupano: 01-Nov-2011].

[2] E. Casey, *Digital evidence and computer crime: forensic science, computers and the Internet*. Academic Press, p. 690, 2004.

[3] E. Casey, *Digital evidence and computer crime-Third edition*. Academic Press, p. 807, 2011.

[4] V. Baryamureeba, T. Florence, “The Enhanced Digital Investigation Process Model,” *Asian Journal of Information Technology*, vol. 5, pp. 790–794, 2004.

[5] K. Michael, J. H. P. Eloff, M. S. Olivier, “UML modelling of digital forensic process models(DFPMs),” in *Proceedings of the ISSA 2008*, 2008.

[6] M. I. Ibrahim, A. Jantan, “A Secure Storage Model to Preserve Evidence in Network Forensic,” in *Communications in Computer and Information Science*, pp. 391–402, 2011.

[7] S. Perumal, “Digital Forensic Model Based On Malaysian Investigation Process,” *Journal of Computer Science*, vol. 9, no. 8, pp. 38–44, 2009.

[8] S. Ó. Ciardhuáin, “An Extended Model of Cybercrime Investigations,” *International Journal of Digital Evidence*, vol. 3, no. 1, pp. 1–22, 2004.

[9] M. Reith, C. Carr, G. Gunsch, “An Examination of Digital Forensic Models,” *International Journal of Digital Evidence*, vol. 1, no. 3, pp. 1–12, 2002.

[10] S. R. Selamat, R. Yusof, S. Sahib, “Mapping Process of Digital Forensic Investigation Framework,” *Journal of Computer Science*, vol. 8, no. 10, pp. 163–169, 2008.

[11] M. Kohn, “Framework for a Digital Forensic Investigation 1,” *Information Security South Africa (ISSA) 2006 from Insight to Foresight Conference*, 2006.

[12] J. Cosic, Z. Cosic, M. Baca, “‘ Chain of Digital Evidence ’ Based Model of Digital Forensic Investigation Process,” *International Journal of Computer Science and Information Security*, vol. 9, no. 8, pp. 18–24, 2011.

[13] C. L. T. Brown, *Computer evidence:Collection and Preservation*. Course Technology PTR, p. 546, 2009.

[14] D. Wyld, “The Most Important Chain of Custody: Improving Evidence Tracking with RFID,” 2009. [Online]. Dostupno: http://www.rfidglobal.org/News/2009-10/20091027145448135.html. [Pristupano: 05-Sep-2011].

[15] R. Yaeger, “Criminal computer forensics management,” in *Proceedings of the 3rd annual conference on Information security curriculum development InfoSecCD 06*, p. 168, 2006.

[16] Ministarstvo pravde SAD, Nacionalni institut pravde, “Digital evidence in the courtroom: A guide for preparing digital evidence for court presentation.”, 2003, [Online]. Dostupno: https://www.ncjrs.gov/pdffiles1/nij/211314.pdf [Pristupano: 05-Sep-2012].

[17] M. C. Calhoun, “Scientific evidence in court: Daubert or Frye,15 years later,” *Legal Backgrounder*, 2008.

[18] J. Cosic, Z. Cosic, and M. Baca, “Modeling Digital Evidence Management and Dynamics Using Petri Nets,” *Journal of Information and Organizational Sciences*, vol. 35, no. 1, pp. 545–549, 2011.

[19] J. Cosic, Z. Cosic, and M. Baca, “An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence,” *Journal of Information and Organizational Sciences*, vol. 35, no. 1, pp. 1–13, 2011.

[20] G. Giova, “Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems,” *International Journal of Computer Science and Network Security*, vol. 11, no. 1, 2011.

[21] H.M.Y., J. H. P. Hai-Cheng Chu, Li-Wei Wu, “Digital Trails Discovering of a GPS Embedded Smart Phone - Take Nokia N78 Running Symbian S60 Ver 3.2 for Example,” *SECURE AND TRUST COMPUTING, DATA MANAGEMENT, AND APPLICATIONS Communications in Computer and Information Science*, Vol. 187, pp. 41–49, 2011.

[22] U. A. D. Peter, “A Framework for Evidence Integrity Preservation in Virtualized Environment : A Digital Forensic Approach”, Magistarski rad, University of Bedfordshire, 2012.

[23] U. Peter, D. Ani, G. Epiphaniou, T. French, “A Novel Evidence Integrity Preservation Framework (EIPF) for Virtualised Environments : A Digital Forensic Approach,” in *The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013)*, 2013.

[24] T. F. Gayed, H. Lounis, M. Bari, “Cyber Forensics : Representing and (Im) Proving the Chain of Custody Using the Semantic web,” in *The Fourth International Conference on Advanced Cognitive Technologies and Application*, pp. 19–23, 2012.

[25] U. P. Daniel, G. Epiphaniou, “Safeguarding Forensic Integrity of Virtual Environment Evidence”, International Journal of Computer Applications, vol. 8, no.6, pp. 43–52, 2013.

[26] N. K.Nandhakumur, U. Aarwal, F. H., “Use of AFF4 ‘ Chain of Custody ’ - Methodology for Foolproof Computer Forensics Operation,” in *International Journal of Communication and Networking System,* vol.1, no.1, pp. 49–57, 2012.

[27] G. Mahoy, A. Anderson, B. Collie, O. DeVel, R. McKemmish, *Computer and Intrusion Forensics*. Artech House , Boston, London, 2003.

[28] M. Losavio, J. Adams, M. Rogers, “Gap Analysis: Judicial Experience and Perception of Electronic Evidence,” *Digital Forensic Practice*, vol. 1, no. 1, pp. 13–17, 2006.

[29] K. Frakes, M. Rogers, S. Martin, C. Scarborough, “Survey of Law Enforcement Perceptions Regarding Digital Evidence,” *International Federation for Information*

Processing Digital Library, Advances in Digital Forensics III, vol. 242, pp. 41–52, 2007.

[30] A. J. Menezes, P. C. Oorschot, S. A. Vanstone, *Handbook of applied cryprography*, CRC press, p.p. 816, 1997.

[31] J. Richter, N. Kuntze, C. Rudolph, "Security Digital Evidence," in *2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 119–130, 2010.

[32] H. Kozushko, "Digital Evidence," *Graduate seminar*, 2003, [Online]. Dostupno: http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Presentations/DigitalEvidence.pdf, [Pristupano: 01-Nov-2013].

[33] R. Zelenika, S. Zelenika, "Klasifikacija znanosti u fokusu metodologije i tehnologije znanstvenoga istraživanja," *Pomorski zbornik*, vol. 44, no. 2006, pp. 11–39, 2007.

[34] J. W. Creswell, *Research Design - Qualitative, Quantitative and Mixed Methods Approaches - Third Edition*. University of Nebraska - Lincoln, SAGE Publications, Inc, p. 296, 2009.

[35] M. Žugaj, K. Dumičić, and V. Dušek, *Temelji znanstvenoistraživačkog rada, Metodologija i metodika*. Varaždin: TIVA i FOI, 2006.

[36] US-CERT, "Computer forensic," 2008. [Online]. Dostupno: http://www.us-cert.gov/reading_room/forensics.pdf. [Pristupano: 01-Dec-2011].

[37] B. Pladna, "Computer Forensics Procedures, Tools, and Digital Evidence Bags : What They Are and Who Should Use Them," in *Computer Forensics Procedures, Tools, and Digital Evidence Bags 3*, pp. 1–15, 2009.

[38] A. Sammes, B. Jankinson, *Forensic Computing: A Practitioner's Guide (Practitioner Series)*. Springer-Verlag, NewYork, 2007.

[39] M. Pollit, A. Whiteledge, "Exploring Big Haystack,Data Mining and Knowledge Management," in *Advances in Digital Forensic II IFIP*, 2006.

[40] “Shorter Oxford English Dictionary (6th ed.),” 2007.

[41] S. Peisert, M. Bishop, K. Marzullo, “Computer forensics in forensis,” *ACM SIGOPS Operating Systems Review*, vol. 42, no. 3, p. 112, Apr. 2008.

[42] J. R. Vacca, *Computer forensics: computer crime scene investigation, Volume 1*. Charles River Media Inc., p. 832, 2005.

[43] M. Bača, *Uvod u računalnu sigurnost*. Varaždin: Narodne Novine Hrvatska, 2004.

[44] FBI-Federal Bureau of Investigaion, IOCE - International Conference for Digital Evidence, “Digital evidence standard and principles.” USA, 2000, [Online]. Dostupno: http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/, [Pristupano: 11-Nov-2012].

[45] “IOCE Principles and Definition,” *International Conference for Digital Evidence - IOCE Conference*, 1999. [Online]. Dostupno: http://www.ioce.org/core.php?ID=5, [Pristupano: 11-Nov-2012].

[46] Scientific Working Group on Digital Evidence (SWGDE) and IOCE, “Digital Evidence: Standards and Principles,” 1999. [Online]. Dostupno: http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm#Definitions. [Pristupano: 11-Nov-2011].

[47] J. Cosic, M. Bača, “Do We Have Full Control Over Integrity in Digital Evidence Life Cycle?,” in *32nd International Conference on Information Technology Interfaces (ITI), 2010*, pp. 429–434, 2010.

[48] J. Cosic and M. Bača, “(Im) Proving Chain of Custody and Digital Evidence Integrity with Time Stamp,” in Proceeding of 33rd International Convention, *MIPRO2010*, Cavtat, Hrvatska, 2010

[49] J. Cosic and M. Bača, “A Framework to (Im)Prove „Chain of Custody“ in Digital Investigation Process,” in *Proceedings of the 21st Central European Conference on Information and Intelligent Systems*, Varaždin, Hrvatska, 2010

[50] R. Yeager, “Criminal computer forensics management,” *Proceedings of the 3rd annual conference on Information security curriculum development - InfoSecCD ’06*, p. 168, 2006.

[51] National Institute of Justice (NIJ), “Crime Scene Investigation: Guides for Law Enforcement,” 2011. [Online]. Dostupno: http://www.nij.gov/topics/law-enforcement/investigations/crime-scene/guides/glossary.htm. [Pristupano: 30-Dec-2011].

[52] M. Nagaraja, “Investigators Chain of Custody in Digital Evidence Recovery,” *Indian Police Service*, pp. 1–7.

[53] FBI-Federal Bureau of Investigation, SWGIT, “Best Practices for Maintaining the Integrity of Digital Images and Digital Video,” 2007, [Online]. Dostupno: http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2008/index.htm/standards/2008_04_standards01.htm [Pristupano: 30-Dec-2011].

[54] J. Patzakis, “Maintaining The Digital Chain of Custody,” Guidance software, in *IFOSEC*, 2003, [Online]. Dostupno: http://www.infosec.co.uk/files/guidance_software_04_12_03.pdf, [Pristupano: 25-Feb-2012].

[55] J. Wegman, “Computer forensic:Admissibility of evidence in criminal cases,” *Journal of Legal, Ethical and Regulatory Issues*, 2010.

[56] C. Ball, “What judges should know about computer forensic,” in *National Workshop for District Judges II Boston,* pp. 1–19, 2010.

[57] G. C. Kessler, “Judges ’ Awareness , Understanding , and Application of Digital Evidence,” Doktorska disertacija, Graduate School of Computer and Information Science Nova Southeastern University, 2010.

[58] R. Rivest, “RFC 1231:The MD5 Message-Digest Algorithm,” 1992, [Online]. Dostupno: [Online]. Dostupno:

http://www.infosec.co.uk/files/guidance_software_04_12_03.pdf, [Pristupano: 25-Feb-2012], [Pristupano: 25-Feb-2012].

[59] C. S. Laboratory, N. I. S. and Technology, "FIPS-180 secure hash standard," 1993, [Online]. Dostupno: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf, [Pristupano: 25-Feb-2012].

[60] M. Stevens, B. De Weger, G. Schmitz, "On collisions for MD5," neobjavljeni magistarski rad, Eindhoven: Eindhoven Univeristy of Technology, 2007, Dostupno: http://www.win.tue.nl/hashclash/On%20Collisions%20for%20MD5%20-%20M.M.J.%20Stevens.pdf, [Pristupano: 23-Jun-2012] .

[61] S. L. Garfinkel, "Providing Cryptographic Security and Evidentiary Chain-of-Custody with the Advanced Forensic Format, Library, and Tools," *International Journal of Digital Crime and Forensics*, vol. 1, no. March, pp. 1–28, 2009.

[62] J. Huang, A. Yasinsac, P. J. Hayes, "Knowledge Sharing and Reuse in Digital Forensics," *Digital Investigation*, pp. 1–6, 2011.

[63] B. Schatz, A. Clark, "An open architecture for digital evidence integration," in *AusCERT Asia Pacific Information Technology Security Conference*, pp. 21–26, 2006.

[64] D. C. Harrill, R. P. Mislan, "A Small Scale Digital Device Forensics ontology," *Small Scale Digital Device Forensics Journal*, vol. 1, no. 1, pp. 1–7, 2007.

[65] H. Park, S. Cho, H. Kwon, "Cyber Forensics Ontology for Cyber Criminal Investigation," in *E-FORENSICS 2009 - 2nd International ICST Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia*, pp. 160 – 165, 2009.

[66] A. Brinson, A. Robinson, M. Rogers, "A cyber forensics ontology: Creating a new approach to studying cyber forensics," *Digital Investigation*, vol. 3, pp. 37–43, Sep. 2006.

[67] L. D. Carver, M. A. Hoss, "Weaving ontologies to support digital forensic analysis," in *ISI'09 Proceedings of the 2009 IEEE international conference on Intelligence and security informatics*, pp. 203–205, 2009.

[68] S. L. Garfinkel, “Digital forensics research: The next 10 years,” *Digital Investigation*, vol. 7, pp. 64–73, 2010.

[69] M. Swimmer, “Towards An Ontology of Malware Classes,” *John Jay College of Criminal Justice*, pp. 1–16, 2008.

[70] S. Raghavan, A. Clark, and G. Mohay, “FIA: An Open Forensic Integration Architecture for Composing Digital Evidence,” *Forensics in Telecommunications, Information and Multimedia*, vol. 8, Part I, pp. 83–94, 2009.

[71] D. Kahvedzic and T. Kechadi, “DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge,” *Digital Investigation*, vol. 6, pp. 23–33, Sep. 2009.

[72] N. Bartlow, “Establishing the Digital Chain of Evidence in Biometric Systems”, PhD Thesys, Virginija University, USA, 2009.

[73] N. Kuntze and R. Carsten, “Secure digital chain of evidence,” in *Sixth International Workshop on Systematic Approaches to Digital Forensic Engeneering*, 2011.

[74] P. Turner, “Applying a Forensic Approach to Incident Response, Network Investigation and System Administration using Digital Evidence Bags,” *Digital Investigation*, vol. 4, no. 1, pp. 30–35, 2007.

[75] DFRWS and CDESF Working Group, “Survey of Disk Image Storage Formats,” 2006, [Online]. Dostupno: http://www.dfrws.org/CDESF/survey-dfrws-cdesf-diskimg-01.pdf, [Pristupano: 12-Jun-2012]. .

[76] M. Cohen and B. Schatz, “Hash based disk imaging using AFF4,” *Digital Investigation*, vol. 7, pp. S121–S128, Aug. 2010.

[77] S. Garfinkel, D. Malan, K. Dubec, C. Stevens, and C. Pham, “Chapter 2 Advances Forensic Format: An Open, Extensible Format For Disk Imaging,” *Advances in Digital Forensic II IFIP*, 2006.

[78] P. Turner, “Unification of digital evidence from disparate sources (Digital Evidence Bags),” *Digital Investigation*, vol. 2, no. 3, pp. 223–228, Sep. 2006.

[79] “Guidance Software, EnCase Forensic.” [Online]. Dostupno: http://www.guidancesoftware.com/. [Pristupano: 10-Oct-2011].

[80] “Gfzip file format specification version 1.0.” [Online]. Dostupno: http://gfzip.nongnu.org/filespec.html. [Pristupano: 01-Dec-2011].

[81] “Technology Pathways, ProDiscover Image File Format.” [Online]. Dostupno: http://www.techpathways.com/DesktopDefault.aspx?tabindex=7&tabid=14. [Pristupano: 12-Dec-2011].

[82] “ASR Data Acquisition and Analysis, SMART.” [Online]. Dostupno: http://www.asrdata.com/forensic-software/smart-linux/. [Pristupano: 01-Nov-2011].

[83] M. Joachim, “Expert Witness Compression Format specification,” *ASR Data*. ASR Data, 2011.

[84] C. Prosise, M. Kevin, *Incident Response&Computer Forensics, Second Edition*, McGraw-Hil. McGraw-Hill/Osborne, p. 548, 2003.

[85] International Conference for Digital Evidence, “Guidelines for best practice in the forensic examination of digital technology,” 2009, [Online]. Dostupno: http://cryptome.org/2014/03/forensic-digital-best-practice.pdf. [Pristupano: 01-Nov-2011] .

[86] “Reference dictionary.” [Online]. Dostupno: http://dictionary.reference.com/browse/framework. [Pristupano: 16-Aug-2013].

[87] H. Lee, T. Palmbach, M. Miller, *Henry Lee Crime Scene Handbook*. Elsevier Publisher,Academic press, 2001, p.p.411.

[88] P. G. Bradford, D. A. Ray, C. R. May, “An Online Algorithm for Generating Fractal Hash Chains Applied to Digital Chains of Custody ∗,” *ArXiv-Cryptography and Security*, vol. 2007, pp. 1–30, 2008.

[89] K. Kent, S. Chevalier, T. Grance, H. Dang, “Guide to Integrating Forensic Techniques into Incident Response,” *National Institute of Standards and Technology*. [Online].

Dostupno: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf. [Pristupano: 16-Aug-2013].

[90] F. C. Freiling and B. Schwittay, "A Common Process Model for Incident Response and Computer Forensics," in *Proceeding of Conference on IT incident Management and IT Forensic*, 2007.

[91] J. Cosic and Z. Cosic, "Digitalna antiforenzika – manipulacija procesom digitalne istrage," in *TELFOR2010*, Beograd, Srbija, pp. 1204–1207, 2010.

[92] J. Cosic, Z. Cosic, and M. Baca, "(Il)Legal Aspects of Digital Antiforensic," in *Proceedings of the 22st Central European Conference on Information and Intelligent Systems*, Varaždin, Hrvatska, no. Il, 2011.

[93] H. M. Gail, "Best Practices for Digital Archiving An Information Life Cycle Approach," 2000. [Online]. Dostupno: http://www.dlib.org/dlib/january00/01hodge.html. [Pristupano: 01-Oct-2011].

[94] C. Hosmer, "Proving the Integrity of Digital Evidence with Time," *International Journal of Digital Evidence*, vol. 1, no. 1, pp. 1–7, 2002.

[95] Scientific Working Group on Imaging Technology, "Best Practices for Maintaining the Integrity of Digital Images and Digital Video," 2007.

[96] C. Hosmer, "Standardizing Digital Evidence Storage," *Communications of the ACM*, vol. 49, no. 2, p. 69, Feb. 2006.

[97] G. C. Kessler, "Judges Awareness, Understanding, and Application of Digital Evidence," Graduate School of Computer and Information Science, Nova Southeastern University, 2010.

[98] A. Frowen, "Computer Forensics In The Courtroom: Is An IT Literate Judge And Jury Necessary For A Fair Trial?," 2009. [Online]. Dostupno: http://www.intaforensics.com/Blog/Computer-Forensics-In-The-Courtroom-Is-An-IT-Literate-Judge-And-Jury-Necessary-For-A-Fair-Trial.aspx. [Pristupano: 22-Aug-2013].

[99] F. Cohen, "Challenges to Digital Forensic Evidence," *ASP Press*, 2008.

[100] S. Mason, “Judges and technical evidence,” in *The 2nd Internationa Conference on Cyberforensics Education and Training*, 2008.

[101] N. M. Zainudin, M. Merabti, D. Lewellyn-Jones, “A Digital Forensic Investigation Model for Online Social Networking,” 2010.

[102] O. S. Kerr, *Computer Crime Law, 2d (American Casebook)*. West; 2 edition, 2009, p. 843.

[103] M. Vujevic, *Uvođenje u znanstveni rad u području društvenih znanosti*. Zagreb: Informator, 1988.

[104] D. Rada, “Measure and control of non-response in a mail survey,” *European Journal of Marketing*, vol. 39, no. 1, pp. 16–32, 2005.

[105] T. Lawson, “A Conception of Ontology,” *The Cambridge Social Ontology*, pp. 1–24, 2004.

[106] T. R. Gruber, “A Translation Approach to Portable Ontology Specifications,” *Knowledge Creation Diffusion Utilization*, vol. 5, pp. 199–220, 1993.

[107] N. Guarino, “Formal Ontology and Information Systems,” in *Proceedings of FOIS’98*, no. June, pp. 3–15, 1998.

[108] A. J. Pretorius, “Ontologies - Introduction and Overview,” *Semantic technology and applications research laboratory*, pp. 1–13, 2004.

[109] W. N. Borst, “Construction of Engineering Ontologies for Knowledge Sharing and Reuse,” *Centre for Telematica and Information Technology*, no. University of Twenty, Enschede, The Netherlands, 1997.

[110] N. Guarino and P. Giaretta, “Ontologies and Knowledge Bases: Towards a Terminological Clarification,” no. IOS Press, Amsterdam, 1995.

[111] R. Jasper and M. Uschold, “A Framework for Understanding and Classifying Ontology Applications,” in *Twelfth Workshop on Knowledge Acquisition Modeling and Management KAW’99*, 1999.

[112] U. Mike and M. Gruninger, “Ontologies: Principles, Methods and Application,” *Knowledge Engineering Review*, vol. 11, no. 2, 2006.

[113] M. Schatten, “Zasnivanje otvorene ontologije odabranih segmenata biometrijske znanosti”, Magistarski rad, FOI, Sveučilište u Zagrebu, 2007.

[114] J. Cosic, Z. Cosic, and M. Baca, “The Necessity of Developing a Digital Evidence Ontology,” in *Central European Conference on Information and Intelligent Systems*, pp. 325–341, 2012.

[115] N. F. Noy and D. L. Mcguinness, “Ontology Development 101 : A Guide to Creating Your First Ontology,”, Knowledge System Laboratory Standford University, 2001.

[116] W. M. Submission, “SWRL: A Semantic Web Rule Language Combining OWL and RuleML.” [Online]. Dosatupno: http://www.w3.org/Submission/SWRL/. [Pristupano: 25-Nov-2013].

[117] O. M, “SWRL Language FAQ,” *ProtegeWiki*, 2013. [Online]. Dostupno: http://protege.cim3.net/cgi-bin/wiki.pl?SWRLLanguageFAQ. [Pristupano: 24-Nov-2013].

[118] M. Kuba, “OWL 2 and SWRL Tutorial,” Institute of Computer Science, Masaryk University, 2012.

[119] A. Meech, “Business Rules Using OWL and SWRL,” in in *Advances in Semantic Computing*, vol. 2, pp. 23–31, 2010.

[120] Clark&Parsia, “Pellet: OWL 2 Reasoner for Java.” [Online]. Dostupno: http://clarkparsia.com/pellet/. [Pristupano: 25-Nov-2013].

[121] E. Sirin, B. Parsia, B. C. Grau, A. Kalyanpur, and Y. Katz, “Pellet: A practical OWL-DL reasoner,” *Web Semantics: Science, Services and Agents on the World Wide Web*, vol. 5, no. 2, pp. 51–53, Jun. 2007.

[122] M. Horridge and S. Bechhofer, “The OWL API : A Java API for OWL Ontologies,” *Semantic Web journal*, pp. 1–11, 2010.

[123] I. Palmisano and O. A. Team, “The Rough Guide to the OWL API,” in *OWLED 2011*, 2011.

[124] D. Vrandečić, “Ontology Evaluation,” doktorski rad, Fakultaet fuer Wirtschaftswissenschaften des Karlsruher Instituts fuer Technologie (KIT), 2010.

[125] S. Tartir, I. B. Arpinar, “Ontology Evaluation and Ranking using OntoQA,” *International Conference on Semantic Computing (ICSC 2007)*, pp. 185–192, Sep. 2007.

[126] S. Tartir, I. B. Arpinar, M. Moore, A. P. Sheth, and B. Aleman-Meza, “OntoQA: Metric-Based Ontology Quality Analysis,” in *IEEE Workshop on Knowledge Acquisition from Distributed, Autonomous, Semantically Heterogeneous Data and Knowledge Sources*, 2005.

[127] S. Tartir, “Ontology-Driven Question Answering And Ontology Quality Evaluation,” doktorski rad, Universitiy of Georgia, 2009.

[128] M. Milosavljević and G. Grubor, *Istraga kompjuterskog kriminala*. Beograd: Univerzitet Singidunum, p.p.291, 2009.

ŽIVOTOPIS

Jasmin Ćosić rođen je 1970. godine u Bosanskoj Krupi u Bosni i Hercegovini, gdje je završio osnovnu školu i srednju školu. Zbog ratnih dešavanja 1992 godine prekida studij na Ekonomskom fakultetu Univerziteta u Banjaluci. Završetkom rata 1997. g. završava višu ekonomsku školu, te upisuje Fakultet informacionih tehnologija (FIT) Univerziteta u Mostaru, na kom uspješno i diplomira na temu „Izrada multimedijalnih materijala za predmet Računarske mreže – Projekt“. Od 2008. godine polaznik je Poslijediplomskog doktorskog studija na Fakultetu organizacije i informatike u Varaždinu. Uposlen je u Ministarstvu unutarnjih poslova Unsko-sanskog kantona u Bihaću, gdje je radio na poslovima inspektora za kripto-zaštitu, programera, šefa odjela za IT, načelnika sektora komunikacija, te načelnika sektora za IKT. Na Odsjeku za matematiku-fiziku, Pedagoškog fakulteta, Univerziteta u Bihaću od 2009. godine ima izbor u zvanje asistenta, te sudjeluje u izvođenju nastave iz kolegija informatika, aplikativni softver, baze podataka i algoritmi i programiranje. Od 2007. godine angažiran je kao vanjski suradnik (predavač) u edukativnom centru „Teledom“ gdje drži tečajeve po ECDL planu i programu. Suradnik je i najtiražnijeg BH časopisa „INFO“ iz Sarajeva, u kom je objavio preko 30 popularnih članaka iz domena digitalne forenzike, sigurnosti i privatnosti na internetu. Od 2013. godine interni je auditor za ISO9001/27002.

Od 2007. godine ekspert je Agencije za državnu službu (ADS FBiH Sarajevo) za informacione tehnologije. Na listi je eksperata za ICT Ministarstva pravde Unsko-sanske županije. Od strane Federalnog Ministarstva Pravde BiH (FMP BiH), nakon položenog stručnog ispita, imenovan je za stalnog sudskog vještaka za IKT. Od strane Federalnog Ministarstva Obrazovanja BiH (FMON BiH Sarajevo) postavljen je za recenzenta za školske udžbenike za znanstveno polje - informatika.

U proteklom periodu uspješno je pohađao profesionalne tečajeve ISO 9001/27002, IBM - Web service development - DataPower administration, Oracle - OCA, Oracle - OCP, Oracle PL/SQL, Oracle forms & reports, CEH (Certified Ethical Hacker), Microsoft SQL server, te Linux mrežna administracija.

Područja interesa su mu digitalna forenzika, informacijska sigurnost, baze podataka i baze znanja, te web tehnologije. Član je Udruge informatičara BiH, te ogranka IEEE i ACM, recenzent je u nekoliko znanstvenih časopisa, te konferencijskih zbornika (JITE, IJCSIS, JCTA, InSite) za domenu informacijske sigurnosti i digitalne forenzike.

Suradnik je „Centra za biometriju“ FOI-a u Varaždinu kao i „Centra za forenziku“ FUP u Sarajevu gdje je bio angažiran na nekoliko projekata i istraživanja. Sretno je oženjen i otac je dvije kćerke – Lejle i Zane.

POPIS RADOVA

KNJIGA:

1. **Ćosić, Jasmin:** Demistificirana Informatika, Grafičar, Bihać, ISBN: 978-9958-781-44-5, COBISS.BH-ID 18540038, Bosna i Hercegovina, 2010

ZNANSTVENI RADOVI

1. Ćosić, Z., **Ćosić, J**., Bača, M.: Biometric System Vulnerability as a Compromising Factor for Admissibility of Digital Evidence: Analysis and Improvement Proposal, JIOS-Journal of Information and Organization Science, VOL38-NO1, Croatia, 2013 (in press)
2. Bača, M.,**Ćosić, J.**,Ćosić, Z.: Social Networks Forensic Analysis, ITI2013-35th International Conference on Information Technology Interfaces, Cavtat/Dubronik-Croatia, 2013
3. **Ćosić, J.**, Ćosić, Z.: Chain of Custody and Life Cycle of Digital Evidence**,** JCTA - Journal of Computer Technology and Application 3, p.p. 126-129, USA, 2012
4. **Ćosić, J**., Ćosić, Z.: The Necessity of Developing an Digital Evidence Ontology, CECIIS2012 - Central European Conference on Information and Intelligent Systems - University of Zagreb – Croatia**,** 2012
5. **Ćosić, J**., Ćosić, Z.: Business impact analysis & methodology of risk analysis as the most important aspects within operational continuity process defining, TELFOR – Beograd, 2012
6. **Ćosić, J.**, Ćosić, Z., Bača, M.: Chain of digital evidence based model of digital forensic investigation process, IJCSIS- International Journal of Computer Science & Information Security 2011, VOL9-NO7, USA, 2011.
7. **Ćosić, J**., Ćosić, Z., Bača, M.: Modeling Digital Evidence Management and Dynamics Using Petri Nets, JCTA - Journal of Computer Technology and Application, USA, 2011

8. **Ćosić, J**., Ćosić, Z., Bača, M.: An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence, JIOS-Journal of Information and Organization Science, VOL35-NO1,Croatia, 2011
9. Ćosić, Z., **Ćosić, J.**, Bača, M.:Additive Model of Reliability of Biometric Systems with Exponential Distribution of Failure Probability, IJCSIS- International Journal of Computer Science & Information Security 2011, VOL9-NO6, USA, 2011.
10. Ćosić, Z., **Ćosić, J**., Bača, M.: Recovery function of Components of Additive model of Biometrics System Reliability in UML , IJCSIS- International Journal of Computer Science & Information Security 2011, VOL9-NO7, USA, 2011
11. **Ćosić, J.**, Ćosić, Z., Bača, M.: (Il)legal aspects of digital antiforensics , CECIIS 2011, Varaždin, Croatia, 2011
12. Ćosić, Z., **Ćosić, J.**, Bača, M.: Implementation as Integration Factor Of Business Consulting And Knowledge Management , INFOTEH, Jahorina, B&H, Vol.10, 2011
13. **Ćosić, J**., Bača, M.: Do We Have Full Control Over Integrity in Digital Evidence Life Cycle?, ITI2010-32nd International Conference on Information Technology Interfaces, Cavtat/Dubronik-Croatia
14. **Ćosić, J**., Bača, M.: Steganography and Steganalysis - Does Local Web Sites Contain "Stego" Contents?, ELMAR, Zadar, 2010
15. **Ćosić, J**., Bača, M.: (Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp, MIPRO2010-33rd International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija-Croatia, pp.171-175
16. Ćosić, Z.,Boban, M., **Ćosić, J.:** Risk Management & Business Continuity Plan as fundamental activites for an implementation and maintaining of Information Security Management Systems, TELFOR – Beograd, 2010
17. **Ćosić, J**., Ćosić, Z., Bača, M.: Digital antiforensic – manipulation with digital forensic, TELFOR – Beograd, Serbia, 2010
18. **Ćosić, J**.,Medić A.,: IT Governance and Security of Web Services at Bosnia and Herzegovina Local Level **,** CECIIS2010 - Central European Conference on Information and Intelligent Systems - University of Zagreb – Croatia**, 2010**
19. **Ćosić, J**., Bača, M.: A Framework to (Im)Prove „Chain of Custody" in Digital Investigation Process, CECIIS2010 - Central European Conference on Information and Intelligent Systems - University of Zagreb – Croatia, 2010

20. Medić, A., Golubović,A., **Ćosić,J**.: Integration of VoIP i PSTN platforms, MIPRO2010-33rd International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija-Croatia (On Croatian)
21. Medić, A.,Golubović, A.,**Ćosić, J**.: Security aspects of business Web 2.0 services , M&S2010, Čakovec-Croatia, 2010 (On Croatian)
22. **Ćosić, J**.,Medić, A.: Information security, standards and state in B&H Institution, M&S2010, Čakovec-Croatia,2010 (On Croatian)
23. **Ćosić, J**., Bača, M.: Stenanography and its implication of forensic investigation, INFOTEH, Jahorina, B&H, Vol.9 pp 861-864 (On Croatian)
24. **Ćosić, J**., Bača, M.: Computer forensic – broad aspects of its application , INFOTEH, Jahorina, B&H, Vol.9 pp 857-860 (On Croatian)
25. **Ćosić, J**., Džanić A.:Web 2.0 Services and their widespread application , 7th International Scientific Conference on Production Engineering, Development And Modernization Of Production, Egipat – Cairo
26. **Ćosić, J**.,Medić A.: eGovernment Maturity & eRediness at B&H Municipality, CECIIS2009- Central European Conference on Information and Intelligent Systems - University of Zagreb – Croatia, pp 395-401
27. **Ćosić, J.:** WEB 2.0 (Security, Reliability & Measurement), Central European Conference on Information and Intelligent Systems - University of Zagreb – Croatia, pp 235-241

STRUČNI RADOVI

1. Bača, M., **Ćosić, J**.: Prevencija računalnog kriminaliteta, Policija i sigurnost, Vol.22 No1, Zagreb, 2013
2. **Ćosić, J.** : Druga strana socijalnih mreža, CUC 2010 – CarNET korisnička konferencija, Split-Croatia, 2010
3. Preko 30 stručnih radova objavljenih u BIH informatičkom časopisu "INFO"