Forenzika baza podataka

Josip, Marijanović

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Josip Marijanović

FORENZIKA BAZA PODATAKA

ZAVRŠNI RAD

Varaždin, 2018.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Josip Marijanović

Matični broj: 44408/15 – R

Studij: Informacijski sustavi

FORENZIKA BAZA PODATAKA

ZAVRŠNI RAD

Mentor/Mentorica:

Izv. prof. dr. sc. Markus Schatten

Varaždin, 2018.

Josip Marijanović

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor potvrdio prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Tema završnog rada je teorija forenzika baza podataka te će teorijski koncepti napisani u završnom radu biti provedeni u praktičnom dijelu. Završni rad podijeljen je u pet glavnih poglavlja: Digitalna forenzika, Baza podataka, PostgreSQL, Forenzika baza podataka te na koncu Praktični dio. U poglavlju digitalna forenzika opisat će se digitalna forenzika kao jedna od grana forenzičkih znanosti, njezinom statusu, primjerima te kratkoj povijesti. U poglavlju Baza podataka objasnit će se osnovni teorijski koncepti baza podataka koji će biti potrebni za lakše shvaćanje kasnijih poglavlja. U poglavlju PostgreSQL opisat će se PostgreSQL kao jedan od mnogih sustava za upravljanje bazom podataka. U poglavlju forenzika baza podataka opisat će se forenzika baza podataka kao jedna od podvrsta digitalne forenzike. U poglavlju Praktični dio prikazat će se izrada praktičnog dijela završnog rada koji se temelji na teorijskim konceptima prethodnih poglavlja.

Ključne riječi: baze podataka, postgresql, forenzika, metapodaci

Sadržaj

1. Uvod

U današnje vrijeme sve su veći zahtjevi za digitalizacijom svih aktivnosti u kojima ljudi imaju neku ulogu. Prilikom digitalizacije tih aktivnosti postoji velika mogućnost da će se podaci korišteni u tim aktivnosti trebati spremati u neko „skladište“ pri čemu baza podataka mogu poslužiti kao jedno od rješenja. Iako baza podataka može biti jedno od jednostavnijih rješenja prilikom takvog postupka, održavanje ali i sama sigurnost baze mogu biti jedno od problematičnijih stavaka. Ako se dogodi neka havarija kao što je pad servera, neautorizirani pristup podacima ili slično, forenzičari mogu vlasnicima otkriti što se zapravo dogodilo. Pri tome im mogu pomoći različite metode i alati koji se koriste u digitalnoj forenzici, grani forenzičke znanosti specijalizirane za slučajeve ilegalnih radnji na digitalnim uređajima. Specifično za baze podataka postoji podvrsta digitalne forenzike naziva forenzika baza podataka koja je i predmet istraživanja ovog završnog rada.

Tema završnog rada je teorija forenzika baza podataka te će teorijski koncepti napisani u završnom radu biti provedeni u praktičnom dijelu. Završni rad podijeljen je u pet glavnih poglavlja: Digitalna forenzika, Baza podataka, PostgreSQL, forenzika baza podataka te na koncu Praktični dio. U poglavlju digitalna forenzika opisat će se digitalna forenzika kao jedna od grana forenzičkih znanosti, njezinom statusu, primjerima te kratkoj povijesti. U poglavlju Baza podataka objasnit će se osnovni teorijski koncepti baza podataka koji će biti potrebni za lakše shvaćanje kasnijih poglavlja. U poglavlju PostgreSQL opisat će se PostgreSQL kao jedan od mnogih sustava za upravljanje bazom podataka. U poglavlju forenzika baza podataka opisat će se forenzika baza podataka kao jedna od podvrsta digitalne forenzike. U poglavlju Praktični dio prikazat će se izrada praktičnog dijela završnog rada koji se temelji na teorijskim konceptima prethodnih poglavlja

2. Metode i tehnike rada

Za izradu završnog rada korištenu su sljedeći alati:

- Microsoft Word 2017 – https://www.office.com/
- PostgreSQL – https://www.postgresql.org/
- LightShot – https://app.prntscr.com/en/index.html
- pgAdmin 4 – https://www.pgadmin.org/download/pgadmin-4-windows/

2.1. Microsoft Word 2016

Microsoft Word 2016 je alat za pisanje, uređivanje i formatiranje teksta razvijen od strane Microsofta. Prva službena verzija alata izdana je 25.10.1983 pod nazivom Multi – Tool Word. Trenutna verzija je Microsoft Word 2016 te spada u paket Office 2016 u koji spadaju također i alati kao što su PowerPoint, Excel, Outlook i Access. Microsoft je najavio izlazak novog Office paketa 6.9.2017. godine. Najavljeni Office paket trebao bi imati naziv Office 2019 te se kao službeni datum izlaska vodi 1.10.2018. godine. Microsoft Word 2016 korišten je u izradi završnog rada upravo zbog svojih mogućnosti pisanja, uređivanja i formatiranja teksta ali i ogromnoj upotrebi na globalnoj razini što čini proučavanje i rješavanje problema lakom zadaćom. („*Microsoft Word*“, bez dat.)

2.2. PostgreSQL

PostgreSQL jedan je od mnogih sustava za upravljanje bazom podataka (SUBP) koji se koriste danas. Odabran je za izradu završnog rada upravo zbog svojih pogodnosti koje pruža prilikom forenzike nad bazama podataka. Pruža sistemske kataloge i informacijsku shemu koji mogu poslužiti za ekstrahiranje metapodataka. Više o PostgreSQL – u rečeno je u kasnijem poglavlju PostgreSQL.

2.3. LightShot

LightShot je alat za slikanje zaslona dostupan na Windows i Mac operacijskim sustavima. LightShot podržava sljedeće formate fotografija: .png, .bmp i .jpg. Alat korisniku nudi sljedeće mogućnosti: Mogućnost odabira područja na zaslonu koji se želi slikati, prijenos slikanog područja na LightShotov poslužitelj, mogućnost dijeljenja slikanog područja na društvene mreže kao što su Facebook, Twitter i Pinterest, automatski ispis slikanog područja, lokalno spremanje slikanog područja te uređivanje slikanog područja kao što je pisanje, potezanje crta, umetanje geometrijskih likova kao što je krug, kvadrat, trokut i tako dalje. Uz dostupnost na Windows i Mac operacijskim sustavima, LightShot također nudi i svoj dodatak za web preglednike Google Chrome, Mozilla Firefox, Internet Explorer te Operu. U svrhu izrade završnog rada LightShot je korišten primarno za lokalno spremanje fotografija te označavanje pojedinih bitnijih područja unutar označenog područja.(„*LightShot*“, bez dat.)

2.4. pgAdmin 4

pgAdmin4 jedan je od najpopularnijih platforma za administraciju i razvoj PostgreSQL baza podataka. Jedan od razloga je zbog toga jer spada u softver otvorenog koda. Također, pgAdmin 4 je prepun značajki koje olakšavaju korisnicima i administratorima lakšu uporabu baza podataka. Pisan je u programskim jezicima Python te JavaScript bibliotekom jQuery.

pgAdmin 4 softver je podržan na Windows, Linux te macOS operacijskim sustavima te je dizajniran za PostgreSQL 9.2 ili kasnije verzije PostgreSQL SUBP – a. Uz sve pogodnosti koje nudi, pgAdmin 4 dostupan je u vidu stolne (engl. *Desktop*) i Web aplikacije. Podržava većinu PostgreSQL kodiranja kao što su: SQL_ASCII, UNICODE / UTF – 8, ISO_8859_8, LATIN1 do LATIN10 verzije. Uz kodiranja, podržava i sve značajke PostgreSQL SUBP – a kao što su agregirajuće funkcije, kreiranje baza podataka, tablica, okidača, pogleda i tako dalje. pgAdmin4 uz sve navedeno nudi i. Odabran je zbog svojeg sučelja koje je veoma jednostavno za upotrebu te („*Features*“, bez dat.)

3. Digitalna forenzika

U ovom poglavlju obradit će se termini vezani uz digitalnu forenziku. U prvom potpoglavlju opisat će se sama definicija digitalne forenzike te će nakon toga biti trenutni status digitalne forenzike u današnjem svijetu odnosno status digitalne forenzike u forenzičkim znanostima. Nakon statusa će uslijediti kratka povijest te na kraju poglavlja primjeri korištenja digitalne forenzike.

3.1. Definicija digitalne forenzike

Digitalna forenzika je grana forenzičke znanosti čiji je cilj legalnim metodama prikupiti i obraditi podatke, odnosno dokaze pohranjene na nekom digitalnom mediju čija je svrha pohrana podataka, koji su vezani za neku vrstu ilegalnih aktivnosti.

(Ristić i Simeunović, 2013)

Prema (B., 2003) digitalna forenzika je upotreba znanstveno izvedenih i djelotvornih metoda kako bi se digitalni podaci izvedeni iz digitalnih izvora mogli prezentirati, sakupljati, potvrditi, identificirati, analizirati, interpretirati te dokumentirati u svrhu olakšavanja i/ili unapređivanja rekonstrukcije događaja čiji su korijeni kriminalne radnje i/ili neovlaštene radnje koje su dokazano ometale planirane operacije.

Digitalna forenzika je prema mišljenju znanstvenika i dalje relativno mlada znanost. U svojim začecima digitalna forenzika je bila smatrana kao računalna forenzika, no to se promijenilo nakon što su i ostale grane forenzike temeljene na digitalnim uređajima došle na vidjelo. Nakon toga, digitalna forenzika je postala znanost koja objedinjuje sve forenzičke znanosti koje svoje temelje nalaze u digitalnim uređajima, odnosno digitalnim medijima za pohranu podataka. (Reith i ostali, 2003)

3.2. Status digitalne forenzike

Zbog svog statusa relativno mlade znanosti, digitalna forenzika i dalje ne sadrži standardnu metodologiju koju bi znanstvenici mogli koristiti za konzistentne rezultate. Jedan od razloga je taj što digitalna forenzika mora biti modelirana tako da objedinjuje sve moguće vrste digitalnih uređaja, što uključuje i digitalne uređaje odnosno tehnologije koji će tek biti izumljeni. Ovaj razlog je jedna od temeljnih stavaka po kojima se digitalna forenzika razlikuje od računalne. Računalna forenzika zadužena je za „čupanje“ odnosno ekstrahiranje dokaza iz specifičnih postojećih platformi uz pomoć postojećih specifičnih metoda.

(Reith i ostali, 2003)

Iako je digitalna forenzika mlada znanost, postala je jedan od najvažnijih dijelova svake istrage. Alati koji se koriste kod digitalne forenzike postali su svakodnevnica analitičarima ali i ispitivačima koji su zaposleni ili u lokalnim ili u državnim zakonodavnim ustanova. No organizacije se sve češće susreću s podacima koji ne mogu biti analizirali ili ispitani današnjim alatima zbog mnogih razloga kao što su: šifriranje i nekompatibilnosti. Iako i dalje većina podataka može biti analizirana postojećim alatima, dolazi do velikih kašnjenja zbog razloga koji su usko povezani sa SUBP – om. (Garfinkel, 2010)

3.3. Povijest digitalne forenzike

Prema (Garfinkel, 2010.) digitalna forenzika je stara otprilike četrdeset godina. U ranim danima digitalne forenzike digitalna forenzika je bila u velikoj mjeri izvedena od strane računalnih stručnjaka koji su radili u bliskoj suradnji s pravnim tijelima. U ovom periodu postojala je ograničena potražnja za digitalnom forenzikom. Dokazi ostavljeni na sustavima na kojima se nalazi mnogo korisnika odjednom mogli su se oporaviti bez za to predviđenih alata za oporavljanje podataka. Veličina sekundarne memorije u to vrijeme je bila izrazito mala tako da su napadači sustava radili opsežne ispise podataka sustava tako da nije bilo potrebe za digitalnom forenzikom. Iako je danas računalno hakiranje ilegalno i jedan je od većih problema s kojima se digitalni forenzičari susreću, u ranim danima to nije bio slučaj jer računalno hakiranje u to vrijeme nije imalo status zločina te sustavi nisu bili podvrgnuti forenzičkim analizama.

Prema (Garfinkel, 2010.) rane dane digitalne forenzike obilježavali su:

- Raznolikost hardvera, softvera i aplikacija
- Stvaranje mnogih novih formata podatkovnih datoteka od je većina bila jako loše dokumentirana
- Jako veliko oslanjanje na centralizirana računalna postrojenja,
- Nedostatak formalnih procesa, alata i iskustva.

Nakon ranih dana digitalne forenzika uslijedilo je takozvano zlatno doba digitalne forenzike. Razdoblje između 1999. i 2007. godine predstavljalo je razdoblje u kojem je digitalna forenzika doživjela nagli rast popularnosti u odnosu na prošlost zbog toga jer se pomoću digitalne forenzike moglo „vidjeti“ u prošlost tako što su se mogli povratiti podaci koji su se do onda smatrali izbrisanim ali i zbog toga jer se moglo „vidjeti“ u kriminalne umove pomoću oporavljanja izbrisane e – mail pošte i poruka. Za vrijeme zlatnog doma porasli su također i istraživanja digitalne forenzike u fakultetskim krugovima.(Garfinkel, 2010.)

Garfinkel je naveo da je 2010. godine 14 fakulteta nudilo certifikate i programe specijalizirane za digitalnu forenziku, 5 ih je nudilo programe specijalizirane za suradnike, 16 prvostupanjskih programa, 13 diplomskih programa te 2 doktorska programa. (Garfinkel, 2010.)

Prema (Garfinkel, 2010.) zlatno doba digitalne forenzike obilježavali su:

- Široka primjena Microsoftova operacijskog sustava Windows XP
- Relativno malo datotečnih formata koji su bili od interesa forenzičara – Microsoft Office za tekstualne dokumente, JPEG za digitalne fotografije te ANVI i WMV za video datoteke
- Istrage su većinom bile ograničene na jedan računalni sustav koji je pripadao osumnjičenom u istrazi
- Mediji za pohranu podataka sadrže standardna sučelja (ATA, IDE) te su povezani s ostalim komponentama s uklonjivim kabelima i priključcima te osigurani uklonjivim vijcima
- Više dobavljača koji prodaju alate koji su relativno dobri u oporavljanju alociranih i obrisanih datoteka

Nakon zlatnog doba uslijedila je kriza digitalne forenzike koja traje sve do danas. Jedan od glavnih razloga je taj što je sav napredak iz prošlosti danas gotovo pa zanemariv zbog brzine mijenjanja i unaprjeđivanja digitalnih tehnologija. (Garfinkel, 2010.)

Prema (Garfinkel, 2010.) krizu su pokrenule sljedeće stavke:

- Zbog sve bržeg rasta kapaciteta memorije sve je teže u nekom razumnom vremenu kreirati forenzičku sliku istrage te obradu svih podataka
- Sve veća učestalost ugrađene pohrane podataka te nastanak novih hardverskih sučelja dovodi do teškog uklanjanja i kreiranja forenzičkih slika zločina
- Nastanak novih operacijskih sustava i datotečnih formata znatno povećavaju kompleksnost alata za iskorištavanja alata što rezultira znatno povećanih troškovima razvoja takvih alata
- Analiza više uređaja u većini slučaja veže i korekciju pronađenih dokaza proziv osumnjičenog
- Poboljšanje enkripcije ne otežava oporavak podataka no upravo zbog nje se podaci u većini slučajeva
- Nastankom oblaka (engl. *Cloud*) za udaljeno spremanje i obradu te za razdvajanje jedne strukture podataka u više manjih dijelova povlači da postoje slučajevi u kojima se podaci ne mogu opće naći
- Zlonamjerni softver (engl. *Malware*) koji nije pisan za stalnu pohranu povlači skupu RAM forenziku
- Legalni izazovi znatno otežavaju forenzičke istrage

3.4. Primjeri korištenja digitalne forenzike

3.4.1. Dennis Lynn Rader

Jedan od najpoznatijih primjera korištenja digitalne forenzike je istraga protiv serijskog ubojice Dennis Lynn Rader poznatijeg kao BTK Killer odnosno BTK Strangler. Dennis Rader počinio je deset ubojstava od kojih je bilo i djece u Wichita, Kansas 1974. godine. (Gilligan, bez dat.)

Rader je bio poznat po tome što je slao provokacijska pisma policija i izdavačkim kućama u kojima je opisivao zločine koje je počinio. Naposljetku ga je takvo ponašanje i odalo jer je jednom prigodom policiju preko prijašnjeg pisma pitao hoće li mu moći ući u trag ako svoja pisma pohrani na disketi (engl. *Floppy disk*). Policija mu je preko izdavačke kuće Wichita Eagle odgovorila kako je to siguran način te je Rader poslao disketu. Digitalni forenzičari su na disketi pronašli izbrisani Microsoft Word dokument u kojem su se nalazili metapodaci. Metapodacima u dokumentu sadržavali su pojam Christ Lutheran Church te su našli kako je dokument bio modificiran od stranje osobe „Dennis“. („Dennis Rader“, bez dat.)

Pretraživanjem pojma Dennis Christ Lutheran Church na internetu forenzičari su doznali kako je Dennis Rader predsjednik crkvenog vijeća. Iako ove informacije nisu bile dovoljne za potpuno povezivanje Radera s ubojstvima, bile su od presudne važnosti za nastavak istrage. (Beyers, 2013.)

Prethodni primjer nam može prikazati kako digitalna forenzika može imati jako veliki utjecaj na istrage zbog sve veće i veće upotrebe digitalnih uređaja u svakodnevnom životu. Iako je policija ta koja je napravila odličan posao prilikom davanja lažne sigurnosti Raderu u digitalnu tehnologiju, bez digitalne forenzike i digitalnih forenzičara policija ne bi imala apsolutno nikakvu prednost komunikacije preko disketa nego dotadašnje komunikacije pomoću pisama.

3.4.2. Scott Tyree

Scott Tyree, tadašnji 38 – godišnjak iz Herndon, Virginia pretvarao se kao tinejdžer na Yahoo sobi za razgovore. U sobi za razgovore pronašao je 13 – godišnju djevojčicu Aliciu Kozakiewicz. Alicia je 1.1.2002. pobjegla od kuće te ju je Tyree oteo. Tyree je nakon otmice poslao fotografiju Alicie privezane za pod u njegovom podrumu nepoznatoj osobi koja je u to vrijeme živjela u Tamba, Florida. Na prvu je osoba mislila kako je Tyree poslao lažne fotografije, no naišao je na priču o nestanku djevojčice u Pittsburghu uz koju je bila priložena njezina fotografija. Nakon toga Tyree je poslao još fotografija iživljavanja nad djevojčicom te je nepoznata osoba odlučila obavijestiti FBI o nestanku Alicie. Dao je FBI – u Tyree – ovo korisničko ime te su forenzičari preko korisničkog imena došli do IP adrese (engl. *Internet Protocol address*) računala kojeg je Tyree koristio. Nakon poznate IP adrese FBI je kontaktirao Verizon, internetski poslužitelj (engl. *Internet Service Provider*), kako bi dobili informacije o fizičkoj adresi te ime osobe kojoj je dodijeljena dobivena IP adresa. Iz dobivenih informacija saznali su kako je počinitelj otmice Scott William Tyree. (Gilkerson, bez dat.)

3.5. Vrste digitalne forenzike

Prema („*Digital Forensics*“, bez dat.) digitalna forenzika se može podijeliti na 5 kategorija:

1. Računalna forenzika
2. Mobilna forenzika
3. Mrežna forenzika
4. Forenzička analiza podataka
5. Forenzika baza podataka

Prema (Beyers, 2013.) digitalna forenzika se može podijeliti na sljedeće kategorije:

1. Forenzika datotečnih sustava
2. Mrežna forenzika
3. Mobilna forenzika
4. Forenzika e – maila i interneta

3.5.1. Forenzika datotečnih sustava

Forenzika datotečnih sustava i forenzika baza podataka imaju neke sličnosti u svojim temeljima. Naime, datotečni sustavi kao i baze podataka imaju visok stupanj ovisnosti o metapodacima koji organiziraju podatke u memoriji. Forenzička istraga nad datotečnim sustavom može se podijeliti na tri komponente kako bi se istraga olakšala. Te komponente su:

- Poznavanje datotečnog sustava
- Pronalazak i pravilna interpretacija artefakata unutar operacijskog sustava
- Upotreba odgovarajućeg forenzičkog softvera

(Beyers, 2013.)

Tijekom povijesti koristili su se mnogi datotečni sustavi, no jedan od zanimljivijih sustava je NTFS (engl. *New Technology File System*) sustav zbog korištenja MFT (engl. *Master File Table*) tablice koja sadrži informacije o svim datotekama i direktorijima. MFT tablica sadrži naziv, sadržaj, adresu, 16 bajtni identifikator te ostale atribute. Zbog MFT tablice mogu se provesti sljedeće tehnike čija je svrha analiziranje datotečnog sustava:

- Pronalazak MFT – a kako bi se mogla analizirati i otkriti struktura datotečnog sustava
- Usporedba broja sektora u datotečnom sustavi i stvarna veličina uređaja za pohrana kako bi se otkrilo postoji li neiskorišteni prostor koji može sadržavati skrivene informacije unutar datotečnog sustava
- Provjera zadnjih redova MFT – a kako bi se otkrilo skrivanje informacija
- Istraga metapodataka datotečnog sustava koji također mogu skrivati informacije
- Kreiranje

(Beyers, 2013.)

3.5.2. Mrežna forenzika

Mrežna forenzika je znanost koja kao primarni zadatak ima hvatanje, bilježenje i analiziranje mrežnog prometa u svrhu otkrivanja i istraživanja kriminalnog djela. Mrežna forenzika spada u područje digitalne forenzike te koristi ogromnu količinu podataka zbog toga jer je potrebno uhvatiti sav mrežni promet kako bi se otkrila kriminalna radnja. Većina napada spada DDos (engl. *Distributed Denial of Service*) napad, to jest pokušaj onesposobljavanja mrežnog servisa preopterećivanjem. Mrežna forenzika koristi tehnike kao što su analiza mrežnih paketa, analiza statističkog tijeka, otkrivanje upada u mrežni sustav poduzeća, analiza upada u mrežnu arhitekturu, analiza logove i tako dalje. (Beyers, 2013; Avasthi, 2012.)

3.5.3. Mobilna forenzika

Mobilna forenzika, kao i ostale grane digitalne forenzike, kao primarnu djelatnost ima prikupljanje podataka i dokaza kako bi se razriješila kriminalna kriza unutar nekog poduzeća. Kao svoj temelj ima mobilne uređaje te uređaje sličnih karakteristika. Temelji se na prikupljanju objekata, artefakata u određenom vremenskom razdoblju kako bi se utvrdila njihova vjerodostojnost i neoštećenost. Postoje tri glavne metoda pomoću kojih se mogu ekstrahirati podaci iz mobilnih uređaja:

1. Ručno ekstrahiranje – pregledava se dokumentacija mobilnog uređaja te se ručno pristupa zapisima.
2. Logično ekstrahiranje – Forenzičar se preko Bluetooth tehnologije spada na mobilni uređaj te se ekstrahiraju svi zapisi koji su dostupni preko operacijskog sustava računala na kojem forenzičar radi istragu.
3. Fizičko ekstrahirane – Svodi se na neprestano umetanje informacija u mobilni uređaj kako bi podaci iz mobilnog uređaja izašli kroz komunikacijski kanal u neki eksterni uređaj za pohranu podataka.

(Anobah, Saleem i Popov,2014.)

3.5.4. Forenzika e – maila i interneta

Forenzika e – maila prikuplja podatke o izvoru i sadržaju e – mail poruka kako bi se identificirali stvarni pošiljatelj i primatelj, datum i vrijeme slanja poruke te ostali atributi koji mogu poslužiti kao digitalni dokaz prilikom istrage. Kao i kod ostalih forenzika, postoje određeni načina na koji se može obaviti istraga te su kod forenzike e – maila najučestaliji: Analiza zaglavlja, istraga poslužitelja, istraga metapodataka, pretraživanje ključnih riječi i tako dalje. Kod ove forenzike postoje alati koji se mogu koristiti kako bi se istraga pojednostavila te su neki od njh: eMailTrackerPro, EmailTracer te Adcomplain. (Banday, 2011.)

Forenzika interneta prikuplja podatke o web preglednicima te na taj način otkriva digitalne dokaze o počinjenom kriminalnom djelu. Kao glavne metode spominju se analiziranje upotrebe web preglednika, analiziranje napada nad web servisima, analiziranje napada nad web stranica, analiziranje sadržaja datoteka koje se nalaze na poslužitelju web stranice te određivanje lokacije korisnika koji je pod sumnjom. (Beyers, 2013.)

4. Baze podataka

Prema (Manger, 2003.) baza podataka je skup međusobno povezanih podataka pohranjenih na vanjskoj memoriji računala. (Rabuzin, 2011.) navodi kako postoji mnogo načina na koji se mogu opisati baze podataka te kako ne postoji jedinstveni način na koji možemo definirati pojam baze podataka. Kaluža (u knjizi „Sustavi baza podataka“, 2008.) navodi kako je baza podataka povezana, organizirana ali i elektronička biblioteka datoteka čiji su podaci zapisani u slogovima datoteke i međusobno su povezani. Kroenke i Auer (kao što citiraju Berg, Seymour i Goel) navode jednu zanimljivu definiciju baze podataka koja glasi: Baza podataka je samo opisujuća kolekcija integriranih zapisa.

Iako su podaci glavna stavka svake baze podataka, oni nisu najbitnija karika. Najbitnija stvar u cijeloj bazi je sama struktura baze podataka, odnosno kako su strukturirani podaci u njoj. Bez pravilne strukture podaci su nam od male koristi jer ih tada ne možemo povezati preko upita u veće cjeline kako bi dobili informacije koje su nam potrebne u tom trenutku. Bez mogućnosti postavljanja upita koji vraćaju informacije baza podataka nam tada služe za pohranu podataka što nije najoptimalniji način upotrebe baze podataka. (Rabuzin, 2011.)

4.1. Povijest

Prema (Berg, 2013.) povijest baza podataka možemo podijeliti u sljedeća razdoblja:

- Davno razdoblje do modernog razdoblja
- Razdoblje 1960. – tih godina
- Razdoblje 1970. – tih godina
- Razdoblje 1980. – tih godina
- Razdoblje 1990. – tih godina
- Rane 2000. – te godine
- NoSQL razdoblje
- UnQL razdoblje
- Nadolazeća razdoblja

4.1.1. Drevno razdoblje do modernog razdoblja

Potreba za pohranjivanjem podataka je od pamtivijeka ljudska sklonost. Tome svjedoče mnoge drevne knjižnice koje upravo služe za pohranjivanje knjiga u kojima možemo pronaći podatke koji tvore neke od najvažnijih informacija u ljudskoj povijesti. Drevno razdoblje se smatra gotovim nakon stvaranja prvih računala (Berg, 2013.)

4.1.2. Razdoblje 1960. – tih godina

1960. – tih godina 20. stoljeća porastao je broj osobnih računala koje su doduše u to vrijeme koristile razna poduzeća te korporacije. To je također sa sobom povuklo još izraženiju želju ali i sve veću potrebu za skladištenjem podataka te njihovo iskorištavanje u svrhu dobiti poduzeća. Tako je nastala prva generacija SUBP – a koji su bili usko povezani s tadašnjim aplikacijama koje su koristile pokazivače kao glavnu stavku prilikom prelaska s jednog sloga baze podataka na drugi. Također, tada je prioritet bio upravo na samo skladištenje podataka odnosno zapisa dok je sam sustav bio zanemariv, što u današnjem vremenu ne može biti dalje od istine. 1960. – tih godina 20. stoljeća zabilježio je sustav SABRE koji se uspio probiti na tržište avio kompanije, točnije American Airlines – a. (Berg, 2013.)

4.1.3.Razdoblje 1970. – tih godina

1970. godine obilježene su razvojem i osnivanjem relacijskog modela podataka. Njegov osnivač je engleski računalni znanstvenik Edgar F. Codd. Relacijski model podataka i dan danas je jedan od najpopularnijih modela podataka koji se koriste prilikom izrade baza podataka upravo zbog toga jer pruža mnoge mogućnosti koje modeli (hijerarhijski te mrežni) nisu pružali, prvenstveno jednostavnost prelaska s jednog zapisa na drugi. Također 1970. – tih godina 20. stoljeća izrađeni su prototipi dvaju sustavi koji su nakon toga postali uspješni:

1. INGRES – prethodnik POSTGRES – a.
2. System R

(Berg, 2013.)

1976. godine predstavljen je ERA model (engl. *Entity -Relationship model*) koji je danas jedan od najkorištenijih modela koji prikazuju poslovnu logiku procesa za koji je napravljen. (Berg, 2013.)

4.1.4.Razdoblje 1980. – tih godina

1980. – tih godine 20. stoljeća nastala je velika komercijalizacija sustava temeljenih na relacijskom modelu podataka te je SQL jezik postao standardni jezik za postavljanje upita nad bazom podataka te općenito upravljanjem bazom podataka. 1980. – te godine su također obilježile promjene kod izdavanja ažuriranja za mrežne i hijerarhijske modele odnosno njihovi razvojni timovi prestali su s ažuriranjima na tim modelima jer su zastarjeli u odnosu na relacijski model podataka. Također, u 80. – tim godinama predstavljen je i razvijen je pojam objektno orijentirane baze podataka, preciznije 1985. godine. Objektno orijentirana baza podataka je u to vrijeme predstavljala prikaz informacija preko objekata umjesto tablica. (Berg, 2013.)

4.1.5. Razdoblje 1990. – tih godina

1990. – te godine obilježile su razvoj alata koje mogu samostalno koristiti svi korisnici osobnih računala kao što su Microsoft Excell i Microsoft Access. Također, 1990. – tih godina započinje razvoj klijentskih alata za izradu aplikacija te klijent server modela. Jedan od najznačajnijih trenutaka u digitalnom svijetu dogodio se sredinom 90. – tih godina kad je po prvi puta Internet infrastruktura postala javno upotrebljiva. U ovo vrijeme po prvi puta su se SUBP – i koji su bili kreirani za objektno orijentirane baze podataka (engl. *OODBMS – Object Oriented Database Management System*) koji su tada služili za spajanje objektno orijentiranih baza podataka s objektno orijentiranim programskim jezicima kao što su Java te C#. 1997. godine predstavljen je XML (engl. *Extensible Markup Language*) jezik koji se od tada integrira u većinu proizvoda nastalih na temelju SUBP – a. (Berg, 2013.)

4.2. Model podataka

Kroz povijest postojali su mnogi modeli podataka koje su koristili računalni znanstvenici kako bi sami sebi olakšali izradu strukture baze podataka. Prema („What is a Database Model, bez dat.) model podataka je model koji nam pokazuje logičku strukturu baze podataka, veze između različitih podataka te ograničenja koja administrator zadaje prilikom kreiranja baze podataka. Manger (u knjizi „Baze podataka“, 2003.) navodi kako model podataka čini osnovu za koncipiranje baze podataka, njezino projektiranje ali i samu implementaciju. Kroz povijest razvijani su mnogi modeli podataka no najpoznatiji od njih su:

1. Relacijski
2. Hijerarhijski
3. Mrežni
4. Objektno orijentirani model podataka
5. Temporalni relacijski
6. Deduktivni
7. Polustrukturirani
8. Aktivni
9. Poopćeni
10. Parcijalni
11. Objektno relacijski

(„*What is a Database Model*“, bez dat.; Manger, 2003.;Schatten i Maleković, 2017.)

4.2.1. Relacijski model podataka

Relacijski model podataka danas je jedan od najpoznatijih modela podataka. Krajem 1960 – tih godina 20. stoljeća E. F. Codd, engleski računalni znanstvenik, je predstavio model koji će 1970. godine službeno objaviti kao relacijski model podataka.

Prema (Damesha, 2015.) relacijski SUBP – ovi imaju sljedeće nedostatke:

- Oskudnu reprezentaciju realnih entiteta
- Normalizacija baze podataka je potrebna ali u nekim slučajevima nije korisna
- Postoji samo jedna semantička struktura
- Oskudnu podršku za ograničenja
- Homogenu strukturu podataka
- Otežan rad s rekurzivnim upitima

4.2.2. Objektno orijentirani model podataka

Objektno orijentirani model podataka temelji se na objektno orijentiranim bazama podataka koje skladište podatke u obliku objekata koji predstavljaju jedinstvene zapise. Objektno orijentirane baze podataka pojavile su se primarno zbog tri razloga:

1. Ograničenja relacijskih SUBP – ova
2. Potražnja za kompliciranijim aplikacijama
3. Rast popularnosti objektno orijentiranog pristupa kod programskih jezika

(Damesha, 2015.)

Prema (Damesha, 2015.) nedostaci objektno orijentiranih SUBP – ova su:

1. Optimizacija upita
2. Ne postoji standardna algebra upita
3. Ne postoje pogledi
4. Sigurnosti problemi

Parametar	Objektno orijentirani SUBP	Relacijski SUBP
Model	Objektno orijentirani model	Relacijski model
Standardi	Nedostatak standarda	Standardizirani SUBP – ovi
Objektno orijentirani pristup	Direktna podrška	Nema direktne podrške
Konceptualni temelji	Nema istaknutih temelja	Relacijska matematika
Naziv standarda	ODMG – 3.0	SQL2 (ANSI X3H2
Korisnički tipovi podataka	Potpuna podrška	Nepotpuna podrška
Napredne aplikacije	Direktna podrška	Nema direktne podrške
Kompleksni objekti	Potpuna podrška	Nepotpuna podrška
Navigacijski pristup	Dobar	Loš
Evolucija sheme	Laka	Teška
Transakcije	Dugovječne	Kratkovječne
Jezik upita	Ovisno o proizvodu	SQL
Rekurzivni upiti	Lagano rukovanje	Teško rukovanje
Normalizacija baze podataka	Nije potrebna	Preporučljiva
Podaci se skladište u	Objektima	Tablicama
Reprezentacija	Dobra reprezentacija stvarnog svijeta	Lošija reprezentacija stvarnog svijeta
Semantička priroda	Snažna semantika	Slaba semantika
Ograničenja	Implementirana ograničenja integriteta i ograničenja poduzeća	Ograničenja poduzeća i integriteta nisu u potpunosti implementirana
Algebra	Objektna algebra	Relacijska algebra
Operacije	Lagano dodavanje operacija	Operacije su zbog relacijske algebre fiksne
Multimedija	Potpuna podrška	Nepotpuna podrška

Tablica 1. Usporedba SUBP – ova (Prema Damesha 2015.)

Na tablici 1. prikazana je usporedba relacijskog i objektno orijentiranog SUBP – a. Može se vidjeti kako objektno orijentirani SUBP ima manje standardiziran model podataka dok relacijski model ima mnogo bolju standardizaciju modela podataka kao i standardizaciju ostalih stavaka kao ograničenja, operacija koje nisu nužno prednost jer su ograničene s tim standardima. Objektno orijentirani SUBP – ovi imaju za prednost stavke kao što su reprezentacija realnog svijeta te operacija jer prikazuju realnu sliku svijeta te nemaju fiksan skup operacija s kojima rade.

4.3. Sustavi za upravljanje bazom podataka

Prema (Manger, 2003.) SUBP je poslužitelj baze podataka koji oblikuje fizički izgled baze podataka i usklađuje je s zatraženom logičkom strukturom te podržava razne modele baza podataka. Jedan od glavnih zadataka SUBP – a je osigurati sigurnost pohranjenih podataka u bazi podataka te automatizirati administrativne poslove koje uključuju bazu podataka. Sharma i Prabhjot (u članku „*Overview of the Database Management System*“, 2017.) navode kako je SUBP softver čija je svrha upravljanje bazom podataka, to jest omogućuje korisniku unos, ažuriranje i brisanje podataka, te administratorima olakšava dizajniranje, održavanje ali i pristupanje bazi podataka. Također, navode kako SUBP korisnika oslobađa od poznavanja načina skladištenja unesenih podataka i algoritama koji se vrte u pozadini cijele priče.

Prema („*Ranking*“, 2019.) u ruju 2019. najpopularniji SUBP – ovi su :

1. Oracle
2. MySQL
3. Microsoft SQL Server
4. PostgreSQL
5. MongoDB
6. DB2

Od navedenih šest SUBP – ova, njih pet su relacijski SUBP – ovi dok je jedina iznimka MongoDB SUBP koji spada u NoSQL grupaciju sustava koji nisu bazirani na relacijski model podataka te ne implementiranu standardni upitni jezik SQL. MongoDB najpopularniji je SUBP NoSQL grupacije te spada u takozvane dokument – baze podataka. (Stojanović, 2016.)

SUBP imaju jako važnu ulogu u samom radu s bazama podataka. Prema („*What is database management system*“, 2014.) SUBP omogućava:

- Apstrakciju i nezavisnost podataka
- Sigurnost podataka i baze podataka
- Jedinstvene administrativne procedure
- Mehanizam zaključavanja za istovremeni pristup
- Sposobnost brzog oporavka nakon rušenja nastalih nakon pogrešaka

No postoje i nedostaci SUBP – a koje je navela Sharma a to su:

- Cijena
- Kompleksnost
- Dodatni troškovi hardvera

5. PostgreSQL

PostgreSQL je objektno relacijski SUBP (engl. *Database management* system). PostgreSQL je softver otvorenog koda (engl. *Open source*) koji koristi i proširuje jezik SQL (engl. *Structured Query Language*) uz brojne značajke koje sigurno spremaju i skaliraju najkompleksnije poslove u kojima su podaci glavna stavka. PostgreSQL nastao je 1986. godine kao projekt sveučilišta University of California u Berkeleyu pod nazivom POSTGRES te ima više od 30 godina aktivnog razvoja. („About, bez dat.)

Prema („About“, bez dat.) PostgreSQL je ACID kompatibilan od 2001. godine te podržava transakcijski SUBP, odnosno posjeduje svojstva koja osiguravaju validnost transakcija baze podataka. ACID je skraćenica za sljedeća četiri svojstva:

1. Atomarnost (engl. *Atomacity*) – svaka promjena podataka je izvedena kao jedna operacija nad podacima to jest promjena je provedena ili nije provedena.
2. Konzistentnost (engl. *Consistency*) – baza podataka je u konzistentnom stanju kad transakcija započne ali je baza podataka i na kraju transakcije u konzistentnom stanju.
3. Izolacija (engl. *Isolation*) – Stanje pojedine transakcije nije vidljivo ostalim transakcijama provedenim nad jednom bazom podataka.
4. Izdržljivost (engl. *Durability*) – Nakon uspješnog završetka transakcije, sve promjene nastale u transakciji ostaju sačuvane i ne mogu se povratiti.

(„ACID properties of transactions“, bez dat.)

PostgreSQL svoju je reputaciju zaslužio zbog svoje arhitekture, podatkovnog integriteta, robusnog skupa značajki koje je razvojni tim dodao na samu SQL sintaksu, nadogradivosti te otvorenosti koda zajednici koja konstantno izdaje nove verzije u kojima dodaju nova rješenja te ispravljaju stara. PostgreSQL je jedan od sustava koji se može pokrenuti na svim popularnijim operacijskim sustavima kao što su Linux, Windows, Solaris te macOS. („About“, bez dat.)

5.1. Povijest

POSTGRES projekt čiji je voditelj bio profesor Michael Stonebraker, bio je sponzoriran od strane četiri sponzora od kojih je jedan od najvećih DARPA (*Defence Advanced Research Project Agency*) te je upravo zbog samih sponzora implementacija projekta započela 1986. godine. Prva verzija sustava koja je bila operabilna 1987. godine te je 1988. godina bila predstavljena na ACM – SIGMOD konferenciji. 1989. godine izdana je Verzija 1 nekolicini vanjskih korisnika no ta verzija nije bila dobra te je dobila kritike od strane korisnika. Verzija 2 izdana je naredne godine u kojoj su bila predstavljena nova pravila sustava. Verzija 3 izdana je 1991. godine u kojoj je dodana podrška za višestruke upravitelje skladištem, poboljšani izvršitelj upita te nova pravila sustava. Sva naredne verzije sustava sve do Postgres95 fokusirale su se na prenosivost i pouzdanost. („A Brief History of PostgreSQL“, bez dat.)

1994. godine nastao je Postgres95, prva verzija sustava u kojoj je dodan SQL interpreter. Također, Postgres95 je prva verzija sustava koja je bila postavljena na Web. Postgres95 bio je mnogo moćniji ali i manji od starijih verzija. Tako prema („A Brief History of PostgreSQL“, bez dat.) Postgres95 je bio 25% manji u smislu veličine u odnosu na svoje pretke te je bio 30 – 50 % brži na Wisconsin vrednovanju od POSTGRES Verzije 4.2.

Značajna unaprjeđenja u odnosu na ostale verzije su:

- Tutorijal koji je objašnjavao SQL značajke ali i Postgres95 značajke
- PostQUEL zaminjen SQL jezikom
- Novi program koji je omogućio interaktivno izvršavanje SQL upita
- Nova biblioteka prednjeg kraja (engl. *Front – end library*) koja podržava TCP klijente.

1996. godine projekt mijenja naziv iz Postgres95 u svoj današnji prepoznatljivi naziv PostgreSQL. PostgreSQL je naziv koji povezuje originalni i početni POSTGRES projekt sa SQL jezikom. („A Brief History of PostgreSQL“, bez dat.)

5.2. Značajke

PostgreSQL sadrži mnoge značajke od kojih su jedne od najvažnijih: Tipovi podataka, Integritet podataka, sigurnost, pouzdanost, performanse i mnoge druge.

5.2.1. Tipovi podataka

Svaki SUBP sadrži svoje osnovne tipove podataka koje korisnik odnosno zaposlenik može koristiti prilikom izrade baze podataka. Prema („*About*“, bez dat.) tipovi podataka koji se koriste u PostgreSQL – u mogu se podijeliti u 5 kategorija:

1. Primitivne
2. Strukturne
3. Geometrijske
4. Prilagodbe
5. Ostale formate datoteka

Prema („*About*“, bez dat.) u primitivne tipove podataka spadaju:

1. Integer
2. Numeric
3. String
4. Boolean

Prema („About“, bez dat.) u strukturne tipove podataka spadaju:

1. Date/Time formati kao što su timestamp, date te time
2. Polja
3. Rasponi tipova podataka
4. Univerzalno jedinstveni identifikatori (engl. *Universally Unique Identifiers*) skraćeno UUID

Prema („About“, bez dat.) u geometrijske tipove podataka spadaju:

1. Točka
2. Crta
3. Krug
4. Mnogokuti

Prema („About“, bez dat.) u podržane formate datoteka spadaju:

1. JSON/JSONB format
2. XML format
3. Hstore format

Prema („About“, bez dat.) u prilagodbene tipove podataka spadaju:

1. Kompozitni tip podataka
2. Prilagođeni tip podataka

5.2.2. Integritet podataka

Jedan od važnijih aspekata baza podataka je taj što spremaju podatke u konzistentnom i pravilnom stanju. Ako taj aspekt nije zadovoljen, tada baza podataka ne može biti upotrjebljena na način na koji je zamišljena te iz toga mogu proizaći mnogi sitni ali i veliki problemi koji tada kreatori baze podataka moraju riješiti kako bi se baza podataka mogla normalno koristiti. SUBP – i ne mogu osigurati pravilnost odnosno korektnost unesenih podataka preko aplikacije ali mogu osigurati njihovu konzistentnost sa definiranim ograničenjima koje su postavili kreatori baze podataka. (Rabuzin, 2011.)

Prema(„*About*“, bez dat.) PostgreSQL sadrži sljedeće mehanizme zaštite integriteta podataka:

- UNIQUE, NOT NULL ograničenja
- Primarni ključ
- Vanjski ključ
- Ograničenja isključenja

6. Forenzika baza podataka

Kao što je već rečeno u uvodnim stranicama, računala i ostali digitalni uređaji postaju jedni od najbitnijih uređaja u današnjem društvo. Takav status, nažalost, donosi i negativne strane kao što su njihova upotreba u kriminalne radnje pojedinaca ali i organizacija. Takve kriminalne radnje mogu se i vršiti nad bazama podataka te se zbog tog razloga mora očuvati sigurnost baze podataka ali se također mora moći izvršiti forenzička istraga ukoliko dođe do proboja sigurnosti baze podataka. Iz toga je proizašla forenzika baza podataka koja spada pod digitalnu forenziku te koristi metode i alate koje su primjenjive na istragama digitalne forenzike. (Beyers, 2013.)

U današnje vrijeme je rijetkost čuti o poduzeću koje uspješno posluje a da ne koristi bazu podataka kao skladište podataka upravo zbog toga jer su digitalni uređaji u takvom porastu popularnosti. Također, svako poduzeće koje uspješno posluje ima svoj informacijski sustav koji kao svoj temelj ima bazu podataka s kojom radi. U takvim bazama podataka skladište se jako bitni podaci koje poduzeće skuplja te pomoću njim može unaprijediti svoje poslovanje te su upravo zbog toga baze podataka meta kriminalaca koji žele iskoristiti pohranjene podatke u svoju svrhu na način da preuzmu kopiju same baze podataka, brisanjem postojećih zapisa ali i samim pogledom na podatke mogu učiniti veliku štetu poduzeću i njegovu poslovanju. (Beyers, 2013.)

Prema (Beyers, 2013.) forenzika baza podataka bitna je zbog sljedećih stavki:

- Sustavi koji koriste baze podataka jako su česti u poslovnom svijetu te se koriste na svakodnevnoj bazi i sadrže veoma važne podatke za to poduzeće
- Područje plana odgovora na incident je u proteklim godinama doživjelo rast uglavnom zbog porasta zahtjeva za oporavak baze podataka ili zahtjeva u kojima se traži odgovor na pitanja što se dogodilo s bazom podataka
- Postoji sklonost skladištenja informacija o kriminalnim radnjama na digitalnim uređajima, počinjenje kriminalnih dijela na digitalnim uređajima ili poduzimanje radnji na digitalnim uređajima. Nakon počinjenih kriminalnih dijela slijedi istraga u kojoj se saznaje što se zapravo dogodilo. Takve radnje su i naposljetku dovele do razvoja digitalne forenzike.

Administratori baza podataka koji su specijalizirani u području forenzike baza podataka mogu reagirati na sljedeće scenarije:

- Brisanja podataka iz baze podataka
- Nekonzistentnosti podataka u bazi podataka
- Otkriće sumnjivih djelatnosti korisnika
- Pad baze podataka

(Infosec Institute [FORENSICS], bez dat.)

Nakon što se dogodi jedan od navedenih scenarija, forenzičari pokušavaju pronaći digitalne dokazi u bazi podataka koji bi mogli otkriti tko je počinitelj kriminalnog djela. Iako je forenzika podataka mlada znanost te ne postoji striktno zacrtana metoda koja bi objasnila sva moguća rješenje za neki od scenarija, postoje koraci koji mogu olakšati posao, od kojih su neki:

- Kreiranje forenzičke kopije baze podataka
- Rekonstruiranje izgubljenih podataka ili log datoteka koje su povezane s kriminalnom radnjom
- Dešifrirati podatke te pronaći razlog zbog kojeg su podaci oštećeni
- Revizija korisničkih aktivnosti te izolirati sumnjive korisnike koji imaju sumnjive ili ilegalne aktivnosti ili ponašanje

([FORENSICS], bez dat.)

6.1. Status

Iako forenzika baza podataka nema status apsolutno nove znanosti te nema sumnje u to da je područje koje zaslužuje punu pozornost i dalje je jedna od znanosti koja rijetko dobiva istraživačku pozornost. Na to ignoriranje to jest zanemarivanje za forenziku baza podataka ukazao je Martin S Olivier u svom radu *On Metadata Context in Database Forensics*, gdje je otkrio kako nije izdan niti jedan znanstveni rad ili znanstveni članak u časopisu *Digital Investigation* nakon njegove publikacije 2004. godine što je i slučaj kod časopisa *International Journal of Digital Evidence* čija je publikacija započela 2002. godine. Također, Olivier je otkrio kako tematika forenzike baza podataka nije bila pokrivena na sastancima IFIP – a (*International Federation for Information Processing)* koji su održani 2009. godine. IFIP je organizacija koja prednjači u spajanju informacijskih i komunikacijskih znanosti i tehnologija u svijetu što je prepoznalo više od četrdeset država svijeta te više od 3500 znanstvenika. Trenutno je učlanjeno više od pola milijuna ljudi u organizaciju te sadrži više od 100 grupa. (Olivier, 2009)

Olivier u svojim drugim radovima također spominje kako forenzika baza podataka dobiva premalu istraživačku pozornost te kako bi se to područje digitalne forenzike moralo dodatno istražiti. Neki radovima u kojima na to ukazuje su: *On Dimensions of Reconstruction*

in Database Forensics kojeg je napisao s O.M. Fasan, *Reconstruction in Database Forensics* kojeg je napisao također s O.M. Fasan, *The role of triggers in database forensics* kojeg je napisao s Werner K. Hauger te *Assembling Metadata for Database Forensics* kojeg je napisao s Hector Beyers te Gerhard Hancke.

Iako je digitalna forenzika uspjela doći iz nejasne znanosti do jedne od najutjecajnijih znanosti u istragama, navedeno ne vrijedi za forenziku baza podataka. U današnje doba postoje brojni istraživački i stručni radovi u područjima koja su usko povezana s forenzikom baza podataka kao što su: digitalna forenzika, teorija baza podataka te sigurnost baza podataka no forenzika baza podataka još nije dobila takav tretman iako su provedena brojna istraživanja o istragama koja koriste bazu podataka i u teorijskom ali i u praktičnom smislu. (Fasan i Olivier, 2012.)

Beyer (u *Database forensics: Investigating Compromised Database Management Systems*, 2013.) navodi kako u sadašnje vrijeme vlada nestašica raspoloživih i efektivnih alata s kojim bi se mogao olakšati postupak forenzike nad bazama podataka. Također je naveo kako literatura koja trenutno postoji odgovara specifičnim napadima na bazu podataka i kako se od njih obraniti ali da ne postoji univerzalan pristup rješavanju zločina. Beyerovo mišljenje je da takav status forenzike baza podataka proizlazi iz same kompleksnosti baza podataka koje u forenzičkom smislu i dalje nisu razumljive računalnim znanstvenicima.

6.2. Podjela

Beyers (u *Database forensics: Investigating Compromised Database Management Systems*, 2013.) navodi kako je u novijim istraživanjima forenzika baza podijeljena u tri dimenzije: forenzika izmijenjenih baza podataka, forenzika ugroženih baza podataka te forenzika oštećenih baza podataka. Beyers također navodi kako podjelom forenzike baza podataka na ove tri dimenzije može pomoći istražiteljima efektivnijom istragom nad kriminalnim radnjama nad bazom podataka jer se tada zna nad kojom dimenzijom je ta radnja počinjena. No Beyers je u toj podjeli prepoznao i jednu manu: nova istraživanja forenzike baza podataka mogu donijeti nove dimenzije, no to danas ne predstavlja veliki problem upravo zbog toga jer je forenzika baza podataka mlada znanost te su potrebna takva istraživanja.

6.2.1. Forenzika izmijenjenih baza podataka

Forenzika izmijenjenih baza podataka je jedna od triju dimenzija forenzika baza podataka koja reprezentira SUBP – ove koji nisu bili ugroženi ali ni oštećeni niti uništeni prilikom podnošenja zahtjeva za istragom nad njim. Također, podaci i metapodaci nisu promijeni prilikom počinjena kriminalnog djela. Promjene koje su nastale nad SUBP – om su nastale prilikom svakodnevnim uporabom baze podataka. Smatra se kako je ova dimenzija najkompliciranija za istragu upravo zbog toga jer nema znakova oštećenja, uništenja ili ugroženosti baze podataka. Istraživanja u ovoj dimenziji su mnogo važna zbog toga jer postoji mogućnost izmjene baze podataka prije ali i poslije učinjene štete. Najčešće metode koje se upotrebljavaju u dimenziji izmijenjenih baza podataka je redo logova, to jest dvije ili više datoteka koje skladište sve promjene izvedene nad bazom podataka. Koriste se u Oracle SUBP – u ali postoje i implementacije takvog koncepta i u ostalim SUBP – ovima. (Beyers, 2013; Adedayo, 2015.)

Iako postoje raznovrsne lokacije u bazi podataka na kojima se mogu pronaći forenzički podaci ili dokazi, većina istraživačkih radova na bilo kojoj od dimenzija forenzike baza podataka temelji se na logovima koji se mogu pronaći u samoj bazi podataka. Logovi forenzičarima mogu biti bogat izvor informacija jer se u njima skladište upiti koji su izmijenili sadržaj pohranjen u bazi podataka. (Adedayo, 2015.)

Olivier i Fasan u radu *Reconstruction in Database Forensics* prikazuju kako se baza podataka može rekonstruirati u neko od prijašnjih verzija iako su nastale promjene nad njom. Definirali su inverzne funkcije svakog operatora u relacijskoj algebri te su prikazali i objasnili kako mogu biti generirani logovi relacijske algebre iz kompleksnog loga baze podataka transformacijom upita u operatore relacijske algebre. Rekonstrukcija baze podataka provodi se upotrebom inverznih funkcija ili operatora te generiranog loga relacijske algebre. (Beyers, 2013.)

Dimenzije forenzike baza podataka smatraju se ortogonalnim, to jest baza podataka može imati elemente svih dimenzija. Primjerice, baza podataka može ličiti na dimenziju izmijenjene baze podataka s elementima oštećene baze ali bez ijednog elementa ugrožene baze podataka. (Beyers, Olivier i Hancke, 2014.)

6.2.2. Forenzika ugroženih baza podataka

Izmijenjenom bazom podataka predstavljaju SUBP – ove u kojima je izmijenjen softver SUBP-a ili metapodaci baze podataka od strane napadača koji unosi podatka u strukturu koda softvera SUBP – a i/ili unosi podatke u metapodatke kako bi oni skladištili te unesene podatke. Unos podataka u metapodatke baze podataka omogućuje sam SUBP samim time što omogućuje kreiranje tablica, pogleda, funkcija i okidača koji sadrže svoje metapodatke. Kao što je omogućen unos, tako je i omogućeno ažuriranje tih metapodataka što može dovesti do mijenjanja njihovog sadržaja. Kod slučajevima u kojima je baza podataka ugrožena postoji problem koji kaže kako dokazi o ugroženom SUBP – u mogu biti veoma lagano negirani zbog promijenjenih metapodataka koje je izmijenio počinitelj. (Beyers, 2013.)

Iako je sama baza podataka najbolji alat za prikupljanje digitalnih dokaza za forenzičku istragu, kod ugroženih baza podataka to nije slučaj zbog toga jer integritet samih podataka ili rezultati dobivenih iz upita nisu pouzdani jer se ne može garantirati njihova sigurnost. Ovakav problem se može pronaći prilikom istrage nad operacijskim sustavima koji sadrže zlonamjerne softvere kao što su rootkit. Alexander Kornbrust, direktor poduzeća Red – Database – Security koje se bavi očuvanjem sigurnosti Oracle SUBP – a, u svojim je radovima identificirao sličnosti arhitekture SUBP – ova i operacijskih sustava te je shvatio kako zlonamjerni softveri mogu imati velike posljedice kako za operacijske sustave tako i za SUBP – ove. (Adedayo, 2015.)

Litchfield, koji je zaslužan za mnoge istraživačke radove u dimenziji oštećenih baza podataka u Oracle SUBP – u, također je uvidio problematiku vezanu uz istragu nad ugroženim bazama podataka prilikom pisanja svojih radova. Prema Litchfieldu jedan od najinstinktivnijih reakcija prilikom incidenta je gašenje sustava ili njegovo isključivanja s mreže kako bi se izbjegle dodatne havarije nad sustavom no također spominje kako ta reakcija i nije najbolje rješenje jer se gašenjem sustava gube dokazi o počinjenom kriminalnom djelu. (Adedayo, 2015.)

Postoje mnogi načini na koje se baza podataka može ugroziti te će biti prikazani sljedeći načini:

- Kreiranje pogleda koji zamjenjuje tablicu
- Zamjena imena dviju baza podataka
- Promjena prava uloga

6.2.3. Forenzika oštećenih baza podataka

U ovu dimenziju forenzike baza podataka spadaju baze podataka koje su oštećene ili potpuno uništene prilikom brisanja, uređivanja ili pomicanja zapisa sadržanih unutar SUBP–a. Ovakve baze podataka mogu ali i ne moraju biti operabilne, ovisno o kakvoj šteti se radi prilikom napada nad njom. Nakon što je baza podataka oštećena ili uništena, uobičajeni administratori nemaju dovoljno znanja u području ekstrahiranja podataka te je potrebno pronaći eksperte u tom području koji posjeduju takva znanja.

Postoje mnogi načini na koje se može oštetiti ili uništiti baza podataka no najčešći su:

- Deinstalacija SUBP – a
- Brisanje datoteka u direktoriju u kojem je instaliran SUBP
- Pokretanje i izvođenje naredbi unutar SUBP – a koje mogu oštetiti ili uništiti podatke

(Beyers, 2013.; Fasan, 2012.)

Iako se u literaturi spominje mala zainteresiranost za forenzikom baza podataka, ova dimenzija je dimenzija koja je dobila najviše pažnje od strane istraživača. Većina istraživanja provedenih na ovoj dimenziji su teoretska no postoji i praktično istraživanje koje je proveo David Litchfield nad Oracle SUBP – om. Njegovo istraživanje smatra se jednim od najpotpunijih istraživanja u ovom području digitalne forenzike ali samo za Oracle SUBP zbog svojih specifičnosti vezanih uz taj SUBP te se ne može previše iskoristiti kao podloga za cijelu forenziku baza podataka. (Beyers, 2013.;Adedayo 2015.)

Uz Oracle SUBP Microsoftov SQL Server je također dobio svoj istraživački rad u dimenziji oštećenih baza podataka. Fowler u knjizi *SQL Server Forensic Analysis* navodi tehnike koje se mogu koristiti prilikom skupljanja i čuvanja artefakata baze podataka. Također, Fowler u istom radu navodi kako artefakti mogu imati mnogo pozitivnih efekata prilikom istrage nad bazom podataka. Uz navedeno, Fowler je obrazložio i specifične metode koje mogu biti korištene prilikom konfiguracije SQL Servera kako bi se olakšala istraga te sama forenzička analiza uz konfiguraciju provjere sigurnosnih incidenata te analizu prikupljenih artefakata. Uz sve navedeno, Fowler se također dotaknuo i zlonamjernog softvera kao što su rootkitovi te njihovih posljedica na prikupljanje i analizu podataka kao i načina na koji se rootkitovi otkrivaju tijekom istrage nad bazom podataka koja je pod SQL Server SUBP – om. (Adedayo, 2015.)

6.3. Metapodaci

Prema (eVision [Metapodaci], bez dat.) metapodaci se mogu definirati kao podaci koji opisuju karakteristike nekog digitalnog izvora. Hećimović (u radu „*Metapodaci*“, 2016.) navodi kako metapodaci opisuju izvore podataka i omogućuju dopunske funkcionalnosti u sustavu.

Metapodaci daju odgovor na sljedeća bitna pitanja:

- Tko je stvorio dokument?
- Što je sadržaj dokumenta?
- Kada je stvoren dokument?
- Koje područje obuhvaćaju podaci dokumenta?
- Zašto su podaci dokumenta prikupljani?
- Kako su podaci dokumenta prikupljani?

(Hećimović, 2016.)

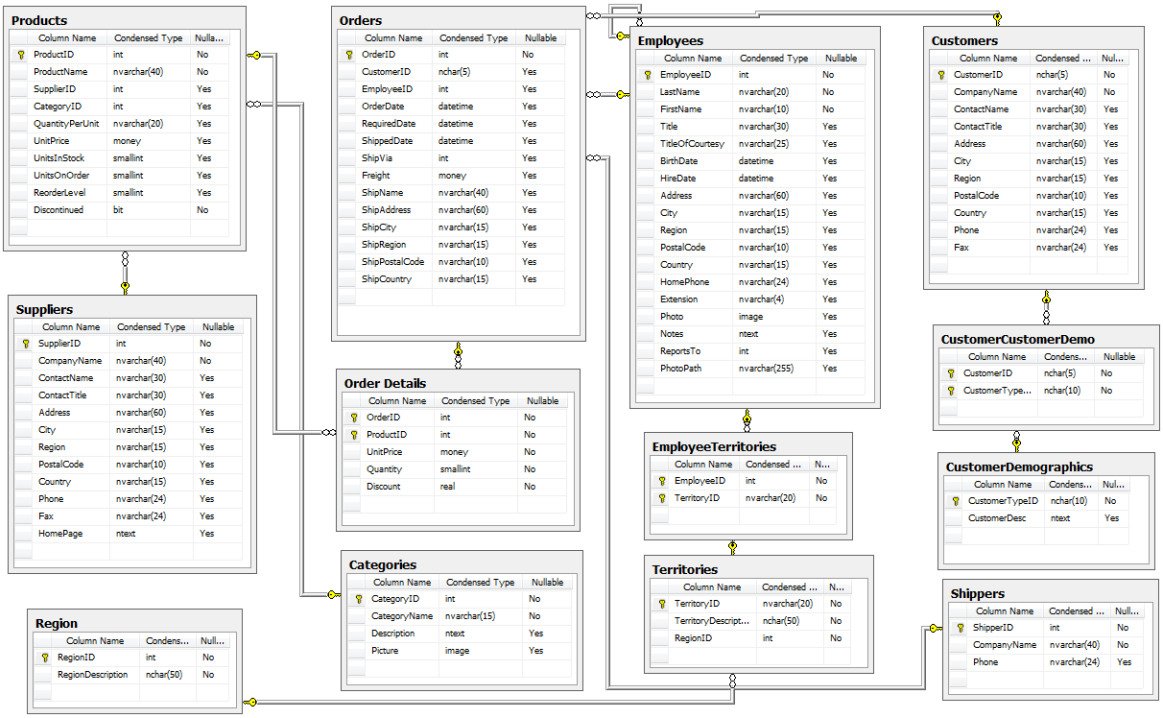
Prema ([Metapodaci], bez dat.) metapodaci su važni zbog efikasnije klasifikacije i organizacije podataka koji nakon grupacije postaje važne informacije. Uz navedenu važnost, metapodaci su također bitni kod stjecanja boljeg uvida u aktivnosti organizacije koji nakon toga može proširiti znanje o radu same organizacije ali i konkretne informacije koje se zatim mogu koristiti za unaprjeđenje automatizacije, dijeljenje podataka, usklađenosti te suradnje.

Metapodaci PostgreSQL baze podataka sadržani su sistemskom katalogu SUBP – a ili u pogledima informacijske sheme te opisuju strukturu same baze podataka ali i svakog objekta koji postoji u njoj kao što su tablice, korisnici, okidači, funkcije, pogledi i tako dalje. Ti metapodaci mogu se ekstrahirati pomoću SQL upita nad pogledima ili sistemskog kataloga. Razlika između sistemskog kataloga i pogleda informacijske sheme je taj što su pogledi informacijske sheme standardizirani i sadrže ih svi SUBP – ovi koji koristi SQL jezik, dok se sistemski katalozi razlikuju od SUBP – a do SUBP – a. Svaka PostgreSQL baza podataka sadrži informacijsku shemu pod nazivom information_schema koja sadrži poglede koji sadrže metapodatke o svim objektima pohranjenim u određenoj bazi podataka. Svaki definirani korisnik SUBP – a može pregledati poglede informacijske sheme. (Gireesh, 2010.)

7. Praktični dio

U ovom poglavlju prikazat će se praktični dio završnog rada. Sastoji se od ERA modela baze podataka te njegova objašnjenja, postupak kreiranja baze podataka te obavljena forenzika nad tom bazom podataka. Baza podataka te ERA Model preuzeti su s GitHub računa pthom koji sadrži bazu podataka prilagođenu za rad u PostgreSQL SUBP – u te ERA model izrađen u alatu SQL Server Management Studio.

7.1. ERA model

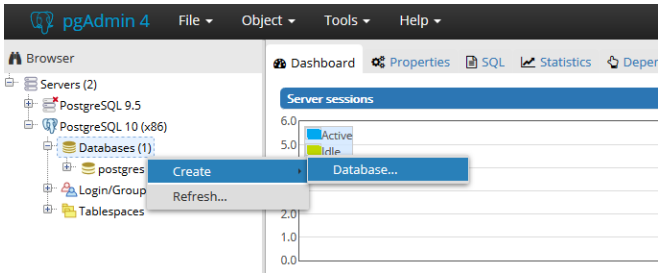


Slika 1. ERA model (Izvor: https://github.com/pthom/northwind_psql)

Na slici 1. možemo vidjeti ERA model preuzete baze podataka. Sastoji se od 13 tablica: Products, Suppliers, Region, Orders, Order Details, Categories, Employees, EmployeeTerritories, Territories, Custumers, CustomerCustomerDemo, CustomerDemographics te Shippers. Iz ERA modela može se iščitati sljedeće: Regija sadrži više teritorija dok teritorij pripada jednoj regiji. Na jednom teritoriju može raditi više zaposlenika te jedan zaposlenik može raditi na više teritorija. Zaposlenik se nalazi na više narudžbi no narudžba je sastavljena od strane jednog zaposlenika. Zaposlenik ima nadređene zaposlenike. Dobavljač dobavlja više proizvoda dok je proizvod dobavljan od strane jednog dobavljača.

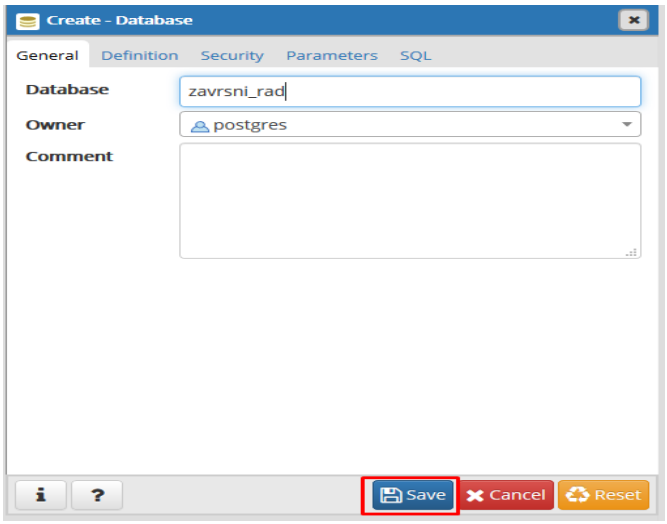
Kategorija sadrži više proizvoda dok proizvod pripada jednoj kategoriji. Proizvod se nalazi na više narudžba dok jedna narudžba može sadržavati više proizvoda. Narudžba je naručena od strane jednog kupca dok kupac može zatražiti više narudžbi. Prijevoznik može prevesti više narudžbi dok jedna narudžba može biti prevezena od strane jednog prijevoznika.

7.2. Kreiranje baze podataka



Slika 2. Kreiranje baze podataka

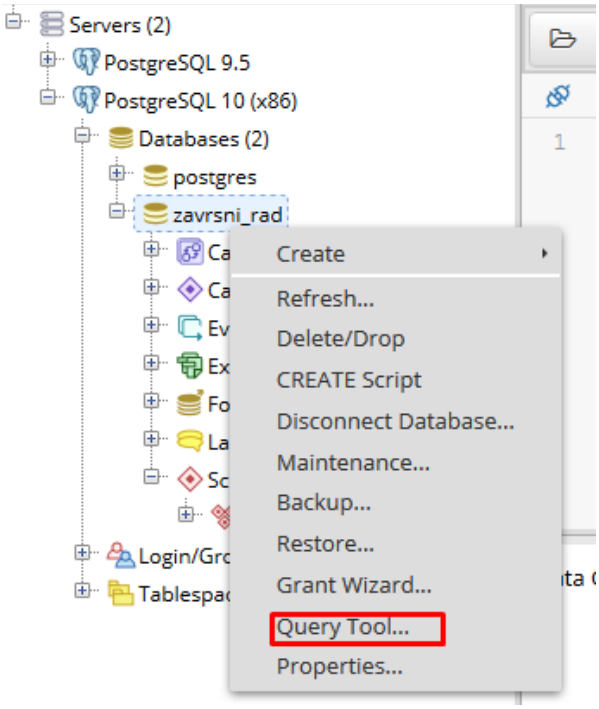
Na slici 2. prikazan je postupak kreiranje nove baze podataka u alatu pgAdmin 4. S lijeve strane može se vidjeti padajući izbornik u kojem su prikazani poslužitelji koji su instalirani na računalu. Odabirom poslužitelja prikazuju se baze podataka koje su kreiranje na njemu ankete sve uloge koje su kreirane na tom poslužitelju. Odabirom baza podataka otvara se padajući izbornik u kojem se mogu vidjeti sve baze podataka kreirane na odabranom poslužitelju. Svaki poslužitelj sadrži sistemsku postgres bazu podataka. Ukoliko korisnik želi kreirati novu bazu podataka, desnim klikom na Databases otvara se padajući izbornik koji sadrži opciju Create (Kreiraj) te Refresh (Osvježi). Odabirom opcije Create otvara se novi padajući izbornik u kojem se može odabrati samo Database (baza podataka). Lijevim klikom miša na Databases otvara se prozor prikazan na slici 3.



Slika 3. Naziv baze podataka

Na slici 3. prikazan je prozor koji se otvara nakon što se pritisne na Create database opciju. Na njemu možemo vidjeti sljedeće kartice: General, Definition, Security, Parameters te SQL. U Kartici General pod opcijom Database upisuje se naziv baze podataka, pod opcijom Owner se odabire uloga koja će biti vlasnik baze podataka te se može napisati komentar. Nakon svih unesenih parametar korisnik može stisnuti na crvenom označen gumbić Save. Nakon pritiska baza podataka se kreira pod zadanim imenom na odabranom poslužitelju.

Nakon što je izrađena baza podataka, može se popuniti sa SQL skriptom koja sadrži sve SQL upite koji kreiraju tablice te ih popunjava podacima. Kako bi se mogle zalijepiti komande u SQL skripti potrebno je otvoriti prozor za unos SQL upita. Prozor se može otvoriti pritiskom desnog klika miša na bazu podataka te odabirom Query Tool opcije iz padajućeg izbornika. Na slici 4. može se vidjeti opisani postupak. Nakon toga zalijepimo SQL komande te je baza podataka popunjena.



Slika 4. Postupak otvaranja prozora za upite

7.3. Primjer 1. Kreiranje pogleda koji zamjenjuje tablicu

Osoba koja ima pristup bazi podataka može ugroziti bazu podataka običnim upitima. Primjerice, osoba odluči naštetiti poduzeću koja posjeduje bazu podataka prema ERA modelu na slici 1. Osoba sljedećim upitom promijeni naziv tablice customers u customerss.

```
ALTER TABLE customers RENAME TO customerss;
```

Te nakon toga napravi pogled koji ima naziv customers te sadrži sve kupce koji nisu iz Argentine.

```
CREATE VIEW customers AS SELECT * FROM customerss
WHERE country!='Argentina';
```

Ovakvu vrstu prevare teško je odmah uočiti jer baza podataka može sadržavati stotine kupaca, no može se veoma lagano otkriti o kakvoj se radnji radi pomoću metapodataka. Sljedećim upitom možemo saznati sve korisnički definirane tablice unutar neke baze podataka.

```
SELECT TABLE_NAME AS imeTablice
FROM information_schema."tables"
WHERE table_type='BASE TABLE'
AND table_schema NOT IN ('pg_catalog','information_schema');
```

Na slici 5. može se vidjeti popis tablica te se lagano uočava kako se na popisu nalazi tablica pod imenom customerss.

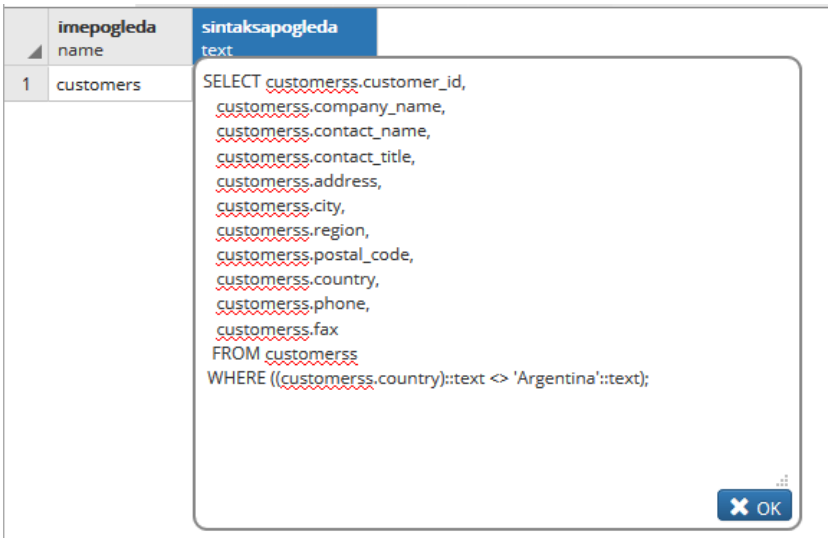
	imetablice character varying
1	us_states
2	shippers
3	orders
4	order_details
5	categories
6	suppliers
7	products
8	region
9	territories
10	employee_territories
11	customer_demographics
12	customer_customer_demo
13	employees
14	customerss

Slika 5. Popis tablica

Sljedećim upitom može se saznati popis korisnički definiranih pogleda

```
SELECT viewname AS imePogleda, definition AS sintaksaPogleda
FROM pg_views
WHERE schemaname='public'
```

Nakon uspješno izvršenog upita pojavljuje nam se pogled naziva customers te je njegova sintaksa prikazana na slici 6.



Slika 6. Sintaksa pogleda customers

Pomoću sistemskih kataloga i informacijske sheme otkrilo se kako u bazi podataka postoji tablica naziva customerss te pogled naziva customers koji isključuje kupce iz Argentine. Iako se pomoću metapodataka ne može otkriti koji korisnik je izmijenio naziv tablice te kreirao pogled, može se pronaći i ukloniti problem poduzeća.

7.4. Primjer 2. Promjena prava uloga

U bazi podataka zavrsni_rad postoji uloga imena joe koja ima pravo prijave u bazu podataka. Nakon nekog vremena joe se ponovno prijavljuje na bazu podataka no ne može. Joe kontaktira glavnog administratora baze podataka te ga obavještava o nemogućnosti prijave u bazu podataka. Administrator pokreće sljedeći upit te može vidjeti kako korisnik joe nema pravo prijave u bazu podataka. Slika rezultata upita nalazi se na slici 7.

```
SELECT rolname AS naziv_uloge,
       rolcanlogin AS login
FROM pg_roles
WHERE rolname='joe'
```

	naziv_uloge name	login boolean
1	joe	false

Slika 7. Rezultat upita o statusu prijave korisnika

7.5. Primjer 3. Zamjena imena dviju baza podataka

Korisnici mogu učiniti veliku štetu ako imaju prevelike ovlasti nad bazom podataka. U ovom primjeru korisnik baze podataka ima pravo promjene naziva baze podataka te je jednostavnim upitima zamijenio bazu podataka o narudžbama s bazom podataka o iznajmljivanju DVD – a. Upiti su redom prikazani ispod.

```
ALTER DATABASE zavrsni_rad RENAME TO pom
ALTER DATABASE dvdrental RENAME TO zavrsni_rad
ALTER DATABASE pom RENAME TO dvdrental
```

Nakon izvršenih upita baze podataka su promijenile nazive te sustav više nema smisla jer korisnici ne mogu izvršavati upite zbog nepostojećih tablica. Forenzičar pristupa problemu tako da iz sistemskog kataloga baze podataka traži popis svih tablica. Na slici 8. prikazan je rezultat upita iz sistemskog kataloga.

	table_name character varying
1	us_states
2	shippers
3	orders
4	order_details
5	categories
6	suppliers
7	products
8	region
9	territories
10	employee_territories
11	customer_demograp...
12	customer_customer...
13	employees
14	customers

Slika 8. Popis tablica u bazi dvdrental

7.6. Metanaredbe

PostgreSQL uz sistemske kataloge i informacijsku shemu nudi i metanaredbe koje također mogu poslužiti za ekstrahiranje metapodataka iz baze podataka. Svaka naredba koja se izvršava u terminalu i kao svoj početni znak ima \ smatra se metanaredbom. Takve naredbe provodi psql te se pomoću njih može olakšati posao administracije i skriptiranja. Važno je napomenuti kako alat kao što je pgAmin 4 ne može izvršiti metanaredbe no postoji opcija koja korisniku dozvoljava otvaranje psql terminala kako bi se takve naredbe mogle izvršiti. Neke od metanaredbi koje psql nudi su:

- \l – naredba koja prikazuje sve baze podataka na poslužitelju
- \d – naredba koja prikazuje sve objekte unutar baze podataka
- \dg – naredba koja prikazuje sve uloge i korisnike
- \d nazivTablice – naredba koja vraća detaljne informacije o upisanoj relaciji unutar baze podataka

```
zavrsni_rad=# \l
                                  List of databases
   Name    |  Owner   | Encoding |        Collate        |        Ctype        |   Access privileges
-----------+----------+----------+-----------------------+---------------------+-----------------------
 postgres  | postgres | UTF8     | Croatian_Croatia.1250 | Croatian_Croatia.1250 |
 template0 | postgres | UTF8     | Croatian_Croatia.1250 | Croatian_Croatia.1250 | =c/postgres          +
           |          |          |                       |                     | postgres=CTc/postgres
 template1 | postgres | UTF8     | Croatian_Croatia.1250 | Croatian_Croatia.1250 | =c/postgres          +
           |          |          |                       |                     | postgres=CTc/postgres
 zavrsni_rad | postgres | UTF8     | Croatian_Croatia.1250 | Croatian_Croatia.1250 | =Tc/postgres         +
           |          |          |                       |                     | postgres=CTc/postgres
(4 rows)
```

Slika 9. Prikaz naredbe \l

Na slici 9. prikazan je rezultat naredbe \l u psqlu. Kao što se može vidjeti, prikazani su nazivi baza podataka koje se nalaze na poslužitelju. Uz nazive, naredba prikazuje vlasnika nad bazom podataka, način kodiranja, način sređivanja nizova (engl. *String*) te privilegije pristupa nad bazom podataka.

```
zavrsni_rad=# \d
                List of relations
 Schema |           Name           | Type  |  Owner
--------+--------------------------+-------+----------
 public | categories               | table | postgres
 public | customer_customer_demo   | table | postgres
 public | customer_demographics    | table | postgres
 public | customers                | table | postgres
 public | employee_territories     | table | postgres
 public | employees                | table | postgres
 public | order_details            | table | postgres
 public | orders                   | table | postgres
 public | products                 | table | postgres
 public | region                   | table | postgres
 public | shippers                 | table | postgres
 public | suppliers                | table | postgres
 public | territories              | table | postgres
 public | us_states                | table | postgres
(14 rows)
```

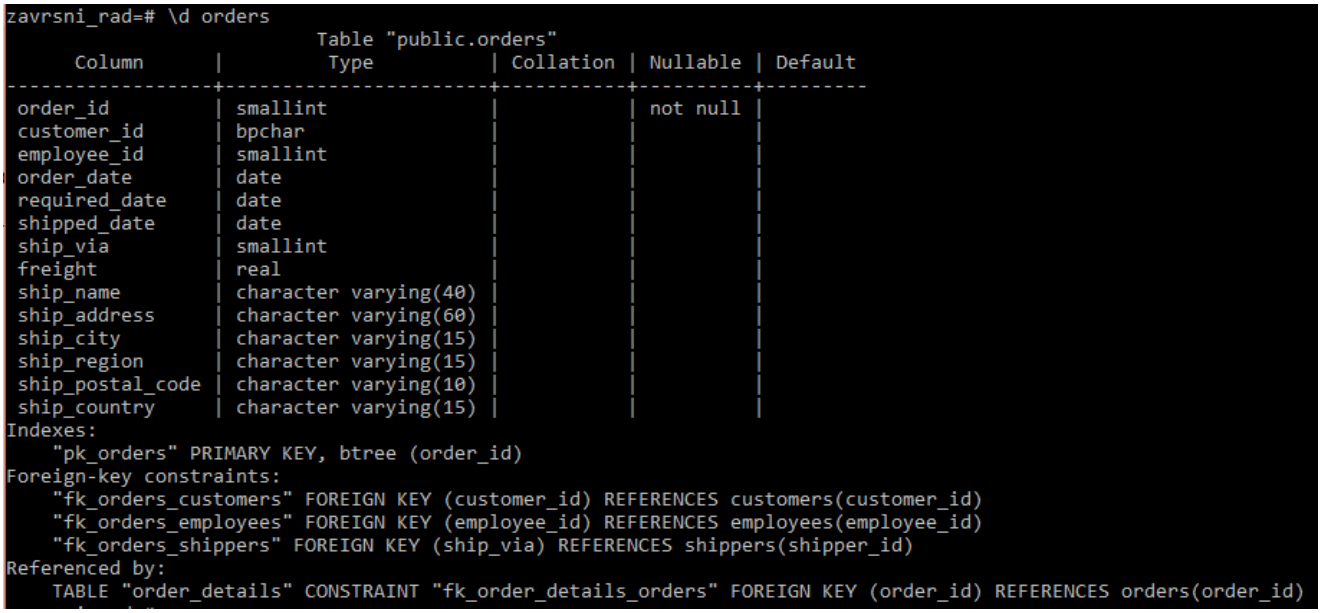
Slika 10. Prikaz naredbe \d

Na slici 10. prikazan je rezultat naredbe \d. Naredba vraća sve objekte baze podataka kao i sistemski katalog pg_catalog kao i odgovarajući upit nad informacijskom shemom. Prikazana je shema, naziv objekta, tip objekta te vlasnik objekta. Pokretanjem \d+ naredbe dobiva se uz sve navedene atribute veličina tablice te opis. Rezultat naredbe \d+ prikazan je na slici 11.

```
 Schema |           Name           | Type  |  Owner   |    Size    | Description
--------+--------------------------+-------+----------+------------+-------------
 public | categories               | table | postgres | 16 kB      |
 public | customer_customer_demo   | table | postgres | 8192 bytes |
 public | customer_demographics    | table | postgres | 8192 bytes |
 public | customers                | table | postgres | 48 kB      |
 public | employee_territories     | table | postgres | 8192 bytes |
 public | employees                | table | postgres | 16 kB      |
 public | order_details            | table | postgres | 120 kB     |
 public | orders                   | table | postgres | 144 kB     |
 public | products                 | table | postgres | 8192 bytes |
 public | region                   | table | postgres | 16 kB      |
 public | shippers                 | table | postgres | 8192 bytes |
 public | suppliers                | table | postgres | 16 kB      |
 public | territories              | table | postgres | 16 kB      |
 public | us_states                | table | postgres | 8192 bytes |
(14 rows)
```

Slika 11. Rezultat naredbe \d+

Ukoliko se pokrene naredbe \d nazivTablice tada administrator dobiva sve relevantne informacije o upisanoj tablici. Na slici 12. prikazan je rezultat nakon što administrator provede naredbu \d orders. Uz naziv atributa, dobiva informacije o tipu podatka atributa, način sređivanja nizova, mogućnost poprimanja NULL vrijednosti te zadanu vrijednost. Uz sve navedeno, administrator ali i forenzičar ima priliku vidjeti indekse u relaciji i vanjske ključeve. Pomoću vanjskih ključeva forenzičar može rekreirati cijelu strukturu baze podataka što mu uvelike pomaže prilikom istrage.



```
zavrsni_rad=# \d orders
                        Table "public.orders"
      Column      |         Type          | Collation | Nullable | Default
------------------+-----------------------+-----------+----------+---------
 order_id         | smallint              |           | not null |
 customer_id      | bpchar                |           |          |
 employee_id      | smallint              |           |          |
 order_date       | date                  |           |          |
 required_date    | date                  |           |          |
 shipped_date     | date                  |           |          |
 ship_via         | smallint              |           |          |
 freight          | real                  |           |          |
 ship_name        | character varying(40) |           |          |
 ship_address     | character varying(60) |           |          |
 ship_city        | character varying(15) |           |          |
 ship_region      | character varying(15) |           |          |
 ship_postal_code | character varying(10) |           |          |
 ship_country     | character varying(15) |           |          |
Indexes:
    "pk_orders" PRIMARY KEY, btree (order_id)
Foreign-key constraints:
    "fk_orders_customers" FOREIGN KEY (customer_id) REFERENCES customers(customer_id)
    "fk_orders_employees" FOREIGN KEY (employee_id) REFERENCES employees(employee_id)
    "fk_orders_shippers" FOREIGN KEY (ship_via) REFERENCES shippers(shipper_id)
Referenced by:
    TABLE "order_details" CONSTRAINT "fk_order_details_orders" FOREIGN KEY (order_id) REFERENCES orders(order_id)
```

Slika 12. Rezultat naredbe \d orders

8. Zaključak

Forenzika baza podataka danas je jedna od najvažnijih znanosti na području baza podataka zbog sve veće upotrebe svih vrsta baza podataka u poduzećima i njihovim informacijskim sustavima. Iako je jedna od najvažnijih, i dalje ne postoji standardizirani postupak prilikom forenzičke istrage nakon otkrivanja sumnjivih aktivnosti nad bazom podataka. Postoje radovi koji objašnjavaju postupke koji olakšavaju forenzičarima rad, no oni su usko povezani s pojedinim SUBP – ovima koji posjeduju jedinstvene mehanizme koji mogu očuvati sigurnost baze podataka i zaštiti bazu podataka od kriminalaca i zlonamjernih softvera. Mnogi radovi M. S. Oliviera ukazuju na manjkavost znanstvenih radova i znanstvenih istraživanja na temu forenzike baza podataka te kao glavne razloge navodi mladost same znanosti ali i kompleksnosti teorije baza podataka ali i kompleksnosti same forenzike nad bazama podataka. Najutjecajniji radovi pripadaju Davidu Litchfieldu koji je svoja istraživanja fokusirao nad bazama podataka kreiranim u Oracle SUBP – u dok postoje i radovi pisani za Microsoftov SQL Server.

Forenzika baza podataka zanimljiva je tema no nedostatak znanstvenih radova je malo stvarao problem prilikom izrade završnog rada, posebice tijekom izrade praktičnog dijela. Većina pronađene teorijske literature potječe iz iste katedre Sveučilišta Pretoria te većina radova ima istog mentora M. S. Oliviera. Mišljenja sam kako bi forenziku baza podataka trebalo mnogo detaljnije proučiti jer su u današnje vrijeme napadi nad informacijskim sustavima sve veći i veći a u pozadini njih se u većini slučajeva nalazi baza podataka koja za poduzeće pod napadom predstavlja ogromno bogatstvo koja ni pod koju cijenu ne smije biti ugrožena, izmijenjena, oštećena i naposljetku uništena.

Popis literature

Ristić N., Simeunović N. (2013)., *Digitalna forenzika u funkciji forenzičkog računovodstva*, INFOTETEH-JAKORINA Vol.12, Preuzeto 28.6.18. s: http://infoteh.etf.unssa.rs.ba/zbornik/2013/radovi/RSS-8/RSS-8-5.pdf

Reith M., Carr C., Gunsch G. (2003)., *An Examination of Digital Forensic Models*, Internal Journal of Digital Evidence Volume 1 Issue 4, Preuzeto 28.6.18. s: http://www.just.edu.jo/~Tawalbeh/nyit/incs712/digital_forensic.pdf

Carrier B. (2003)., *Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers*, Internal Journal of Digital Evidence Volume 1 Issue 4, Preuzeto 28.6.18. s: https://pdfs.semanticscholar.org/424d/aafd9ac88cf67efd046d02ed1eed4f65fd41.pdf

Olivier S. M. (2009)., *On Metadata Context in Database Forensics*, ICSA Research Group, University of Pretoria, South Africa, Preuzeto 28.6.18. s: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.566.7390&rep=rep1&type=pdf

Garfinkel L. S. (2010), *Digital forensics research: The next 10 years*, Naval Postgraduate School, Monterey, USA, *Digital Investigation 7*, Preuzeto 29.6.18. s: https://calhoun.nps.edu/bitstream/handle/10945/44251/Garfinkel_%20Digital_Forensics_2010.DFRWS.Next10Years.pdf?sequence=1&isAllowed=y

Gilligan M. (bez dat.), *Nightmare in Kansas: The Story of the BTK Serial Killer, Dennis Rader*, Preuzeto 31.7.18. s https://didyouknowfacts.com/nightmare-kansas-story-btk-serial-killer-dennis-rader/

Dennis Rader (bez dat.), U Wikipedia. Preuzeto 31.7.18. s https://en.wikipedia.org/wiki/Dennis_Rader

Beyers Quintus Hector (2013)., *Database Forensics: Investigating Compromised Database Management Systems*, Department of Electircal, Electronic and Computer Engineering, Faculty of Engineering, Built Environment and Information Techology, University of Pretoria

Gilkerson L. (bez dat.), *Caught By a Predator: Woman Speaks Out 10 Years After Her Abduction*, Preuzeto 31.7.18. s http://www.covenanteyes.com/2012/01/13/caught-by-a-predator-10-years-after-her-abduction/

Garfinkel L. S. (2010), *Digital forensics research: The next 10 years*, Digital Investigation, S64 – S73

Manger R. (2003.), *Baze podataka*, Sveučilište u Zagrebu, Prirodoslovno Matematički Fakultet

Rabuzin K. (2011.), *Uvod u SQL*, Sveučilište u Zagrebu, Fakultet organizacije i informatike

PostgreSQL (bez dat.), *About*, Preuzeto 7.8.18. s https://www.postgresql.org/about/

PostgreSQL (bez dat.), U Wikipedia. Preuzeto 7.8.18. s https://en.wikipedia.org/wiki/PostgreSQL#cite_note-OS_X_Lion_Server-11

IBM (bez dat.), *ACID properties of transactions*, Preuzeto 7.8.18. s https://www.ibm.com/support/knowledgecenter/en/SSGMCP_5.3.0/com.ibm.cics.ts.productoverview.doc/concepts/acid.html

PostgreSQL (bez dat.), *A Brief History of PostgreSQL*, Preuzeto 7.8.18. s https://www.postgresql.org/docs/current/static/history.html

Digital Forensics (bez dat.), Preuzeto 15.8.18. s https://cybernetic-gi.com/digital-forensics/

Kaluža M. (2008.), *Sustavi baza podataka*, Veleučilište u Rijeci, Rijeka

Berg L. K., Seymour T., Goel R. (2013.), *History Of Databases*, International Journal of Management & Information Systems, Preuzeto 16.8.18. s https://www.researchgate.net/profile/Dr_Tom_Seymour/publication/298332910_History_Of_Databases/links/578902dc08ae5c86c99acd01/History-Of-Databases.pdf

What is a Database Model (bez dat.), Lucidchart, Preuzeto 16.8.18. s https://www.lucidchart.com/pages/database-diagram/database-models

Sharma N., Prabhjot (2017.),*Overview of the Database Management System*, International Journal of Advanced Research in Computer Science, Preuzeto 17.8.18. s http://www.ijarcs.info/index.php/Ijarcs/article/viewFile/3778/3259

What is database management system (2014.), TechTarget, Preuzeto 17.8.18. s https://searchsqlserver.techtarget.com/definition/database-management-system

O.M. Fasan, M.S. Olivier (2012.), *On Dimensions of Reconstruction in Database Forensics*, University of Pretoria, ICSA, Computer Science, Preuzeto 20.8.18. s https://pdfs.semanticscholar.org/e861/533de8e67f40c279b5413e77432b6bca67af.pdf

Infosec Institute [FORENSICS] (bez dat.), *What is Database Forensics*, Preuzeto 21.8.18.
https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/application-forensics/overview-types-of-database-forensics/#gref

H. S. Damesha (2015.), *Object Oriented Database Management Systems-Concepts, Advantages, Limitations and Comparative Study with Relational Database Management Systems*,Global Journal of Computer Science and Technology, Global Journals, Preuzeto 23.8.18. s https://pdfs.semanticscholar.org/341c/86339e7b803290016ff5a080965ab2f956fe.pdf

O. M. Adedayo (2015.) , *Reconstruction in Database Forensics*, Department of Computer Science, University of Pretoria, Preuzeto 26.8.18. s https://pdfs.semanticscholar.org/51c0/f19c4b38e7c48abfbef0b0a2ef619992f6ae.pdf

eVision (bez dat.) [Metapodaci], *Metapodaci i njihova važnost*, Preuzeto 28.8.18. s https://www.evision.hr/hr/Novosti/Stranice/sto-su-metapodaci-i-zasto-su-vazni.aspx

Ž. Hećimović (2016.), *Metapodaci*, Sveučilište u Splitu, Katedra za geodeziju i geoinformatiku, Preuzeto 28.8.18. s https://bib.irb.hr/datoteka/834001.ZHecimovic_Metapodaci.pdf

T. Gireesh (2010), *Getting meta information of a PostgreSQL database*, Preuzeto 28.8.18. s https://tharas.wordpress.com/2010/01/12/getting-meta-information-of-a-postgresql-database/

H. Q. Beyers, M. S. Olivier, G. P. Hancke (2014.), *Databse Application Schema Forensics*, Department of Computer Science, Department Of Electrical, Electronic and Computer Engineering, Univeristy of Pretoria, Preuzeto 30.8.18. s https://repository.up.ac.za/bitstream/handle/2263/45150/Beyers_Database_2014.pdf?sequence=1

pgAdmin (bez dat,), *Features*, Preuzeto 11.9.18. s https://www.pgadmin.org/features/

LightShot (bez dat.), *LightShot*, Preuzeto 11.9.18. s https://app.prntscr.com/en/index.html

Microsoft Word (bez dat.), U Wikipedia. Preuzeto 11.9.18. s https://en.wikipedia.org/wiki/Microsoft_Word#Word_for_Mac

A. Stojanović (2016.), *Osvrt na NoSQL baze podataka – četiri osnovne tehnologije*, Tehničko veleučilište u Zagrebu, Polytechnic & Design, Vol. 4, No. 1

DB-Engines, *DB-Engines Ranking*, Preuzeto 11.9.18. s https://db-engines.com/en/ranking

D. Avasthi (2012.), *Network Forensic Analysis with Efficient Preservation for SYN attack*, Amity University, International Journal of Computer Applications

M. Anobah, S. Saleem, O. Ppov (2014.). *Testing Framework for Mobile Device Forensics Tools*, The Journal of Digital Forensics, Security and Law, Volume 9, Number 2, Article 18, Preuzeto 11.9.18. s https://pdfs.semanticscholar.org/9dc5/01f4a48957cdc8473367d25034fc3251ec10.pdf

M. T. Banday (2011.), *Techniques and Tools for Forensic Investigation of E – Mail*, P.G. Department of Electronics and Instrumentation Technology, University of Kashmir

M. Schatten, M. Maleković (2017.), *Teorija i primjena baza podataka*, Fakultet organizacije i informatike

Popis slika

Popis tablica