Digitalna forenzika baza podataka

Cobović, Patricija

Undergraduate thesis / Završni rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:211:918156

Rights / Prava: Attribution 3.0 Unported/Imenovanje 3.0

Download date / Datum preuzimanja: **2024-03-28**

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
VARAŽDIN

Repository / Repozitorij:

Faculty of Organization and Informatics - Digital Repository

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Patricija Cobović

DIGITALNA FORENZIKA BAZA PODATAKA

ZAVRŠNI RAD

Varaždin, 2021.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Patricija Cobović

Matični broj: 0016135793

Studij: Poslovni sustavi

DIGITALNA FORENZIKA BAZA PODATAKA

ZAVRŠNI RAD

Mentor:

Prof. dr. sc. Kornelije Rabuzin

Varaždin, rujan 2021.

Patricija Cobović

Izjava o izvornosti

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

Autorica potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Tema završnog rada glasi digitalna forenzika baza podataka. U završnom radu biti će navedene informacije o bazama podataka, vrstama baza podataka, važnosti zaštite baze te metodama enkripcije. Nadalje, detaljno će se obrađivati tematika digitalne forenzike, odnosno kako je ona nastala, koje metodologije koristi, tko su digitalni forenzičari te što su digitalni dokazi. Isto tako, rad će se baviti tematikom kibernetičkog kriminala. U radu su korišteni brojni internetski izvori, istraživanja i knjige kako bi završni rad bio što bolje i detaljnije obrađen.

Ključne riječi: digitalna forenzika, forenzika baza podataka, enkripcija, sigurnost baza podataka, digitalni dokazi, kibernetički napad

Sadržaj

Sadržaj v
1. Uvod 1
2. Metode i tehnike rada 2
3. Baza podataka 3
3.1. Modeliranje podataka 3
3.2. Relacijski model podataka 4
3.3. Jezici za rad s bazama podataka 5
3.4. SQL vs.NoSQL baze podataka 5
3.5. Životni ciklus baza podataka 6
3.5.1. Analiza potreba 6
3.5.2. Modeliranje podataka 7
3.5.3. Normalizacija relacijske sheme 7
3.5.4. Implementacija 7
3.5.5. Testiranje 8
3.5.6. Održavanje 8
4. Sigurnost baza podataka 9
4.1. Sigurnosne prijetnje 9
4.1.1. Namjerne sigurnosne prijetnje 9
4.1.2. Nenamjerne sigurnosne prijetnje 10
4.2. Kontrola pristupa 10
5. Enkripcija podataka 12
5.1. Povijest enkripcije podataka 12
5.1.1. Cezarova šifra 12
5.1.2. Jefferson's disks 13
5.1.3. Enigma 13
5.2. Oblici enkripcije 13
5.3. Standardi za kriptiranje 14

6. Kibernetički kriminalitet 15
6.1. Povijest 15
6.2. Vrste kibernetičkih napada 16
6.3. Obrana od kibernetičkih napada 17
7. Digitalna forenzika 19
7.1. Definicija 19
7.2. Povijest 19
7.3. Digitalni forenzičari 20
7.4. Vrste digitalne forenzike 21
7.4.1. Forenzika datotečnih sustava 21
7.4.2. Mrežna forenzika 21
7.4.3. Forenzika mobilnih uređaja 21
7.4.4. Forenzika e-maila i interneta 22
7.5. Proces digitalne forenzike 22
7.6. Digitalni dokazi 23
8. Forenzika baza podataka 24
8.1. Podjela forenzike baze podataka 25
8.1.1. Forenzika izmijenjenih baza podataka 25
8.1.2. Forenzika ugroženih baza podataka 25
8.1.3. Forenzika oštećenih baza podataka 26
8.2. Alati za forenzičku analizu baze podataka 26
9. PostgreSQL 28
9.1. ERA model i pgAdmin 4 28
9.2. pgAdmin 4 29
9.3. Promjena prava uloga 31
9.4. Kreiranje pogleda kao zamjena za tablicu 32
10. Sleuth Kit 33
10.1. Sloj datotečnog sustava 33
10.2. Sloj podataka 33

10.3. Sloj metapodataka 34
11. Zaključak 35
Popis literature 36
Popis slika 39
Popis tablica 40

1. Uvod

Baza podataka skup je međusobno organiziranih podataka koje nadziru sustavi za upravljanje bazama podataka (SUBP), a svaka od njih temelji se na određenom modelu. Ogroman broj osjetljivih i krucijalnih podataka pohranjeno je u bazama, stoga je nužno naglasiti kako je njihova zaštita i sigurnost jedan od najvažnijih aspekata prilikom kreiranja same baze podataka. Kako se digitalni svijet brže razvija od realnog svijeta, tako sve više rastu i bivaju korištene baze podataka za koje je u posljednjih 10 godina nastao enorman interes, stoga i često dolazi do krađe i zloupotrebe korisničkih podataka, a kako bi se to spriječilo nužno je zaštititi baze različitim mehanizmima zaštite.

No, s obzirom da ponekad mali propust kod zaštite baze podataka može dovesti do krađe i zlouporabe podataka, potrebna nam je digitalna forenzika – znanost koja pronalazi, analizira, dokumentira i interpretira digitalne dokaze, odnosno podatke koji se prenose u digitalnom obliku. Ona podrazumijeva korištenje računalnih znanosti i istraživačkih metoda, a njome se bave digitalni forenzičari. Digitalni forenzičari koriste različite hardverske i softverske alate te metode i tehnike pomoću kojih pokušavaju pronaći krivca za krađu podataka, zlouporabu podataka ili kibernetički napad.

Svrha ovog rada je ukazati na važnost zaštite baza podataka, obraditi pojam digitalne forenzike i digitalnih dokaza te razraditi tematiku kibernetičkih napada i kako se svatko od nas što bolje može zaštititi od njih.

2. Metode i tehnike rada

Za izradu završnog rada korišteni su brojni internetski izvori, istraživački radovi te knjige. Isto tako korišten je Microsoft Office Word, PostgreSQL te pgAdmin 4.

3. Baza podataka

Baza podataka je skup međusobno ovisnih podataka koji su spremljeni bez zalihosti te se obrađuju u nekoj organizaciji [1]. Zalihost ili rendundancija pojam je koji se često spominje kod sustava za upravljanje bazama podataka, a predstavlja pojavu gdje se u više tablica u bazi pojavljuju „jednaka polja“ (u više tablica pojavljuju se polja sa istim sadržajem).

Baze podataka omogućuju korisnicima jednostavan i brz pristup, organiziranje, unošenje, brisanje i ažuriranje podataka, a pristupaju joj putem sučelja. Obično postoji grafičko korisničko sučelje preko kojeg korisnik razmjenjuje podatke i informacije sa sustavom za upravljanje bazama podataka (SUBP). Ono omogućava definiciju baze podataka, upisivanje i ispisivanje podataka te obradu i korištenje podataka koji se nalaze u samoj bazi.

3.1. Modeliranje podataka

SUBP predstavlja softver čija je osnovna komponenta model podataka [2].
Danas su najzastupljeniji sljedeći SUBP (engl. Database Management Systems):

- My SQL
- Microsoft SQL Server
- Oracle
- DB2
- PostgreSQL
- MongoDB

Model podataka apstraktna je reprezentacija podataka. Čini ga skup pravila koji određuju kako će baza podataka biti logički strukturirana.
Model podataka obuhvaća strukturalnu, integritetnu i operativnu komponentu. Strukturalna komponenta odnosi se na skup koncepata za opis strukture podataka. Integritetan komponenta odnosi se na skup ograničenja za očuvanje integriteta, a operativna komponenta odnosi se na skup operatora kojima je moguće opisati promjenu stanja podataka [2].
S obzirom na nivo apstrakcije model podataka možemo podijeliti na [1]:

1. Konceptualni
2. Logički
3. Fizički

U logičke modele podataka ubrajamo hijerarhijski model podataka, mrežni model podataka, relacijski model podataka, objektni model podataka, itd.

3.2. Relacijski model podataka

Podaci u relacijskom modelu podataka zapisani su u obliku relacija, odnosno tablica [2]. Relacijske se baze podataka zasnivaju na relacijskoj algebri, a pojam relacijske algebre označava skup formalnih operacija nad relacijama relacijske baze podataka.
Relacijski model podataka u teoriji se pojavio davnih 60-ih godina 20.stoljeća, no tada nije bio uvelike korišten, već je svoju veću primjenu doživio 80-ih godina. Današnji sustavi za upravljanje bazama podataka najčešće su temeljeni upravo na relacijskom modelu podataka.

Relacijski model podataka iziskuje da se baza podataka temelji na principu tablica, tj.relacija. Relacija, odnosno tablica, može se sastojati od redova, odnosno n-torki (primjeraka entiteta) te stupaca koji nazivamo atributima. Atribut posjeduje vlastito ime, a vrijednosti jednog atributa istog su tipa. Ukoliko se u relaciji zamijene mjesta redaka ili stupaca, relacija ostaje ista, jedino je zapis te relacije drugačiji.

STUDENT

PK	IME	PREZIME	GODINA_ROĐENJA	GODINA_STUDIJA	MJESTO
1	Emanuel	Manić	1998.	4.	Zagreb
2	Nora	Norić	1999.	3.	Split
3	Noa	Noić	2001.	1.	Zagreb
4	Zorana	Zoranić	1999.	3.	Sisak

Tablica 1 Relacija s podacima o studentu

(Vlastita izrada u Microsoft Office Word 2010.)

Građu relacije opisujemo shemom relacije koja se sastoji od samog imena relacije te popisa imena atributa koje navodimo u zagradama. Svaki od entiteta, u ovom je slučaju jednoznačno određen primarnim ključem (PK) kojeg u shemi relacije prikazujemo podvučenom linijom.

Shema relacije za navedeni primjer glasi:
STUDENT(PK, IME, PREZIME, GODINA_ROĐENJA, GODINA_STUDIJA, MJESTO).
Relacija se naziva STUDENT, primarni ključ je PK, a imena atributa relacije su IME, PREZIME, GODINA_ROĐENJA, GODINA_STUDIJA i MJESTO.

3.3. Jezici za rad s bazama podataka

Najpoznatiji jezici za rad s bazama podataka je SQL. Komponente SQL-a su:

1. **Jezik za opis podataka** (DDL – eng. Data Definition Language) – definiramo na logičkoj razini podatke i vezu između podataka
2. **Jezik za manipuliranje podacima** (DML – eng. Data Manipulation Language) – omogućava unos, brisanje, mijenjanje, ažuriranje baze podataka i slično
3. **Jezik za postavljanje upita** (QL – eng. Query Language) – omogućava postavljanje upita i pretraživanje baze podataka

Ovakva podjela je kod relacijskih baza podataka ujedinjena u jedan integrirani jezik koji se naziva SQL. Njegova zadaća je definiranje, manipuliranje i pretraživanje podataka.

3.4. SQL vs.NoSQL baze podataka

Svaka baza podataka temelji se na odgovarajućem modelu. Danas je to najčešće relacijski model podataka, no postoje i brojni drugi. No, zbog uvećanih zahtjeva (primjerice velikih količina podataka, brzine postavljanja upita, fleksibilnosti sheme, brze promjene podataka) relacijska baza podataka, čija je osnovna komponenta relacijski model, sadrži određene nedostatke te su se zbog toga u posljednje vrijeme pojavile alternative relacijskim bazama podataka, odnosno NoSQL baze podataka.

Usprkos nedostatcima koje SQL baze podataka imaju, one sadrže i brojne prednosti. SQL baze podataka omogućavaju visoku razinu zaštite te budući da podržavaju ACID svojstva (atomnost, konzistentnost, izolacija i trajnost) moguće je osiguravanje pouzdanih transakcija podataka. Isto tako SQL omogućuje jednostavno pohranjivanje i pretraživanje podataka pomoću upita.

NoSQL baze podataka razlikuju se od relacijskih baza tako što omogućuju fleksibilnost sheme te različitost podataka. Svojstvo fleksibilnosti jedno je od najvažnijih svojstava jer omogućuje nadopunjivanje i izmjenu modela baze podataka što znači da model u samom početku ne treba biti u potpunosti završen već s vremenom može biti ažuriran i nadopunjivan. U usporedbi s SQL bazama podataka, NoSQL baze podataka nisu toliko pogodne za postavljanje složenih upita budući da ne postoji fiksna struktura upita kako je to kod SQL baza.

SQL	NoSQL
Relacijske baze podataka.	Nerelacijske baze podataka.
Structured Query Language (SQL).	Ne postoji univerzalni jezik upita.
Relacije (tablice).	Graf-baze/ključ-vrijednosti/dokumenti...
Definirana shema.	Dinamična shema za nestrukturirane podatke
Vertikalna skalabilnost.	Horizontalna skalabilnost.
ACID (Atomna, konzistentna, izolacija, trajnost).	BASE (BA - Većina podataka dostupna većinu vremena, S – Promijenjivo stanje sustava, E – Konzistentnost sustava s vremenom)
Zasnovan na modelu.	Dinamičan model koji nastaje s vremenom.
Izmjena i dodavanje podataka može utjecati na dizajn (smanjena fleksibilnost).	Jednostavna izmjena, dodavanje podataka bez izmjene dizajna.
Nije uvijek najbolje rješenje za Big Data.	Big Data

Tablica 2 SQL vs. NoSQL

(Izrađeno prema: https://www.guru99.com/sql-vs-nosql.html)

3.5. Životni ciklus baza podataka

Životni ciklus baza podataka predstavlja skup faza kroz koje baza podataka (odnosno podaci) mora proći kako bi bila implementirana u neko poduzeće ili organizaciju.

Faze koje čine životni ciklus baza podataka jesu: analiza potreba, modeliranje podataka, implementacija, testiranje i održavanje [3].

3.5.1. Analiza potreba

Analiza potreba prva je i najvažnija faza u životnom ciklusu baza podataka. Ova faza podrazumijeva praćenje i razumijevanje podataka, veza među podacima te kretanje informacija u samom poduzeću. Na taj se način analiziraju informacijske potrebe poduzeća što omogućuje dizajniranje baze podataka u skladu s tim potrebama.
Nadalje, utvrđuju se vrste transakcija koje će se izvršavati u bazi podataka te se definiraju ograničenja integriteta, sigurnosti ili ostala administrativna rješenja koja zatim moraju biti implementirana u finalnoj bazi podataka. Rezultat analize potreba je temeljito napisan

dokument u kojem su evidentirane sve prethodno navedene spicifikacije koje baza podataka mora sadržavati, a naziva se specifikacija potreba.

3.5.2.Modeliranje podataka

Nakon što je odrađena prva faza, odnosno analiza potreba, slijedi modeliranje prethodno otkrivenih podataka. U ovoj je fazi prvotno kreiran konceptualni model koji je obično dijagram entiteta-veza (ER) koji prikazuje entitete(tablice), polja i primarne ključeve baze podataka te njihovu međusobnu povezanost. Nakon toga slijedi normalizacija relacija iz ER dijagrama.

3.5.3.Normalizacija relacijske sheme

Dobro oblikovana baza podataka sastoji se od skupa podataka koji nije redundantan i koji posjeduje semantički integritet.
Redundancija ili zalihost označava da se određeni podatak pojavljuje na više različitih mjesta te to predstavlja nedostatak zbog toga što se obrada redundatnih podataka mora ponavljati. Konzekventno se javljaju anomalije pri dodavanju podataka, brisanju ili izmjeni te se se kao rezultat mogu pojaviti neispravni odgovori na postavljene upite.

Normalizacija je postupak prevođenja relacija iz nižih u više normalne forme s ciljem stvaranja učinkovite i pouzdane baze podataka te osiguravanja fleksibilnosti i optimalnosti baze. Postupak je zasnovan na pojmu normalnih formi, od kojih su 3 najznačajnije: Prva normalna forma (1NF), Druga normalna forma (2NF), Treća normalna forma (3NF); a od kojih se u svakoj sljedećoj dobiva poboljšana, učinkovitija i fleksibilnija struktura baze negoli u prethodnoj.

3.5.4.Implementacija

Treća faza u životnom ciklusu baza podataka je implementacija. Implementacija baze podataka vrši se na osnovi shema te dostupnog SUBP-a. SUBP sadrži parametre kojima se utječe na fizičku organizaciju baze, a njih treba podesiti tako da omoguće što veću efikasnost transakcija [3].
Zaključno možemo reći da je najvažnija funkcija ove faze povećati učinkovitost baze podataka, odnosno osmisliti načine za poboljšanje performansi.

3.5.5. Testiranje

Testiranje je faza u kojoj korisnici rade s bazom podataka i provjeravaju odgovara li ona prethodno specificiranim zahtjevima. Naime, u ovoj fazi trebalo bi biti minimalni broj grešaka jer je preporučljivo da se prije finalne implementacije razvijaju prototipovi baza podataka koje onda testiraju korisnici te se tada ispravljaju greške. Na taj način greške je lakše ispraviti, negoli u finalnoj implementaciji baze u samom poduzeću. Najčešće se prototipovi izrađuju pomoću jezika 4.generacije i objektno-orijentiranih jezika.

3.5.6. Održavanje

Održavanje je posljednja faza u životnom ciklusu baza podataka. Faza održavanja kreće kada je odrađena implementacija baze. U ovoj fazi dolazi do ispravaka prethodno neotkrivenih grešaka te uvođenje nekih promjena, dodataka ili preinaka. Ova faza omogućava da se konstatno usavršava baza te da se implementiraju novi zahtjevi na način da se ne ometa rad korisnika [3].

4. Sigurnost baza podataka

Sigurnost baza podataka obuhvaća metode zaštite baze podataka od neovlaštenog pristupa, preinaka ili uništenja podataka. Osim važnosti zaštite samih podataka, bitno je i zaštititi privatnost samih korisnika čije podatke baza sadrži.
Zaštita informacija definirana je po CIA (engl. *Confidentiality Integrity Availability*) modelu [4].
Povjerljivost (engl. *Confidentiality*) podrazumijeva da korisnički podaci budu zaštićeni od nedozvoljenih pristupa kako bi očuvali svoju privatnost. Održavanje povjerljivosti odnosi se na različite metode enkripcije podataka kako nebi došlo do razotkrivanja i zlouporabe povjerljivih informacija. Uz enkripciju koriste se i procesi autorizacije, identifikacije i autentifikacije.
Integritet (engl. *Integrity*) se odnosi na korektnost vrijednosti podataka te na međusobnu suglasnost između podataka. Isto tako, važno je napomenuti da podaci moraju biti zaštićeni od nedopuštenih izmjena kao što su umetanje neželjenih podataka, mijenjanje stanja podataka, ažuriranje i slično kako ne bi došlo do gubljenja integriteta što može dovesti do daljnjih nepravilnosti u sustavu te pogrešnih odluka.
Pravila za čuvanje integriteta [5]:

1. Pravila za čuvanje integriteta domene
2. Pravila za čuvanje integriteta unutar relacije
3. Pravila za referencijski integritet

Raspoloživost (engl. *Availability*) se odnosi na dostupnost informacija u trenutku zahtijevanja autoriziranih korisnika.

4.1. Sigurnosne prijetnje

Sigurnosne prijetnje su događaji ili situacije koje mogu štetiti sustavu kompromitirajući privatnost i/ili povjerljivost baza podataka [4].

4.1.1. Namjerne sigurnosne prijetnje

Namjerne sigurnosne prijetnje pojavljuju se kada korisnik s namjerom izvodi neovlašteni pristup podacima u bazi podataka kako bi naštetio pojedincu ili organizaciji. Postoje brojne vrste namjernih sigurnosnih prijetnji, a neke od njih jesu špijunaža, softverski napadi, iznuda podataka, krađa identiteta te kibernetički napadi.
Špijunaža se događa kada neovlaštena osoba pokušava ilegalno dohvatiti informacije određene organizacije. Razlikujemo konkurentsku, odnosno obavještajnu špijunažu te industrijsku špijunažu. Konkurentska špijunaža odnosi se prikupljanje podataka i informacija

od organizacijskih konkurenata, prikupljanja tehnika i slično s ciljem poboljšanja vlastitih proizvoda i/ili usluga te se ona ne smatra ilegalnom dok industrijska špijunaža prelazi zakonske regulative.
Softverski napadi današnjice sofisticiraniji su negoli na početku. U prošlosti je cilj softverskih napada, odnosno širenja zlonamjernih programa bio zaraziti što veći broj računala, a danas se napadi baziraju prvenstveno na zaradi i to putem interneta.
Iznuda podataka događa se kada napadač traži od „insidera“ u tvrtci otkrivanje tajnih informacija, prijeti mu ili traži novac u zamjenu za njegovu slobodu.
Pod **krađom identiteta** podrazumijevamo ilegalno preuzimanje tuđih podataka i predstavljanje pod drugim identitetom u svrhu dobivanja pristupa financijskim detaljima dotične osobe.
Kibernetički napad je svaki pokušaj otkrivanja, izmjene, prikupljanja, krađe ili dobivanja podataka i informacija preko neovlaštenog pristupa.

4.1.2.Nenamjerne sigurnosne prijetnje

Nenamjerne sigurnosne prijetnje jesu događaji ili situacije nastale nenadano bez zle namjere, ali predstavljaju prijetnju informacijskoj sigurnosti.
Primjeri nenamjernih sigurnosnih prijetnji jesu slanje e-maila pogrešnoj osobi te se na taj način otkrivaju povjerljive informacije. Nadalje, ukoliko osoba zatraži pristup određenoj funkcionalnosti u aplikaciji bez odgovarajućeg ovlaštenja, može je izvršiti i slično.

Više o sigunosnim prijetnjama te inernetskim napadima biti će objašnjeno u poglavlju Kibernetički kriminalitet.

4.2. Kontrola pristupa

Kontrola pristupa služi kao kontrola tko ima pristup podacima u bazi podataka kako bi podaci bili osigurani od neovlaštenog pristupa.

a) **Autentikacija**
   Ovom provjerom provjerava se je li osoba koja želi pristupiti podacima u bazi podataka ona za koju se tvrdi, odnosno utvrđuje se sam identitet osobe. Provjera se odvija na način da korisnik unosi svoje korisničko ime i lozinku kako bi korisniku bio odobren pristup podacima.

b) Korisničke ovlasti

Nakon što je korisniku odobren pristup bazi podataka, on unutar baze ovisno o njegovim ovlastima može obavljati određene zadatke. Korisničke su ovlasti određene privilegijama koje predstavljaju aktivnosti kao što su dodavanje objekata u bazu, brisanje, uređivanje i slično.

c) Pogledi

Pogledi skrivaju od korisnika određene dijelove baze podataka kojima nemaju pristup jer su osjetljive prirode. Oni se stvaraju prilikom izrade upita nad tablicom.

d) Revizijski trag

Revizijski trag predstavlja bilježenje svih aktivnosti korisnika koje obavlja u bazi podataka. Pritom je važno napomenuti kako su administratoru baze podataka vidljive sve aktivnosti korisnika pa tako i pokušaji izvođenja neovlaštenih radnji, stoga je veoma lako doći do podataka tog korisnika.

e) Kontrola toka

Kontrola toka služi za praćenje informacija unutar određenih objekata. Pomoću kontrole toka upravlja se brzinom prijenosa informacija te se definiraju kanali kojima se informacije mogu izmijenjivati.

5. Enkripcija podataka

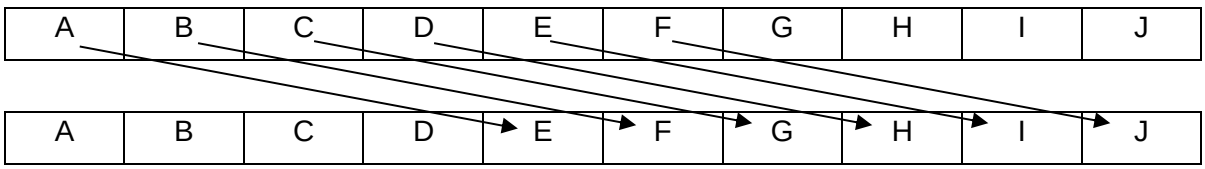
Enkripcija baze podataka obavlja se kako bi se dodatno zaštitili podaci od neovlaštenog pristupa. Jednostavno rečeno, enkripcija funkcionira na način da se određeni podatak, primjerice lozinka, sprema u bazu podataka na način da se „izmiješaju slova“ na temelju dogovorenog ključa za kojeg zna samo taj SUBP. Na taj način kada ovlašteni korisnik želi dohvatiti podatke iz baze za koje ima dopušten pristup može pomoću odgovarajućeg enkripcijskog ključa vrlo lako dohvatiti.
Enkripcija se može uporabiti u slučaju slanja poruka na način da se enkriptiraju poruke kako bi u slučaju krađe ili preusmjeravanja poruka sadržaj poruke ostao nedohvaćen zbog zaštićenosti odgovarajućim ključem enkripcije.
Enkripcija zahtjeva sustav za šifriranje koji se sastoji od:

1. Ključa za enkripciju
2. Algoritma za enkripciju (tekst pretvara u kriptirani tekst)
3. Ključa za dekripciju
4. Algoritma za dekripciju (kriptirani tekst pretvara u čitljiv tekst)

5.1. Povijest enkripcije podataka

5.1.1. Cezarova šifra

Prvi put kada je šifriranje upotrijebljeno u vojne svrhe dogodilo se prije više od dvije tisuće godina za vrijeme vladavine Rimljana kada je tadašnji car Cezar trebao pronaći način kako da pošalje komunikacijske poruke svojim trupama na terenu. Tada je smislio jednostavno šifriranje poruka koje se naziva Cezarova šifra (engl. *Ceaser Cipher*). Cezarova šifra vrlo je jednostavan način šifriranja u kojem se svako slovo teksta u riječi zamjenjuje određenim slovom abecede pomaknutim za određeni definirani broj (ključ enkripcije). U nastavku je prikazan primjer pomaka za 4.



Slika 1. Cezarova šifra

(Vlastita izrada u Microsoft Office Word 2010)

5.1.2.Jefferson's disks

Thomas Jefferson 1790-ih godina izumio je tzv. Jeffersonove diskove, odnosno engl. „*wheel cypher*“. Naprava se sastojala od 36 drvenih diskova od kojih su se na svakom nalazila nasumično poredana slova abecede [6]. Ova naprava nije bila isprva prihvaćena, već se ona počela koristiti između 1920-ih i 1950-ih u vojne svrhe, no zanimljivo je napomenuti kako vojska nije znala da je to Jeffersonov izum jer je naprava bila preimenovana u M-64.

Način na koji Jeffersonovi diskovi obavljaju kriptiranje podataka jest da se prvotno trebaju poredati identični diskovi te kao takvi poslati osobi s kojom se namjerava komunicirati. Nakon toga poreda se 36 slova teksta uzduž jednog retka po svim diskovima. Nakon toga odabere se bilo koji redak izmiješanih slova te je to šifrirani tekst. Nakon toga nastavi se princip šifriranja za sva ostala slova.

Da bi se poruka dešifrirala, primatelj mora slagati šifrirani tekst uzduž retka svih diskova te pretražiti svih 25 redaka tražeći jedan koji ima smisla [6].

5.1.3.Enigma

Enigma je uređaj kojeg su prvotno osmislili Nijemci za komunikaciju između vojnika tijekom Drugog svjetskog rata. Sam uređaj bio je smješten u malu drvenu kutiju zbog čije je veličine bio jednostavan za nošenje i dovoljno malen da ga posjeduje i koristi svaki od njemačkih vojnika. Uređaj je bio napravljen u obliku pisaćeg stroja.

Enigma kod prvotno su dešifrirali Poljaci u ranim 1930-im pod vodstvom matematičara Mariana Rejewskog [7].

Enigma radi na principu elektromehaničkog rotorskog mehanizma koji kodira među 26 slova abecede. Pritiskom tipke na tipkovnici zasvijetli se slovo kojim je ono zamijenjeno u šifriranoj poruci. Obrnuto, da se dešifrira poruka, unese se šifrirani tekst, a slova koja zasvijetle originalni su tekst. Unutar kutije sustav je izgrađen oko tri fizička rotora. Svaki uzima slovo i prikazuje ga kao drugo. To slovo prolazi kroz sva tri rotora, odbija se od "reflektora" na kraju i prolazi natrag kroz sva tri rotora u drugom smjeru.

5.2. Oblici enkripcije

Postoje dva oblika enkripcije: simetrični i asimetrični. Oba oblika nude sigurnost pri prijenosu podataka, no razlikuju se u tome što asimetrična enkripcija ne iziskuje distribuciju privatnog ključa što pridonosi većoj sigurnosti.

1. Simetrična enkripcija – jedan ključ koristi se za kodiranje i dekodiranje
   Prednosti:

- Velika brzina i jednostavnost implementacije
- Mala duljina ključa

Nedostaci:

- Složenost razmjene ključa
- Nemogućnost korištenja digitalnih potpisa
- Potreba traženja pouzdanog kanala za prijenos ključa

2. Asimetrična enkripcija – jedan ključ po algoritmu

   Prednosti:

   - Ključ dešifriranja poznat samo jednoj strani
   - Čuvanje ključa na sigurnom mjestu

   Nedostaci:

   - Dugačak ključ šifriranja
   - Sporija brzina dešifriranja
   - Potreba za velikim računalnim resursima

[8]

5.3. Standardi za kriptiranje

1977. razvijen je standard za enkripciju podataka (engl. *Data Encryption Standard* – DES). DES koristi 56-bitni ključ na 64-bitni blok teksta kojim se stvara 64-bitni blok kriptiranog teksta te se posljedično pri kriptiranju podaci razdvajaju na 64-bitne blokove. U blokovima se znakovi premještaju u skladu s vrijednosti ključa. DES algoritam temelji se na simetričnoj enkripciji podataka te sve što je potrebno za njegovu specifikaciju jest okrugla funkcija, raspored ključa te početna i konačna permutacija.

AES (engl. *Advanced Encryption Standard*) nastao je 2001. godine. AES uključuje tri blok šifre: AES-128 (128-bitna duljina ključa), AES-192 (192-bitna duljina ključa) i AES-256 (256-bitna duljna ključa). Vlada klasificira informacije u tri kategorije: povjerljive, tajne te strogo povjerljive. Svaka od duljina ključeva može se koristiti za zaštitu povjerljive i tajne razine podataka dok strogo povjerljive informacije zahtijevaju duljinu ključa od 192 ili 256 bita [9].

6. Kibernetički kriminalitet

Kibernetički kriminalitet je aktivnost koji mogu provoditi pojedinci ili organizacije, a odnosi se na kriminalnu aktivnost koja kao sredstvo koristi računalo, računalnu mrežu ili umreženi uređaj. Iako kriminalci pokušavaju prikriti svoje tragove, oni često ostavljaju tragove o svom identitetu i mjestu te se ti tragovi moraju slijediti kako bi se uhvatili kriminalci te spriječilo daljnje širenje krhkih i osjetljivih podataka.

Najčešće cyber kriminalci koriste napredne tehnike te posjeduju vrhunske tehničke vještine. Isto tako, kibernetički kriminal u većini slučajeva događa se zbog zarade, a rijetko zbog nekih drugih osobnih ili političkih razloga.

6.1. Povijest

1940-ih godina kibernetički kriminalitet još uvijek nije bio razvijen. Pristup jakim digitalnim uređajima bio je ograničen na mali broj ljudi koji su se njima znali koristiti tako da kibernetički kriminalitet gotovo nije ni postojao.
1940. godine Rene Carmille, pripadnik Otpora u nacističkoj Francuskoj, doznaje da nacisti koriste različite uređaje za pronalazak Židova. On je bio stručnjak za računala te je za francusku vladu Vichy prikupljao razne informacije [22].

1955. godine Joe Engressia (Joybubbles), slijepi sedmogodišnjak, je čuo visoki ton na telefonskoj liniji te počeo zviždati na frekvenciji od 2600Hz te na taj način komunicirao preko telefonskih linija i postao prvi američki telefonski haker (engl. *phone freak*) [21]. Izraz „*phone freaking*“ sve se više počeo koristiti krajem 50-ih godina te se odnosio na ljude koji presreću protokole koji su telekomunikacijskim inženjerima omogućavali daljinski rad na mreži radi besplatnih poziva [22].

1969.godine pojavio se virus koji se smatra prvim računalnim virusom pod nazivom „*Rabbit Virus*“. Na Sveučilištu u Washingtonu anonimna je osoba instalirala zloćudni program na računalo koji je na računalu radio svoje kopije sve dok se računalo nije preopteretilo i prestalo raditi [22]. Već u ovom razdoblju su tvrtke počele investirati u tehnologije koje su pomagale u očuvanju sigurnosti podataka te upravljanju podacima i sustavima.

1970-e godine možemo nazvati godinama rasta i važnosti internetske sigurnosti. Kako su organizacije sve više počele koristiti telefoniju te je umrežavanje raslo, svaki dio povezanog hardvera trebalo je dodatno zaštiti. Svima je postalo jasno koliko je važna sigurnost i zaštita podataka [21]. Najtraženiji kriminalac tog vremena bio je Kevin Mitnick koji je s kibernetičkim kriminalom započeo 1970. godine pa sve do 1995. On je uspio hakirati

neke od najčuvanijih mreža na svijetu kao što su Nokia i Motorola, a pritom je koristio različite inženjerske tehnike [22].

1987. godina bila je godina rođenja komercijalnog antivirusa [21]. Godinu dana kasnije, Robert Morris stvorio je ono što je danas poznato kao prvi crv na internetu. Crv je pušten s računala na MIT-u da bi se moglo sugerirati da je tvorac tamošnji student, no ta vježba rezultirala je puno bržom brzinom zaraze, negoli su to očekivali. **1989**. godine pojavio se Trojanski konj. Tisućama istraživača AIDS-a poslana je disketa koja je navodno sadržavala bazu podataka o AIDS-u, no zapravo je sadržavala destruktivni program [22].

90-e su bile godine kada je naglo porastao interes za umrežavanjem te je internet postao jedna od glavnih tematika. Stvoreni su prvi poliformni virus, Britanski računalni magazin je objavio izdanje s besplatnim diskom koji je sadržavao virus te je osnovan EICAR (Europski institut za računalna antivirusna istraživanja) [21].

Kako je internet postajao rasprostranjeniji te dostupniji sve većem broju ljudi, kibernetički kriminalci imali su mogućnost pristupa sve većem broju osjetljivih i krhkih podataka i softvera negoli ikad prije. Nakon 2000.godine tvrtke su sve veću pažnju počele pridavati zaštiti osjetljivih podataka te različitim metodama enkripcije kako bi mogli zaštititi svoje korisnike. Isto tako, sve veću ulogu danas ima forenzika baza podataka koja pomaže u vraćanju ukradenih podataka.

6.2. Vrste kibernetičkih napada

Većina kibernetičkih napada spada u dvije kategorije: kibernetički napad koji ciljano napada računalo pomoću virusa i drugih vrsta zlonamjernih softvera te kibernetički napad koji koristi računala za počinjenje drugih kaznenih kriminalnih djela.

1. **Internetska prijevara**

   Internetska prijevara je upotreba internetskih usluga ili softvera pomoću interneta s ciljem prevare žrtava. Preko internetskog kriminala, od ljudi se godišnje ukradu milijuni dolara različitim inovativnim prevarama [23]. Internetske su prevare dobro prikrivene kako bi bilo što lakše nasjesti na njih, a ciljim je iznuda povjerljivih podataka ili zadobivanje profita. Glavno obilježje je njihova realnost te se najčešće šalju putem e-maila.

   Neke od internetskih prevara su:

   a) ***Phishing prevare***

      Phishing je najčešća internetska prevara kojoj je glavni cilj doći do povjerljivih podataka kao što su lozinke društvenih mreža, detalji o bankovnim računima i slično. Phishing funkcionira na način da se od ljudi traže prethodno navedeni podaci

u svrhu verifikacije računa, unapređivanja sigurnosnog sustava ili drugih sličnih uvjerljivih razloga.

*b) **Ransomware napad***

Ransomware je oblik zlonamjernog softvera usmjeren na ljudske i tehničke slabosti u organizacijima kojem je cilj dohvaćanje kritičnih podataka i/ili sustava. Kada organizacija utvrdi da više ne može pristupiti svojim podacima, cyber počinitelj zahtijeva plaćanje otkupnine [23].

*c) **DoS napad***

DoS (engl. Denial of Service) odnosi se na prekid pristupa ovlaštenog korisnika bilo kojem sustavu ili mreži [23].

2. **Krađa identiteta**

Krađa identiteta (engl. Identity theft) odnosi se na vrstu kibernetičkog kriminala lažnog predstavljanja radi zadobivanja materijalne ili neke druge koristi. Najčešće se događa zbog pribavljanja osobnih ili financijskih podataka te korištenje ukradenog identiteta za počinjenje prevara, transakcija i raznih kupnji.

3. **Cyber špijunaža**

Kibernetička špijunaža je čin pribavljanja tajnih podataka te informacija bez dopuštenja i unanja nositelja podataka. Kibernetičkom špijunažom različitim internetskim metodama postiže se zadobivanje neke vrste prednosti, bilo to osobne, ekonomske, vojne ili političke koristi.

6.3. Obrana od kibernetičkih napada

Tvrtke raznih veličina još uvijek misle da će za zaštitu korisničkih podataka te sigurnost sustava biti dovoljno razviti strategiju za kibernetičku sigurnost te da je njeno postojanje te provođenje sigurnosnih politika jedino rješenje za zaštitu od kibernetičkog kriminala.

Kako bi se organizacije što uspješnije zaštitile od kibernetičkih napada, potrebno je koristiti različite sigurnosne mjere u poslovanju. Osim korisničkih imena i lozinka koje svaki djelatnik ima, zaposlenici bi trebali proći edukaciju o sigurnom korištenju interneta te potencijalnim opasnostima kako bi se spriječio bilo kakav pokušaj neovlaštenog pristupa i krađe podataka. Isto tako, za svakog zaposlenika preporučljivo je da instalira aplikaciju za geolokacijski pronalazak uređaja u slučaju njegove krađe. Nadalje, bitno je napomenuti kako bi svaki zaposlenik trebao stvarati sigurnosne kopije podataka koji bi se pohranjivali na drugim

lokacijama. Na taj način, u slučaju gubitaka podataka, vrlo će lako moći povratiti podatke te neće biti na meti ucjenjivača [24].

Isto tako, da povećaju sigurnost u svojoj okolini, poduzeća mogu ograničiti pristup neprikladnim i nepotrebnim web mjestima za tu organizaciju kako bi se smanjio rizik od izloženosti zlonamjernim programima. Nadalje, kako bi se dodatno zaštitili od vanjskih prijetnji, mogu povećati zaštitu svojih mreža koristeći proxy te popis pristupa.

5 načina zaštite podataka prema Popatu [24]:

1. Sigurnost hardvera
2. Enkripcija i izrada sigurnosnih kopija podataka
3. Investiranje u osiguranje kibernetičke sigurnosti
4. Edukacija zaposlenih o sigurnosti (radna mjesta fokusirana na sigurnost)
5. Korištenje softvera za zaštitu od zlonamjernih programa i vatrozid

7. Digitalna forenzika

Digitalna forenzika jedna je od relativno novijih znanosti, odnosno grana forenzičke nauke. Osnovni cilj digitalne forenzike je da različitim metodama i tehnikama prikuplja te procesira dokaze (podatke) pohranjene na računalu ili nekom drugom digitalnom mediju koji su vezani uz određene ilegalne radnje.

7.1. Definicija

Digitalna forenzika definirana je kao uporaba znanstveno izvedenih i dokazanih metoda za očuvanje, prikupljanje, provjeru valjanosti, identifikaciju, analizu, tumačenje, dokumentiranje i iznošenje digitalnih dokaza izvedenih iz digitalnih izvora u svrhu olakšavanja utvrđivanja događaja koji su moguće kriminalni ili u svrhu predviđanja neovlaštenih radnji za koje se pokazalo da remete rutinske radnje [10].

7.2. Povijest

Iako uporaba znanosti u kriminalnim istragama postoji još od prije vremena Rimskog Carstva, ideja forenzičke znanosti kao discipline stara je tek stotinjak godina. Do sredine 19.stoljeća raspravljalo se o toj znanosti, no njezina primjena nije bila u potpunosti definirana.

Prva uporaba znanstvenih studija za vođenje kriminalističke istrage vezana je uz znanstvenika Hansa Grossa [11]. Hans Gross bio je austrijski profesor i sudac koji se smatra jednim od osnivačem kriminalistike zbog knjige objavljene 1891. godine pod nazivom *Handbuch fur Untersuchungsricter als System Der Kriminalistik* koja je 1907. godine objavljena na engleskom jezikom pod nazivom *Criminal Investigation*.
24.11.1932. smatra se datumom kada je FBI osnovao laboratorij kao pomoć terenskim agentima i drugim pravnim tijelima diljem SAD-a [11]. Osnivanje laboratorija odvijalo se kroz nekoliko mjeseci, no ovaj datum uzima se kao službeni nakon što je agent Appel uz pomoć tehnologije riješio kriminalni slučaj.
Nadalje, važan događaj za digitalnu forenziku bio je 1978. godine kada je prepoznat prvi računalni zločin [11].
Digitalna forenzika kao znanost stoga postoji otprilike četrdesetak godina. U samim počecima, digitalna forenzika bila je korištena od stručnjaka koji su surađivali s pravnim tijelima.

Ranu digitalnu forenziku karakterizira raznolikost hardvera, softvera i aplikacija, oslanjanje na centralizirana računalna postrojenja te nedostatak alata i metodologije [12].
Procvat digitalne forenzike obilježava manja raznolikost softvera i hardvera, ograničene istrage na jedan računalni sustav koji je pripadao osumnjičeniku, više dobavljača koji dobavljaju alate korisne za oporavljanje obrisanih datoteka, široka primjena Windowsa XP [12].
Nakon 2007. godine digitalna forenzika nije se znatno razvijala. Stagnaciji razvoja digitalne forenzike pridonijela je velika brzina razvoja tehnologije i nemogućnost brze obrade svih podataka i kreiranja forenzičke slike; veća razina enkripcije, zaštite podataka; nastanak oblaka.

7.3. Digitalni forenzičari

Istražitelji digitalne forenike stručnjaci su za pronalaženje, čuvanje, obradu i analizu podataka iz različitih izvora. Digitalni forenzičari često imaju kritičnu ulogu u istrazi kršenja kibernetičke sigurnosti. Oni nisu zaslužni samo za istraživanje prekršaja i zločina povezanih s računalima i putem interneta, već i za istragu izvanmrežnih slučajeva kao što su automobilske nesreće i slično [13].

Posao digitalnih forenzičara jest prikupljanje ključnih podataka, razvijanje strategije pronalaska osumnjičenika za kriminalno djelo te defineniranje metoda i alata koji će se koristiti prilikom same istrage. Najpoznatiji su po radu u analizi podataka u pravne svrhe, no digitalni forenzičari mogu biti i zaduženi za testiranje sigurnosti informacijskih sustava. Isto tako, kada je oprema oštećena, digitalni forenzičar mora pokušati obnoviti sustav kako bi oporavio izgubljene podatke. Nakon što povrati podatke, mora pisati izvještaje u kojima detaljno opisuje kako su zadobiveni svi računalni dokazi te koji su koraci i postupci poduzeti u njihovom zadobivanju.

Važne kompetencije digitalnih forenzičara:

- Izvrsno poznavanje svih aspekata računalnog sustava
- Poznavanje zakona, propisa, politike i etičkih pravila vezana uz računalnu sigurnost i privatnost
- Poznavanje sigurnosnih prijetnji
- Poznavanje koncepata obrnutog inženjerstva
- Poznavanje anti-forenzičke strategije, tehnika i postupaka
- Poznavanje metodologija hakiranja i algoritama šifriranja

[13]

7.4. Vrste digitalne forenzike

Digitalnu forenziku možemo podijeliti na sljedeće vrste:

1. Forenzika datotečnih sustava
2. Mrežna forenzika
3. Forenzika mobilnih uređaja
4. Forenzika e-maila i interneta

[14]

7.4.1. Forenzika datotečnih sustava

Kako bi se olakšala forenzička istraga nad datotečnim sustavom, može se podijeliti na tri komponente [14]:

1. **Poznavanje datotečnog sustava:**
   Za pohranu i dohvaćanje, datotečni sustavi koriste metapodatke koji uključuju datum stvaranja datoteke, promjene u datoteci i slično. Same datoteke pohranjuju se na medij u obliku sektora. Neiskorišteni sektori mogu se iskoristiti za pohranu podataka u blokovima (skupinama sektora). Definirana struktura datotečnog sustava veoma je bitna jer ukoliko ne bi postojala, dohvaćanje i brisanje određene datoteke ne bi bilo moguće.
2. **Pronalazak i pravilna interpretacija artefakata unutar OS-a**
3. **Upotreba odgovarajućih forenzičkih alata**

7.4.2. Mrežna forenzika

Mrežna forenzika kao znanost ima za zadaću nadziranje i analiziranje računalnog mrežnog prometa uključujući LAN/WAN mreže kao i internetski promet. Glavni zadaci mrežne forenzike jesu hvatanje, prikupljanje, otkrivanje, bilježenje i analiziranje mrežnog prometa s ciljem utvrđivanja ugroženosti podataka te otkrivanja i istraživanja kriminalnog djela.

Neke od tehnika koje mrežna forenzika koristi jesu analiza statističkog tijeka, analiza mrežnih paketa, analiza upada u mrežnu arhitekturu, prepoznavanje upada u mrežni sustav poduzeća i slično.

7.4.3. Forenzika mobilnih uređaja

Forenzika mobilnih uređaja bavi se ispitivanjem i analizom mobilnih uređaja. Primarni zadaci ove vrste forenzike jesu obnavljanje digitalnih dokaza ili podataka s mobilnih uređaja.

To može uključivati podatke o pozivima, porukama, informacije o lokacijama ili web-mjestima i tako dalje.
Postoje tri glavne metode kojima se dobavljaju podaci s mobilnog uređaja:

1. Ručna ekstrakcija (ručno pristupanje podacima na mobilnom uređaju)
2. Logička ekstrakcija (digitalni forenzičar se preko Bluetootha-a spaja na mobilni uređaj i dohvaća podatke koji su dostupni preko operacijskog sustava)
3. Fizička ekstrakcija (neprestano umetanje zapisa na mobilni uređaj kako bi eventualno zapisi izašli kroz komunikacijski kanal u vanjski uređaj za pohranjivanje podataka)

[15]

7.4.4. Forenzika e-maila i interneta

Forenzika e-maila bavi se analiziranjem i oporavljanjem e-mail adresa, uključujući izbrisane e-mailove, kontakte, kalendare i slično.

7.5. Proces digitalne forenzike

Proces digitalne forenzike odvija se na sljedeći način [11]:

- Identifikacija
- Očuvanje
- Analiza
- Dokumentacija
- Prezentacija

Prvi korak u procesu digitalne forenzike je proces identifikacije. Identifikacija obuhvaća prepoznavanje dokaza, gdje su smješteni podaci te kako su formatirani. Nadalje, u ovom koraku identificiraju se potrebni resursi za istragu te sama svrha istrage.
Sljedeći korak je očuvanje prikupljenih podataka. U fazi očuvanja čuvaju se i izoliraju prikupljeni podaci.
U fazi analize digitalni forenzičari proučavaju prikupljene podatke i vrše određene analize nad digitalnim dokazima. Nakon obavljenih analiza vrše zaključak izveden iz samih dokaza.
Nakon analize slijedi dokumentacija digitalnih dokaza te na kraju prezentiranje rezultata provedene digitalne forenzike te objašnjenje zaključaka i postupaka korištenih pri samom procesu.

7.6. Digitalni dokazi

Digitalni uređaji rasprostranjeni su širom svijeta te su omogućili veoma jednostavno komuniciranje te različite vrste interakcija između ljudi bez obzira gdje se nalazili. Kao izvor digitalnih dokaza najčešće se uzimaju računala, mobiteli te internet, no bitno je napomenuti kako se bilo koji tip tehnologije može upotrijebiti u ilegalne svrhe. Tako primjerice ručne igre mogu nositi kriptirane poruke za međusobnu komunikaciju između kriminalaca. Stoga, digitalni forenzičari moraju veoma brzo prepoznati i moći pravilno iskoristiti svaki potencijalni digitalni uređaj za digitalne dokaze.

Digitalni dokazi su podaci pohranjeni ili preneseni u binarnom obliku obično spremljeni na tvrdom disku računala, mobilnom telefonu i slično. Digitalni se dokazi često povezuju s elektroničkim kriminalom, no sve češće se koriste i za kazneni progon svih vrsta kaznenih djela, a ne samo elektroničkog kriminala.

Vrste digitalnih dokaza [16]:

1. Izbrisivi – Memorija koja izgubi sadržaj nakon isključivanja napajanja poput podataka pohranjenih u RAM-u
2. Neizbrisivi – Bez promjene sadržaja i kad nema napajanja (kaseta, tvrdi disk, CD...)

Za prikupljanje digitalnih dokaza potrebna su različita znanja i specifične vještine. Problem koji se javlja je to što se kod digitalnih dokaza mijenjaju metode zbog toga što se mijenjaju i uređaji na kojima dokazi bivaju pohranjeni, ali i vrlo je jednostavno promijeniti podatke u digitalnom obliku ili ih obrisati. Isto tako, na digitalne dokaze mogu utjecati i ekstremne temperature koje mogu promijeniti i sam fizički uređaj te komponente na kojem se dokazi nalaze. Stoga je važno da prikupljanju digitalnih dokaza pristupaju certificirani stručnjaci koji posjeduju vještinu prikupljanja digitalnih dokaza i kreiraju dokumentacije koja posljedično dokazuje cjelovitost prikupljenih podataka.

8. Forenzika baza podataka

Kako korporacije poduzimaju velike mjere zaštite te primjenjuju sve modernije načine kriptiranja podataka, tako i hakeri razvijaju svoje metode napada što rezultira izlaganjem osjetljivih podataka te same privatnosti korisnika. Zbog toga je potrebna digitalna forenzika baza podataka.

Forenzička istraga potrebna je kako bi se prikupili eventualni digitalni dokazi te utvrdilo kakav kriminal je počinjen te tko i kako ga je počinio. S obzirom da ne postoji standardizirana metodologija i pristup koji bi digitalni forenzičar trebao slijediti prilikom istraživanja, oni moraju polaziti iz različitih izvora te osmisliti vlastiti pristup kako bi što uspješnije mogli povratiti digitalne dokaze te pronaći krivca za kriminalno djelo.

Prilikom prikupljanja baza podataka za analizu one se obavezno moraju kopirati te se analiza mora obaviti na kopiji izvorne baze kako bi otkriveni dokazi bili prihvatljivi u eventualnom sudskom procesu.

Forenzika baza podataka bitna je zbog sljedećeg:

- Baze podataka djeluju kao primarni izvor elektroničkih dokaza za svaku organizaciju bez obzira na njezinu veličinu i složenost
- Potreba brze reakcije za oporavkom baze podataka je posljednjih godina naglo porasla
- Često se informacije o kriminalnim radnjama čuvaju na digitalnim uređajima, stoga je bitna istraga uređaja koja je posljedično dovela do razvoja same digitalne forenzike

[14]

Iako je forenzika baza podataka mlada znanost te za nju ne postoje standardizirani postupci i metode kojima se obavlja postupak istraživanja, dohvaćanja i analize podataka, postoje neki generalizirani koraci koji mogu olakšati istragu, a to su:

1. Kreiranje kopije baze podataka
2. Obnavljanje izgubljenih podataka
3. Analiza i dešifriranje podataka te pronalazak razloga njihove oštećenosti
4. Analiza i kontrola korisničkih aktivnosti

[17]

8.1. Podjela forenzike baze podataka

Beyers forenziku baza podataka dijeli u tri dimenzije:

- Forenzika izmijenjenih baza podataka
- Forenzika ugroženih baza podataka
- Forenzika oštećenih baza podataka.

[14]

8.1.1. Forenzika izmijenjenih baza podataka

Pod terminom izmijenjene baza podataka podrazumijevamo bazu podataka koja nije bila kompromitirana ili uništena prilikom kriminalnog djela, no u njoj su izvedene promjene koje su potom utjecale na samu istragu podataka. Kako baza podataka nije kompromitirana i uništena, već samo sadrži izmijenjene podatke, tako je teža njena istraga i analiza jer nema nikakvih lako vidljivih znakova uništenja ili ugroženosti same baze podataka, a promjene koje su nastale nad SUBP posljedica su svakodnevne uporabe baze podataka.

Fasan i Olivier istraživali su kako se baza podataka može rekonstruirati iako je nastao veći niz promjena nad njome. Istraživači su predstavili pojam logova relacijske algebre, blokova vrijednosti te inverzne relacijske algebre. Isto tako, predložili su algoritam rekonstrukcije baze podataka koji se provodi upotrebom loga relacijske algebre te inverznim funkcijama [14].

8.1.2.Forenzika ugroženih baza podataka

Ugroženu bazu podataka možemo definirati kao bazu podataka u kojoj je napadač modificirao neke od metapodataka ili softver SUBP-a, no baza podataka još je uvijek operativna. Velik nedostatak kod forenzike ugroženih baza podataka je taj što digitalni forenzičar ne može vjerovati podacima koji su pohranjeni u bazi jer ne može sa sigurnošću znati jesu li ti podaci već izmijenjeni prije negoli je istraga pokrenuta.

Postoje različiti načini kojima se može ugroziti baza podataka, a neki od njih su:

- Zamjena imena dviju baza podataka
- Promjena prava uloga
- Pogreške u konfiguraciji baze podataka u oblaku
- Slaba autentifikacija
- Kreiranje pogleda koji zamjenjuje tablicu
- Nesigurna arhitektura sustava

8.1.3. Forenzika oštećenih baza podataka

Pod forenzikom oštećenih baza podataka klasificiramo baze podataka koje su oštećene, djelomično uništene prilikom brisanja, uređivanja ili prilikom kopiranja s originalne lokacije na neka druga mjesta.

8.2. Alati za forenzičku analizu baze podataka

Kako ne postoji strogo definirana metodologija te standardi za forenzičku analizu baze podataka, tako ne postoje ni namjenski alati samo za forenzičko analiziranje baze podataka. Neki od alata koji se koriste za analizu baza jesu:

1. **ProDiscover Forensic**

   ProDiscover Forensic pokrenut je 2001. godine te se od tada koristi u više od 70 zemalja širom svijeta [18]. Ovaj alat razvijen je kao sigurnosni alat koji pomaže istražiteljima u otkrivanju podataka na disku računala. Alat funkcionira na način da kreira kopiju toka podataka diska koju zatim cijelu pretražuje. Isto tako, omogućuje i pronalazak skrivenih i obrisanih datoteka. Prednosti ovog alatu su brzina, točnost, lakoća upotrebe i pristupačnost [18].

2. **Idea**

   Idea je softver za osmišljen za detekciju prevara i analizu podataka. Prednosti ovog alata za analizu je otkrivanje promjena napravljenih nad bazom te održavanje logova. Pod pojmom održavanja logova podrazumijevamo pohranjivanje i bilježenje svakog umetanja, brisanja i/ili ažuriranja zapisa u bazi podataka. Održavanje logove od bitne je važnosti jer ukoliko se pojavi hakerski napad, na taj će se način brže i jednostavnije otkriti krivci.

3. **ACL**

   ACL (engl. *Audit Command Language*) je softver za analizu i izdvajanje podataka koji se koristi za otkrivanje i prevenciju prijevara kao i upravljanje rizikom. Prednosti ACL-a su da može brzo i jednostavno obrađivati velike količine zapisa, a da pritom koristi minimalistički skriptni jezik za većinu jezika. Pod pojmom minimalističkog skriptnog jezika podrazumijevamo jezik koji se u većini slučajeva izvršava interpretiranjem te je fokusiran na sadržavanje što manjeg broja naredbi, odnosno pokušava sadržati svojstvo minimalizma. Sadrži integriranu revizijsku analitiku za složenu obradu podataka, daljinsku izvanmrežnu reviziju, timske analitičke tokove podataka, analitiku javnog sektore i mnoge druge [19].

4. **FTK**

   FTK (engl. Forensic Toolkit) alat je za digitalnu forenziku baze podataka koji služi za detekciju krađe podataka na internetu te radi na principu skeniranja tvrdog diska s ciljem pronalaska raznih informacija.

   FTK u potpunosti koristi računala s više jezgara te distribuiranu obradu kao i 100% svojih hardverskih resursa. Isto tako, FTK koristi jednu zajedničku bazu podataka slučajeva između timova preko koje koriste iste podatke te se na taj način smanjuju troškovi i složenost stvaranja više skupova podataka [20].

5. **Sleuth Kit**

   Sleuth Kit forenzički je alat koji može raditi i na Windows i na Unix platformama kako bi dohvatio i obradio skrivene i obrisane datoteke. U osnovi, to je zbirka alata naredbenog retka i C biblioteke koji omogućuje analizu slika diska te oporavak datoteka.

6. **EnCase**

   EnCase softver je za digitalnu forenziku koji se koristi najčešće u kriminalnim istragama, ali i u vojnim, obavještajnim i sigurnosnim svrhama. EnCase omogućuje brzo pretraživanje, prepoznavanje i određivanje prioriteta potencijalnih dokaza na digitalnim uređajima.

9. PostgreSQL

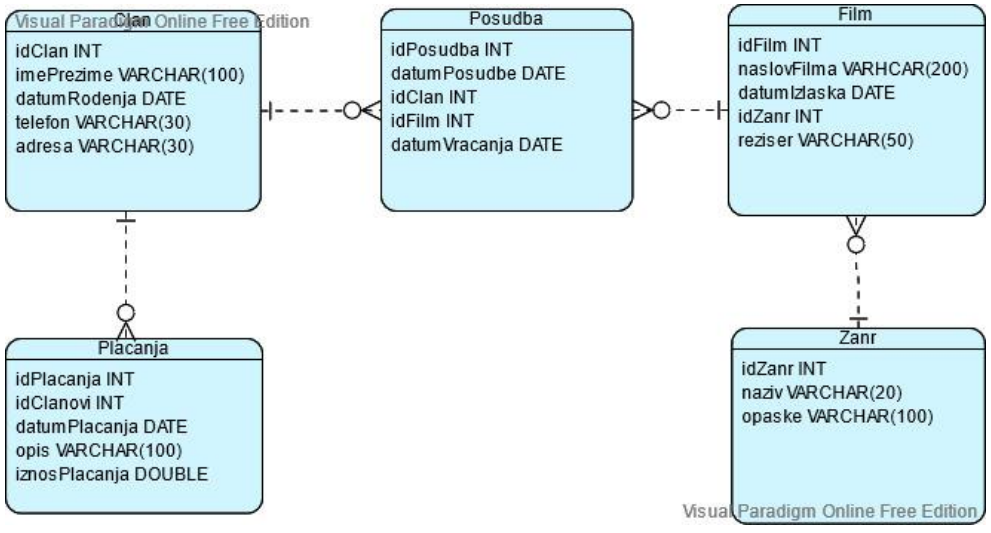
PostgreSQL je relacijski sustav otvorenog koda je priznatost u IT svijetu stekao svojom pouzdanošću, robusnim skupom značajki, arhitekturom te brojnim suradnicima koji zajedno stoje iza zajednice proširevši ovu bazu otvorenog kod novim značajkama [25]. PostgreSQL besplatan je za korištenje i održavanje te se ne mora kupovati.

U nastavku ćemo prikazati kreiranje baze podataka u PostgreSQL-u i zaštitu iste.

9.1. ERA model i pgAdmin 4

ERA model skraćeni je naziv za model entiteta-veza. ERA model prikazuje entitete i odnose između tih entiteta. Svaki od entiteta sadrži svoje atribute, odnosno karakteristike tih entiteta od kojih svaki ima svoje ime te često bivaju implementirani kao polja s vrijednošću.

ERA model koji će biti prikazan u ovome radu napravljen je prema jednostavnom primjeru sa stranice guru99.com u programu Visual Paradigm Online te će na njemu biti prikazano kreiranje baze podataka u PostgreSql-u te mehanizmi zaštite iste.



Slika 2. ERA model

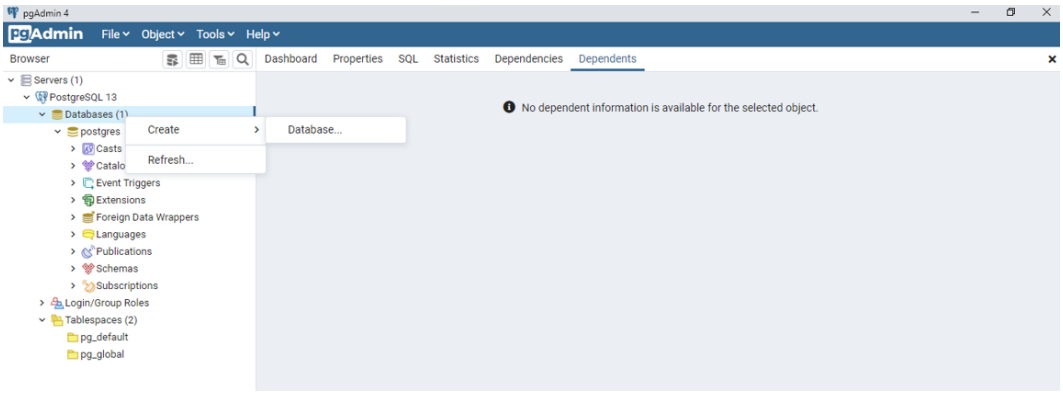
(Prema: https://www.guru99.com/er-modeling.html)

ERA dijagram prikazan na Slici 2. prikazuje princip posuđivanja filmova. Na modelu su prikazana 5 entiteta: Član, Plaćanja, Posudba, Film i Žanr između kojih se nalaze određeni odnosi. Entiteti Član i Plaćanja povezani su vezom jedan naprema više što možemo definirati na sljedeći način: jedan član može imati više plaćanja, no jedno plaćanje specifično je za jednog člana. Nadalje, entiteti Član i Posudba određeni su odnosom jedan naprema više,

odnosno jedan član može imati više posudbi filmova, no jedna posudba filma odnosi se na jednog člana. Navedeni odnosi vrijede i između entiteta Posudba i Film te entiteta Film i Žanr.

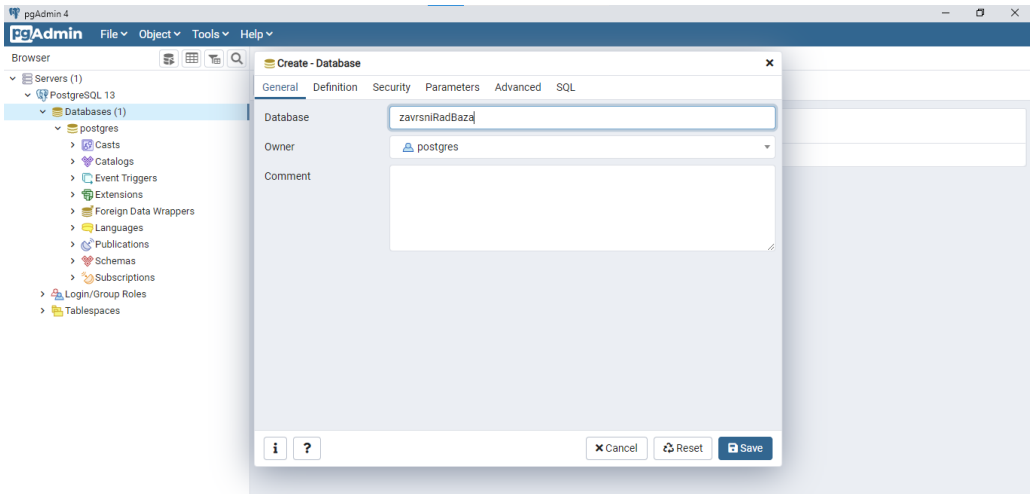
9.2. pgAdmin 4

pgAdmin platforma je otvorenog koda za PostgreSQL. U ovom radu biti će prikazano kreiranje baze podataka te zaštita iste u alatu pgAdmin 4.

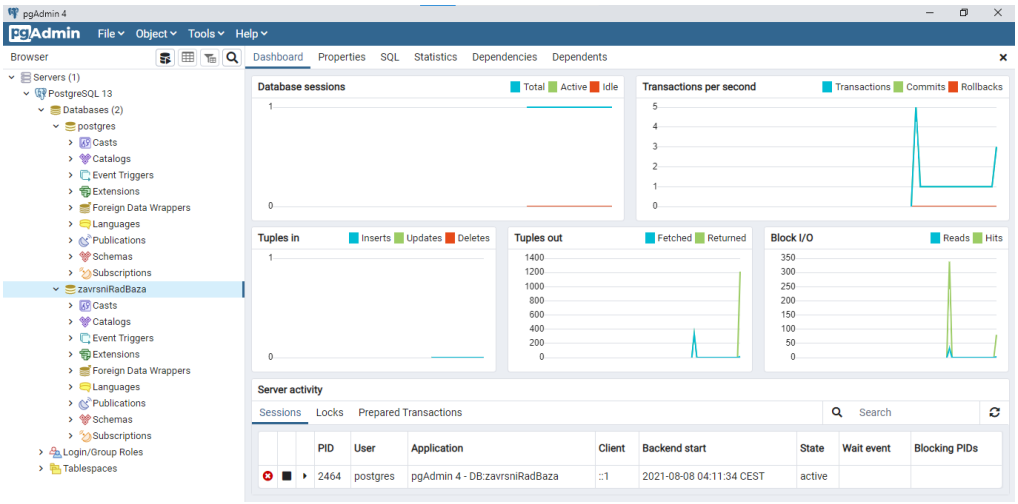


Slika 3. Kreiranje baze podataka

Slika 3. prikazuje kreiranje baze podataka. U lijevom dijelu alata vidi se padajući izbornik koji prikazuje poslužitelje koji su kreirani na računalu. Klikom na poslužitelj, PostgreSQL 13 otvara se popis baza podataka koji se nalaze na tom poslužitelju. Kako na tom poslužitelju još nije kreirana baza podataka, na njemu se nalazi samo serverski kreirana baza podataka, odnosno baza prikazana na slici pod nazivom Databases. Kako bi se kreirala baza podataka potrebno je kliknuti desnom tipkom miša na Databases te u izborniku koji sadrži opcije Create i Refresh odabrati Create Database. Nakon što je odabrana opcija Create Database otvara se novi prozor u kojem je potrebno imenovati novokreiranu bazu podataka te je moguće ostavljanje dodatnih komentara. Postavljanje imena bazi podataka prikazano je Slikom 4.

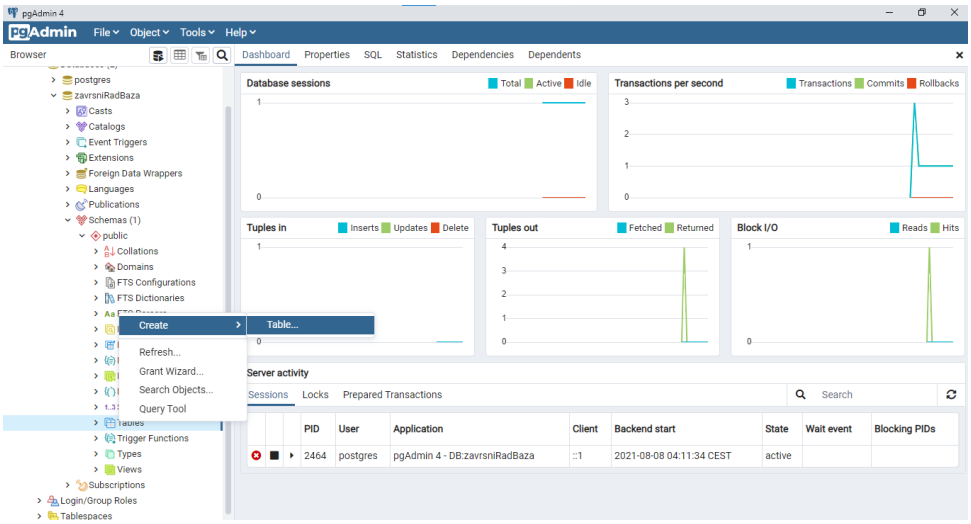


Slika 4. Imenovanje baze podataka



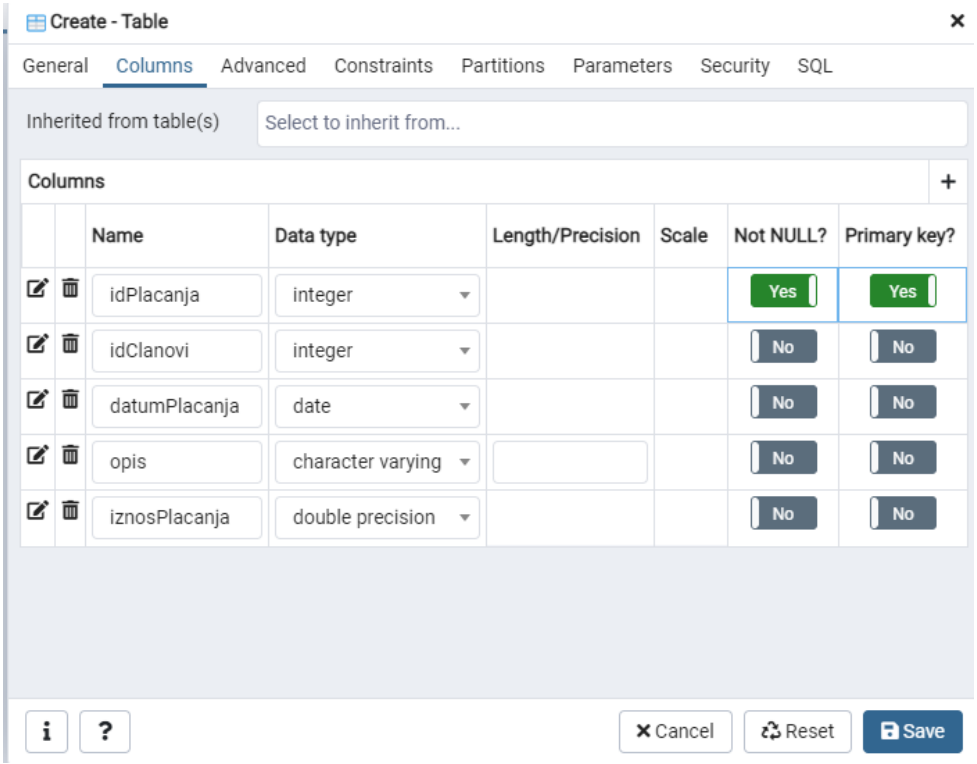
Slika 5. Izgled nakon kreiranja baze podataka

Slika 5. prikazuje izgled pgAdmina nakon kreiranje nove baze podataka. U lijevom dijelu sada se na poslužitelju PostgreSQL 13 prikazuje ne samo sistemska baza (Databases), već i novokreirana baza pod nazivom završniRadBaza. Novokreirana baza posjeduje ista obilježja kao i sistemska poput kataloga, jezika, shema i tako dalje.



Slika 6. Kreiranje tablice

Slika 6. prikazuje kreiranje tablice u pgAdminu 4. dok Slika 7. prikazuje dodavanje atributa i tipova u samu tablicu u bazi podataka.



Slika 7. Kreiranje tablice

9.3. Promjena prava uloga

Jedna od najčešćih prijetnji bazi podataka je promjena prava uloga. U sustavu se nalazi korisnik, član pod imenom Marko koji je učlanjen već nekoliko godina i redovito posuđuje filmove. Prilikom jedne prijave Marku je bila onemogućena prijava već postojećim korisničkim imenom i lozinkom te je obavijestio administratora o nemogućnosti prijave na sustav. Naime, nakon što je aministrator krenuo u forenziku baze podataka uvidio je da navedeni član Marko

više nema omogućeni pristup bazi podataka jer je netko promijenio ulogu (engl. role) te više nema pristup sustavu. Administrator je otkrio da je uzrok njegovoj nemogućnosti prijave promjena uloge pomoću sljedećeg upita:

```
SELECT rolname AS uloga,
Rolcanlogin AS login
FROM pg_roles
WHERE rolname='Marko'
```

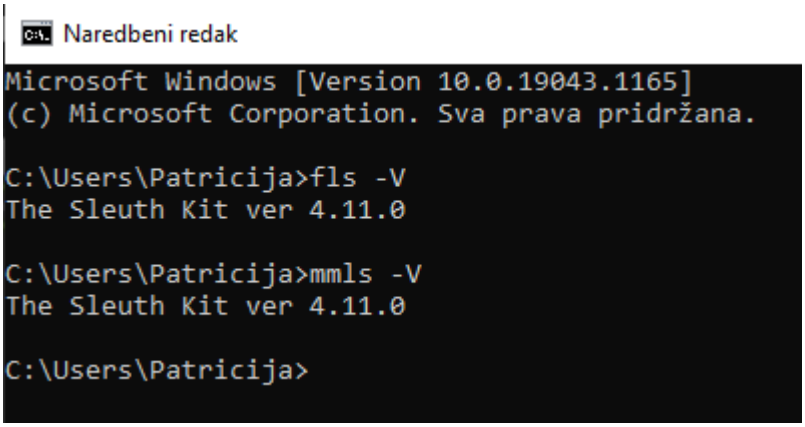
9.4. Kreiranje pogleda kao zamjena za tablicu

Kreiranje pogleda kao zamjena za tablicu jedan je od načina kako se može napraviti izmjena koja će posljedično prikazivati pogrešne rezultate. Primjerice, tablica Placanja u bazi podataka preimenuje se u PlacanjaOriginal te se stvara novi pogled pod nazivom Placanja. U novom pogledu Placanja mogu se sakriti određeni retci te prikazati samo neki čime mogu biti ugroženi brojni podaci. Primjerice, ukoliko u pogledu Placanja budu prikazani samo datumPlaćanja i retci, smatrat će se da članarina nije plaćena te će se pomisliti da član nije platio članarinu s obzirom da je redak iznosPlacanja sakriven. SQL naredba koja se može koristiti za stvaranje navedenog pogleda je:

```
CREATE VIEW Placanja AS SELECT idPlacanja, idClanovi, datumPlacanja, opis
FROM PlacanjaOriginal;
```

10. Sleuth Kit

Sleuth Kit forenzički je alat koji može raditi i na Windows i na Unix platformama kako bi dohvatio i obradio skrivene i obrisane datoteke. On čini temelj za Autopsy, jedan od poznatijih alata koji dolazi u paketu sa Sleuth Kit-om. Temeljna funkcija ovog alata je mogućnost analize podataka. Kako Sleuth Kit čine brojne knjižnice, tako se ono može ugraditi u veće digitalne forenzičke alate.



Slika 8. Verzija Sleuth Kit-a

Slika 8. prikazuje instaliranu verziju forenzičkog alata. Upisivanjem naredbe fls -V ili mmls -V u naredbenom retku prikazana je verzija instalirana na Windows 10, a to je Sleuth Kit 4.11.0.

10.1. Sloj datotečnog sustava

Sloj datotečnog sustava prikazuje povezanost između imena i indeksnog čvora. Naredba *fsstat* prikazuje podatke o datoteci sustava kao što su to veličine podatkovnih jedinica, statistički podaci o stanju datotečnog sustava i slično.
fsstat pruža osnovne podatke o datotečnom sustavu, ali i informacije koje mogu biti ključne prilikom važne istrage kao što su to posljednje zapisani podaci.

10.2. Sloj podataka

U ovom sloju pohranjeni su podaci najčešće u blokovima od 512B, 1024B, itd. Sloj podataka najmanja je jedinica za pohranu podataka u datotečnom sustavu.

- blkcat: prikazuje sadržaj zadanog bloka diska
- blkls: prikazuje sadržaj izbrisanih blokova diska u neobrađenoj slici
- blkstat: navodi statistiku povezanu s određenim blokovima diska

```
blkstat -f ext2 slika.img 300
Fragment: 300
Allocated

Group: 0
```

Ukoliko bismo htjeli ispisati sadržaj određenog bloka diska, potrebna je sljedeća naredba:

```
blkcat -f ext2 slika.img 300
```

10.3. Sloj metapodataka

Sloj metapodataka sadrži vrijednosti i strukturu koje definiraju datoteku.

- ils: prikazuje pojedinosti indeksnog čvora
- istat: prikazuje informacije o određenom indeksnom čvoru
- icat: prikazuje sadržaj blokova diska dodijeljenog određenom indeksnom čvoru

11. Zaključak

Digitalna forenzika baza podataka znanost je koja se koristi brojnim istraživačkim metodama i različitim kombinacijama znanosti kako bi analizirala i interpretirala digitalne dokaze. Ona je jedna od najvažnijih znanosti današnjice iako s obzirom na kratko postojanje i kompleksnost nije toliko istraživana.

S obzirom da je 21. stoljeće doba društvenih mreža i interneta vrlo su lako mogući propusti pri zaštiti baze podataka što može dovesti do krađe i zlouporabe podataka. Kako bi se podaci što brže povratili digitalna forenzika bavi se različitim metodama i tehnikama kojima se u što kraćem vremenskom roku pronalaze krivci za kibernetički napad i/ili zlouporabu podataka. Kako bi se što uspješnije spriječile krađe i zlouporabe podataka potrebno je razviti strategiju kibernetičke sigurnosti i uložiti više vremena i novaca na sigurnost baze u početku s obzirom da je provođenje sigurnosnih politika najbolje rješenje za zaštitu od kriminala.

Popis literature

[1] Varga M.: *Baze podataka - konceptualno, logičko i fizičko modeliranje podataka*. DRIP, Zagreb,1994. Dostupno na [https://books.google.at/books?id=UQPoDwAAQBAJ&printsec=frontcover&hl=hr#v=onepage&q&f=false]. Pristupano 15.03.2021.

[2] M. Maleković, K. Rabuzin: *Uvod u baze podataka*, Fakultet organizacije i informatike, Varaždin, 2016.

[3] Znanje.org, [bez dat.], Dostupno na [https://www.znanje.org/abc/tutorials/accessMMX/01/Baze_podataka.htm] . Pristupano 22.04.2021.

[4] Jones and Bartlett Learning: *Introduction to Database Security*. Dostupno na [https://samples.jbpub.com/9781284056945/DBICHAP8.pdf]. Pristupano 22.04.2021.

[5] I.Batistić: *Integritet i sigurnost podataka*, Fizički odsjek, PMF, Zagreb, 2004. Dostupno na [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjJ3NjsuJLwAhWcgf0HHdKoDAsQFjAAegQIAhAF&url=http%3A%2F%2Fgrdelin.phy.hr%2F~ivo%2FNastava%2FBaze_podataka%2Fpredavanja-2004%2F16b_pred.pdf&usg=AOvVaw1fbyeXhk_pAK6VXOTUvF9N]. Pristupano 22.04.2021.

[6] Eric Conrad, Seth Misenar and Joshua Feldman: *CISSP Study Guide*. 2012. Pristupano 10.05.2021.

[7] Britannica, The Editors of Encyclopaedia Britannica, [07.04.2005.].Dostupno na [https://www.britannica.com/topic/Enigma-German-code-device]. Pristupano 10.05.2021.

[8] Flipperworld, Simetrično i asimetrično šifriranje: definicija pojma, primjena, primjeri. [01.02.2019.] .Dostupno na [https://hr.flipperworld.org/pc/simetricno-i-asimetricno-sifriranje-definicija-pojma-primjena-primjeri]. Pristupano 10.05.2021.

[9] Michael Cobb, *Advanced Encryption Standard (AES)*, [travanj 2020.]. Dostupno na [https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard] .Pristupano 10.05.2021.

[10] Reith M., Carr C., Gunsch G. [2003.], *An Examination of Digital Forensic Models*, Internal Journal of Digital Evidence Volume 1 Issue 4. Dostupno na [http://www.just.edu.jo/~Tawalbeh/nyit/incs712/digital_forensic.pdf]. Preuzeto 11.05.2021.

[11] Guru99, *What is Digital Forensics? History, Process, Types, Challenges*, [bez dat.]. Dostupno na [https://www.guru99.com/digital-forensics.html]. Pristupano 11.05.2021.

[12] Garfinkel L. S. [2010.], *Digital forensics research: The next 10 years*, Naval Postgraduate School, Monterey, USA, *Digital Investigation 7*. Dostupno na

[https://calhoun.nps.edu/bitstream/handle/10945/44251/Garfinkel_%20Digital_Forensics_2010.DFRWS.Next10Years.pdf?sequence=1&isAllowed=y]. Preuzeto 11.05.2021.
[13] Dr.Nick Oberheiden, *5 Keys to Selecting the Right Digital Forensics Investigator*, [29.01.2021.].Dostupno na [https://www.natlawreview.com/article/5-keys-to-selecting-right-digital-forensics-investigator]. Pristupano 11.05.2021.
[14] 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
[15] 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. Dostupno na [https://pdfs.semanticscholar.org/9dc5/01f4a48957cdc8473367d25034fc3251ec10.pdf]. Preuzeto 11.05.2021.
[16] EC-Council, *What is Digital Evidence and why is it important?,* [19.02.2021.] Dostupno na [https://blog.eccouncil.org/what-is-digital-evidence-and-why-is-it-important/]. Pristupano 11.05.2021.
[17] Infosec Institute [FORENSICS] (bez dat.), *What is Database Forensics*, Dostupno na [https://resources.infosecinstitute.com/topic/computer-forensics-overview-types-database-forensics/]. Pristupano 12.05.2021.
[18] ProDiscover.com, [bez datuma]. Dostupno na [https://www.prodiscover.com/]. Pristupano 24.05.2021.
[19] Crozdesk.com, *What is ACL Analytics?*, [bez datuma]. Dostupno na [https://crozdesk.com/operations-management/governance-risk-compliance-grc-software/acl-analytics]. Pristupano 24.05.2021.
[20] Accessdata.com, Forensics Toolkit (FTK), [bez datuma]. Dostupno na [https://accessdata.com/products-services/forensic-toolkit-ftk]. Pristupano 24.05.2021.
[21] K. Chadd, Cybersecurityventures.com, *The Hirsory Of Cybercrime And Cybersecurity, 1940-2020*, [30.11.2020.]. Dostupno na [https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/]. Pristupano 25.05.2021.
[22] R.Herjavec, Herjavec Group, *Cybersecurity CEO: The History Of Cybercrime, From 1834 To Present*, [18.07.2019.]. Dostupno na [https://www.herjavecgroup.com/history-of-cybercrime/]. Pristupano 25.05.2021.
[23] Fbi.gov, *Safety and Scams*, [bez datuma]. Dostupno na [https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud]. Pristupano 25.05.2021.
[24] Popat, A. (2018), Five Ways To Protect Yout Company Against Cyber Attacks. Dostupno na [https://www.entrepreneur.com/article/316886]. Pristupano 25.05.2021.

[25] Postgresql.org, *About PostgreSQL*, [bez datuma]. Dostupno na [https://www.postgresql.org/about/]. Pristupano 2.7.2021.

Popis slika

Slika 1. Cezarova šifra.....12
Slika 2. ERA model 28
Slika 3. Kreiranje baze podataka 29
Slika 4. Imenovanje baze podataka.....30
Slika 5. Izgled nakon kreiranja baze podataka.....30
Slika 6. Kreiranje tablice 31
Slika 7. Kreiranje tablice 31
Slika 8. Verzija Sleuth Kit-a *33*

Popis tablica

Tablica 1 Relacija s podacima o studentu..... 4
Tablica 2 SQL vs. NoSQL 6