Ekstrakcija podataka sustava za razmjenu poruka društvenih mreža u svrhu forenzičke analize

Bošnjak, Zvonimir

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Zvonimir Bošnjak

EKSTRAKCIJA PODATAKA SUSTAVA ZA RAZMJENU PORUKA DRUŠTVENIH MREŽA U SVRHU FORENZIČKE ANALIZE

DIPLOMSKI RAD

Zagreb, 2018.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 19. ožujka 2018.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Forenzička analiza informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 4505

Pristupnik: **Zvonimir Bošnjak (0135234006)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Ekstrakcija podataka sustava za razmjenu poruka društvenih mreža u svrhu forenzičke analize**

Opis zadatka:

Opisati principe forenzičke analize terminalnog uređaja. Objasniti važnost društvenih mreža kao izvora digitalnih dokaza. Prikazati značajke aplikacija društvenih mreža na uređajima Android OS-a. Analizirati sadržaja terminalnog uređaja prikupljenog forenzičkom analizom.

Mentor:

dr. sc. Siniša Husnjak

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

EKSTRAKCIJA PODATAKA SUSTAVA ZA RAZMJENU PORUKA DRUŠTVENIH MREŽA U SVRHU FORENZIČKE ANALIZE

EXTRACTION OF SOCIAL NETWORK MESSAGING SYSTEM DATA FOR PURPOSES OF FORENSIC ANALYSIS

Mentor: dr. sc. Siniša Husnjak

Student: Zvonimir Bošnjak
JMBAG: 0135234006

Zagreb, rujan 2018.

SAŽETAK

Forenzička analiza mobilnih terminalnih uređaja je provedba određene forenzičke metodologije nad mobilnim terminalnim uređajem s ciljem prikupljanja digitalnih dokaza. Takva forenzička analiza uključuje pripremu, provedbu ekstrakcije podataka te obradu tih podataka kako bi se prikazali prikupljeni dokazi. Trenutno se veliki dio komunikacije vrši putem sustava za razmjenu poruka društvenih mreža, a aplikacije koje omogućuju takvu razmjenu poruka podatke pohranjuju lokalno. Analizom i obradom ekstrahiranih podataka s uređaja koji koriste aplikacije društvenih mreža moguće je doći do podataka koji omogućuju rekonstrukciju razgovora obavljenih putem sustava za razmjenu poruka društvenih mreža.

KLJUČNE RIJEČI: forenzička analiza, ekstrakcija podataka, društvene mreže, prikupljanje dokaza

SUMMARY

Mobile forensic analysis is implementation of forensic methodology on mobile device with goal of recovering digital evidence. This type of forensic analysis includes preparation, data acquisition and data processing, examination and analysis. Currently large amount of the communication is done through social network messaging systems and applications which allow social network users to exchange messages store their data locally on the device. With analysis and processing data acquired from mobile device it is possible to reconstruct conversation which was done through social network messaging systems.

KEYWORDS: forensic analysis, data acquisition, social networks, evidence recovery

SADRŽAJ

1. UVOD

Razvoj i rast popularnosti društvenih mreža prethodnih godina, popraćen usporednim razvojem mobilnih terminalnih uređaja, prouzrokovao je odljev značajnog dijela komunikacije, osobito one u tekstualnom obliku, na aplikacije vezane za društvene mreže. Korištenje sustava za razmjenu poruka unutar aplikacija društvenih mreža konkurentno je klasičnoj razmjeni tekstualnih poruka *SMS*-om i usluzi trenutačnog poručivanja.

Zbog značajnog udjela ovakvog načina komunikacije pojavljuje se potreba za razvojem metodologije prema kojoj će se provoditi forenzička analiza u tu svrhu. Takav postupak forenzičke analize za pristup sadržaju komunikacije nije ovisan o pristupanju samom korisničkom računu društvene mreže. Razlog tome je što su poslužitelji *online* društvenih mreža rasprostranjeni na područje više različitih država i to predstavlja problem, koji je sličan izazovima s kojim se susreće *cloud* forenzika, u smislu određivanja pravne nadležnosti. Kako bi se taj problem izbjegao, to jest istražiteljima omogućilo prikupljanje dokaza koji su upotrebljivi i dostupni moguće je koristiti sadržaj koji je lokalno pohranjen na terminalnom uređaju od strane aplikacije društvene mreže.

Ekstrakcijom podataka pohranjenih na mobilnom terminalnom uređaju omogućuje se pristup podacima koji su generirani od strane sustava za razmjenu poruka aplikacija društvenih mreža. Ti podaci, ovisno o kojoj se aplikaciji društvene mreže radi, sadrže podatke kao što su pošiljatelj, primatelj, njihove identifikatore, vrijeme slanja te u konačnici sam sadržaj poruke. Na osnovu tih podataka moguće je izvršiti rekonstrukciju razgovora koji odgovara njegovom izvornom obliku i kao takav se može koristiti kao dokaz.

Ekstrakcija podataka sustava za razmjenu poruka društvenih mreža u svrhu forenzičke analize je naslov ovoga diplomskog rada. Ovaj diplomski rad je podijeljen u šest poglavlja:

1. Uvod
2. Forenzička analiza terminalnog uređaja
3. Društvene mreže kao izvor digitalnih dokaza
4. Aplikacije društvenih mreža na uređajima Android OS-a
5. Obrada i prikaz sadržaja prikupljenog forenzičkom analizom
6. Zaključak

U drugom poglavlju opisan je sam pojam forenzike u općenitom smislu te kako se pojam forenzike prenosi u digitalno okruženje. Definirana je podjela digitalne forenzike i sinonimi koji se koriste kao nazivi pojedinih grana. Objašnjen je cilj digitalne forenzike, to jest prikupljanje digitalnih dokaza i metodologija koja se koristi kako bi se isto postiglo uključujući onu koja predstavlja referentnu metodologiju za forenzičku analizu mobilnih terminalnih uređaja. Ukratko su opisane

vrste ekstrakcija korištene u ovome diplomskom radu te detaljno opisan postupak fizičke ekstrakcije podataka s uređaja, odnosno izrada *image*-a unutrašnje pohrane uređaja.

Digitalni dokazi na društvenim mrežama su tema trećeg poglavlja. Detaljnije je prikazana tema same popularnosti društvenih mreža kao sredstvo za komunikaciju, odnosno usporedba određenih statistika o komunikaciji putem društvenih mreža i *instant messaging* u odnosu na klasične načine komunikacije putem mobilnih terminalnih uređaja. Opisane su vrste digitalnih dokaza vezane za društvene mreže uz poseban osvrt na komunikaciju između korisnika istih.

Četvrto poglavlje usmjereno je na dvije aplikacije društvenih mreža koje omogućuju komunikaciju između svojih korisnika. Poglavlje je usredotočeno na način pohrane u memoriju uređaja podataka koje generira aplikacija uključujući podatke sustava za razmjenu poruka. U poglavlju je opisana struktura tih podataka te su prepoznati elementi koji omogućavaju rekonstrukciju samog razgovora.

Obrada prikupljenih podataka je tema petog poglavlja. Obrada je izvršena tako da su se saznanja prikupljenih iz prethodnih poglavlja primjenila za razvoj programskog koda za generiranje izvještaja. Taj programski kod neobrađene podatke prikupljene ekstrakcijom koristi za generiranje izvještaja koji sadrži rekonstruirani razgovor sa svim pratećim podacima.

Svrha ovog istraživanja je prikazati postupak prikupljanja dokaza iz sustava za razmjenu poruka aplikacija društvenih mreža forenzičkom analizom pametnih mobilnih terminalnih uređaja.

Cilj istraživanja je prikazati mogućnost korištenja društvenih mreža, to jest komunikacije između njihovih korisnika, kao izvor dokaza i potrebu za razvijanjem forenzičkih postupaka za prikupljanje tih istih dokaza iz pametnih mobilnih terminalnih uređaja. Kroz opis karakteristika različitih društvenih mreža i njihovog sustava za razmjenu poruka će se prepoznati mogući elementi tih aplikacija koji se mogu koristiti kao izvor dokaza. Cilj istraživanja je prikazati metodologiju forenzičke analize uređaja koja je primjenjiva u ovu svrhu, načine ekstrakcije podataka i procesiranja tih ekstrahiranih podataka te analizu dobivenog sadržaja s namjerom korištenja istog kao dokaza.

2. FORENZIČKA ANALIZA TERMINALNOG UREĐAJA

Značenje riječi forenzika je uporaba znanosti za rješavanje pravnih problema. Forenzička znanost predstavlja skupinu znanstvenih disciplina koje su usmjerene na primjenu saznanja iz svoje znanstvene discipline za utvrđivanje činjenica u sudskim postupcima, [1]. Dok prema [2] forenzika predstavlja primjenu znanstvenih saznanja za skupljanje, analiziranje i prezentaciju dokaza sudovima.

Jedna od tih grana forenzike je digitalna forenzika. Iako prvotno termin digitalna forenzika je bio korišten kao sinonim za računalnu forenziku, digitalna forenzika ipak pokriva šire područje od same forenzike računala. Prema [3] digitalna forenzika je primjena znanstvenih saznanja u svrhu prikupljanja informacija, odnosno dokaza, iz digitalnog uređaja.

Postoji nekoliko različitih podjela digitalne forenzike ovisno o korištenoj literaturi, ali iz svih se kao osnovne grane digitalne forenzike mogu izdvojiti računalna forenzika, forenzika mreža i forenzika mobilnih uređaja, [4].

Osim već navedenih naziva za ovo područje forenzike u nekim literaturama kao sinonim za digitalnu forenziku koristi se i termin *cyber* forenzika, [5]. Inače sama riječ *cyber* je često netočno prevedena na hrvatski jezik kao kibernetika i korištenje tog prijevoda bi upućivalo na nešto što ne predstavlja sinonim za digitalnu forenziku, [6].

Cilj digitalne forenzike je prikupljanje digitalnih dokaza. Takvi dokazi se nalaze pohranjeni na tvrdim diskovima, mobilnim uređajima, stolnim i prijenosnim računalima, tabletima, usmjerivačima i svim drugim digitalnim uređajima koji posjeduju nekakvu mogućnost pohrane podataka koji bi se mogli u nekom slučaju mogli iskoristiti kao dokaz. Kako bi digitalni dokazi bili prihvatljivi na sudu, oni moraju biti relevantni za taj slučaj te prikupljeni na prihvatljiv način. Prikupljanje digitalnih dokaza na prihvatljiv način znači da je čitav postupak provođenja forenzičke analize nekog uređaja obavljen prema metodologiji koja je namijenjena za takav tip uređaja, [7].

Prema [8] metodologija forenzičke analize je logičan i promišljen niz postupaka provedenih za vrijeme istrage. Dobra metodologija forenzičke analize osigurava da ja istraga, odnosno sama analiza, dobro dokumentirana, ponovljiva i izvedena tako da su prikupljeni dokazi prihvatljivi na sudu. Iz tog razloga je razvijena metodologija forenzičke analize za mobilne terminalne uređaje.

2.1. Metodologija forenzičke analize terminalnog uređaja

Referentna metodologija prilikom provođenja forenzičke analize mobilnog terminalnog uređaja je "*Cellular Phone Evidence Data Extraction and Documentation*" stvorena od strane detektivke Cindy Murphy. Svrha razvoja

metodologije je kako bi se istražitelji lakše snašli u velikom broju slučajeva na kojima rade i koriste različitu opremu i alate. Neki od ovih koraka su nužni kako bi se očuvali dokazi na uređaju u onakvom stanju kako su i bili prije same obrade. Ova metodologija definira smjernice prema kojima se provodi proces pripreme, ekstrakcije, obrade i dokumentacije podataka s mobilnih terminalnih uređaja. Prema [9] metodologija forenzičke analize mobilnih terminalnih uređaja sastoji se od devet koraka ili faza:

- Preuzimanje ili uvođenje
- Identifikacija
- Priprema
- Izolacija
- Obrada
- Validacija
- Dokumentiranje
- Prezentacija
- Arhiviranje

Prvi korak odnosno preuzimanje slučaja ili uvođenje u slučaj odnosi se na prikupljanje općih informacija o slučaju i potrebne dokumentacije uključujući lanac posjeda dokaza te okvirne ciljeve istrage. Faza identifikacije definira utvrđivanje zakonskih prava na obradu uređaja, ciljeve istrage, identificiranje samog uređaja, prepoznavanje prijenosne i vanjske pohrane te drugih izvora dokaza kao što su na primjer tragovi *DNK* i otisci. Deoksiribonukleinska kiselina, odnosno *DNK*, je nositelj genetičke informacije koji se može iskoristiti za identifikaciju, [10].

U koraku pripreme istražitelj planira postupke i procese koje će upotrijebiti prilikom analize te forenzičke alate i opremu koje će koristiti za potrebe forenzičke analize. Osim toga, u ovom koraku istražitelj se odlučuje za postupak ili postupke ekstrakcije koje će koristiti. Izolacija predstavlja odvajanje mobilnog terminalnog uređaja od svih bežičnih načina komunikacije korištenjem *Faraday*-evog kaveza ili slične metode. Faza obrade odnosno procesiranja predstavlja izvršavanje zadataka i ciljeva definiranih u prethodnim koracima. To uključuje provođenje ekstrakcije podataka i obradu ti istih prikupljenih podataka s ciljem dobivanja konkretnih dokaza iz istih.

Korak validacije se odnosi na uspoređivanje podataka dobivenih korištenjem različitih alata i postupaka ekstrakcije kako bi se utvrdila ispravnost podataka. Dokumentiranje je korak u kojemu se postupci provedeni tijekom prethodnih koraka bilježe. Korak prezentacije je prikaz rezultata forenzičke analize nekome za čije potrebe se uopće krenulo u provedbu forenzičke analize. Arhiviranje uključuje trajnu pohranu prikupljenih i dokumentiranih podataka i dokaza te evidenciju istih, [9].

Zbog same svoje teme ovaj diplomski rad je više usmjeren na neke od faza ove metodologije u odnosu na druge. To uključuje korake pripreme, obrade i

prezentacije u smislu stvaranja jasnih dokaza iz prikupljenih podataka. Za potrebe ovoga diplomskog rada korištene su tri metode ekstrakcije podataka čiji su rezultati međusobno uspoređivani kako bi se validirao sadržaj prikupljen korištenjem tih metoda. Najjednostavnija korištena metoda je bila ručna ekstrakcija podataka koja se temeljila na uzimanju preslika zaslona uređaja. Osim toga, korištena je logička ekstrakcija u obliku izrade kopija pojedinačnih datoteka iz pohrane uređaja. Fizička ekstrakcija podataka provedena je izradom *image*-a cijele unutarnje pohrane uređaja korištenjem metoda koje su navedene u sljedećem potpoglavlju.

2.2. Priprema uređaja i fizička ekstrakcija podataka

Za demonstraciju forenzičke analize sustava razmjene poruka aplikacija društvenih mreža korišten je pametni mobilni terminalni uređaj *LG L70 Dual SIM D325*. Operativni sustav ovog uređaja je *Android 4.4.2 KitKat*, a verzija *kernel*-a je 3.4.0+. Interna memorija ovoga uređaja je veličine samo 4 *GB* što čini samu ekstrakciju podataka s ovoga uređaja jako brzom.

Na uređaju su instalirane aplikacije *Instagram* i *Messenger Lite* te su korištenjem istih aplikacija razmijenjene poruke između tri korisnička računa za pojedinu aplikaciju. Po jedan od tih računa je korišten na samom mobilnom terminalnom uređaju koji je analiziran, a druga dva na osobnom računalu.

Kako bi se ostvario pristup svim podacima na uređaju potreban je *root* pristup. *Root*-anje uređaja je ostvarivanje administratorskih ovlasti na uređaju iskorištavanjem ranjivosti operativnog sustava. *Root* pristup na ovom uređaju je ostvaren korištenjem aplikacije *KingoRoot*, [11].

Nakon uspješnog *root*-anja instalirana je aplikacija *BusyBox* koja omogućuje nekoliko različitih *Unix* alata. Kako je *Android* operativni sustav temeljen na *Linux*-u, *BusyBox* uz *root* pristup omogućuje korištenje naredbe *dd* na uređajima s *Android OS.* Tom naredbom je moguće napraviti bit po bit kopiju memorije uređaja što predstavlja fizičku ekstrakciju podataka. Naredbe *BusyBox*-a je moguće koristiti na samom uređaju korištenjem *Terminal Emulator*-a ili putem računala korištenjem *Android Debug Bridge*-a, [12].

Sama ekstrakcija podataka obavljena je na računalu s instaliranom *Santoku Linux* distribucijom verzije 0.5. Uz prethodno pripremljen uređaj, ovaj operativni sustav posjeduje sve potrebne alate kako bi se izvršila ekstrakcija *image file*-a s uređaja, [13]. Dok je naknadna analiza obavljena na računalu s *Windows* operativnim sustavom i potrebnim programskim alatima.

Android Debug Bridge je jednostavni konzolni alat koji omogućuje komunikaciju s uređajem i upravlja njime, a što je najvažnije omogućuje korištenje *Unix* naredbi na uređaju. *Android Debug Bridge* se sastoji od tri djela:

- klijent na računalu putem kojeg se unose naredbe,

- *daemon* na uređaju koji izvršava naredbe
- i server koji upravlja komunikacijom između klijenta i *daemon*-a.

Nakon spajanja računala s testnim uređajem putem *USB* kabela, korištenjem terminala *Santoku Linux* operativnog sustava pozvana je naredba *adb devices*, kao što je prikazano na slici 1, kojom se ispisuju trenutno povezani uređaji. Kada je utvrđeno da je mobilni uređaj spojen, naredbom *adb –d shell* ulazi se u naredbenu ljusku (eng. *command shell*) uređaja, u ovom slučaju s *root* pristupom. Dio naredbe *–d* označava da se naredba odnosi na jedini spojeni uređaj, [14].

Kako je prikazano na slici 1, nakon ulaska u ljusku na terminalu se ispisuje *shell@w5ds.* Korištenjem naredbe *su*, odnosno *switch user,* dolazi se do korisnika *root@w5ds*, što označava da će se upisana naredba izvršiti na uređaju uz *root* ovlasti. Naredba *cat* je jedna od naredbi omogućenih *BusyBox*-om i pojavljuje se u gotovo svim *Unix* temeljenim i *Unix* sličnim operativnim sustavima, a zadaća joj je ispis datoteka zadanih u njezinim parametrima. Ta naredba u kombinaciji sa */proc/partitions* kao zadanim parametrom ispisuje informacije o alokaciji blokova na particijama memorije uređaja, [15].

Ispis dobiven prethodno korištenom naredbom jasno prikazuje da je memorija uređaja podijeljena u *mmc* blokove. *MultiMediaCard*, to jest *mmc* ili *MMC*, je memorijski standard korišten za memorijske kartice, [16]. Budući da je barem jedan od blokova prikazan na slici 1 predstavlja internu memoriju uređaja možemo reći da se radi o *eMMC* memoriji, odnosno *Embedded MultiMediaCard,* [17]. Na slici 1 vidljivo je da su nazivi dvaju najvećih blokova *mmcblk0* i *mmcblk1.* Budući da je blok memorije pod nazivom *mmcblk0* podijeljen u više particija, odnosno od particije *mmcblk0p1* pa sve do *mmcblk0p35*m za razliku od bloka *mmcblk1* koji se sastoji samo od jedne particije moguće je zaključiti da je blok *mmcblk0* zapravo interna pohrana uređaja. Na tom bloku se nalaze podaci o korisnikovim aktivnostima, kao što su pozivi, podaci aplikacija, postavke i slično. Kako se svi potrebni podaci za ovu analizu nalaze na *mmcblk0*, vršit će se ekstrakcija samo tog bloka.

```
santoku@santoku:~$ adb devices
List of devices attached
LGD325e5c7d4a9  device

santoku@santoku:~$ adb -d shell
shell@w5ds:/ $ su
root@w5ds:/ # cat /proc/partitions
major minor  #blocks  name

   7        0      47849 loop0
 179        0    3817472 mmcblk0
 179        1      65536 mmcblk0p1
 179        2       1024 mmcblk0p2
 179        3        512 mmcblk0p3
 179        4        512 mmcblk0p4
 179        5        512 mmcblk0p5
 179        6       2048 mmcblk0p6
 179        7        512 mmcblk0p7
 179        8        512 mmcblk0p8
 179        9       2048 mmcblk0p9
 179       10       2048 mmcblk0p10
 179       11       3072 mmcblk0p11
 179       12       3072 mmcblk0p12
 179       13      16384 mmcblk0p13
 179       14      32768 mmcblk0p14
 179       15      22528 mmcblk0p15
 179       16      22528 mmcblk0p16
 179       17      22528 mmcblk0p17
 179       18       3072 mmcblk0p18
 179       19        512 mmcblk0p19
 179       20        512 mmcblk0p20
 179       21        512 mmcblk0p21
 179       22        512 mmcblk0p22
 179       23        512 mmcblk0p23
 179       24       8192 mmcblk0p24
 179       25       8192 mmcblk0p25
 179       26      20480 mmcblk0p26
 179       27      32768 mmcblk0p27
 179       28       1024 mmcblk0p28
 179       29      32768 mmcblk0p29
 179       30      51200 mmcblk0p30
 179       31        512 mmcblk0p31
 259        0    1535488 mmcblk0p32
 259        1     256000 mmcblk0p33
 259        2    1605632 mmcblk0p34
 259        3      32751 mmcblk0p35
 179       32        512 mmcblk0rpmb
 179       64    3977216 mmcblk1
 179       65    3973120 mmcblk1p1
 254        0      47848 dm-0
```

Slika 1. *Prikaz particija memorijskog prostora uređaja*

Nakon prikupljanja informacija o memoriji i odabira particije za ekstrakciju potrebno je kreirati konekciju između uređaja i računala kojom će se ti podaci ekstrahirati i pohraniti na uređaj u obliku *image file*-a. U zasebnom terminalu, u kojem se naredbe izvršavaju na računalu, a ne na uređaju, naredbom sa slike 2 omogućuje se komunikacija *Android Debug Bridge*-a putem porta 8888.

```
santoku@santoku:~$ adb forward tcp:8888 tcp:8888
santoku@santoku:~$
```

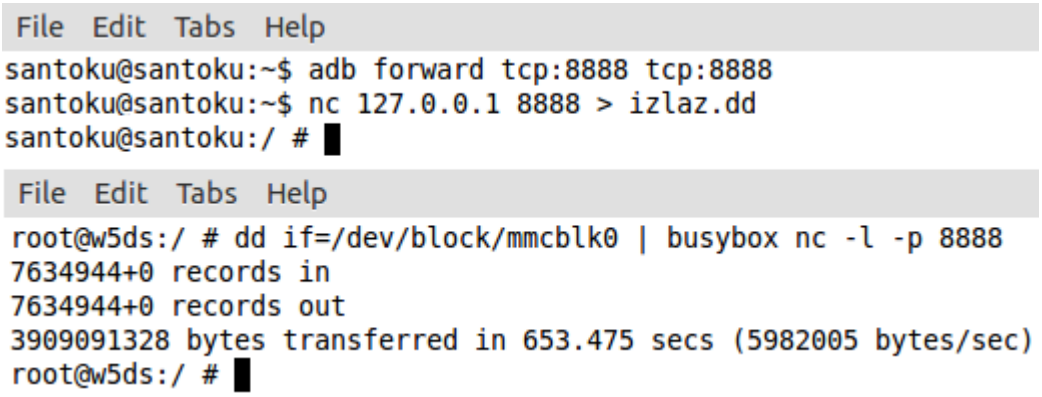
Slika 2. *Uspostava konekcije TCP portom*

Uspostavljena konekcija će se iskoristiti kako bi se korištenjem prethodno spomenute *dd* naredbe, kojoj je primarna svrha kopiranje i konvertiranje datoteka, pohranio sadržaj *mmcblk0* na memoriju računala. Naredba *dd* sadrži kao parametre *input* i *output* dio. *Input* dio koji se zapisuje iza ključne riječi *if* je blok s *user* podacima kojemu je točna lokacija na memoriji uređaja */dev/blocks/mmcblk0.* U ovom slučaju *output* dio je potrebno napisati iza znaka „|*“* kojim se označava da će se izlazni dio koristiti kao ulazni dio druge naredbe, to se još naziva *piping. Output* korištenjem *Netcat*-a*,* u terminalu pozvan kao *nc,* će usmjeriti podatke s bloka *mmcblk0* na *TCP port* 8888. Korištenje *Netcat*-a je na mobilnom uređaju omogućen putem *BusyBox*-a, a on predstavlja alat koji omogućuje čitanje i upisivanje korištenjem *TCP* i *UDP* protokola. *Transmission Control Protocol* i *User Datagram Protocol* su temeljni protokoli transportnog sloja *TCP/IP* složaja, a u ovom primjeru *TCP* protokol je korišten za ekstrakciju podataka. Izgled cijele naredbe izvršene na uređaju je prikazan na slici 3, nakon pokretanja naredbe ona se ne izvršava istovremeno nego zbog *-l ,* koji označava *listen,*dijela naredbe u izlaznom dijelu ona osluškuje dok se sljedeća naredba spoji na njezin izlaz kako bi se pokrenulo slanje fizičkog sadržaja tog dijela memorije, [18].

```
root@w5ds:/ # dd if=/dev/block/mmcblk0 | busybox nc -l -p 8888
```

Slika 3. *Korištena naredba za ekstrakciju interne memorije uređaja*

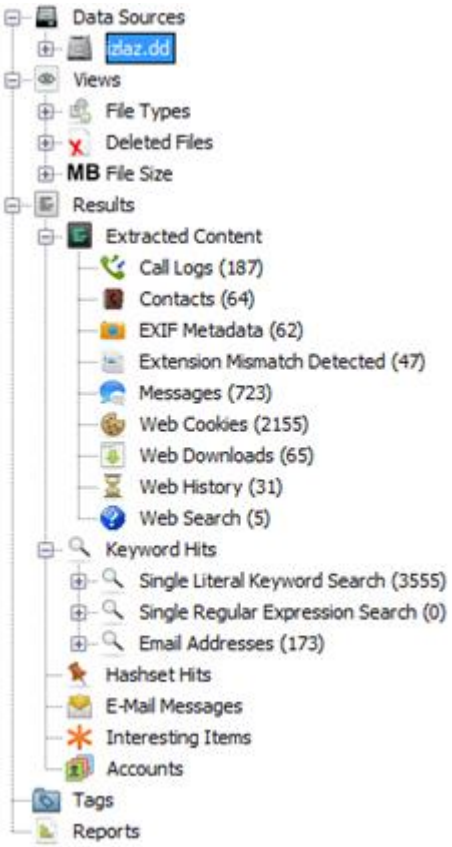
Kako bi se sadržaj pohranio na računalo potrebno je uspostaviti drugu stranu *Netcat* veze. To se radi korištenjem naredbe *nc* na terminalu koji izvršava naredbe na računalu sa *Santoku Linux* operativnim sustavom. Ta *nc* naredba se također sastoji od ulaznog i izlaznog dijela, ulazni dio je u ovom slučaju *port* 8888 na lokalnoj *IP* adresi 127.0.0.1 čija je veza uspostavljena u prethodnim koracima. Izlazni dio je upisan iza znaka *„>“* koji označava da će se naredba svoj *output* pohraniti negdje u obliku datoteke. Izlazna datoteka je nazvana *„izlaz.dd“,* a *.dd* je jedan od formata *image file*-ova uz *.img*, *.raw* i druge. Kako je prikazano na slici 4, pokretanje ove naredbe okida *-l* iz prethodne naredbe i tako da započinje fizičku ekstrakciju sadržaja *mmcblk0*, [19].



Slika 4. *Pokretanje i izvršavanje ekstrakcije bloka mmcblk0*

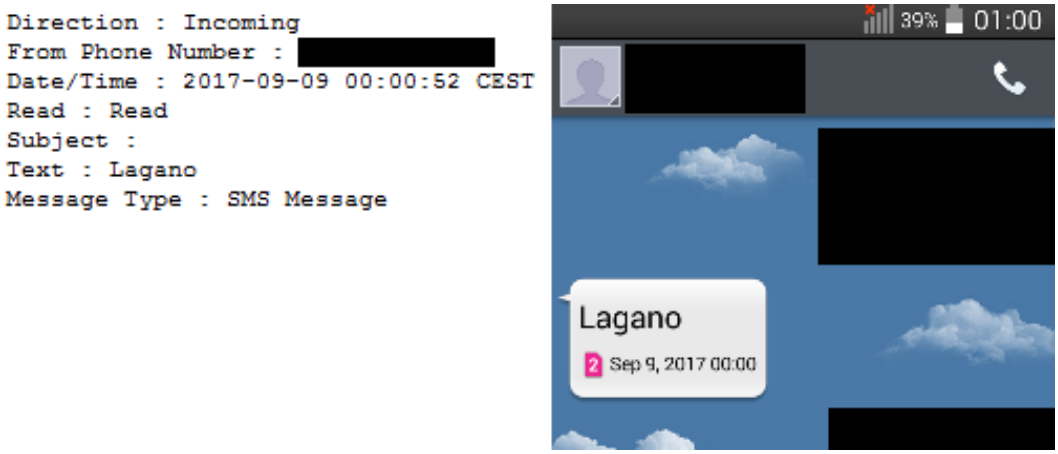
Ekstrakcija interne memorije pametnog mobilnog terminalnog uređaja veličine oko 4 GB traje nešto više od 20 minuta i pohranjuje se na memoriju računala. Datoteka „*izlaz.dd“* nakon toga spremljena na računalo s *Windows* operativnim sustavom gdje se korištenjem programskog alata *Autopsy* obavljena daljnja analiza.

Programski alat *Autopsy Forensic Browser* omogućuje provedbu forenzičke analize putem grafičkog sučelja. *Autopsy* je zapravo grafičko sučelje za *The Sleuth Kit* kojemu je pridodano nekoliko alata. Ovaj programski alat omogućuje učitavanje *image* datoteke koju potom analizira. Analizom *image*-a memorije *Autopsy* prepoznaje sadržaj na njemu, uključujući i onaj obrisani u slučaju da su u memoriji ostale potrebne informacije za povrat tih datoteka. Kako je prikazano na slici 5. učitavanjem *image*-a unutrašnje pohrane „*izlaz.dd*“ u grafičko sučelje programskog alata *Autopsy* učitavaju se sve dostupne datoteke, [20].



Slika 5. *Datoteke učitane u programski alat Autopsy iz "izlaz.dd"*

Kao korak validacije podataka na slici 6. prikazana je usporedba *SMS* poruke na uređaju prikupljenog ručnom ekstrakcijom i sadržaj iste poruke na korištenjem alata *Autopsy* s podacima prikupljenim fizičkom ekstrakcijom kao izvorom.



Slika 6. *Validacija usporedbom prikupljenih dokaza korištenjem različite metode ekstrakcije*

3. DRUŠTVENE MREŽE KAO IZVOR DIGITALNIH DOKAZA

Od početka pojave pametnih mobilnih terminalnih uređaja pa sve do danas najčešće korištene i najznačajnije mogućnosti takvih uređaja je pristup društvenim mrežama i usluzi trenutačnog poručivanja.

Prema podacima [21] *WhatsApp* je već 2015. godine samostalno dostigao globalni sustav razmjene *SMS* poruka u broju poslanih poruka. Putem *WhatsApp Messenger*-a te godine je dnevno poslano 30 milijardi poruka, što je za 10 milijardi više od broja dnevno poslanih *SMS* poruka.

Kako navodi [22] postoji značajna demografska razlika u korisnicima koji za tekstualni oblik udaljene komunikacije biraju *Instant Messagning* odnosno sustave razmjene poruka društvenih mrežu umjesto klasičnih *SMS* poruka. To se prvenstveno odnosi na samu dob korisnika te njihovu lokaciju što prvenstveno utječe na pakete usluga telekomunikacijskih operatora koje su dostupne korisnicima.

Postoji više vrsta društvenih mreža, od onih opće namjene kao što je *Facebook* koji je jednako usmjeren običnim korisnicima putem profila, ali poslovnim korisnicima putem *Facebook* stranica, pa do striktno poslovnih društvenih mreža kao što je *LinkedIn*. Osim po namjeni, društvene mreže je moguće podijeliti prema vrsti sadržaja koji njima dominira. Prema sadržaju društvena mreža Instagram je usmjerena slikovnom sadržaju i video sadržaju kratke duljine, a društvena mreža *Twitter* prvenstveno tekstualnom sadržaju. Za razliku od tih mreža koje imaju poprilično definiran tip sadržaja na *Facebook*-u je sadržaj mješovite prirode. Ono što sve ove društvene mreže posjeduju je sustav razmjene poruka između korisnika te aplikacije za pametne mobilne terminalne uređaje koje omogućavaju pristup društvenim mrežama, a s time i njihovom sustavu za razmjenu poruka.

Sve objave na društvenim mrežama imaju objavitelja, koji može koristi pravi identitet ili pseudonim, vremensku oznaku objave te nekakav sadržaj koji može biti tekstualnog, slikovnog, zvukovnog, video ili nekog drugog oblika. Osim toga, ovisno o društvenoj mreži i tipu, objave mogu sadržavati identitete osoba kojima su direktno upućene, geolokaciju i vremensku oznaku nastanka u slučaju da se radi o slikovnom ili video sadržaju te još neke metapodatke ovisno o društvenoj mreži. Informacije koje sadrži objava ili aktivnost na društvenoj mreži se mogu iskoristiti kao digitalni dokaz ako se prikupe i obrade na ispravan način. Sve se to prenosi i na sustave razmjene poruka društvenih mreža. Trenutno svaka društvena mreža ima sustav razmjene poruka sličnoga oblika, to jest sastoje se od razgovora koji mogu činiti dva ili više korisnika koji međusobno razmjenjuju poruke s vremenskom oznakom bilo tekstualnog, slikovnog ili video sadržaja te je na pojedinim sustavima razmjene poruka društvenih mreža vidljiva aktivnost ili dostupnost korisnika.

Digitalne dokaze vezane uz društvene mreže možemo podijeliti na one koji nastali objavama samih korisnika na takve mreže te na dokaze koji su nastali privatnom komunikacijom između dva ili više korisnika društvene mreže.

Prema [23] u moguće digitalne dokaze prikupljenih na društvenoj mreži *Facebook* pripadaju svaka interakcija korisnika s tom društvenom mrežom na način da joj se može pridodati određena obavljena aktivnost i vremenska oznaka. Među takve aktivnosti pripadaju korištenje tražilice, objavljivanje na zid društvene mreže, stvaranje događaja te, ono što je tema ovog diplomskog rada, razgovor između korisnika te društvene mreže.

Važno je spomenuti da se veliki dio digitalnih dokaza prilikom korištenja društvenih mreža na osobnim računalima niti u jednom trenutku ne pohranjuju na samu lokalnu pohranu računala, za razliku od korištenja istih društvenih mreža putem odgovarajućih aplikacija za mobilnih terminalne uređaje koje gotovo u svakom slučaju dio podataka spremaju na lokalu pohranu, [23].

Osim toga, prema [24] neki od tih digitalnih dokaza koje aplikacije društvenih mreža pohranjuju na uređaj ostaju i nakon deinstalacije same aplikacije te to čini razvijanje postupaka koji mogu iz podataka dobivenih fizičkom ekstrakcijom memorije uređaja još bitnijim.

Dokazi koji se prikupljaju sa samih uređaja putem kojih su korištene društvene mreže nisu jedini izvor ovakvih digitalnih dokaza. Forenzikom mrežnog prometa koji sadrži komunikaciju putem društvenih mreža također može biti izvor dokaza. Prema [25] dio podataka prilikom korištenja nekih društvenih mreža se prenosi u nekriptiranom obliku i iz prikupljenog mrežnog prometa mogu se iščitati informacije kao što su lokacija, poslane poruke, slike i video sadržaj.

4. APLIKACIJE DRUŠTVENIH MREŽA NA UREĐAJIMA ANDROID OS-A

Društvene mreže koje su obrađene u ovome diplomskom radu su *Facebook* i *Instagram.* Obje društvene mreže imaju pripadajuće aplikacije za *Android* operativni sustav koje omogućuju razmjenu poruka između korisnika istih. Aplikacije za *Android OS* pohranjuju podatke aplikacije unutar baza podataka koje stvaraju u datotečnom sustavu uređaja. Fokus ovog poglavlja je na pronalasku lokacija tih baza za analizirane aplikacije te analiziranje sadržaja samih baza s ciljem rekonstrukcije razgovora obavljenih korištenjem tih aplikacija, [26].

4.1. Instagram

Aplikacija *Instagram* za uređaje s *Android* operativnim sustavom [27] je danas jedna od najpopularnijih aplikacija na *Google*-ovom servisu za distribuciju aplikacija *Google Play* s preko milijardu preuzimanja.

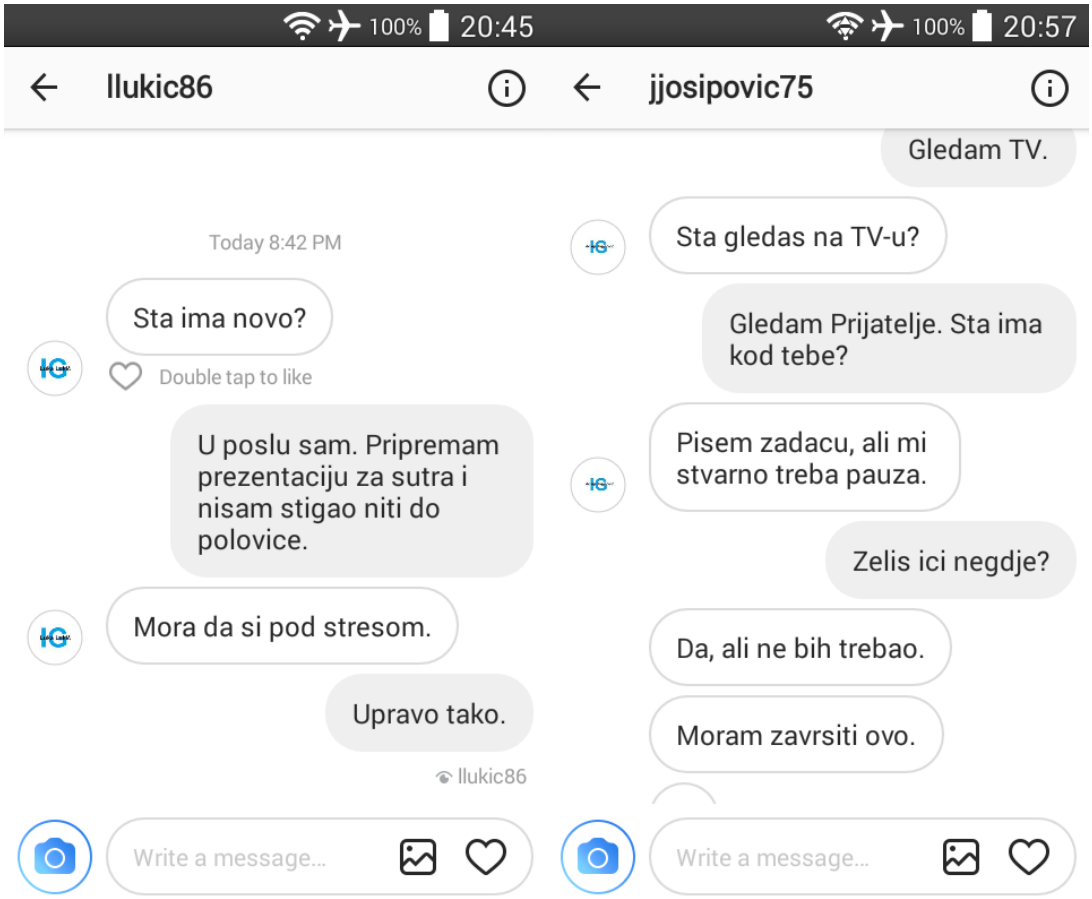
Instagram, često stiliziran kao *IG*, je društvena mreža u vlasništvu *Facebook*-a koja je usmjerena na razmjenu slika i video sadržaja. *Instagram* je pokrenut 2010. godine te je postojala samo aplikacija namijenjena *Apple*-ovom *iOS* operativnom sustavu [28]. Od 2012. godine postoji verzija aplikacije za *Android OS* te je razvijeno *web* sučelje za *Instagram* kojim se omogućuje pristup istome putem *web* preglednika uz ograničene mogućnosti. Takve ograničene mogućnosti *web* sučelja su zadržane i do danas te se sustav razmjene poruka ove društvene mreže ne može koristiti putem *web* preglednika na osobnom računalu bez korištenja posebnih dodataka (eng. *plug-in* ili *add-on*) za preglednik.

Instagram Direct, odnosno sustav za razmjenu poruka ove društvene mreže, pojavio se 2013. godine te je omogućio privatnu komunikaciju između korisnika u obliku teksta, slika ili video sadržaja. Korisnici koji se međusobno prate mogu izravno komunicirati, a ako korisnik zaprimi poruku od korisnika kojeg ne prati poruka će biti stavljena na čekanje (eng. *pending*) sve dok je korisnik ne odobri, [29].

U *Instagram Direct* se od 2015. godine uvodi niz novih mogućnosti među kojima je "*conversation threading"* što korisnicima omogućuje uvid u povijest korespondencije i lakše praćenje razgovora u odnosu na pojedinačne poruke koje su prije bile dostupne korisnicima. Osim toga, *threading* omogućuje stvaranje grupnih razgovora unutar *Instagram*-ovog sustava za razmjenu poruka.

Na uređaju namijenjenom za prikaz primjera forenzičke analize u svrhu ovog diplomskog rada ja instalirana aplikacija *Instagram* verzije 49.0.0.15.89 koja je izdana u lipnju 2018. godine, [30]. Otvorena su tri korisnička računa za društvenu mrežu *Instagram* i jedan od tih računa se koristio na uređaju dok su preostala dva

korištena na osobnom računalu za razmjenu poruka s korisničkim računom na uređaju s ciljem naknadne provedbe forenzičke analize nad istim. Tekst razgovora je preuzet s [31] i [32], i primjer rezultata ručne ekstrakcije podataka sustava za razmjenu poruka društvene mreže *Instagram* je prikazan na slici 7.



Slika 7. *Ručna ekstrakcija podataka sustava za razmjenu poruka aplikacije Instagram*

Logička ekstrakcija podataka na kojima se nalazi ovaj razgovor je tema sljedećeg podpoglavlja. Podaci prikupljeni tim načinom ekstrakcije potrebno je validirati usporedbom s podacima prikupljenim fizičkom ekstrakcijom koja je opisana u drugom poglavu rada.

4.1.1. Logička ekstrakcija podataka aplikacije Instagram

Svaka aplikacija namijenjena *Android* operativnom sustavu posjeduje *applicationId* u obliku *com.primjer.aplikacija* koji predstavlja jedinstveni identifikator aplikacije na razini uređaja, ali i na *Google*-ovom servisu za distribuciju aplikacija namijenjenim *Android OS – Google Play*. Ovo je osnovni identifikator aplikacije te se na njega vežu sve verzije iste aplikacije. U slučaju promjene *applicationId*-a pri objavljivanju nove verzije aplikacije *Google Play* će tretirati novu verziju kao potpuno drugu aplikaciju, [33].

Identifikator, *applicationId* za aplikaciju *Instagram* namijenjenu *Android OS*-u je *com.instagram.android,* [34]. Na uređaju se prilikom instalacije aplikacije u direktoriju *"/data/data"* stvara mapa koja imenom odgovara navedenom *applcationId*-u te se u nju pohranjuju podaci aplikacije. Inače, u direktoriji *"/data/data"* se pohranjuju podaci svih aplikacija, bilo instalirane od sustava ili samog korisnika. Kako se mape predinstaliranih aplikacija za lokaciju, pozive i razmjenu poruka nalaze unutar ovoga direktorija na svim *Android* uređajima, on predstavlja jednu od ključnih lokacija pohrane prilikom provođenja forenzičke analize, [35].

Kako *Android* operativni sustav koristi sustav zaštite temeljen na *Linux*-u u smislu identificiranja i razdvajanja aplikacijskih resursa svakoj aplikaciji se dodjeljuje korisnički *ID* (*UID*). Aplikacija se pokreće pod tim korisnikom i to je specifično za *Android* operativni sustav u odnosu na ostale gdje se više aplikacija pokreće pod istim korisnikom, [36].

Poddirektorij *"/data/data/com.instagram.android"* ima dozvole *chmod 751* pod vlasništvom *UID*-a te same aplikacije. To znači da samo sama aplikacija ima pravo čitanja i zapisivanja unutar tog istog poddirektorija. Da bi se obavila logička ekstrakcija sadržaja tog direktorija potrebno je promijeniti dozvolu istoga, [37].

Na slici 8 prikazan je sadržaj poddirektorija *"com.instagram.android"* i mape "*databases*" unutar njega.

```
root@w5ds:/ # cd /data/data/com.instagram.android
root@w5ds:/data/data/com.instagram.android #
app_acra-reports
app_batch_counter
app_funnel_backup
app_ig_analytics_beacon
app_light_prefs
app_minidumps
app_overtheair
app_webview
cache
code_cache
databases
files
lib
lib-main
shared_prefs
root@w5ds:/data/data/com.instagram.android # cd databases
root@w5ds:/data/data/com.instagram.android/databases # ls
direct.db
direct.db-journal
root@w5ds:/data/data/com.instagram.android/databases #
```

Slika 8. *Sadržaj mape "databases" unutar poddirektorija "com.instagram.android"*

Od prikazanog sadržaja poddirektorija aplikacije *Instagram* za potrebu forenzičke analize sustava za razmjenu poruka društvene mreže *Instagram* najvažnija je datoteka "*direct.db*".

Radi se o bazi podataka u koju aplikacija *Instagram* pohranjuje sve podatke svoga sustava za razmjenu poruka – *Instagram Direct*. Ovakva lokalna pohrana podataka sustava za razmjenu poruka omogućuje korisniku uvid u poruke na toj aplikaciji čak i kad on nije spojen na mrežu.

Prema ekstenziji ove datoteke "*.db*" može se zaključiti da se radi o *SQLite* bazi podataka. Datoteke s ekstenzijom "*.db*" su korištene na raznim mobilnim terminalnim uređajima s operativnim sustavima *Android*, *iOS* i *Windows Phone 7*, a unutar njih se pohranjuju i podaci imenika, *SMS* i između ostalog podaci aplikacija kao što je u ovom slučaju, [38].

Datoteka "*direct.db-jurnal*" je datoteka koje se automatski generira prilikom provođenja transakcija u *SQLite* bazama podataka. Transakcije, u smislu baza podataka, su nizovi operacija nad bazom koje je moguće potvrditi ili opozvati, što vraća bazu u početno stanje prije ulaska u niz operacija unutar transakcije, [39].

Kako bi se obavila logička ekstrakcija datoteke "*direct.db*" potrebno je promijeniti dozvole nad tom datotekom. Korištenjem naredbe "*chmod 777"* nad tom datotekom, kao što je prikazano na slici 9 omogućuje se čitanje, a s tim i kopiranje, te datoteke od svih korisnika. Kao što je prikazano na slici 10 naredbom "*adb pull*" se datoteka "*direct.db*" kopira, odnosno preuzima, na domaćinsko računalo, [40].

```
root@w5ds:/data/data/com.instagram.android/databases # chmod 777 direct.db
root@w5ds:/data/data/com.instagram.android/databases # ls -l
-rwxrwxrwx u0_a96   u0_a96      73728 2018-08-26 20:58 direct.db
-rw------- u0_a96   u0_a96      53864 2018-08-26 20:58 direct.db-journal
```

Slika 9. *Izmjena dozvola datoteke "direct.db"*

```
santoku@santoku:~$ adb pull /data/data/com.instagram.android/databases/direct.db
835 KB/s (73728 bytes in 0.086s)
```

Slika 10. *Logička ekstrakcija datoteke "direct.db"*

Za validaciju datoteka prikupljenih različitim metodama ekstrakcije koristi se usporedba *hash* vrijednosti datoteka. *Hash* funkcija je algoritam koja pretvara ulaz varijabilne veličine u izlaz određene veličine, odnosno *hash* vrijednost. Digitalni forenzički alati često sami računaju *hash* vrijednosti datoteka. *Hash* funkcije koje se najčešće koriste u digitalnoj forenzici su *MD5* i *SHA-1*, [41].

Na ovom primjeru je za računanje *MD5 hash* vrijednosti datoteke "*direct.db*" prikupljene logičkom ekstrakcijom je korišten programski paket *md5sum* za *Linux* operativne sustave. Ovaj programski paket se inače često koristi pri validaciji integriteta preuzetog sadržaja, [42]. Korištenje *md5sum* nad navedenom datotekom i rezultat, odnosno dobivena *hash* vrijednost su prikazani na slici 11.

```
santoku@santoku:~$ md5sum direct.db
e5445255a0de5ac1a9d8076d06728102  direct.db
```

Slika 11. *Generiranje MD5 vrijednosti baze podataka*

Baza podataka koja je prikupljena fizičkom ekstrakcijom se nalazi unutar *image*-a koji je urađen u drugom poglavlju te pokrenut u forenzičkom alatu *Autopsy*. Pretraživačem ugrađenim unutar forenzičkog alata *Autopsy* pronađena je datoteka "*direct.db*" te se odabirom svojstva te datoteke dolazi do tablice koja sadržava detaljnije podatke o toj datoteci. Između ostaloga među tim podacima se nalazi i vrijednost *MD5 hash* funkcije za navedenu datoteku. Rezultat *hash* funkcije za navedenu datoteku prikupljenu fizičkom ekstrakcijom je *e5445255a0de5ac1a9d8076d06728102,* kao što je i prikazano na slici 12 i on odgovara hash vrijednosti datoteke prikupljene logičkom ekstrakcijom.

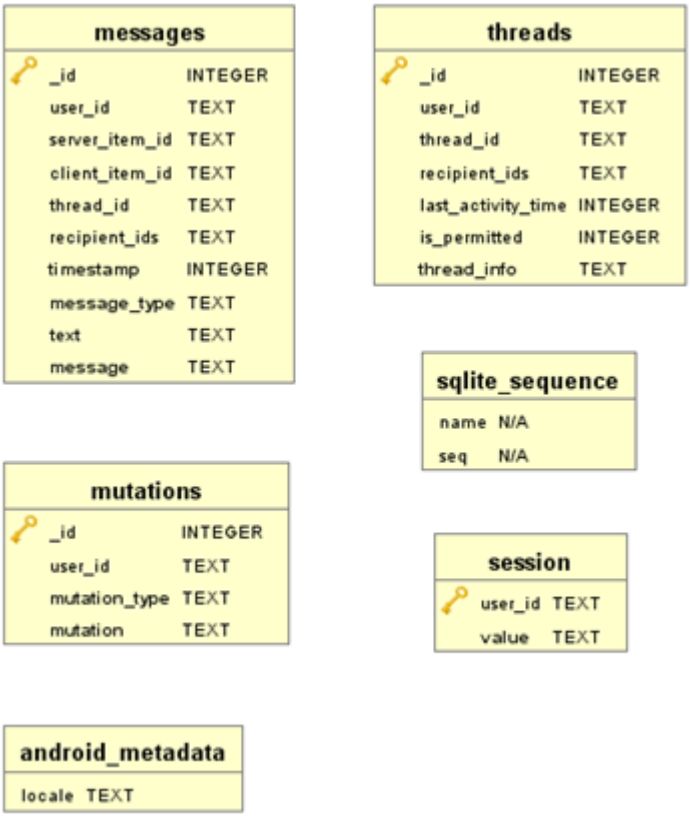
Name	direct.db
Location	/img_izlaz.dd/vol_vol46/data/com.instagram.android/databases/direct.db
Modified Time	2018-08-26 20:58:09 CEST
Change Time	2018-08-26 20:58:09 CEST
Access Time	2018-08-26 13:59:05 CEST
Created Time	2018-08-26 13:59:05 CEST
Size	73728
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Mode	rrw-rw----
UserID	10096
GroupID	10096
Meta Addr.	54412
Attr. Addr.	1-0
Type(Dir)	r
Type(Meta)	r
Known	unknown
In Hashsets	
MD5 Hash	e5445255a0de5ac1a9d8076d06728102
Object ID	18306
MIME Type	application/x-sqlite3
Extension	db
Keyword Preview	«direct.db«

Slika 12. *Detaljni podaci o datoteci "direct.db" iz forenzičkog alata Autopsy*

Nakon validacije prikupljene datoteke, odnosno baze podataka je potrebno analizirati. Za analizu ovih baza podataka korišteni su programski alati koji omogućavaju čitanje sadržaja *SQLite3* baza podataka. Struktura i sadržaj prikupljenih baza podataka je obrađena u sljedećem potpoglavlju.

4.1.2. Analiza podataka aplikacije Instagram

Grafički prikaz *SQLite3* baze podataka "*direct.db*" generiran je korištenjem programskog alata *DbVisualizer*. Ovaj programski alat omogućuje spajanje na sve popularne vrste baza podataka te generira grafički prikaz te baze podataka u obliku tablica s ispisanim poljima, odnosno stupcima te pripadajući tip podataka koji je vezan za taj stupac. Na grafikonu 1 prikazana je shema baze podataka sustava za razmjenu poruka aplikacije *Instagram*, [43].



Grafikon 1. *Struktura baze podataka "direct.db"*

Korištenjem programskog paketa *sqliteman,* koji je dostupan na *Santoku Linux*-u pristupljeno je bazi podataka "*direct.db*". Programski paket *sqliteman* je razvojni i administracijski alat koji omogućuje rad sa *Sqlite3* bazama podataka putem grafičkog sučelja, [44].

U ovom radu za potrebe forenzičke analize svi potrebni podaci se nalaze unutar tablica *messages* i *threads.* Ti podaci uključuju sam sadržaj poruke i vremenske oznake istih, nude još neke informacije kao što su *URL* profilne slike korisnika i slično. Kao što je prije navedeno *thread* predstavlja razgovor u kojemu sudjeluju dva ili više korisnika. U ovom slučaju svaki *thread* je posjeduje jedinstveni identifikator *_id* na lokalnoj razini te *thread_id* na razini cijele društvene mreže *Instagram*. To znači da će isti razgovor na strani primatelja poruke sigurno imati jedan *thread_id* jednake vrijednosti kao onaj prikazan u bazi podataka analiziranog uređaja dok će se *_id* iz tablice *threads* vjerojatno razlikovati.

Ostala dva identifikatora u tablici *threads* predstavljaju identifikator samog korisnika te identifikator primatelja s nazivima stupaca *user_id* i *recipients_id.* Kako je naziv samog stupca *recipients_id* u pluralnom obliku govori nam da se u tom polju mogu nalaziti više primatelja. Sva tri polja identifikatora u ovoj tablici su definirana kao tekstualna polja iako je njihova vrijednost iskazana samo znamenkama. Prikaz sadržaja identifikatora unutar tablice *threads* baze podataka "*direct.db*" prikazano je na slici 13.

	_id	user_id	thread_id	recipient_ids
1	10	8483455570	340282366841710300949128165592689504989	8484376335
2	11	8483455570	340282366841710300949128228911742363466	8483771150

Slika 13. *Prikaz sadržaja tablice threads*

Sljedeće polje u ovoj tablici je *last_activity_time* čiji sadržaj predstavlja vremensku oznaku posljednje aktivnosti unutar ovog razgovora. Ta vremenska oznaka je izražena u *Unix* vremenu, koje je također poznato kao *UNIX Epoch time.* Tim se oblikom vremenske oznake prikazuje koliko je sekundi, odnosno u ovom slučaju se radi o mikrosekundama na što ukazuje šesnaesteroznamenkasti zapis unutar ovoga polja, proteklo od 1. siječnja 1970. godine u 00:00 po vremenskoj zoni koordiniranog svjetskog vremena (eng. *Coordinated Universal Time, UTC*). Sve vremenske oznake u *Linux* sustavima, među koje spade i *Android OS*, se mjere na ovaj način, [45].

Na slici 14 prikazane su vremenske oznake posljednjih aktivnosti u razgovorima iskazane u mikrosekundama proteklim od *Unix Epoch* korištenjem programskog alata *DbVisualizer*.

*	_id	thread_id	last_activity_time
1	10	340282366841710300949128165592689504989	1535309854004977
2	11	340282366841710300949128228911742363466	1535309105291023

Slika 14. *Prikaz sadržaja tablice threads*

Posljednja dva stupca u tablici *threads* baze podataka "*direct.db"* su *is_permited* i *thread_info*. Unutar stupca *is_permited* brojevima 0 ili 1 označuje se je li je ovaj razgovor odobren. Vrijednosti 0 i 1 predstavljaju vrijednost netočno (eng. *false*) i točno (eng. *true*) u logičkoj algebri. Kao što je prije spomenuto u ovom poglavlju, ukoliko korisnik zaprimi poruku od korisnika kojeg ne prati poruka će biti stavljena na čekanje što znači da će *is_permited* imati vrijednost 0 sve dok potencijalni primatelj ne odobri razgovor s korisnikom kojeg ne prati. Korisnici u ovom primjeru su se međusobno pratili (eng. *follow*) na *Instagram*-u stoga početna vrijednost ovoga polja je bila 1, odnosno razgovor nije savljen na čekanje do odobravanja nego je od početka odobren.

Stupac *thread_info* sadrži detaljne informacije o razgovoru, odnosno *thread*-u pohranjenom u *JSON* formatu. *JavaScript Object Notation* ili *JSON* je format za razmjenu podataka koji je, iako mu samo ime naznačuje drugačije, namijenjen razmjeni strukturiranih podataka između svih programskih jezika, [46]. Iako se podaci unutar njega zapisuju u tekstualnom obliku koji je čovjeku čitljiv. U slučaju složenije strukture bez korištenja dodatnih alata on može biti teško shvatljiv i nerazumljiv, kao što je u slučaju u ovom primjeru.

Korištenjem alata za formatiranje i validaciju *JSON* podataka pod nazivom *JSON Formatter* [47] sadržaj stupca *thread_info* je preoblikovan u lakše čitljiv oblik. Na slici *15* je prikazan je dio korisničkog sadržaja ovoga polja i vidljivo je da sadrži neke podatke koji su se već nalazili u tablici, kao što su *thread_id* i vremenska oznaka, te neke dodatne podatke i metapodatke o korisniku kao što su *URL* njegove profilne slike, broj pratitelja i da li se radi o verificiranom *Instagram* korisniku.

```
{ ⊟
   "life_cycle_state":"UPLOADED",
   "last_seen_at":{ ⊞ },
   "local_last_seen_retry_count":0,
   "seen_state":"ALL_SEEN",
   "thread_id":"340282366841710300949128165592689504989",
   "last_message":{ ⊟
      "content_type":"TEXT",
      "status":"UPLOADED",
      "user":{ ⊟
         "username":"jjosipovic75",
         "full_name":"josipjosipovic75",
         "profile_pic_url":"https://instagram.fzag1-1.fna.fbcdn.net/vp/b7b6af/5BFE31A0
/t51.2885-19/s150x150/39318469_301287367117374_549739505897177088_n.jpg",
         "profile_pic_id":"1854632918602085758_8484376335",
         "has_anonymous_profile_picture":false,
         "id":"8484376335",
         "usertag_review_enabled":false,
         "follower_count":1,
         "show_besties_badge":false,
         "is_private":false,
         "allowed_commenter_type":"any",
         "is_verified":false,
         "byline":"1 follower",
         "is_new":false,
         "social_context":"Following",
         "search_social_context":"Following",
         "unseen_count":0,
         "reel_auto_archive":"unset",
         "feed_post_reshare_disabled":false
      },
      "item_type":"text",
      "item_id":"28321467950674186375221276502392832",
      "timestamp":"1535309854004977",
      "timestamp_in_micro":1535309854004977,
      "user_id":"8484376335",
      "text":":(",
      "hide_in_thread":false,
      "seen_count":0,
      "replay_expiring_at_us":0
```


Slika 15. *Prikaz sadržaja polja thread_info tablice threads*

Tablica koja sadrži najviše podataka unutar baze "*direct.db*" sa stajališta forenzičke analize je tablica *messages*. Unutar ove tablice su pohranjene najbitnije informacije koje je potrebno prikazati kod forenzičke analize bilo kakvog sustava razmjene poruka. Ti podaci uključuju identiteti pošiljatelja i primatelja, odnosno sudionika razgovora, sadržaj poruka i vremenske oznake istih poruka. Tablica *messages* sadrži nekoliko redundantnih stupaca u odnosu s tablicom *threads,* kao što su *user_id*, *thread_id* i *recipient_ids* te dva identifikatora koja su jedinstvena za ovu tablicu, *client_item_id* i *server_item_id*. U recima unutar kojih se nalazi poruka koja je generirana od strane korisnika uređaja polje *client_item_id* posjeduje vrijednost dok u ostalima, odnosno zaprimljenim porukama, zauzima vrijednost *null.*

U stupac *timestamp* je kao zapisana vremenska oznaka trenutka u kojemu je poruka poslana te je ona kao i u slučaju kod tablice *threads* zapisana u *Unix Epoch* mikrosekundama. Stupac *message_type* definira tip sadržaja poruke, koji su u ovom primjeru svi tekstualni, te ga slijedi stupac *text* u kojemu se nalazi sami tekst poruke. Sadržaj tablice *messages* prikazan je na slici 16.

*	user_id	server_item_id	client_item_id	thread_id
1	23 8483455570	28321462413909814986490699751358464	(null)	340282366841710300949128165592689504989
2	24 8483455570	28321462877974647882522258302828544	63f23e43-2e29-48a1-8115-bf10bfc5dd42	340282366841710300949128165592689504989
3	25 8483455570	28321463411839101108139335188742144	(null)	340282366841710300949128165592689504989
4	26 8483455570	28321464055493871140736867357425664	9c8f8479-79bd-4740-aec1-dabc9575a014	340282366841710300949128165592689504989
5	27 8483455570	28321465730716136962458687331368960	(null)	340282366841710300949128165592689504989
6	28 8483455570	28321465949137743199524353059323904	0c8f6e18-3a96-45e4-a534-3e8bdc9150d9	340282366841710300949128165592689504989
7	29 8483455570	28321467346603417453425606797557760	(null)	340282366841710300949128165592689504989
8	30 8483455570	28321467614630015605151038099685376	(null)	340282366841710300949128165592689504989
9	31 8483455570	28321467950674186375221276502392832	(null)	340282366841710300949128165592689504989
10	32 8483455570	28321451603323637013576182868738048	(null)	340282366841710300949128228911742363466
11	33 8483455570	28321453024292363232022997449572352	f5ccb2a8-894a-48d4-90ad-9fd3548d9bf0	340282366841710300949128228911742363466
12	34 8483455570	28321453535331571657338897257463808	(null)	340282366841710300949128228911742363466
13	35 8483455570	28321454139339492522075438519943168	1926febc-69aa-469a-b9cb-5b4dd6808c94	340282366841710300949128228911742363466

*	_id	recipient_ids	timestamp	mess...	text	message
1	23	8484376335	1535309553856379	text	Sta radis sada?	{"content_type":"TEXT","status":"UPLOADED","user":{"username":"jjc
2	24	8484376335	1535309579013384	text	Gledam TV.	{"content_type":"TEXT","status":"UPLOADED","user":{"username":"iiv
3	25	8484376335	1535309607954234	text	Sta gledas na TV-u?	{"content_type":"TEXT","status":"UPLOADED","user":{"username":"jjc
4	26	8484376335	1535309642846829	text	Gledam Prijatelje. Sta ima kod...	{"content_type":"TEXT","status":"UPLOADED","user":{"username":"iiv
5	27	8484376335	1535309733660810	text	Pisem zadacu, ali mi stvarno t...	{"content_type":"TEXT","status":"UPLOADED","user":{"username":"jjc
6	28	8484376335	1535309745501469	text	Zelis ici negdje?	{"content_type":"TEXT","status":"UPLOADED","user":{"username":"iiv
7	29	8484376335	1535309821258235	text	Da, ali ne bih trebao.	{"content_type":"TEXT","status":"UPLOADED","user":{"username":"jjc
8	30	8484376335	1535309835787986	text	Moram zavrsiti ovo.	{"content_type":"TEXT","status":"UPLOADED","user":{"username":"jjc
9	31	8484376335	1535309854004977	text	:(	{"content_type":"TEXT","status":"UPLOADED","user":{"username":"jjc
10	32	8483771150	1535308967813328	text	Sta ima novo?	{"content_type":"TEXT","status":"UPLOADED","user":{"username":"llu
11	33	8483771150	1535309044844197	text	U poslu sam. Pripremam prez...	{"content_type":"TEXT","status":"UPLOADED","user":{"username":"iiv
12	34	8483771150	1535309072547688	text	Mora da si pod stresom.	{"content_type":"TEXT","status":"UPLOADED","user":{"username":"llu
13	35	8483771150	1535309105291023	text	Upravo tako.	{"content_type":"TEXT","status":"UPLOADED","user":{"username":"iiv

Slika 16. *Prikaz sadržaja tablice messages*

Kao i kod tablice *threads,* stupac s najviše informacija je onaj zapisan u *JSON* formatu. I u ovome polju se nalaze neki redundantni podaci iz prethodnih polja kao što su *timestamp*, identifikatori, tip poruke te sam sadržaj poruke. Važno je spomenuti da se u ovome polju u *JSON* format pohranjuju samo detaljniji podaci o pošiljatelju poruke, a da se primatelj referencira samo u obliku identifikatora *thread_id* i *recipient_ids.* Osim toga, važno je spomenuti i da se unutar jednog *Instagram* korisničkog računa razlikuju dvije vrste imena, to su *username* i *full_name*. Formatirani sadržaj ovoga polja prikazan je na slici 17.

```
{
  "content_type":"TEXT",
  "status":"UPLOADED",
  "user":{
    "username":"iivic64",
    "full_name":"ivan.ivic64",
    "profile_pic_url":"https://instagram.fzag1-1.fna.fbcdn.net/vp/eb63ee6c2/
/t51.2885-19/s150x150/39203094_1979467712073492_3289640104842231808_n.jpg",
    "profile_pic_id":"1854613297355495643_8483455570",
    "hd_profile_pic_url_info":{
      "url":"https://instagram.fzag1-1.fna.fbcdn.net/vp/777ea858098a/
/39203094_1979467712073492_3289640104842231808_n.jpg",
      "width":188,
      "height":188,
      "type":0
    },

  },
  "item_id":"28321462877974647882522258302828544",
  "client_context":"63f23e43-2e29-48a1-8115-bf10bfc5dd42",
  "timestamp":"1535309579013384",
  "timestamp_in_micro":1535309579013384,
  "user_id":"8483455570",
  "text":"Gledam TV.",
  "hide_in_thread":false,
  "thread_key":{
    "thread_id":"340282366841710300949128165592689504989",
    "recipient_ids":[
      "8484376335"
    ]
  },
  "seen_count":0,
  "replay_expiring_at_us":0
}
```


Slika 17. *Prikaz sadržaja polja message unutar tablice messages*

Unutar tablica baze podataka ”*direct.db*” dostupni su podaci kao što su pošiljatelj, primatelj, vremenska oznaka i sadržaj poruke, a to su svi podaci potrebni za definiranje jedne tekstualne poruke. U šestom poglavlju ti podaci će biti iskorišteni za rekonstrukciju razgovora obavljenih korištenjem sustava za razmjenu poruka aplikacije *Instagram*.

4.2. Aplikacije za razmjenu poruka društvene mreže Facebook

Službene aplikacije za operativni sustav *Android* izdane od tvrtke *Facebook* uključuju aplikaciju *Facebook*, *Facebook Lite*, *Messenger* i *Messenger Lite* te one zajedno imaju preko 2,5 milijardi instalacija na *Android* uređaje putem *Google*-ovog servisa za distribuciju aplikacija, [48], [49], [50], [51].

Facebook je zasnovan 2004. godine kao društvena mreža za studente *Harvard*-a, a poslije i drugih sveučilišta. Unatoč brzom širenju *Facebook* je bio zatvorena ili polu-zatvorena društvena mreža sve do 2007. godine kada se u potpunosti otvorio i postao dostupan svim korisnicima, [52].

Instant messaging mogućnost za *Facebook* se prvi put pojavljuje 2008. godine na *web* temeljenom sučelju, a *Facebook Messenger* aplikacija za uređaje s *Android* i *iOS* operativnim sustavom se pojavljuje istovremeno na tržištu 2011. godine, [53], [54].

Facebook Messenger Lite je verzija ove aplikacije namijenjena starijim i sporijim uređajima te korisnicima sa sporijim brzinama pristupa. Ova verzija aplikacije je izdana 2017. godine te je vrlo brzo dostigla preko 200 milijuna korisnika.

Messenger Lite verzije 35.1.0.18.192 izdan u lipnju 2018. godine je korišten u ovome diplomskom radu kao primjer, [55]. Kao i u primjeru s *Instagram*-om otvorena su tri korisnička računa za društvenu mrežu *Facebook* i jedan od tih računa se koristio na uređaju. Korištenjem osobnog računala putem ostala dva korisnička računa razmijenjene su poruke s korisničkim računom na uređaju s ciljem naknadne provedbe forenzičke analize nad istim. Tekst razgovora je preuzet s [31] i [32], i primjer rezultata ručne ekstrakcije podataka sustava s aplikacije *Messenger Lite* je prikazan na slici 18.

Slika 18. *Ručna ekstrakcija podataka aplikacije Messenger Lite*

Logička ekstrakcija podataka na kojima se nalazi ovaj razgovor je tema sljedećeg podpoglavlja. Podaci prikupljeni tim načinom ekstrakcije potrebno je validirati usporedbom s podacima prikupljenim fizičkom ekstrakcijom koja je opisana u drugom poglavlju rada.

4.2.1. Logička ekstrakcija podataka aplikacije Messenger Lite

Identifikator aplikacije *applicationId* koji je spomenut u prethodnom potpoglavlju za aplikaciju *Messenger Lite* je *com.facebook.mlite,* [33]. Kao i u slučaju aplikacije Instagram, na uređaju se prilikom instalacije aplikacije u direktoriju *"/data/data"* stvara mapa koja imenom odgovara navedenom *applicationId*-u te se u nju pohranjuju podaci aplikacije. Sadržaj i lokacija datotečnog sustava *"/data/data/com.facebook.mlite"* i *"/data/data/com.facebook.mlite/databases"* su prikazani na slici 19.

```
root@w5ds:/data/data/com.facebook.mlite # ls
app_analytics
app_gatekeepers
app_light_prefs
app_minidumps
app_qe_sessioned
app_qe_sessionless
app_sessionless_gatekeepers
cache
databases
files
lib
lib-main
no_backup
shared_prefs
root@w5ds:/data/data/com.facebook.mlite # 
root@w5ds:/data/data/com.facebook.mlite # cd databases
root@w5ds:/data/data/com.facebook.mlite/databases # ls
core.db
core.db-journal
cross_account.db
cross_account.db-journal
omnistore.db
omnistore.db-shm
omnistore.db-wal
```

Slika 19. *Sadržaj poddirektorija "com.facebook.mlite"*

Za razliku od aplikacije *Instagram,* u poddirektoriju "*databases*" se ne nalazi jedna nego tri baze podataka. Kako bi se izvršila logička ekstrakcija ovih baza s uređaja potrebno je kao i u prethodnom slučaju promijeniti dozvole tih datoteka te nakon toga izvršiti naredbu "*adb pull*" za te datoteke kako bi se one pohranile na domaćinsko računalo. Taj postupak je prikazan na slikama 20 i 21, [40].

```
root@w5ds:/data/data/com.facebook.mlite/databases # chmod 777 core.db
ss_account.db                                                          <
root@w5ds:/data/data/com.facebook.mlite/databases # chmod 777 omnistore.db
root@w5ds:/data/data/com.facebook.mlite/databases # ls -l
-rwxrwxrwx u0_a79   u0_a79     323584 2018-09-02 20:46 core.db
-rw------- u0_a79   u0_a79     119528 2018-09-02 20:46 core.db-journal
-rwxrwxrwx u0_a79   u0_a79      40960 2018-08-26 14:00 cross_account.db
-rw------- u0_a79   u0_a79      29240 2018-08-26 14:00 cross_account.db-journal
-rwxrwxrwx u0_a79   u0_a79     151552 2018-08-28 04:05 omnistore.db
-rw------- u0_a79   u0_a79      40960 2018-09-02 20:46 omnistore.db-shm
-rw------- u0_a79   u0_a79     436752 2018-09-02 20:46 omnistore.db-wal
```

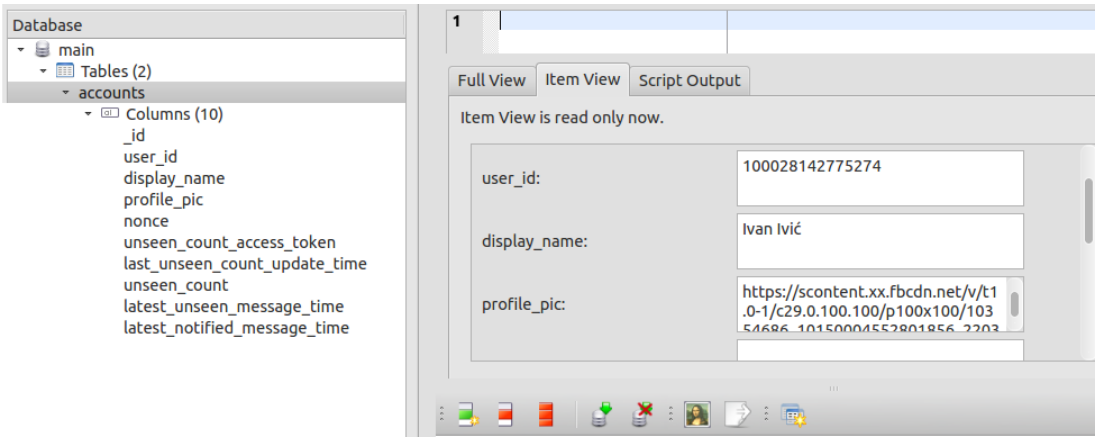
Slika 20. *Izmjena dozvola datoteka unutar poddirektorija "databases"*

```
santoku@santoku:~$ adb pull /data/data/com.facebook.mlite/databases/core.db
2159 KB/s (323584 bytes in 0.146s)
santoku@santoku:~$ adb pull /data/data/com.facebook.mlite/databases/cross_accoun
t.db
484 KB/s (40960 bytes in 0.082s)
santoku@santoku:~$ adb pull /data/data/com.facebook.mlite/databases/omnistore.db

1505 KB/s (151552 bytes in 0.098s)
```

Slika 21. *Logička ekstrakcija datoteka*

Korištenjem programskog paketa *sqliteman* analizirane su *SQLite3* datoteke baza podataka "*core.db*", "*cross_account.db*" i "*omnistore.db*". Sadržaj baze podataka "*cross_account.db*" uključuje tablicu *accounts* unutar koje je ispunjen postoji samo jedan redak, onaj s podacima o korisničkom računu vlasnika uređaja, to jest o *Facebook* korisničkom računu korisnika koji je trenutno prijavljen unutar ove aplikacije. Ti podaci, kao što je prikazano na slici 22 uključuju jedinstveni identifikator korisnika *user_id,* korišteno korisničko ime kao *display_name* te *URL* za profilnu sliku korisnika koji se pohranjuje unutar stupca *profile_pic*.



Slika 22. *Sadržaj baze "cross_account.db"*

Baza podataka "*omnistore.db*" sadrži veći broj tablica koje se koriste za rad same aplikacije, ali nisu bitne za provođenje ove forenzičke analize. Ono što je kod aplikacije Instagram bila baza podataka "*direct.db*", odnosno datoteka gdje su pohranjeni podaci o razgovorima, sudionicima razgovora i sadržaji samih poruka kod aplikacije *Messenger Lite* je baza "*core.db*". Kako bi usporedili datoteku, to jest bazu podataka "*core.db*" prikupljenu logičkom ekstrakcijom s onom prikupljene fizičkom ekstrakcijom prilikom *image*-a interne memorije uređaja generirana je *MD5* hash vrijednost te baze podataka korištenjem "*md5sum*" kao što je prikazano na slici 23.

```
santoku@santoku:~$ md5sum core.db
d2e922c21088738ecec2a1578cd9d0b8  core.db
```

Slika 23. *Generiranje MD5 vrijednosti baze podataka "core.db"*

Za validaciju potrebno je usporediti podatke prikupljene korištenjem različitih metoda ekstrakcije. Baza podataka prikupljena fizičkom ekstrakcijom, koja je opisana u drugom poglavlju rada, se nalazi unutar *image*-a koji je kreiran te pokrenut u forenzičkom alatu *Autopsy*. Pretraživačem ugrađenim unutar forenzičkog alata *Autopsy* pronađena je datoteka "*core.db*" te se odabirom svojstva te datoteke dolazi do tablice koja sadrži detaljnije podatke o toj datoteci. Između ostaloga među tim podacima se nalazi i vrijednost *MD5 hash* funkcije za navedenu datoteku. Rezultat *hash* funkcije za navedenu datoteku prikupljenu fizičkom ekstrakcijom je *d2e922c21088738ecec2a1578cd9d0b8,* kao što je i prikazano na slici 24. i on odgovara *hash* vrijednosti datoteke prikupljene logičkom ekstrakcijom.

Name	core.db
Location	/img_izlaz.dd/vol_vol46/data/com.facebook.mlite/databases/core.db
Modified Time	2018-08-28 04:17:46 CEST
Change Time	2018-08-28 04:17:46 CEST
Access Time	2018-08-26 13:59:29 CEST
Created Time	2018-08-26 13:59:29 CEST
Size	323584
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Mode	rrw-rw----
UserID	10079
GroupID	10079
Meta Addr.	92849
Attr. Addr.	1-0
Type(Dir)	r
Type(Meta)	r
Known	unknown
In Hashsets	
MD5 Hash	d2e922c21088738ecec2a1578cd9d0b8
Object ID	17057
MIME Type	application/x-sqlite3
Extension	db
Keyword Preview	«core.db«

Slika 24. *Detaljni podaci o datoteci "core.db" iz forenzičkog alata Autopsy*

Nakon validacije prikupljene datoteke, odnosno baze podataka je potrebno analizirati. Za analizu ovih baza podataka korišteni su programski alati koji omogućavaju čitanje sadržaja *SQLite3* baza podataka. Struktura i sadržaj prikupljenih baza podataka je obrađena u sljedećem potpoglavlju.

4.2.2. Analiza podataka aplikacije Messenger Lite

Kao i u slučaju aplikacije *Instagram* grafički prikaz *SQLite3* baze podataka generiran je korištenjem programskog alata *DbVisualizer*. Na grafikonu 2. prikazana je shema baze podataka sustava "*core.db*" aplikacije *Messenger Lite*. Ova baza je znatno složenija i njoj se nalazi znatno više tablica u odnosu na bazu podataka unutar koje se pohranjuju podaci sustava za razmjenu poruka aplikacije društvene mreže *Instagram*. Jedan od razloga tomu je to što unutar "*core.db*" ne postoje polja u koje je unesen *JSON* zapis s detaljnim opisom poruke nego je za svaki podatak korišten zaseban stupac, [43].

Grafikon 2. *Struktura baze podataka "core.db" dobivena korištenjem alata DbVisualizer*

Tablica *threads* sadrži stupce kao što su identifikator *thread_key,* ime razgovora *thread_name,* sadržaj posljednje poruke u razgovoru unutar stupca *last_message* te vremensku oznaku posljednje poruke u razgovoru. Vremenske

oznake u ovoj bazi su kao i u "*core.db"* izražene u *Unix Epoch* vremenu samo što su za razliku od mikrosekunda koje su korištene u aplikaciji *Instagram* ovdje kao mjerna jedinica vremenskog zapisa korištene milisekunde, odnosno trinaesteroznamenkasti brojevni zapis, [45].

Unutar tablice *contact* zapisani su pojedini detalji o svim korisnicima s kojima je korisnik kontaktirao koristeći sustav za razmjenu poruka društvene mreže *Facebook* s tim da su unutar retka s identifikatorom *_id* s vrijednosti 1 zapisani podaci o samom korisniku koji je prijavljen na *Messenger Lite* aplikaciju analiziranog uređaja. Bitni stupci iz ove tablice za provedbu forenzičke analize u svrhu ovog diplomskog rada su *contact_user_id* koji se referira na *user_id* unutar drugih tablica, kao što je tablica *messages*, te *name* stupac koji sadrži ima korisnika.

Kao što je i u prethodnom potpoglavlju bio slučaj, najsadržajnija tablica unutar baze "*core.db*" sa stajališta forenzičke analize je tablica *messages*. Unutar ove tablice su pohranjene najbitnije informacije koje je potrebno prikazati kod forenzičke analize bilo kakvog sustava razmjene poruka. Ti podaci uključuju identitete pošiljatelja i primatelja, odnosno sudionika razgovora, sadržaj poruka i vremenske oznake istih poruka. Unutar ove tablice se nalazi stupac *thread_key* koji se referira na stupac s istim nazivom unutar tablice *threads* te stupac *user_id* koji predstavlja identifikator korisnika koji je generirao poruku te ste vrijednosti toga stupca referiraju na vrijednosti unutar *contact_user_id* stupac tablice *contact*.

U stupac *timestamp* je kao zapisana vremenska oznaka trenutka u kojemu je poruka poslana te je zapisana u *Unix Epoch* milisekundama. Sami tekst poruke poslane korištenjem aplikacije *Messenger Lite* se pohranjuje unutar stupca *snippet,* kao što je prikazano na slici 25. Osim toga unutar ove tablice postoje stupci message_id gdje se pohranjuje jedinstveni identifikator pojedine poruke te *profile_image_url* gdje je pohranjen *URL* profilne slike pošiljatelja poruke.

_id	thread_key	message_id	user_id
1	ONE_TO_ONE:100028142775274	ONE_TO_ONE:100028142775274:PLACEHOLDER	100028142775274
4	ONE_TO_ONE:100028096518105	mid.$cAAAAAAbD_DNrqOQLH1ld57AVw8zg	100028142775274
5	ONE_TO_ONE:100028096518105	mid.$cAAAAAAbD_DNrqOROUVld58OmafDY	100028096518105
6	ONE_TO_ONE:100028096518105	mid.$cAAAAAAbD_DNrqOTjaFld5-XRPz37	100028142775274
7	ONE_TO_ONE:100028096518105	mid.$cAAAAAAbD_DNrqOUc5Fld5_dGbeBI	100028096518105
8	ONE_TO_ONE:100028096518105	mid.$cAAAAAAbD_DNrqOVAflld6AA8ROIB	100028096518105

profile_image_url	timestamp	snippet
https://scontent.xx.fbc...	1535310185219	New conversation
https://scontent.xx.fbc...	1535310218015	Bok Josipe! Sta radis?
https://scontent.xx.fbc...	1535310235217	Bok Ivane! Ispunjavam prijavu za posao.
https://scontent.xx.fbc...	1535310273384	Jesi li zavrsio sa skolovanjem?
https://scontent.xx.fbc...	1535310288100	Ne.
https://scontent.xx.fbc...	1535310297214	Ostao mi je jos jedan semestar, ali bilo bi dobro da već nadjem posao.

Slika 25. *Sadržaj tablice messages baze podataka "core.db"*

Iz priloženog je vidljivo da svi potrebni podaci koji definiraju jednu tekstualnu poruku, a to su pošiljatelj, primatelj, vremenska oznaka i sadržaj poruke, se nalaze unutar tablica u bazi podataka “*core.db*”. Pomoću tih podataka moguće je rekonstruirati razgovore obavljene korištenjem aplikacije *Messenger Lite,* što je tema sljedećeg poglavlja.

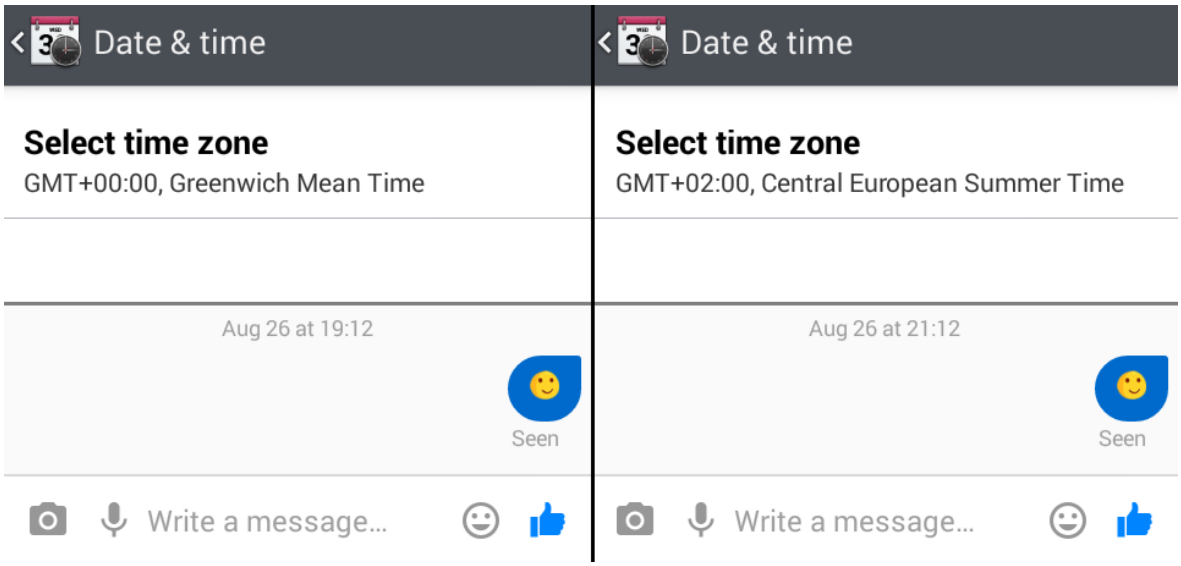
5. OBRADA I PRIKAZ SARŽAJA PRIKUPLJENOG FORENZIČKOM ANALIZOM

Kako bi se faza prezentacije provedbe forenzičke analize mobilnog terminalnog uređaja prema referentnoj metodologiji proveo što jednostavnije, odnosno kako bi se u fazi prezentacije što jasnije prikazao sadržaj samih dokaza potrebno ih je dostaviti u lako razumljivom obliku. Same baze podataka će neupućenim osobama biti nejasne iako se iz njihovog sadržaja jasno vidi da se radi o porukama koje su slane ili primane. Osim toga, vremenske oznake su zapisane u ljudima nerazumljivom obliku i potrebno ih je pretvoriti u svima čitljiv oblik.

Skripta koja radi parsiranje sadržaja baza podataka *"core.db"* i *"direct.db"* napisana je u programskom jeziku *Python*. Ta skripta služi kako bi se generirao sadržaj sustava za razmjenu poruka aplikacija društvenih mreža *Instagram* i *Facebook* u prezentnom i čovjeku lako čitljivom obliku u usporedbi na sadržaj koji je dostupan pregledom baze iz programskog alata *Sqliteman* i *DbVisualizer*. *Python* je skriptni programski jezik visoke razine, koji je interpretiran, interaktivan i objektno orijentiran. Dizajniran je tako da ga je jako lako čitati. Često se koriste ključne riječi na engleskome jeziku gdje drugi programski jezici koriste interpunkciju te zahtjeva manji broj sintaksnih konstrukcija, [56].

Pri izvedbi ove skripte korišteni su moduli *sqlite3*, *time* i *JSON* koji redom omogućavaju rad sa *SQLite3* bazama podataka unutar *Python*-a, generiranje vremena i rad s vremenom te rad s *JSON* objektima, [57]. Dodatne korištene programske biblioteke koje je potrebno preuzeti su *pandas* i *fpdf*. Moduli koje sadrži biblioteka *pandas* pružaju alate za strukturiranje i analizu podataka. U ovome primjeru *pandas* moduli su korišteni za pretvaranje *Unix Epoch* vremenskih oznaka u lako čitljiv oblik. Programska biblioteke *fpdf*, odnosno *PyFPDF* omogućuje generiranje *PDF* dokumenata u *Python* programskom jeziku, [58], [59].

Razlog korištenja *UTC* vremena, odnosno univerzalnog vremena, je zato što se svi vremenski zapisi u bazama podataka aplikacija pohranjuju u tom obliku, a vremenske oznake prikazane unutar aplikacije se računaju korištenjem postavki vremenske zone. To znači da u slučaju promjene same vremenske zone na uređaju promijenit će se prikazano vrijeme, ali će vrijeme unutar baze ostati jednako, kako je prikazano na slici 26, [60].



***Slika 26**. Prikaz povezanosti postavki vremenske zone i prikazane vremenske oznake unutar aplikacije*

Na početku skripte se uvoze potrebni moduli te se otvara tekstualni dokument koji u nazivu sadrži "*ig_izlaz*" i vremensku oznaku trenutka izvršavanja pisanu prema *ISO* 8601 standardu, kao što je prikazano na slici 27. Nakon toga se spaja na bazu podataka i deklariraju se kursori koji će vršiti *SQL* upite nad istom bazom podataka. U tekstualni dokument se upisuje zaglavlje stranice koje sadrži naslov, vrijeme obrade te korisničko ime vezano za navedenu bazu podataka uključujući prije spomenute *username* i *full_name*, [61].

```
## Učitavanje potrebnih modula
import sqlite3
import json
import pandas
import time
from fpdf import FPDF
## Dohvaćanje vremena
vrijeme=time.time()
fnvrijeme=time.strftime('%Y-%m-%dT%H%M%S', time.gmtime())
## Otvaranje tekstualne datoteke
file=open("ig_izlaz_"+fnvrijeme+"Z.txt","w")
## Spajanje na bazu i deklariranje cursora
conn=sqlite3.connect('direct.db')
c=conn.cursor()
c1=conn.cursor()
c2=conn.cursor()
c3=conn.cursor()
c4=conn.cursor()
c5=conn.cursor()
## Upisivanje zaglavlja
file.write("-"*47+"\n")
file.write("Ispis razgovora putem aplikacije Instagram"+"\n")
result_s=pandas.to_datetime(int(vrijeme),unit='s')
file.write("Datum i vrijeme obrade: "+str(result_s)[:19]+" UTC"+"\n")
file.write("Vremenska zona svih vremenskih oznaka je UTC."+"\n")
## Dohvaćanje imena prijavljenog korisnika unutar aplikacije
c5.execute("SELECT message FROM messages where client_item_id IS NOT Null"+"\n")
nime=json.loads(c5.fetchone()[0])
unime=nime['user']
vlasnik=(str(unime['username'])+"("+(str(unime['full_name']))+")")
file.write("Korisnicko ime vlasnika uredjaja: "+vlasnik+"\n")
file.write("-"*47+"\n")
## Upiti za identifikator razgovora i ukupan broj razgovora
c.execute("SELECT count(thread_id) FROM threads")
c1.execute("SELECT thread_id FROM threads")
```

***Slika 27**. Prvi dio skripte "igizl.py"*

Prva petlja prebrojava broj razgovora odnosno *thread*-ova iz tablice *threads* te u tekstualnu datoteku upisuje korisnika s kojim je razgovor obavljen. Druga ugniježđena petlja pretvara poruke iz tablice *messages* u čovjeku lako čitljiv oblik zajedno s vremenskom oznakama formatiranim korištenjem modula *pandas* i korisničkim imenima kao što je prikazano na slici 28.

```
## Definiranje uvjeta za petlju razgovora i ulazak u istu
m=c.fetchone()[0]
i=0
while i<m :
    i+=1
    t=c1.fetchone()
    ## Upiti za dohvaćanje svih poruka i vremenskih oznaka koje pripadaju
    ## istome razgovoru
    c2.execute("SELECT message FROM messages WHERE thread_id=?", t)
    c3.execute("SELECT count(text) FROM messages WHERE thread_id=?", t)
    c4.execute("SELECT thread_info FROM threads WHERE thread_id=?", t)
    z=c3.fetchone()[0]
    o=0
    file.write(' '+"\n")
    file.write("-"*47+"\n")
    razgovor=json.loads(c4.fetchone()[0])
    razrec=razgovor['recipients'][0]
    rec=(str(razrec['username'])+"("+str(razrec['full_name'])+")")
    ## Upisivanje imena drugog sudionika razgovora
    file.write(str(i)+". Razgovor sa "+rec+"\n")
    ## Petlja za poruke unutar istoga razgovora
    while o<z:
        a=json.loads(c2.fetchone()[0])
        u=a['user']
        ime=(str(u['username'])+"("+(str(u['full_name']))+"): ")
        timeu=a['timestamp']
        time=(str(pandas.to_datetime(timeu,unit='us'))[:19]+" ")
        text=str(a['text'])
        ## Upisivanje vremenske oznake, imena pošiljatelja i sadržaja poruke
        file.write(time+ime+text+"\n")
        o+=1
    file.write("-"*47+"\n")
file.close()
```

Slika 28. *Drugi dio skripte "igizl.py"*

Na posljetku se taj tekstualni dokument pretvara u *PDF* datoteku korištenjem mogućnosti *fpdf* modula koja se generira u istu mapu sa skriptom i bazom podataka kao što je prikazano na slici 29.

```
## Generiranje PDF datoteke
stra = open("ig_izlaz_"+fnvrijeme+"Z.txt", 'r').readlines()
pdf = FPDF()
pdf.add_page()
pdf.set_font('Arial', '', 10)
i2=0
m2=len(stra)
while i2<m2:
    stra[i2]=stra[i2].replace('č', 'c')
    stra[i2]=stra[i2].replace('Č', 'C')
    stra[i2]=stra[i2].replace('ć', 'c')
    stra[i2]=stra[i2].replace('Ć', 'C')
    stra[i2]=stra[i2].replace('š', 's')
    stra[i2]=stra[i2].replace('Š', 'S')
    stra[i2]=stra[i2].replace('đ', 'd')
    stra[i2]=stra[i2].replace('Đ', 'D')
    stra[i2]=stra[i2].replace('ž', 'z')
    stra[i2]=stra[i2].replace('Ž', 'Z')
    stra[i2]=stra[i2].replace('\n', '')
    pdf.cell(40, 5,stra[i2], ln=1)
    i2+=1
pdf.output("ig_izlaz_"+fnvrijeme+"Z.pdf", 'F')
```

Slika 29. *Treći dio skripte "igizl.py"*

Izgled sadržaja izvještaja generiranog pokretanjem *Python* skripte "*igizl.py*" prikazan je na slici 30.

Slika 30. *Sadržaj generiranog izvještaja "ig_izlaz_2018-09-01T110252Z.pdf"*

Na sličan način kao skripta koja generira izvještaj o sadržaju sustava za razmjenu poruka aplikacije *Instagram* radi i skripta koja sa spaja na bazu podataka *"core.db"* koju koristi *Messenger Lite* te iz nje generira izvještaj u obliku *PDF* datoteke. Kod same skripte s upisanim komentarima prikazan je na slikama 31, 32 i 33.

```
## Učitavanje potrebnih modula
import sqlite3
import pandas
import time
from fpdf import FPDF
## Dohvaćanje vremena
vrijeme=int(time.time())
fnvrijeme=time.strftime('%Y-%m-%dT%H%M%S', time.gmtime())
## Otvaranje tekstualne datoteke
file=open("fb_izlaz_"+fnvrijeme+"Z.txt","w")
## Upisivanje zaglavlja
file.write("-"*47+"\n")
file.write("Ispis razgovora putem aplikacije Messanger Lite"+"\n")
result_s=pandas.to_datetime(int(vrijeme),unit='s')
file.write("Datum i vrijeme obrade: "+str(result_s)[:19]+" UTC"+"\n")
file.write("Vremenska zona svih vremenskih oznaka je UTC."+"\n")
```

***Slika 31**. Prvi dio skripte "fbizl.py"*

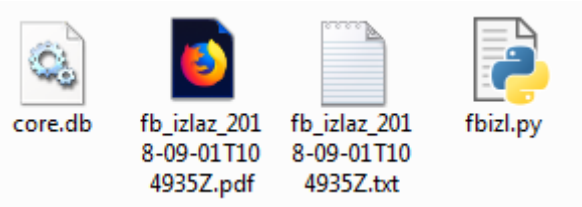
```
## Spajanje na bazu i deklariranje cursora
conn =sqlite3.connect('core.db')
c=conn.cursor()
c1=conn.cursor()
c2=conn.cursor()
c3=conn.cursor()
c4=conn.cursor()
c5=conn.cursor()
c6=conn.cursor()
c7=conn.cursor()
c8=conn.cursor()
## Dohvaćanje imena prijavljenog korisnika unutar aplikacije
c8.execute("SELECT name FROM contact WHERE _id IS 1")
vlasnik=str(c8.fetchone()[0])
file.write("Korisnicko ime vlasnika uredjaja: "+vlasnik+"\n")
file.write("-"*47+"\n")
## Upiti za identifikator razgovora i ukupan broj razgovora
c.execute("SELECT thread_key FROM threads WHERE _id IS NOT 1")
c1.execute("SELECT count(thread_key) FROM threads WHERE _id IS NOT 1")
## Definiranje uvjeta za petlju razgovora i ulazak u istu
i=0
m=c1.fetchone()[0]
while i<m:
    tk=c.fetchone()
    i+=1
    ## Upiti za dohvaćanje svih poruka i vremenskih oznaka koje pripadaju
    ## istome razgovoru
    c2.execute("SELECT snippet FROM messages WHERE thread_key=?", tk)
    c3.execute("SELECT count(snippet) FROM messages WHERE thread_key=?", tk)
    c4.execute("SELECT timestamp FROM messages WHERE thread_key=?", tk)
    c5.execute("SELECT thread_name FROM threads WHERE thread_key=?", tk)
    c6.execute("SELECT user_id FROM messages WHERE thread_key=?", tk)
    z=c3.fetchone()[0]
    o=0
    file.write(' '+"\n")
    file.write("-"*47+"\n")
    ## Upisivanje imena drugog sudionika razgovora
    file.write(str(i)+". Razgovor sa "+str(c5.fetchone()[0])+"\n")
    ## Petlja za poruke unutar istoga razgovora
    while o<z:
        o+=1
        vo=c4.fetchone()[0]
        vrijeme=(str(pandas.to_datetime(int(vo),unit='ms'))[:19])
        ui=c6.fetchone()
        c7.execute("SELECT name FROM contact WHERE contact_user_id=?", ui)
        ime=str(c7.fetchone()[0])
        poruka=str(c2.fetchone()[0])
        ## Upisivanje vremenske oznake, imena pošiljatelja i sadržaja poruke
        file.write(vrijeme+" "+ime+": "+poruka+"\n")
    file.write("-"*47+"\n")
```

***Slika 32**. Drugi dio skripte "fbizl.py"*

```
file.close()
time.sleep(1)
## Generiranje PDF datoteke
stra = open("fb_izlaz_"+fnvrijeme+"Z.txt", 'r').readlines()
pdf = FPDF()
pdf.add_page()
pdf.set_font('Arial', '', 10)
i2=0
m2=len(stra)
while i2<m2:
    stra[i2]=stra[i2].replace('č', 'c')
    stra[i2]=stra[i2].replace('Č', 'C')
    stra[i2]=stra[i2].replace('ć', 'c')
    stra[i2]=stra[i2].replace('Ć', 'C')
    stra[i2]=stra[i2].replace('š', 's')
    stra[i2]=stra[i2].replace('Š', 'S')
    stra[i2]=stra[i2].replace('đ', 'd')
    stra[i2]=stra[i2].replace('Đ', 'D')
    stra[i2]=stra[i2].replace('ž', 'z')
    stra[i2]=stra[i2].replace('Ž', 'Z')
    stra[i2]=stra[i2].replace('\n', '')
    pdf.cell(40, 5,stra[i2], ln=1)
    i2+=1
pdf.output("fb_izlaz_"+fnvrijeme+"Z.pdf", 'F')
```

***Slika 33**. Treći dio skripte "fbizl.py"*

Pokretanje skripte *"fbizl.py"* s dostupnom bazom podataka "*core.db*" generira izvještaje u tekstualnom obliku kao *.txt* datoteku i *PDF* datoteku kao što je prikazano na slici 34.



***Slika 34**. Generirane datoteke*

Format generirane *PDF* datoteke je sličan onome kojeg generira prethodna skripta te je sadržaj te datoteke prikazan na slici 35.

Ispis razgovora putem aplikacije Messanger Lite
Datum i vrijeme obrade: 2018-09-01 10:49:35 UTC
Vremenska zona svih vremenskih oznaka je UTC.
Korisnicko ime vlasnika uredjaja: Ivan Ivic

---
1. Razgovor sa Josip Josipovic
2018-08-26 19:03:38 Ivan Ivic: Bok Josipe! Sta radis?
2018-08-26 19:03:55 Josip Josipovic: Bok Ivane! Ispunjavam prijavu za posao.
2018-08-26 19:04:33 Ivan Ivic: Jesi li zavrsio sa skolovanjem?
2018-08-26 19:04:48 Josip Josipovic: Ne.
2018-08-26 19:04:57 Josip Josipovic: Ostao mi je jos jedan semestar, ali bilo bi dobro da vec nadjem posao.

---
2. Razgovor sa Luka Lukic
2018-08-26 19:10:46 Luka Lukic: Gdje ides sada?
2018-08-26 19:11:05 Ivan Ivic: Idem u banku.
2018-08-26 19:11:20 Luka Lukic: Zar ne bi trebao biti na poslu?
2018-08-26 19:11:50 Ivan Ivic: Radim trenutno. Polazem novac za tvrtku.
2018-08-26 19:12:05 Luka Lukic: Gdje radis?
2018-08-26 19:12:24 Ivan Ivic: U restoranu kao voditelj.
2018-08-26 19:12:38 Luka Lukic: Zvuci sjajno!
2018-08-26 19:12:49 Ivan Ivic: Da.
2018-08-26 19:12:57 Ivan Ivic: (:

***Slika 35**. Sadržaj generiranog izvještaja "fb_izlaz_2018-09-01T104935Z.pdf"*

6. ZAKLJUČAK

U ovom diplomskom radu naslovljenom *Ekstrakcija podataka sustava za razmjenu poruka društvenih mreža u svrhu forenzičke analize* obrađena je tema forenzike i digitalne forenzike te uže grane digitalne forenzike u obliku forenzičke analize mobilnih terminalnih uređaja. Prikazana je referentna metodologija koja se koristi pri provođenju forenzičke analize mobilnih terminalnih uređaja i postupci ekstrakcije podataka s kojima se dolazi do sadržaja koji obradom postaje digitalni dokaz. Korištenjem raznih alata na više platformi obrađen je sadržaj unutarnje pohrane mobilnog terminalnog uređaja. Opisani su trendovi koji prate društvene mreže, komunikaciju putem istih i dokazi koji su dostupni na različitim društvenim mrežama. Detaljno su obrađene dvije aplikacije društvenih mreža namijenjene *Android* operativnom sustavu te je detaljno istražen način na koji njihov sustav za razmjenu poruka pohranjuje podatke na memoriju mobilnog terminalnog uređaja. Korištenjem spoznaja o bazama podataka koje se nalaze na samom uređaju na koje te iste aplikacije lokalno pohranjuju sadržaj sustava za razmjenu podataka uspješno je rekonstruiran razgovor koji se vodio putem društvene mreže.

U ovom diplomskom radu je prikazano kako korištenjem programskih paketa i forenzičkih alata otvorenog koda doći do digitalnih dokaza koji se nalaze u sustavima za razmjenu podataka aplikacija društvenih mreža za pametne mobilne terminalne uređaje s *Android* operativnim sustavom. Nakon provedene ekstrakcije podataka na različite načine uspješnost istih je potvrđena validacijom usporedbom *hash* vrijednosti i samog sadržaja. Analizirana je struktura i sadržaj baza podataka aplikacija *Instagram* i *Messenger Lite* te su u njima prepoznati identifikatori, vremenske oznake te sam sadržaj poruka. Korištenjem tih spoznaja napisana je skripta u programskom jeziku *Python* koja iz podataka prikupljenih forenzičkom analizom generira ispis koji sadrži rekonstruirane razgovore zajedno s imenima sudionika, vremenskim oznakama poruka i sadržajem istih. Za pretpostaviti je da se saznanja prikupljena tijekom proučavanja ovih dviju aplikacija mogu prenijeti i na druge aplikacije koje sadrže sustav za razmjenu poruka koji podatke ili barem dio njih pohranjuje na memoriju uređaja. Kod takvih aplikacija, korištenjem sličnih metoda kao u slučaju s dvije aplikacije obrađene u ovom diplomskom radu, moguće je izvršiti rekonstrukciju razgovora obavljenih putem njih.

LITERATURA

[1] Prahlow JA. Forensic Pathology for Police, Death Investigators, Attorneys, and Forensic Scientists. SAD: Springer; 2010.

[2] US-CERT. Computer Forensic, SAD, 2008.

[3] Gogolin G. Digital Forensic Explained. SAD: CRC Press; 2013.

[4] Cybersecurity Nexus. Overview of Digital Forensics, SAD: ISACA; 2015.

[5] Marcella AJ, Menendez D. Cyber Forensics. SAD: Auerbach Publications; 2008.

[6] Vojković G, Štambuk-Sunić M. Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske. Zbornik radova Pravnog fakulteta u Splitu. 2006;43(1): 123-136.

[7] Sadiku MNO, Tembely M, Musa SM. Digital Forensics. International Journal of Advanced Research in Computer Science and Software Engineering. 2017;7(4): 274-276.

[8] Khanuja HK, Adane DS. A Framework for Database Forensic. Computer Science & Engineering: An International Journal. 2012;2(3): 27-41.

[9] Murphy CA. Developing Process for Mobile Device Forensics, SAD, 2013.

[10] The Royal Society. Forensic DNA Analysis: primer for courts, UK, 2017.

[11] Barton T, Hannan Bin Azhar MA. Forensic Analysis of the Recovery of Wickr's Ephemeral Data on Android Platforms, CYBER 2016 : The First International Conference on Cyber-Technologies and Cyber-Systems, Italija, 2016.

[12] BusyBox. Preuzeto sa: https://busybox.net/ [Pristupljeno: lipanj 2018.]

[13] Santoku Linux. Preuzeto sa: https://santoku-linux.com/ [Pristupljeno: lipanj 2018.]

[14] Android Debug Bridge. Preuzeto sa: https://developer.android.com/studio/command-line/adb.html [Pristupljeno: lipanj 2018.]

[15] Red Hat. Red Hat Enterprise Linux 6: Deployment Guide, SAD, 2017.

[16] SanDisk. MultiMediaCard Product Manual, SAD, 2003.

[17] Kingston Technology. Embedded Multimedia Card, Tajvan, 2014.

[18] Live imaging an Android device. Preuzeto sa: http://freeandroidforensics.blogspot.ba/2014/08/live-imaging-android-device.html [Pristupljeno: lipanj 2018.]

[19] Vandeven S. Forensic Images: For Your Viewing Pleasure. SAD: The SANS Institute; 2014.

[20] Keffer J. Autopsy Forensic Browser User Guide, Kanada, 2013.

[21] Texting Is In Decline. http://uk.businessinsider.com/whatsapp-vs-texting-statistics-2015-1 [Pristupljeno: lipanj 2018.]

[22] SMS vs IM. Preuzeto sa: https://smswarriors.com/sms-vs-im/ [Pristupljeno: lipanj 2018.]

[23] Wonk K, Lai ACT, Yeung JCK, Lee WL, Chan PH. Facebook Forensics. Hong Kong: Valkyrie-X Security Research Group; 2011.

[24] Yusoff MN, Dehghantanha A, Mahmod R. Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp and Line as Case Studies, Contemporary Digital Forensic Investigations Of Cloud And Mobile Applications, SAD, 2017.

[25] Walnycky D, Baggili I, Marrington A, Moore J, Breitinger F. Network and device forensic analysis of Android social.messaging applications. Digital Investigation. 2015;14(1): 77-84.

[26] Bair J. Seeking Truth from Mobile Evidence. UK: Academic Press; 2018.

[27] Instagram - Apps on Google Play. Preuzeto sa: https://play.google.com/store /apps/details?id=com.instagram.android [Pristupljeno: lipanj 2018.]

[28] 4imprint. Instagram Blue Paper, SAD, 2014.

[29] Herman J. The Ultimate Begginer's Guide to Instagram, USA, 2014.

[30] Instagram 49.0.0.15.89 APK. Preuzeto sa: https://www.apkmirror.com/apk /instagram/instagram-instagram/instagram-instagram-49-0-0-15-89-113249-release/ [Pristupljeno: lipanj 2018.]

[31] How is your day - Example Conversation. Preuzeto sa: https://www.talkenglish.com/lessondetails.aspx?ALID=529 [Pristupljeno: kolovoz 2018.]

[32] How is your day - Interactive Practice . Preuzeto sa: https://www.talkenglish.com/lessonpractice.aspx?ALID=553 [Pristupljeno: kolovoz 2018]

[33] Set the application ID. Preuzeto sa: https://developer.android.com/studio/build /application-id [Pristupljeno: lipanj 2018.]

[34] Chandrakumar FJ. An evidence-based Android cache forensics model, Australija, 2014.

[35] Levin J. Android Internals: A Confectioner's Cookbook. SAD: Technologeeks; 2015.

[36] Google. Android Security White Paper, SAD, 2016.

[37] Directory Permission 751 for Mac Linux and Unix. Preuzeto sa: http://www.filepermissions.com/directory-permission/751 [Pristupljeno: srpanj 2018.]

[38] DB File Extension. Preuzeto sa: https://fileinfo.com/extension/db [Pristupljeno: srpanj 2018.]

[39] Manger R. Baze podataka – skripta, Prirodoslovno-matematički fakultet, Zagreb, 2003.

[40] Android ADB Shell – adb pull. Preuzeto sa: http://adbshell.com/commands/adb-pull [Pristupljeno: srpanj 2018.]

[41] Kumar K, Sofat S, Jain SK, Aggarwal N. Significance of Hash Value Generation in Digital Forensic: A Case Study. International Journal of Engineering Research and Development. 2012;2(5): 64-70.

[42] Cisco. How to Validate the Integrity of Downloaded File, SAD, 2018.

[43] DbVisualizer. Preuzeto sa: https://www.dbvis.com/ [Pristupljeno: srpanj 2018.]

[44] Sqliteman. Preuzeto sa: http://sqliteman.yarpen.cz/ [Pristupljeno: srpanj 2018.]

[45] Matthew N, Stones R. Beginning Linux Programming. SAD: Wiley; 2008.

[46] ECMA: The JSON Data Interchange Syntax, Švicarska, 2017.

[47] JSON Formatter & Validator. Preuzeto sa: https://jsonformatter.curiousconcept.com [Pristupljeno: srpanj 2018.]

[48] Facebook - Apps on Google Play. Preuzeto sa: https://play.google.com/store/apps/details?id=com.facebook.katana [Pristupljeno: kolovoz 2018.]

[49] Facebook Lite - Apps on Google Play. Preuzeto sa: https://play.google.com/store/apps/details?id=com.facebook.lite [Pristupljeno: kolovoz 2018.]

[50] Messenger - Apps on Google Play. Preuzeto sa: https://play.google.com/store/apps/details?id=com.facebook.orca [Pristupljeno: kolovoz 2018]

[51] Messenger Lite - Apps on Google Play. Preuzeto sa: https://play.google.com/store/apps/details?id=com.facebook.mlite [Pristupljeno: kolovoz 2018.]

[52] Croft C. A Brief History of The Facebook, Kanada, 2008.

[53] Facebook Chat Launches, For Some. Preuzeto sa: https://techcrunch.com/2008/04/06/facebook-chat-enters-pre-release-beta/ [Pristupljeno: kolovoz 2018.]

[54] Facebook Launches Standalone iPhone/Android Messenger App. Preuzeto sa: https://techcrunch.com/2011/08/09/facebook-launches-standalone-mobile-messenger-app-and-it's-beluga/ [Pristupljeno: kolovoz 2018.]

[55] Messenger Lite 35.1.0.18.192 APK. Preuzeto sa: https://mobile.softpedia.com /apk/messenger-lite/35.1.0.18.192/ [Pristupljeno: kolovoz 2018.]

[56] Tutorials Point. Python Programming Language, Indija, 2014.

[57] Ivić S, Crnković B, Škifić J, Čavrak M. Python u računarskom inženjerstvu, Tehnički fakultet, Rijeka, 2015.

[58] pandas: Python Data Analysis Library. Preuzeto sa: https://pandas.pydata.org/ [Pristupljeno: kolovoz 2018.]

[59] PyFPDF. Preuzeto sa: https://pypi.org/project/fpdf/ [Pristupljeno: kolovoz 2018.]

[60] TimeZone. Preuzeto sa: https://developer.android.com/reference/java/util /TimeZone [Pristupljeno: kolovoz 2018.]

[61] International Standard Organization. ISO/WD 8601 - Data elements and interchange formats, Švicarska, 2016.

POPIS KRATICA

SMS – Short Message Service

DNK – deoksiribonukleinska kiselina, nositelj genetičke informacije

GB – *gigabyte*

OS – operativni sustav

USB – Universal Serial Bus

mmc, MMC – Multi Media Card

eMMC – Embedded Multi Media Card

TCP – Transfer Control Protocol

UDP – User Datagram Protocol

TCP/IP - IP grupa protokola

nc - netcat

IG – Instagram

ID – identity

UID – user identity

MD5 – message-digest algorithm

SHA-1 – Secure Hash Algorithm 1

URL – Uniform Resource Locator

UTC – Coordinated Universal time

JSON – JavaScript Object Notation

PDF – Portable Document Format

ISO – International Standard Organization

SQL – Structured Query Language

POPIS SLIKA

POPIS GRAFIKONA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom **Ekstrakcija podataka sustava za razmjenu poruka društvenih mreža u svrhu forenzičke analize**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 14.9.2018

Student/ica:
Zvonimir Bošnjak
(potpis)