Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.633
DOI: https://doi.org/10.24867/32BE23Gasic

DIGITALNA FORENZIKA DRUŠTVENIH MREŽA

DIGITAL FORENSICS OF SOCIAL NETWORKS

Nikolina Gašić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U ovom radu je istražen proces digitalne forenzike društvenih mreža, sa fokusom na pregled tehnika i alata za prikupljanje, pregledanje i analizu digitalnih dokaza. Primena forenzičkih tehnika i alata prikazana je na praktičnom primeru istrage na društvenim mrežama kroz studiju slučaja.*

Ključne reči: *forenzika, digitalna forenzika, društvene mreže*

Abstract – *This paper explores the process of digital forensics of social networks, with a focus on reviewing the techniques and tools for collecting, examining, and analyzing digital evidence. The application of these forensic techniques and tools is demonstrated through a practical example of an investigation on social networks through a case study.*

Keywords: *forensics, digital forensics, social networks*

1. UVOD

Razvoj tehnologije i sve veća dostupnost interneta, doveli su do vrtoglavog porasta broja društvenih mreža, kao i njihovih korisnika. Služeći kao sredstvo komunikacije, razmene informacija i zabave, danas su društvene mreže postale sastavni deo svakodnevnog života miliona ljudi širom sveta. Međutim, uporedo sa njihovim rastom, dolazi i do porasta kriminalnih aktivnosti koje se odvijaju na ovim platformama. Digitalna forenzika i digitalni forenzičari igraju sve važniju ulogu u analiziranju i otkrivanju ovih zločina.

Digitalna forenzika ili digitalna forenzička nauka je grana forenzičke nauke koja se fokusira na pronalaženje i pregledanje materijala pronađenog na digitalnim uređajima [1]. Digitalna forenzika obuhvata više celina, a to su: identifikacija, prikupljanje, čuvanje, pregledanje, analiza i prezentacija digitalnih dokaza korišćenjem naučno i pravno valjanih metoda i alata [2]. Faza identifikacije predstavlja početak istrage i uključuje identifikaciju svih mogućih izvora digitalnih dokaza. U fazi prikupljanja forenzičar dobija pristup digitalnom uređaju koji sadrži neobrađene podatke koji su identifikovani kao relevantni za slučaj. Podaci se prikupljaju sa digitalnih uređaja pravljenjem digitalne kopije, korišćenjem forenzički valjanih metoda i alata, tako da se ne kompromituju originalni podaci. Faza čuvanja se odnosi na čuvanje prikupljenih podataka primenom forenzički valjanih metoda i alata. Faza pregledanja obuhvata pripremu i ekstrakciju potencijalnog digitalnog dokaza iz prikupljenih izvora podataka [2]. Tokom ove faze sirovi podaci se obrađuju u format koji se može analizirati. Faza analize je suština procesa digitalne forenzike. U ovoj fazi, forenzičari koriste specijalizovane alate i tehnike kako bi detaljno ispitali pripremljene podatke i izvukli relevantne informacije. Poslednja faza je faza prezentacije, odnosno deljenje informacija koje su otkrivene forenzičkom istragom, što uključuje pisanje sveobuhvatnog izveštaja i prezentaciju dokaza na sudu. Sve faze moraju da budu u skladu sa standardnim forenzičkim procedurama kako bi dokazi bili forenzički validni na sudu.

2. DRUŠTVENE MREŽE

Društvene mreže su digitalne platforme koje omogućavaju povezivanje ljudi preko interneta deljenjem raznih tekstualnih ili multimedijalnih sadržaja. One omogućavaju ljudima da kreiraju svoj onlajn identitet, da komuniciraju sa prijateljima, porodicom ili strancima i dele svoja mišljenja i informacije sa bilo koje lokacije na kojoj se nalaze. Fejsbuk (Facebook), Vocap (WhatsApp) i Instagram su platforme koje se nalaze na prvom, trećem i četvrtom mestu liste najpopularnijih društvenih mreža po podacima iz avgusta 2024. godine [3]. Zbog svoje dominantne pozicije i velikog broja korisnika, kao i činjenice da su sve tri platforme deo Meta Platforms Inc. kompanije, ove tri društvene mreže predstavljaju idealan predmet istraživanja za ovaj rad. Sve tri platforme su besplatne aplikacije koje omogućavaju olakšanu komunikaciju između ljudi. Nažalost, zbog anonimnosti koju ove mreže omogućavaju podložne su za delovanje zlonamernih korisnika. Neke od najčešćih kriminalnih aktivnosti koje se dešavaju na ovim platformama su krađa identiteta, fišing napadi, prevare u vezi sa prodajom i kupovinom i širenje mržnje i lažnih glasina. U borbi protiv sajber kriminala na društvenim mrežama, digitalna forenzika ima ključnu ulogu. Ona pruža alate za efikasnu istragu, može pomoći u hvatanju i kažnjavanju počinilaca i stvaranju bezbednijeg okruženja za sve.

3. TEHNIKE DIGITALNE FORENZIKE DRUŠTVENIH MREŽA

U ovom odeljku su prvo opisane tehnike prikupljanja podataka direktno od provajdera društvenih mreža na osnovu sudskog naloga kao i ekstrakcije iz oblaka. Pošto se društvenim mrežama najčešće pristupa putem aplikacije na mobilnom uređaju ili veb pretraživača na računaru, podaci od interesa se mogu naći i na ovim uređajima, što ih čini potencijalnim izvorom dokaza za forenzičku istragu. Kako bi istraživanje društvenih mreža bilo

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Stevan Gostojić, red. prof.

kompletno u nastavku su opisane i tehnike digitalne forenzike računara, digitalne forenzike mobilnih uređaja i digitalne forenzike računarskih mreža.

3.1. Ekstrakcija podataka dobijenih direktno od provajdera društvenih mreža

Istražitelji mogu zatražiti sudski nalog za dobijanje podataka direktno od provajdera društvenih mreža, odnosno od kompanije Meta Platforms Inc. Kada je reč o dobijanju podataka od američkih internet kompanija poput ove, u krivičnim postupcima u Srbiji, neophodno je pokrenuti postupak međunarodne pravne pomoći. Ovaj proces se obično odvija putem molbe za pravnu pomoć koju nadležni organi u Srbiji upućuju nadležnim organima u Sjedinjenim Američkim Državama. Međutim, postoji i efikasnija procedura, opisana u Obaveštenju Ministarstva spoljnih poslova Republike Srbije [4], koja omogućava brže dobijanje podataka. Meta Platforms Inc. ima jednostavan sistem za slanje onlajn zahteva (Law Enforcement Online Request System), gde se zahtev može podneti isključivo zvaničnom mejl adresom organa reda. Podaci dobijeni na ovaj način mogu uključivati osnovne podatke o nalogu, kao što su korisničko ime, mejl povezan sa nalogom, puno ime korisnika, broj telefona, datum rođenja i datum kreiranja naloga; podatke vidljive javno, kao što su biografija, profilna slika, prijatelji/pratioci, slike i videi podeljeni od strane korisnika, uključujući opise, komentare, lajkove i sve povezane metapodatke; privatne podatke, kao što su privatne poruke, uključujući tekstualne poruke, fotografije, dokumenta, video i audio zapise, informacije o pretrazi korisnika u aplikaciji, IP adrese uređaja koji su se koristili za pristup nalogu, istorija prijavljivanja i pokušaja prijavljivanja, promene lozinke i izmene podešavanja naloga.

3.2. Ekstrakcija iz oblaka

Prikupljanje podataka sa naloga društvenih mreža moguće je ekstrakcijom iz oblaka. Ova tehnika se može obaviti ručno, u aplikaciji na mobilnom uređaju ili preko veb stranice na računaru, ili uz pomoć nekog od forenzičkih alata. Za ovu tehniku je potrebno imati kredencijale za pristup nalogu sa koga se prikupljaju podaci, ili pristup uređaju na kome je instalirana aplikacija sa već ulogovanim nalogom. Ukoliko istražitelji nemaju kredencijale korisničkog naloga od interesa niti pristup uređaju na kome se nalazi aplikacija sa ulogovanim nalogom mogu da ekstrahuju javne podatke iz oblak servera društvenih mreža koristeći neke od forenzičkih alata.

3.3. Digitalna forenzika mobilnih uređaja

Kako se društvene mreže danas uglavnom koriste preko mobilnih uređaja, oni postaju značajan izvor potencijalnih dokaza u forenzičkim istragama. Forenzika mobilnih uređaja je nauka o prikupljanju digitalnih dokaza ili podataka sa mobilnog uređaja pod forenzički ispravnim uslovima koristeći prihvaćene metode [5]. Osnovni načini ekstrakcije, odnosno prikupljanja podataka sa mobilnih uređaja se mogu podeliti u tri kategorije – ručna, logička i fizička ekstrakcija. Ručna ekstrakcija se odnosi na posmatranje i snimanje sadržaja sa ekrana mobilnog uređaja. Ovo je najlakši metod ekstrakcije, ali može zahtevati puno vremena. Logička ekstrakcija se primenjuje uz pomoć rezervnog kopiranja i sinhronizacije uređaja sa računarom. Fizička ekstrakcija omogućava kreiranje bit po bit kopije mobilnog uređaja. Ovom metodom se mogu preuzeti i neki izbrisani podaci. Preuzeti podaci su često u sirovom formatu i nisu čitljivi, pa je potrebno dekodiranje kako bi se podaci pretvorili u razumljiv oblik. Metode fizičke ekstrakcije su hex dump, JTAG, chip-off i mikro čitanje. Za mnoga forenzička istraživanja potrebno je koristiti više različitih kategorija ekstrakcija kako bi se dobili što bolji rezultati.

Dva najzastupljenija operativna sistema koja koriste mobilni uređaji su Android i iOS. Ovi uređaji koriste različite operativne sisteme i različite fajl sisteme koji kreiraju podatke u različitim oblicima i imaju različite mehanizme za zaštitu podataka. Na Android uređajima enkripcija zavisi od verzije i proizvođača, dok iOS koristi snažnu hardversku enkripciju. Sa iOS uređajima ima manje mogućnosti da se dođe do podataka bez lozinke zbog njihovih bezbednosnih mera. Iako se osnovni principi digitalne forenzike primenjuju na obe platforme, postoje značajne razlike u praksi.

3.4. Digitalna forenzika računara

Digitalna forenzika računara je grana digitalne forenzike koja uključuje pronalaženje i analizu digitalnih informacija sa računara i uređaja za skladištenje podataka [6]. Računari mogu igrati ključnu ulogu u prikupljanju podataka sa društvenih mreža.

Forenzika veb pretraživača igra vitalnu ulogu u digitalnoj forenzici računara nudeći dragocene uvide u onlajn aktivnosti korisnika. To uključuje informacije kao što su posećene veb stranice, istorija pretrage, istorija preuzimanja, kolačići, kredencijali za prijavu, obeleživači i instalirane ekstenzije ili dodaci. Ispitivanjem ovih informacija forenzičari mogu razumeti ponašanje, preferencije i interakcije korisnika, pomažući u rekonstrukciji događaja, identifikovanju tragova i utvrđivanju motiva. Neki od najčešće korišćenih veb pretraživača su Google Chrome, Safari, Microsoft Edge i Mozilla Firefox.

3.5. Digitalna forenzika računarskih mreža

Mrežna forenzika, kao podoblast digitalne forenzike, sastoji se od praćenja i analize mrežnog saobraćaja i komunikacija računarskih sistema i uređaja u svrhu prikupljanja dokaza. Slično RAM memoriji, mrežna forenzika se u velikoj meri bavi promenljivim podacima koji su dostupni samo kratak vremenski period [7]. Postoje dve vrste mrežne forenzike – prikupljanje i analiza u realnom vremenu, kao i retroaktivna analiza već prikupljenih podataka. Istražitelji mrežne forenzike koriste analizatore protokola i snifere paketa. Analizator protokola je alat za tumačenje koji obezbeđuje ljudima razumljivo značenje mrežnih protokola. Sniferi paketa se koriste za presretanje podataka koji prolaze kroz bežičnu ili žičanu mrežu. Saobraćaj koji se odvija ka društvenim mrežama kao što su Fejsbuk, Instagram i Vocap je šifrovan, pa ga je teže analizirati. Forenzički alati za mrežni saobraćaj i dalje mogu biti korisni u određenoj meri. Iako se ne može videti sadržaj poruka, može se identifikovati da li je uopšte došlo do komunikacije sa serverima ovih platformi. Može se analizirati učestalost i vreme komunikacije, IP adrese i portovi. Neki alati omogućavaju i identifikaciju operativnih sistema, aplikacija i uređaja koji komuniciraju

sa serverima društvenih mreža. Mrežna forenzika je najefikasnija kada se kombinuje sa drugim forenzičkim tehnikama, kao što su digitalna forenzika računara i digitalna forenzika mobilnih uređaja.

4. ALATI DIGITALNE FORENZIKE DRUŠTVENIH MREŽA

Brz napredak tehnologije i sve veća upotreba računara i mobilnih uređaja doveli su do razvoja forenzičkih alata. S obzirom na stalni razvoj novih modela uređaja i njihovih operativnih sistema, forenzički alati se konstantno unapređuju. Stručnjaci često koriste više alata kako bi uporedili rezultate i osigurali tačnost istrage.

4.1. Alati za ekstrakciju iz oblaka

Pomoću alata poput Magnet AXIOM, Oxygen Forensic Suite i Cellebrite UFED podaci se mogu dobiti direktno sa oblak servera društvenih mreža. Ovi alati imaju slične funkcionalnosti uz male razlike u opcijama i u korisničkom interfejsu. Ukoliko istražitelji imaju kredencijale korisnika Instagram naloga čiji su podaci ključni za istragu, mogu da ekstrahuju sve podatke sa tog naloga. U zavisnosti od potreba, kroz konfiguraciju se može odabrati koja vrsta podataka će biti ekstrahovana (objave, poruke, fotografije, lokacije i drugo). Takođe se može podesiti i vremenski period iz kog će se obaviti ekstrakcija podataka. Ukoliko istražitelji nemaju kredencijale korisničkog naloga od interesa pomoću ovih alata mogu da ekstrahuju i javne podatke iz oblak servera društvenih mreža.

4.2. Alati za digitalnu forenziku mobilnih uređaja

Postoji veliki broj alata koji se koriste za ekstrakciju podataka iz mobilnih uređaja. Vocap podaci mogu biti dostupni na samom mobilnom uređaju u aplikaciji, u starim lokalnim sigurnosnim kopijama ili u oblak servisima Gugla, Ajklauda ili Vocapa. Ukoliko je mobilni uređaj otključan i podaci sa Vocap aplikacije nisu obrisani, poruke se lako mogu ekstrahovati putem nekih od forenzičkih alata kao što je Oxygen Forensic Detective. Ekstrahovanjem lokalnih sigurnosnih kopija možemo videti i poruke koje su u međuvremenu izbrisane iz aplikacije. Za prikupljanje podataka sa Fesjbuk, Instagram i Vocap aplikacija na mobilnom uređaju se može koristiti alat Cellebrite UFED. Potrebno je povezati mobilni uređaj kablom, pokrenuti alat i izabrati redom opcije „Mobile Device“, „File System“ i „Qualcomm Live“. Zatim se bira lokacija za čuvanje fajla sa ekstrahovanim podacima i pokreće ekstrakcija. Za uspešnu ekstrakciju potrebno je ispratiti sva uputstva koja ovaj softver daje, kao što je aktiviranje opcija za developere, USB debagovanja i „Stay awake“ opcije, kao i isključivanje automatskog zaključavanja ekrana. Da bi se ekstrahovali podaci samo iz određenih mobilnih aplikacija bira se opcija „Selective File System“. Ona pruža spisak svih instaliranih aplikacija na mobilnom uređaju i omogućava da se pretraže i izaberu samo određene aplikacije, koje su relevantne za istragu. Kada se završi selekcija aplikacija Fejsbuka, Instagrama ili Vocapa, ekstrakcija se nastavlja klikom na opciju „Extract“.

U nastavku je dat primer ekstrakcije mobilnog uređaja sa iOS operativnim sistemom uz pomoć Cellebrite UFED alata koji koristi checkm8. Cellebrite UFED i checkm8 kombinuju alate zajedno i omogućavaju pristup mobilnom uređaju i kada je oštećen, bez gubljenja vremena za popravku. Mobilni uređaj prvo treba povezati USB kablom za računar na kom je instaliran Cellebrite UFED. Kada se učita, potrebno je u alatu izabrati opciju „Mobile device“ i pretražiti tačan naziv modela povezanog uređaja. Zatim se bira opcija „Advanced Logical“, pa „Full File System (checkm8)“ i upisuje lokacija gde će biti ekstrahovan sadržaj povezanog mobilnog uređaja. Da bi sve bilo spremno za ekstrakciju, sledeći korak je prebacivanje uređaja na DFU mod i pokretanje ekstrakcije klikom na „Continue“. U toku procesa ekstrakcije prikazaće se prozor za upisivanje lozinke uređaja. Ukoliko lozinka nije poznata može se kliknuti na „Cancel“ i ekstrakcija će se svakako nastaviti, ali će biti ekstrahovani samo podaci koji nisu zaštićeni lozinkom.

Nakon uspešne ekstrakcije podataka sa mobilnih uređaja, pristupa se ključnim fazama forenzičke istrage, a to je pregledanje i analiza podataka. U ovim fazama, prikupljeni podaci se pažljivo ispituju i tumače kako bi se izdvojili relevantni podaci i došlo do zaključaka bitnih za istragu. Primer alata za pregledanje i analizu je UFED Physical Analyser. Sekcija „Home“ prikazuje podatke o uređaju sa koga su preuzeti podaci i neke opšte informacije o ekstrakciji, dok sekcija „Analyzed data“ sadrži detaljan prikaz ekstrahovanih podataka. Podaci su organizovani u stablu sa leve strane. Grupisani su u kategorije, radi lakšeg pregleda i pristupa, u kojima se nalaze specifični tipovi podataka izvučeni sa mobilnog uređaja. Sa desne strane se nalazi deo gde se može videti više detalja o izabranom podatku.

Još jedan koristan alat za analizu podataka ekstrahovanih sa mobilnih uređaja je Social Graph u alatu Oxygen Forensic Detective. Ovaj alat grafički prikazuje veze između različitih entiteta pronađenih na mobilnom uređaju, kao što su osobe, brojevi telefona, nalozi na društvenim mrežama i slično. Maltego je još jedan moćan alat koji se koristi u digitalnoj forenzici za vizuelizaciju i analizu podataka, otkrivanje veza i obrazaca u podacima i prikupljanje dokaza iz javno dostupnih izvora.

Za pregledanje i analizu podataka iz aplikacija koje koriste SQLite za skladištenje, što je tipično za Android uređaje, mogu se koristiti alati DB Browser for SQLite i SQLite Expert. Plist Editor Pro je alat sa naprednim funkcijama za analizu plist datoteka, koje se često koriste u iOS mobilnim aplikacijama.

4.3. Alati za digitalnu forenziku računara

Neki od najpoznatijih besplatnih alata otvorenog koda za prikupljanje i analizu podataka sa računara su The Sleuth Kit (TSK) i Autopsy. TSK je skup programa koji se pokreću iz komandne linije i omogućavaju detaljno ispitivanje slika diskova i fajl sistema. Autopsy je program sa grafičkim okruženjem koji olakšava korišćenje TSK alata, jer ne zahteva poznavanje korišćenja komandne linije.

DB Browser for SQLite je jedan od alata koji može da učita i omogući pregledanje i analizu podataka o pretraživanju iz veb pretraživača. Ovakvi podaci za Google Chrome veb pretraživač se nalaze na lokaciji C:\Users\<User Name>\AppData\Local\Google\Chrome\User Data\Default na Windows operativnom sistemu, ~/.config/google-chrome/Default na Linuks operativnom

sistemu i /Users/<User Name>/Library/Application Support/Google/Chrome/Default na Mek operativnom sistemu.

4.4. Alati za digitalnu forenziku računarskih mreža

Neki od alata koji se najčešće koriste u digitalnoj forenzici računarskih mreža su Wireshark, tcpdump i Network Miner. Wireshark je besplatan alat, otvorenog koda koji omogućava snimanje mrežnog saobraćaja sa računara ili mobilnog uređaja u realnom vremenu. Pored snimanja mrežnog saobraćaja u realnom vremenu moguće je i čitanje postojećih snimaka. U Wireshark-u se mogu pregledati datoteke u PCAP ili PCAPNG formatu prikupljene iz prethodnih arhiva. Wireshark ima filtere za izolovanje relevantnog saobraćaja, čime se može izolovati saobraćaj vezan za društvene mreže. Može se filtrirati tako da se prikaže samo saobraćaj ka određenim domenima ili sa određenim protokolima, HTTP ili HTTPS. Većina društvenih mreža koristi HTTPS za komunikaciju, pa se zbog toga ne može analizirati ceo sadržaj paketa. U ovim slučajevima, Wireshark može da otkrije samo neke metapodatke kao što su izvorna i odredišna IP adresa, vreme komunikacije, ali ne i tačan sadržaj komunikacije.

5. STUDIJA SLUČAJA

U ovom poglavlju obrađen je ceo proces forenzičke istrage slučaja prodaje ilegalnih supstanci preko Instagrama. Osumnjičeni je koristio Instagram nalog za prodaju narkotika, a kupci su ga kontaktirali putem privatnih poruka. Policija je dobila sudski nalog za pretres stvari osumnjičenog i preuzimanje podataka sa njegovog Instagram naloga od Meta Platforms Inc. Tokom faze identifikacije pronađen je Instagram nalog sa koga su vršeni dogovori za prodaju narkotika, kao i mobilni uređaj osumnjičenog. U fazi prikupljanja istražitelji su podneli inicijalni onlajn zahtev preko sistema za slanje onlajn zahteva kompanije Meta Platforms Inc. Pošto ovaj slučaj nije procenjen kao hitan, traženi podaci su dobijeni posle dužeg vremenskog perioda. U međuvremenu istražitelji su prikupili podatke sa mobilnog uređaja uz pomoć alata Cellebrite UFED. U fazi čuvanja napravljene su identične kopije prikupljenih podataka i podaci su uskladišteni na hard-disku koji se nalazi na sigurnom mestu sa ograničenim pristupom i kontrolisanom temperaturom i vlagom. Svakoj datoteci, kako originalnoj tako i kopiji, dodeljen je jedinstveni heš kod. Takođe je vođena detaljna dokumentacija o pristupu podacima. Tokom faza pregledanja i analize korišćeni su forenzički alati UFED Physical Analyser i Magnet AXIOM Examine. Kroz analizu podataka iz aplikacije Instagram sa mobilnog uređaja potvrđeno je da je osumnjičeni koristio svoj mobilni uređaj za pristup Instagram nalogu za prodaju narkotika. Analizom podataka dobijenih sudskim nalogom od Meta Platform Inc. su pronađene obrisane poruke koje svedoče o ilegalnoj prodaji narkotika. U fazi prezentacije su kreirani izveštaji korišćenjem pomenutih alata radi prezentovanja dokaza na sudu.

6. ZAKLJUČAK

Sa porastom upotrebe platformi poput Fejsbuka, Instagrama i Vocapa, ove mreže su postale plodno tlo za kriminalne aktivnosti. U ovom radu su detaljno opisane faze digitalne forenzike, specifičnosti i izazovi forenzičke istrage na društvenim mrežama. Navedene su brojne tehnike i alati koji doprinose uspešnom prikupljanju, pregledanju i analizi dokaza. Kroz studiju slučaja, prikazan je ceo proces forenzičke istrage od početka do kraja. Brz napredak tehnologije donosi nove izazove za digitalnu forenziku. Stalna pojava novih modela, operativnih sistema i metoda enkripcije čini zadatak forenzičara sve težim. Iako se forenzički alati konstantno razvijaju, ne mogu da drže korak sa najnovijim tehnologijama. Zaobilaženje sigurnosnih mehanizama i dekriptovanje podataka postaje sve komplikovanije, što može da oteža ili onemogući pristup potencijalnim dokazima. Uprkos izazovima koje donosi brz tehnološki razvoj, digitalna forenzika društvenih mreža ostaje ključna u borbi protiv sajber kriminala. Njen dalji razvoj biće omogućen kontinuiranim ulaganjem u usavršavanje i razvijanje novih forenzičkih alata i tehnika.

7. LITERATURA

[1] https://www.upguard.com/blog/digital-forensics (pristupljeno u avgustu 2024.)

[2] Brian Carrier, Research Scientist, Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers, International Journal of Digital Evidence, Winter 2003.

[3] https://explodingtopics.com/blog/top-social-media-platforms (pristupljeno u septembru 2024.)

[4] https://www.mpravde.gov.rs/tekst/12714/medjunarodna-pravna-pomoc-neposredna-komunikacija.php (pristupljeno u novembru 2024.)

[5] Jansen W, Ayers R. Guidelines on cell phone forensics. NIST Special Publication. 2007.

[6] https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-digital-forensics/ (pristupljeno u septembru 2024.)

[7] Jason Sachowski, Digital Forensics and Investigations, 2018

Kratka biografija:

Nikolina Gašić je rođena u Kikindi 1997. godine. Školske 2016/2017. godine je upisala osnovne akademske studije na Fakultetu tehničkih nauka u Novom Sadu, smer Računarstvo i automatika, modul Primenjene računarske nauke i informatika. Diplomirala je 2020. godine i upisala master akademske studije na istom fakultetu, smer Računarstvo i automatika, modul Primenjene računarske nauke i informatika - Elektronsko poslovanje.