# Izvori podataka terminalnih uređaja za potrebe forenzičke analize

**Stepić, Matija**

**SVEUČILIŠTE U ZAGREBU**
**FAKULTET PROMETNIH ZNANOSTI**

**Matija Stepić**

# IZVORI PODATAKA TERMINALNIH UREĐAJA ZA POTREBE FORENZIČKE ANALIZE

**ZAVRŠNI RAD**

**Zagreb, 2017.**

Sveučilište u Zagrebu
Fakultet prometnih znanosti

# ZAVRŠNI RAD

# IZVORI PODATAKA TERMINALNIH UREĐAJA ZA POTREBE FORENZIČKE ANALIZE

# TERMINAL DEVICE DATA SOURCES FOR THE PURPOSE OF FORENSIC ANALYSIS

Mentor: dr. sc. Siniša Husnjak

Student: Matija Stepić
JMBAG: 0135237627

Zagreb, rujan 2017.

# IZVORI PODATAKA TERMINALNIH UREĐAJA ZA POTREBE FORENZIČKE ANALIZE


## SAŽETAK

Forenzička analiza mobilnih terminalnih uređaja provodi se kako bi se došlo do podataka koji mogu biti od velikog značaja za sudske postupke. Do podataka se može doći različitim vrstama ekstrakcije i različitim forenzičkim alatima. Od osnovnih ekstrakcija koriste se ručna, logička, datotečna, fizička, JTAG i chip-off, a neke od ostalih metoda ekstrakcije su Flasher Box, Micro Read, itd. Forenzički alati se koriste za analizu digitalnih podataka i često za pronalaženje dokaza da je netko počinio ili nije počinio zločin. Alati su namijenjeni za pomoć osoblju, policiji i pravnim istražiteljima u prikupljanju, čuvanju i ispitivanju podataka koji se odnose na neprikladne i ilegalne aktivnosti. Podaci koji se prikupljaju nazivaju se digitalni dokazi, a digitalni dokaz je informacija uskladištena ili prenošena u digitalnoj formi koja se koristi u sudskim postupcima. Svaki mobilni terminalni uređaj sadrži potencijalne izvore podataka, a oni se mogu nalaziti u SIM kartici, lokaciji, SMS porukama, zapisima poziva, e-pošti itd. To su uglavnom podaci koji govore o korisnikovim neprimjerenim radnjama. Npr. iz lokacije mobilnog terminalnog uređaja mogu se otkriti nedavne adrese, rute, pohranjene lokacije osumnjičene osobe. Svi izvori podataka su detaljno opisani u radu.



KLJUČNE RIJEČI: mobilni terminalni uređaj; digitalna forenzička analiza; ekstrakcija podataka; izvor podataka; digitalni dokaz



## SUMMARY

Forensic analysis of mobile terminal devices is carried out in order to obtain data that can be of great importance for court proceedings. Data can be obtained by different types of extraction and by various forensic tools. Manual, logical, file, physical, JTAG and chip-off are used for basic extraction, and some of the other methods of extraction are Flasher Box, Micro Read, etc. Forensic Tools are used to analyze digital data and often to find evidence that someone has committed or did not commit a crime. The tools are intended to assist staff, police and legal investigators in collecting, storing and testing data related to inappropriate and illegal activities. Collected data is called digital evidence. Digital evidence is the information stored or transmitted in the digital form used in court proceedings. Each mobile terminal device contains potential sources of information, which can be found in the SIM card, location, SMS messages, call records, emails, etc. These are mainly information that tells about inappropriate actions by the user. Eg. from the location of the mobile terminal device can be detected the recent addresses, routes, stored locations of the suspect, etc. All data sources are described in detail in the paper.



KEY WORDS: mobile terminal device; digital forensic analysis; data extraction; data source; digital evidence

# Sadržaj

# 1. Uvod

Razvojem računalnih tehnologija dolazi do sve većeg broja mobilnih terminalnih uređaja na tržištu, a samim time povećava se broj kaznenih djela koja se mogu povezati s mobilnim terminalnim uređajima. Zbog svakodnevnih zlonamjernih aktivnosti potrebno je moći doprijeti do podataka smještenih u mobilnom terminalnom uređaju koji bi mogli otkriti ili pojasniti određeni događaj. Do podataka u mobilnim terminalnim uređajima dolazi se digitalnom forenzičkom analizom. Digitalna forenzička analiza predstavlja proces otkrivanja i tumačenja elektroničkih podataka, a provode ju forenzički istražitelji. Najvažniji dio forenzičke analize mobilnih terminalnih uređaja jest ekstrakcija podataka, tj. kako će se podaci dobaviti iz određenog mobilnog terminalnog uređaja. U trećem poglavlju opisane su najvažnije vrste ekstrakcija te prednosti i mane svake od njih. Također, ekstrakcija dokaza i forenzičko ispitivanje svakog mobilnog uređaja može se razlikovati.

Kako postoje različiti načini ekstrakcije podataka, tako postoje i različiti forenzički alati koji provode ekstrakciju podataka. Forenzički alati su u stalnom razvoju i moraju pratiti trendove novih mobilnih uređaja kako bi njihova svrha ne bi bila uzaludna. Alati se koriste u prvom redu za pomoć istražiteljima u otkrivanju digitalnih dokaza, a nude tri glavne mogućnosti: stjecanje, skupljanje, očuvanje.

Glavni dio ovoga rada su izvori podataka terminalnih uređaja, a pomoću njih se rješavaju razna kriminalna djela. Skup značajki podataka razlikuje se ovisno o razdoblju u kojem je mobilni terminalni uređaj izrađen. Digitalni dokazi predstavljaju podatke koji se prikupljaju kada se istražuje određeni uređaj, a to se najčešće povezuje s kriminalnim radnjama. Forenzičkom analizom dolazi se do podataka do kojih obični korisnik ne može jednostavno doći, a ti podaci uglavnom opisuju osumnjičenikove radnje, poslane poruke, posjećena mjesta, odlazne i dolazne pozive, itd.

Cilj i svrha ovog završnog rada je prikazati podatke koji se nalaze u terminalnim uređajima, a do kojih se dolazi forenzičkom analizom.

Rad se sastoji od 7 poglavlja:

1. Uvod
2. Karakteristike forenzičke analize mobilnih uređaja
3. Postupci i značajke ekstrakcije podataka u forenzičkoj analizi
4. Svrha i korištenje alata forenzičke analize
5. Izvori podataka terminalnih uređaja za potrebe forenzičke analize
6. Anketni upitnik – osviještenost korisnika o prikupljanju podataka terminalnih uređaja
7. Zaključak

U drugom poglavlju opisuje se pojam forenzičke analize, povijest forenzičke analize, razni izazovi te na koji način se može opisati kvaliteta forenzičke istrage.

Trećim poglavljem opisuju se načini ekstrakcije podataka, njihove značajke, prednosti i mane. Opisuju se i faze pri ekstrakciji podataka iz mobilnih uređaja, a opis je popraćen slikom.

U četvrtom poglavlju se opisuje svrha alata za forenzičku analizu. Opisuje se i popis najčešće korištenih alata te koji su im osnovni zahtjevi.

Peto poglavlje je ujedno i najvažnije poglavlje rada u kojemu se opisuje značenje podataka koji se ekstrahiraju iz mobilnih terminalnih uređaja. Za svaki izvor podataka opisane su njegove značajke.

U šestom poglavlju nalazi se anketa u kojoj je sudjelovalo 82 ispitanika, a opisano je koliko je pojam forenzičke analize i ekstrakcije podataka poznat ljudima i svijest korisnika o podacima koji se nalaze unutar njihovih uređaja.

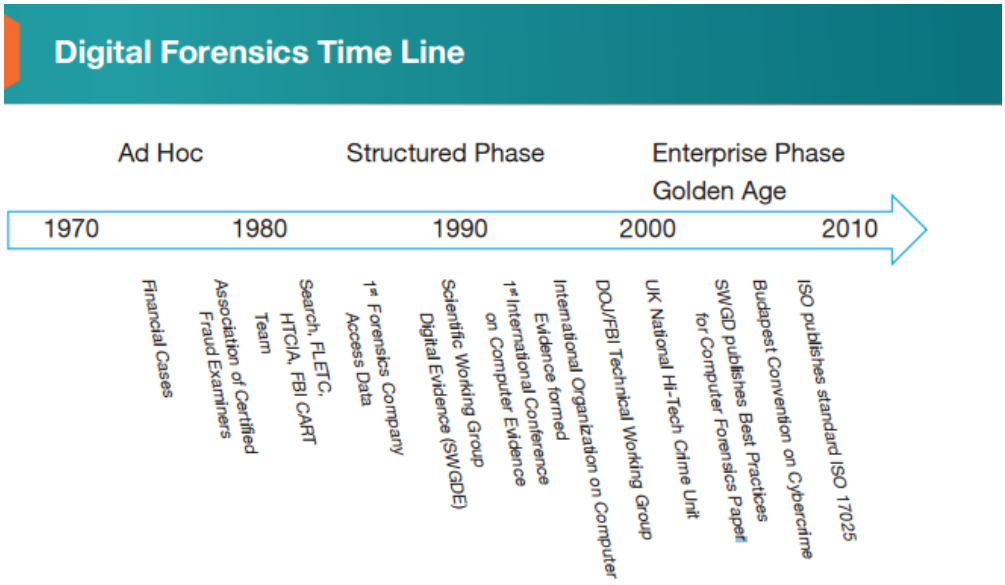
# 2. Karakteristike forenzičke analize mobilnih uređaja

Forenzička analiza mobilnog uređaja može se provesti pomoću višestrukih metoda koje se kasnije definiraju. Svaka od tih metoda utječe na potrebnu količinu potrebne analize, što će se detaljnije raspravljati u predstojećim poglavljima. Ako jedna metoda ne uspije, mora se pokušati druga. Mogući su višestruki pokušaji i alati kako bi dobili najviše podataka s mobilnog uređaja, [1].

Mobilni uređaji su dinamični sustavi koji predstavljaju mnogo izazova ispitivaču u ekstrakciji i analizi digitalnih dokaza. Brzo povećanje broja različitih vrsta mobilnih uređaja različitih proizvođača otežava razvoj procesa ili alata za ispitivanje uređaja. Mobilni uređaji neprekidno se razvijaju kao napredak postojećih tehnologija ili uvođenja novih poboljšanih tehnologija. Nadalje, svaki mobilni uređaj dizajniran je s različitim ugrađenim operativnim sustavima. Stoga su od forenzičara potrebna posebna znanja i vještine kako bi analizirali uređaje, [1].

## 2.1. Povijest digitalne forenzičke analize

Digitalna forenzika se pojavila prije skoro 40 godina, počevši od kraja 1970-ih godina. Većina prvih kaznenih slučajeva koji su uključivali računala bili su financijski orijentirani. U osamdesetim godinama, razvili su se tečajevi digitalne forenzike, koje su razvile organizacije kao što su udruga ovlaštenih ispitivača prijevara (engl. *Association of Certified Fraud Examiners*), nacionalni konzorcij za informiranje i statistiku pravosuđa (engl. *The National Consortium for Justice Information and Statistics*) te udruga za istraživanje visokog kriminala (engl. *High Technology Crime Investigation Association*, HTCIA), [2].




**Slika 1:** Povijest digitalne forenzičke analize, [3]

Prvi dio povijesti predstavlja razdoblje koje obuhvaća razdoblje do ranih osamdesetih godina. Mnogo toga što se događalo u tom razdoblju, danas bi bilo ne zamislivo, odnosno metode i postupci su bili znatno kompliciraniji i drugačiji. Zapravo, pojam jednostavno nije postojao. Funkcija računala u tom razdoblju bila je uglavnom obrada podataka, a oni su bili u vlasništvu i upravljanju korporacija, sveučilišta, istraživačkih centara i vladinih agencija. Zahtijevali su veliku fizičku infrastrukturu, uključujući velike iznose snage i klimatizacije te visoko kvalificiranog osoblja. Administratori sustava su bili najvećim dijelom odgovorni za vlastitu sigurnost njihovih sustava, od kojih većina nije bila značajno povezana s vanjskim svijetom. Sustavne revizije osmišljene su kako bi se osigurala učinkovitost i točnost obrade podataka, što je u to vrijeme bilo vrlo skupo, a može se i reći da te revizije predstavljaju prvi sustavni pristup računalnoj sigurnosti. Pod proizvodom ovih napora bilo je da se informacije prikupljene tijekom revizija mogu koristiti za istraživanje pogrešaka. Obično su istraživači koji su bili obučeni za rad na računalu bili u suradnji s administratorima sustava. Tradicionalnim menadžerima i istražiteljima bilo je teško shvatiti potencijal računala da budu alati i žrtve kriminala, [2].

Sljedeće razdoblje naziva se razdobljem „nepunoljetnosti“. Pojava IBM-ovih računala početkom 1980-ih godina, rezultirala je eksplozijom hobija koji se vežu uz računala. Računala iako snažna imala su relativno malo aplikacija i nisu, unatoč reklamnoj kopiji, jednostavni za uporabu. Rana računala omogućila su ljudima pisanje programskog koda i pristup unutar operacijskog sustava i hardvera. Te su vještine usmjerene na nova računala, koja se i danas koriste. Među hobistima su bili čak i policijski službenici iz velikog broja organizacija. Upravo te organizacije koje su u svojim krugovima imale ljude kojima je hobi bio istraživanje računala i njegovih funkcionalnosti, bile su i prve organizacije posvećene digitalnoj forenzici a grupni naziv za njih je bio IACIS (engl. *International Association of Computer Investigative Specialists*) tj. Međunarodno udruženje stručnjaka za istraživanje računala. Predmeti koji su istraženi od strane tadašnjih istraživača, rješavali su se na slične načine kao i danas, tj. današnja forenzička analiza se temelji na tadašnjoj. Fokus je bio na oporavku podataka iz samostalnih računala. Oporavak podataka bio je glavni problem jer je pohrana bila skupa i korisnici su rutinski izbrisali podatke i ponovo formatirali medije. Internet tada još nije bio popularan, ali kriminalci su koristili dial-up pristup kompromisnim računalima. Telefonska usluga bila je naplaćivana na temelju udaljenosti i veličine korištenja, [3].

Sljedeće razdoblje, tj. desetljeće pokazalo se desetljećem ogromnog rasta veličine i zrelosti. Ovaj je rast imao brojne značajke, ali tri su bile najvažnije. Prva značajka je eksplozija tehnologije koja se dogodila tijekom razdoblja razvijanja. Računala su postala sveprisutna, mobilni uređaji su postali neophodni i Internet je postao središte svega. Na početku epohe, većina glasovnih poziva bila su putem fiksne mreže, većina mrežnih računala je bila povezana, a većina ljudi nije čula za Internet. Do kraja epohe, gotovo svatko je imao e-mail adresu, mobilni uređaj i oslonio se na Internet, a većina domova i tvrtki su imali pristup mreži. Računalna tehnologija ugrađena je gotovo u svaki element svakodnevnog života i to uključuje kriminalne aktivnosti. Druga značajka je eksplozija slučajeva dječje pornografije. Internet i računala koristila su se u nezakonite svrhe, i ta nova kršenja rezultirala su oduzimanjem sve većih količina digitalnih dokaza i bila je glavni pokretač rasta digitalne

forenzike. Uz povećanje volumena, tehničke sofisticiranosti i pravnih studija, postalo je još važnije odabrati i poboljšavati digitalnu forenziku. Digitalni audio, video i ugrađeni uređaji kao što su mobilni telefoni, zahtijevaju specifična znanja i obuku, odvojeno od tradicionalnih medija za pohranu i forenzičara usmjerenih na mrežu. Čak su se ta dva područja počela raspadati na nekim razinama, budući da je istraživanje mrežnog upada postalo složeno. Stručnost digitalne forenzike počela je voditi vladine i profesionalne organizacije, a ne pojedinci, [2].

Novo razdoblje se naziva „mladost ili adolescencija“ koje traje od 2005.-2010. godine. Od 2005. godine, digitalna forenzika se proširila i u dubinu i širinu. Sudovi Američkih država usvojili su 2006. godine nova pravila za građanski postupak kojim su digitalni podaci definirani kao novi oblik dokaza i implementirali su novi obvezni sustav, nazvan elektroničko otkrivanje ili „e-Discovery“, za rješavanje digitalnih dokaza. Profesionalci informacijske sigurnosti sada prepoznaju digitalnu forenziku kao osnovno područje primjene. Iako se njihovi ciljevi i potrebe često razlikuju od onih koji se primjenjuju u zakonima, koncepti i alati su često identični. Dok financijska sredstva za istraživanje digitalnih forenzika zaostaju u drugim tradicionalnim disciplinama kao što su informacijska sigurnost, fakulteti i sveučilišta prepoznali su popularnost i tržišnu vrijednost digitalnog forenzičkog obrazovanja. Tehnički odbor E-30 američkog društva za ispitivanje materijala ASTM (engl. *The American Society of Testing Materials*) formulirao je nacrt standarda za digitalne forenzičke programe obrazovanja i osposobljavanja. Policijske, vojne i obavještajne zajednice dizajnirale su organizacijske strukture i procese kako bi podržale svoje mišljenje o misiji. Određivanje forenzičkih proizvoda u budućnosti još je jedan izazov. Postoji jaki taktički pristup, ali nedostaje dugoročni strateški plan, [3].

Sljedeće razdoblje je „razdoblje budućnosti“. Forenzičari više neće imati linearan proces usredotočen na oporavak podataka, već proces koji se temelji na dokazima koji će se integrirati u istrage, analizu obavještajnih podataka, sigurnost informacija i elektronska otkrića, tj. razvoj. Digitalni forenzički alati morati će se poboljšati radi većih izazova u smislu sigurnosti. Da bi se prevladao običan volumen, alati će morati imati ugrađene analitičke sposobnosti, što omogućuje prepoznavanje važnih stavki bez potrebe za pregledom svake stavke. Alati će morati biti semiotički, razumijevajući ljudski jezik i komunikaciju, te sposobni interpretirati sadržaj i kontekst. Organizacije koje koriste digitalnu forenziku i one koje se oslanjaju na njih će se morati razvijati, [2].

## 2.2. Mobilna forenzika

Digitalna forenzika je proces otkrivanja i tumačenja elektroničkih podataka. Cilj procesa je očuvanje bilo kojeg dokaza u svom najoriginalnijem obliku pri obavljanju strukturiranog istraživanja prikupljanjem, identifikacijom i potvrdom digitalnih informacija u svrhu rekonstrukcije prošlih događaja, [4].

Digitalna forenzika je također grana forenzičke znanosti koja je usmjerena na oporavak i istraživanje osnovnih podataka koji se nalaze u elektroničkim ili digitalnim uređajima. Mobilna forenzika je grana digitalne forenzike koja se odnosi na oporavak digitalnih dokaza s mobilnih uređaja. Važno je odrediti kada se određena forenzička tehnologija ili metodologija treba primjenjivati. Glavno načelo u određivanju ispravne metodologije ili tehnologije je da se izvorni dokazi ne smiju mijenjati, što je izrazito teško kod mobilnih uređaja. Neki forenzički alati zahtijevaju komunikacijski vektor s mobilnim uređajem, stoga standardna zaštita pisanja neće funkcionirati tijekom forenzičke istrage. Druge forenzičke metode ekstrakcije mogu uključivati uklanjanje čipa ili instalaciju *bootloader*-a na mobilnom uređaju prije izdvajanja podataka za sudsku provjeru. U slučajevima kada ispitivanje ili prikupljanje podataka nije moguće bez promjene konfiguracije uređaja, postupak i promjene moraju biti testirani, potvrđeni i dokumentirani. Sljedeći pravilnu metodologiju i smjernice od presudne je važnosti u pregledavanju mobilnih uređaja jer donosi najvrijednije podatke. Kao i kod prikupljanja dokaza, neodgovarajući postupak tijekom ispitivanja može rezultirati gubitkom ili oštećenjem dokaza ili ga učiniti nedopuštenim na sudu, [1].

Digitalna forenzička ispitivanja imaju različite primjene. Najčešće je korištena u potvrdi ili opovrgavanju hipoteza pred kaznenim ili građanskim (kao dio elektroničkog procesa otkrivanja) sudovima. Forenzika se također može pojaviti u privatnom sektoru, kao što je to slučaj kod internih korporativnih istraga ili ulaza u neovlašteno područje. Osim identifikacije izravnih dokaza o zločinu, digitalna forenzika može se koristiti za atribuiranje dokaza određenim osumnjičenicima, potvrditi alibije ili izjave, utvrditi namjeru, identificirati izvore (npr. slučajevi autorskog prava) ili autentificirati dokumente. Istraživanja su mnogo šira od drugih područja forenzičke analize (gdje je uobičajen cilj pružiti odgovore na niz jednostavnih pitanja) i često uključuju složene vremenske linije ili hipoteze, [4].

Forenzika mobilnih uređaja je grana digitalne forenzike koja se odnosi na oporavak digitalnih dokaza ili podataka s mobilnog uređaja pod određenim forenzičnim uvjetima. Izraz mobilni uređaj obično se odnosi na mobilne telefone, međutim, može se odnositi i na bilo koji digitalni uređaj koji ima unutarnju memoriju i sposobnost komunikacije, uključujući PDA uređaje, GPS uređaje i tablet računala. Korištenje telefona u zločinu već je poznato nekoliko godina, no forenzička studija mobilnih uređaja relativno je novo područje, koje se proteže od ranih 2000-tih i kasnih 1990-ih. Veliki porast broja telefona (osobito pametnih) i drugih digitalnih uređaja na tržištu potrošača uzrokovalo je zahtjev za detaljnim forenzičkim pregledom uređaja, što nisu mogle ispuniti postojeće forenzičke tehnike. Mobilni uređaji mogu se koristiti za spremanje nekoliko vrsta osobnih podataka kao što su kontakti, fotografije, kalendari i bilješke, SMS i MMS poruke. Pametni telefoni mogu dodatno sadržavati video, e-poštu, informacije o pregledavanju weba, informacije o lokaciji te poruke i kontakte društvenih mreža, [5].

Postoji sve veća potreba za korištenjem mobilne forenzike, a neki od istaknutih razloga su:

- Korištenje mobilnih telefona za pohranu i prijenos osobnih i korporativnih informacija

- Korištenje mobilnih telefona u mrežnim transakcijama
- Provedba zakona, kriminalci i veliki broj mobilnih telefona

Forenzika mobilnih uređaja može biti osobito izazovna na više razina. Postoje dokazni i tehnički izazovi, primjerice:

- Kako bi ostali konkurentni, proizvođači originalnih opreme često mijenjaju faktore mobilnog telefona, strukture datoteka operativnog sustava, pohranu podataka, usluge, periferne uređaje, pa čak i ulazne konektore i kabele
- Kapacitet pohrane i dalje raste zahvaljujući potražnji za snažnijim „mini računalnim" uređajima
- Ne samo da se vrste podataka, već i način korištenja mobilnih uređaja neprestano razvijaju
- Ponašanje hibernacije u kojem se procesi obustavljaju kada se uređaj isključi ili ne radi, ali istodobno ostaje aktivan

Kao rezultat tih izazova postoji širok raspon alata za izdvajanje dokaza iz mobilnih uređaja. Nitko, niti alat niti metoda ne mogu steći sve dokaze iz svih uređaja. Stoga se preporučuje da sudski ispitivači, posebno oni koji se žele kvalificirati kao vještaci na sudu, prolaze kroz opsežnu obuku kako bi razumjeli kako svaki alat i metoda stječu dokaze, [4].

Proces mobilne forenzike se dijeli u tri glavne kategorije: otkrivanje, stjecanje i ispitivanje/analiza. Forenzični ispitivači suočavaju se s nekim izazovima, dok se mobilni uređaj koristi kao izvor dokaza. Na mjestu zločina, ukoliko je mobilni uređaj pronađen isključen, ispitivač bi ga trebao staviti u Faraday vrećicu/torbu[1] kako bi spriječio moguće promjene ako se uređaj sam uključi. Ako je uređaj pronađen uključen, isključivanje bi moglo nanijeti određene posljedice. Ako je uređaj zaključan PIN-om ili lozinkom ili je šifriran, ispitivač će morati zaobići zaključavanje ili odrediti PIN za pristup uređaju. Mobilni uređaji su mrežni uređaji i mogu slati i primati podatke putem različitih izvora, kao što su telekomunikacijski sustavi, Wi-Fi pristupne točke i *Bluetooth*. Dakle, ako je uređaj u stanju pokretanja, kriminalac može sigurno izbrisati podatke pohranjene na telefonu izvršavanjem naredbe udaljenog brisanja. Kada je uređaj uključen, treba ga staviti u veliku torbu. Ako je moguće potrebno je izvršiti odspajanje mobilnog uređaja od mreže prije stavljanja u Faraday torbu, kako bi se zaštitili dokazi. To će također sačuvati bateriju uređaja koji se nalazi u Faraday torbi. Nakon što se mobilni uređaj pravilno zaplijeni, ispitivač može trebati više forenzičkih alata za prikupljanje i analizu podataka pohranjenih na telefonu, [1].

## 2.3. Izazovi mobilne forenzike

Jedan od najvećih forenzičkih izazova kada je u pitanju mobilna platforma je činjenica da se podacima može pristupiti, da se mogu pohraniti i sinkronizirati na više uređaja. Budući

[1] Faraday vrećica/torba – mjesto u koje se pohranjuje mobilni uređaj kako bi se izolirao od mreže

da su podaci nestabilni i mogu se brzo preoblikovati ili brisati na daljinu, potrebno je više napora za očuvanje tih podataka. Mobilna forenzika razlikuje se od računalne i predstavlja jedinstvene izazove za forenzičare, [1].

Forenzičari se često bore za dobivanje digitalnih dokaza s mobilnih uređaja. Slijede neki od razloga:

- **Hardverske razlike:** Tržište je preplavljeno različitim modelima mobilnih uređaja različitih proizvođača. Forenzični ispitivači mogu naići na različite vrste mobilnih modela koji se razlikuju po veličini, hardveru, značajkama i operacijskom sustavu. Također, s kratkim ciklusom razvoja proizvoda, novi modeli pojavljuju se vrlo često. Kako se mobilni krajolik mijenja svakim danom, ključno je da se ispitivač prilagodi svim izazovima i ostaje ažuriran na forenzičke tehnike mobilnih uređaja.
- **Mobilni operacijski sustavi:** Kod većine računala, glavni operativni sustav desetaka godina unazad je Windows. Mobilni uređaji koriste više vrsta operacijskih sustava kao što su Apple's iOS, Google's Android, RIM's, BlackBerry OS, Microsoft's Windows Mobile, HP's webOS, Nokia's Symbian OS i mnogi drugi.
- **Sigurnosne značajke mobilne platforme:** Moderne mobilne platforme sadrže ugrađene sigurnosne značajke za zaštitu korisničkih podataka i privatnosti. Ove značajke djeluju kao prepreka tijekom fizičke akvizicije i ispitivanja. Na primjer, moderni mobilni uređaji dolaze sa zadanim mehanizmima enkripcije od hardverskog sloja do softverskog sloja. Ispitivač bi možda trebao proći kroz ove mehanizme šifriranja kako bi izvadio podatke s uređaja.
- **Nedostatak resursa:** Kao što je ranije spomenuto, s rastućim brojem mobilnih uređaja, alati koje zahtijevaju forenzični ispitivači također bi se povećali. Forenzički pribor, kao što su USB kabeli, baterije i punjači za različite mobilne uređaje, moraju se održavati kako bi uspješno istraživali uređaje.
- **Generičko stanje uređaja:** Čak i ako se čini da je uređaj izvan stanja rada, pozadinski procesi mogu i dalje raditi. Na primjer, u većini mobilnih uređaja budilica i dalje radi čak i kad je uređaj isključen. Nagli prijelaz iz jedne države u drugu može rezultirati gubitkom ili promjenom podataka.
- **Anti-forenzičke tehnike:** Anti-forenzičke tehnike, kao što su skrivanje podataka, krivotvorenje podataka i sigurno brisanje otežavaju istraživanja digitalnih medija.
- **Dinamička priroda dokaza:** Digitalni dokazi mogu se lako promijeniti ili namjerno ili nenamjerno. Na primjer, pregledavanje aplikacije na uređaju može promijeniti podatke pohranjene od strane aplikacije na uređaju.
- **Slučajno poništavanje:** Mobilni uređaji omogućuju restartiranje svega. Ponovno pokretanje uređaja tj. restartiranje tijekom pregleda može rezultirati gubitkom podataka.
- **Promjena uređaja:** Mogući načini izmjene uređaja mogu se razlikovati od premještanja podataka aplikacije, preimenovanja datoteka i izmjene proizvođačkog operacijskog sustava. U ovom slučaju treba uzeti u obzir stručnost osumnjičenog.
- **Obnavljanje zaporke:** Ako je uređaj zaštićen zaporkom, forenzičar mora pristupiti uređaju bez oštećenja podataka na uređaju.

- **Komunikacijska zaštita:** Mobilni uređaji komuniciraju putem mobilnih mreža, Wi-Fi mreža, Bluetooth i infracrvene mreže. Kako komunikacija uređaja može promijeniti podatke uređaja, mogućnost daljnje komunikacije treba ukloniti nakon preuzimanja uređaja.
- **Nedostatak dostupnosti alata:** Postoji širok raspon mobilnih uređaja. Jedan alat možda ne podržava sve uređaje ili obavlja sve potrebne funkcije pa treba koristiti kombinaciju alata. Odabir odgovarajućeg alata za određeni telefon može biti teško.
- **Zlonamjerni programi:** Uređaj može sadržavati zlonamjerni softver, poput virusa ili trojanskog konja. Takvi zlonamjerni programi mogu se pokušati proširiti na druge uređaje preko žičnog sučelja ili bežičnog uređaja.
- **Pravna pitanja:** Mobilni uređaji mogu biti uključeni u zločine koji mogu prelaziti zemljopisne granice. Kako bi se riješila ova pitanja pravde, forenzični ispitivač treba biti svjestan prirode zločina i regionalnih zakona, [5].

## 2.4. Kvaliteta forenzičke istrage

Budući da je područje digitalne forenzike evoluiralo prvenstveno s tvrdim diskovima, uključujući sve vrste računalnih sustava, jedan od najvažnijih izazova je ažuriranje opće prihvaćene prakse. U tijeku je napor da se uravnoteži potreba za izdvajanje najkorisnijih digitalnih dokaza što je moguće učinkovitije i želja za stjecanjem netaknute kopije svih raspoloživih podataka, a da pri tome ne mijenjaju ništa u tom procesu. U mnogim situacijama koje uključuju novu tehnologiju, posebno kada se bave iscrpljujućim podacima u memoriji računala, mobilnim uređajima i ostalim ugrađenim sustavima, nije moguće izvući vrijedne dokaze, a da se na neki način ne mijenjaju izvorni podaci. Slično tome, kada se bave digitalnim dokazima distribuiranim na mnogim računalnim sustavima, možda neće moći biti moguće sačuvati sve. U suvremenim digitalnim istraživanjima praktičari se moraju baviti rastućim brojem računalnih sustava u jednoj istrazi, posebice u kaznenim istragama organiziranih grupa, elektroničkim otkrićima velikih korporacija i instruktivnim istraživanjima međunarodnog opsega. U takvim velikim digitalnim istraživanjima potrebno je ispitati stotine ili tisuće računala, kao i zapisnike na mrežnoj razini za povezane dokaze, što ga čini neprikladnim za stvaranje forenzičnih duplikata svakog sustava, [6].

Kako količina digitalnih dokaza raste, a zaostali slučajevi rastu, odmičemo se od resursnog intenzivnog pristupa stvaranjem forenzičke slike i provođenjem detaljnih forenzičkih pretraga svake stavke. Različiti pristup digitalnim forenzičkim ispitivanjima se koristi za brzo prepoznavanje stavki veće dokazne vrijednosti i stvaranje djelotvornih rezultata, rezervirajući dubinsku forenzičku analizu za određene situacije. Istodobno, došlo je do razvoja u očuvanju i korištenju većih promjenjivih podataka koji mogu biti korisni u digitalnoj istrazi. Memorija u računalnim sustavima može uključivati lozinke, šifrirane količine koje su zaključane prilikom isključivanja računala i pokretanje programa koji koriste neki sumnjivac ili računalo uljez. Napredak u forenzici podataka, kriminalističke forenzike i mrežne forenzike mobilnih uređaja omogućuju istražiteljima stjecanje forenzičke slike punog sadržaja memorije i izdvajanje značajnih informacija, [5].

Može se očekivati kontinuirani pristup ljudskim sposobnostima da se bave velikim digitalnim istraživanjima i izvući više informacija pojedinačnih sustava. Svrha forenzičkog ispravnog postupka autentifikacije je podrška identifikaciji i provjeri autentičnosti dokaza. Dokumentacija je ključna komponenta forenzičke ispravnosti. Funkcionalno, ovaj proces uključuje i dokumentiranje jedinstvenih obilježja dokaza poput ID-ova uređaja i MD5 hash-ova te kontinuiranog posjedovanja i kontrole tijekom cijelog životnog vijeka. Stoga je potrebno ne samo zabilježiti detalje o postupku prikupljanja već i svaki put kada se transportira ili prenese i tko je odgovoran za što. Razmatranja kvalitete forenzičke istrage ne završavaju prikupljanjem podataka. Opet, dokumentacija je ključna komponenta, omogućujući drugima da procjenjuju rezultate. Kako bi se cijenila važnost forenzičke ispravnosti, dobro je razmotriti konkretne probleme koji mogu proizaći iz neodgovarajuće obrade digitalnih dokaza, a to može ugroziti slučaj i temeljnu vjerodostojnost forenzičara. Neki najgori scenariji koji proizlaze iz dovoljno velikih prekida u lancu uključuju pogrešnu identifikaciju dokaza, onečišćenje dokaza i gubitak dokaza ili relevantnih elemenata (metapodataka). U jednom slučaju prikupljeni su dokazi iz nekoliko identičnih računalnih sustava, ali proces prikupljanja nije bio temeljito dokumentiran, što je vrlo teško za utvrditi koji su dokazi proizašli iz kojeg sustava, [6].

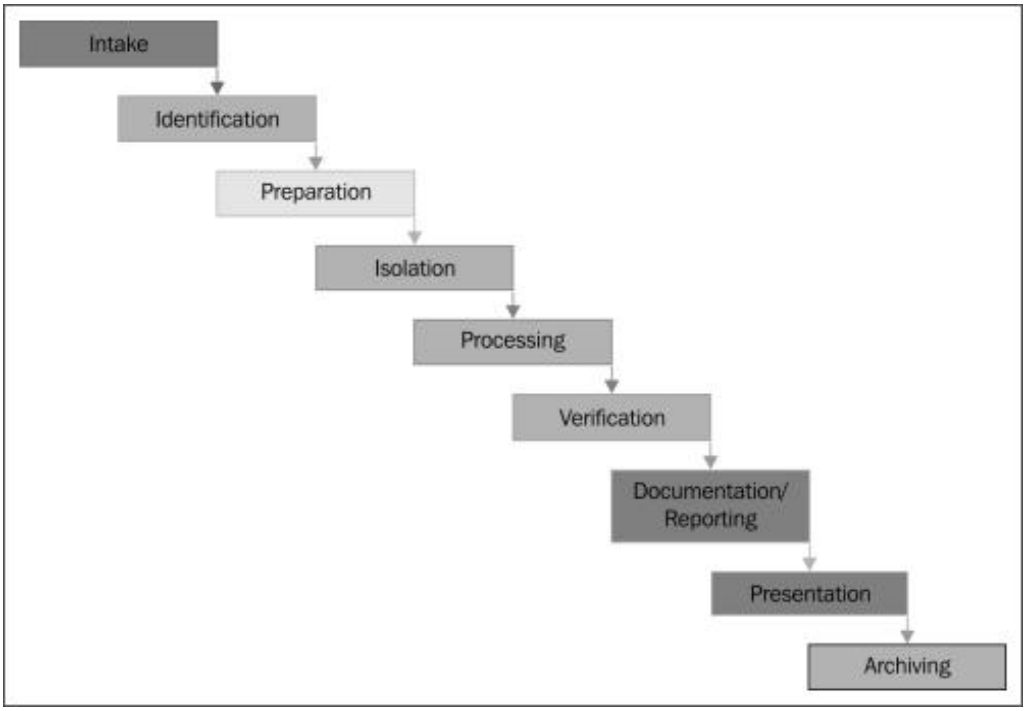
Nedostaci sudske procjene uključuju uništavanje izvornih dokaza prepisivanjem medija s nulama, ne pohranjivanjem podataka u stečenim datotekama koje su sadržavale dokaze na izvornim medijima i ažuriranje metapodataka do trenutnog datuma. Najčešći nedostaci forenzičkih pregleda su pogrešna interpretacija podataka, bilo pomoću alata ili osobe. Pod uvjetom da forenzični praktičari paze na potpuno i precizno čuvanje odabranih digitalnih dokaza, temeljito dokumentiraju proces i objektivno provjeravaju svoj rad na mogućim pogreškama ili propustima, takvi se kvarovi mogu izbjeći ili prevladati, [1].

# 3. Postupci i značajke ekstrakcije podataka u forenzičkoj analizi

Ekstrakcija podataka predstavlja načine prikupljanja podataka iz različitih medija s ciljem daljnje obrade ili pohrane. Postupak ekstrakcije od velikog je značaja za forenzičku analizu MTU-a, [1].

Izdvajanje dokaza i forenzičko ispitivanje svakog mobilnog uređaja se može razlikovati. Međutim, ako se slijede pravilni postupci pristupa pojedinom uređaju te njegova ispitivanja, do potrebnih podataka se dolazi lakše. Iako se trebaju slijediti neka pravila za pojedine uređaje, standardnog postupka mobilne forenzike nema. Sve metode ekstrakcija moraju biti prethodno testirane, odobrene i dobro dokumentirane, [7].

Na sljedećoj slici bit će prikazane osnovne faze pri ekstrakciji podataka iz mobilnih uređaja.




**Slika 2:** Faze ekstrakcije podataka iz mobilnih uređaja, [1]

Faza uvrštenja dokaza (engl. *Intake*) je faza koja je ujedno i početna faza i podrazumijeva obrasce zahtjeva i potrebnu dokumentaciju vezanu uz informacije o vlasništvu i vrstu incidenta u koju je mobilni uređaj uključen te opisuje vrstu podataka ili informacija koje traži podnositelj zahtjeva. Kritični dio ove faze je razvijanje specifičnih ciljeva za svaki postupak koji se primjenjuje, [1].

Faza identifikacije (engl. *Identification*) predstavlja identifikacijski dio kod kojeg ispitivač tj. istražitelj treba identificirati sljedeće pojedinosti za svaki pregled mobilnog uređaja:

- **Zakonsko tijelo** – važno je da forenzični istražitelj utvrdi i dokumentira koja zakonska ovlaštenja postoje za pristup i pregled uređaja, kao i sva ograničenja koja su postavljenja na medij prije pregleda uređaja.
- **Ciljevi ispitivanja** – istražitelj mora utvrditi koliko se detaljno ispitivanje mora provesti, tj. na kojim podacima će biti temeljeno. Cilj ispitivanja predstavlja značajnu razliku u odabiru alata i tehnika za ispitivanje uređaja i povećanja učinkovitosti postupka istraživanja.
- **Izraditi, identificirati i modelirati podatke za uređaj** – pomaže pri određivanju alata koji će raditi s uređajem.
- **Odvojiva i vanjska pohrana podataka** – mnogi uređaji omogućuju proširenje memorije s izmjenjivim tj. prijenosnim uređajima za pohranu, kao što je „Micro SD kartica“. U slučaju kada se takva kartica nađe u mobilnom uređaju koji se ispituje, karticu treba otkloniti i obraditi pomoću tradicionalnih digitalnih forenzičkih tehnika.
- **Ostali izvori potencijalnih dokaza** – mobilni uređaji djeluju kao dobri izvori otiska prsta i drugih bioloških dokaza. Izvori otiska prsta često služe kao način otključavanja mobilnog uređaja, a korištenjem mobilnog uređaja prsti su stalno u doticaju s ekranom što ostavlja velik broj otisaka na samom uređaju. Takvi dokazi trebali bi se prikupiti prije ispitivanja mobilnog uređaja kako bi se izbjeglo moguće oštećenje ili stavljanje otisaka ispitivača na mobilni uređaj, a preventivno tomu, ispitivači trebaju nositi rukavice prilikom rukovanja s dokazima, [7].

Zatim slijedi faza pripreme (engl. *Preparation*) gdje se uključuje istraživanje vezano za određeni mobilni uređaj koji se ispituje te uključuje alate koji će se koristiti za pregled uređaja, [1].

Kod faze izolacije (engl. *Isolation*) mobilni telefoni dizajnirani su za različite vrste komunikacija, kao što su putem mobilnih mreža, *Bluetooth*-a, infracrvene tehnologije itd. Kada je mobilni telefon povezan s mrežom, dolaze novi podaci putem poziva, poruka i podataka o aplikaciji, koji mijenjaju dokaze u uređaju. Kompletno uništavanje podataka je također moguće putem daljinskog pristupa ili daljinskog brisanja naredbi. Zbog toga je prije pregleda, tj. istraživanja uređaja važna izolacija uređaja gledano prema komunikacijskim izvorima. Izolacija uređaja može se ostvariti korištenjem Faraday vrećica, koje blokiraju radio signale prema i od uređaja. Također jedan od načina je postavljanje krpe za zaštitu frekvencije preko samog uređaja ili stavljanjem uređaja u zrakoplovni način rada, [8].

Nakon što je uređaj izoliran, slijedi faza obrade (engl. *Processing*). Uređaj bi se trebao obrađivati testiranim metodama, koje su ponovljive. Fizička ekstrakcija je jedna od poželjnijih metoda jer izvlači podatke osnovne memorije[2] i sam uređaj se obično isključuje tijekom postupka forenzičke analize. Na većini uređaja prilikom korištenja metode fizičke ekstrakcije,

[2] Zapis memorije bit-po-bit

nema promjena. Ako fizička ekstrakcija nije moguća ili ne uspije, potrebno je pokušati doći do datotečnog sustava mobilnog uređaja, [5].

Kod faze provjere (engl. *Verification*) istražitelj mora potvrditi točnost podataka izvađenih iz mobilnog uređaja kako bi osigurali podatke, tj. kako se oni ne bi mijenjali. Provjera izdvojenih podataka se može vršiti na veliki broj načina:

- **Uspoređivanje izdvojenih podataka s podacima u uređaju** – Potrebno je provjeriti jesu li podaci izvađeni iz uređaja u skladu s podacima koje prikazuje uređaj. Izdvojeni podaci mogu se usporediti sa samim uređajem ili logičkim izvješćem, ovisno o tome što se traži i što je poželjno. Rukovanje originalnim uređajem može izmijeniti samo dokaz.
- **Korištenje više alata i uspoređivanje rezultata** – Koriste se različiti alati te se rezultati uspoređuju. Poboljšava točnost.
- **Upotreba hash vrijednosti** – Sve slikovne datoteke trebaju biti zaštićene, tj. na neki način kriptirane nakon izvlačenja, kako bi podaci ostali nepromijenjeni. Ako je ekstrakcija datotečnog sustava podržana, ispitivač izvlači datotečni sustav i izračunava zaštite za izvađene datoteke. Kasnije se svaka pojedinačno izvađena zaštićena datoteka izračunava i provjerava prema izvornoj vrijednosti kako bi se provjerila njegova cjelovitost. Svako odstupanje kod hash vrijednosti mora biti objašnjeno, [9].

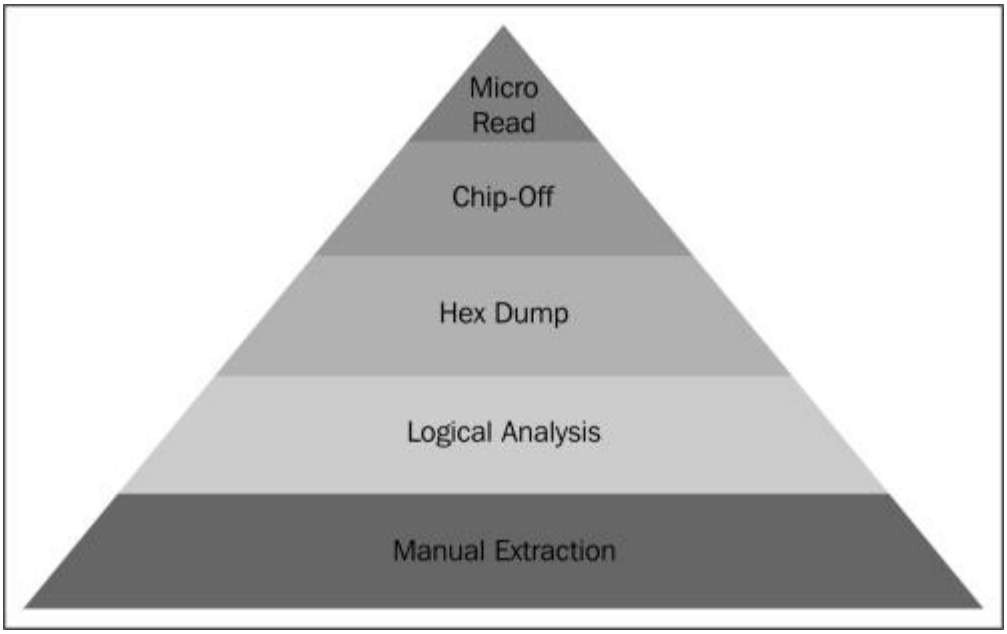
Nakon faze provjere slijedi faza dokumenta i izvješćivanja (engl. *Document and reporting*) kod koje je forenzični ispitivač dužan dokumentirati postupak ekstrakcije u obliku suvremenih bilješki koje se odnose na ono što je učinjeno tijekom pregleda uređaja. Nakon što ispitivač dovrši istragu, rezultati moraju proći kroz neki oblik recenzija kako bi provjerili jesu li u redu i da je istraga završena. Bilješke ispitivača i dokumentacija mogu uključivati informacije kao što su:

- Datum i vrijeme početka ispitivanja
- Fizičko stanje uređaja
- Fotografije uređaja i pojedinačnih komponenti
- Status uređaja kada je primljen (uključen, isključen)
- Model uređaja
- Alati koji se koriste za izvlačenje
- Alati za ispitivanje
- Podaci koji su pronađeni tijekom ispitivanja, [10]

Zatim slijedi faza prezentacije (engl. *Presentation*) koja osigurava jasno prezentiranje podataka bilo kojem ispitivaču ili sudu. Važno je izraditi forenzičko izvješće o podacima koji su izvađeni iz mobilnog uređaja tijekom ekstrakcije ili analize. To može uključivati podatke u papirnatom ili elektroničkom obliku. Rezultati istrage trebaju biti jasni, sažeti i ponovljivi. Analiza vremenske linije i značajke koje nude mnogi komercijalni alati za forenzičku analizu, mogu pomoći u izvještavanju i objašnjavanju nalaza na više mobilnih uređaja, [8].

Zadnja faza je faza arhiviranja (engl. *Archiving*). Očuvanje podataka iz mobilnih uređaja važan je dio cjelokupnog procesa ekstrakcije podataka. Također je važno da se podaci čuvaju u upotrebljivom obliku za sudski proces koji je u tijeku, [10].

Ekstrakcija podataka s mobilnog uređaja uglavnom ovisi o veličini i količini podataka koju istraživač želi izvući. Onim najlakšim i najjednostavnijim metodama dobiva se najmanje podataka i najmanja efikasnost, ali su najbrže jer nema kompliciranih zadataka. U usporedbi s laganim metodama, kompleksnije metode daju  najveću efikasnost, tj. najviše podataka, ali je cijeli postupak vrlo kompliciran i dugotrajan i zahtjeva posebne uvjete u kojima se mora obavljati te skupu opremu i posebno kvalificirano osoblje. Upravo zbog tih svih zahtjeva, kompleksnije metode se koriste za tajne službe, vojsku i policiju. Na slici 2 bit će prikazana piramida koja pokazuje ovisnost brzine ekstrakcije podataka i količine izvučenih podataka, [7].




**Slika 3:** Piramida ovisnosti brzine kvarenja i količine ekstrahiranih podataka, [1]

Na slici je prikazana piramida kod koje se glavne metode ekstrakcije mogu podijeliti u dva dijela. Prvi dio obuhvaća sve metode kod kojih nije potreban dodatni hardver ni softver. Također uključuju minimalno osposobljavanje ili osposobljavanje nije potrebno za izvedbu ekstrakcije. Drugi dio obuhvaća metode koje zahtijevaju dodatan hardver, i za te metode je potrebno duže osposobljavanje istražitelja, [1].

Polazeći od dna piramide i radeći prema gore, metode i alati postaju tehnički složeniji i kompleksniji i zahtijevaju dulje vrijeme analize. Postoje prednosti i nedostaci za obavljanje analize na svakom sloju na koje bi forenzični ispitivač trebao obratiti pozornost. S obzirom na te prednosti i nedostatke, alati za ispitivanje se koriste na različite načine. Dokazi koji se

prikupljaju mogu se potpuno uništiti ako se određena metoda ili alat ne koriste pravilno. Svaki forenzički alat se može svrstati u jednu od pet razina prikazanih na piramidi, [9].

## 3.1. Ručna, logička i datotečna ekstrakcija podataka

### 3.1.1. Ručna ekstrakcija

Ručna ekstrakcija podataka pregledava podatkovni sadržaj pohranjen na mobilnom uređaju te zahtijeva manipulaciju fizičkih komponenti (tipkovnica, zaslon osjetljiv na dodir). Vrši se preko sučelja mobilnog uređaja gdje se izvodi forenzička analiza. Istražitelj procesa pregledava sadržaj mobilnog uređaja, njegove postavke i sav sadržaj koji je dostupan i običnom korisniku, koristeći navigaciju kroz datotečni sustav koji mobilni uređaj pruža svojim grafičkim sučeljem. Uključuje jednostavno pretraživanje i pregledavanje podataka na uređaju izravno pomoću tipkovnice ili zaslona osjetljivog na dodir, [1].

Prilikom prikaza nove informacije na ekranu, uzima se slika ekrana pomoću stranog fotoaparata. Tim postupkom se sprema sadržaj ekrana na drugom, vanjskom uređaju, kako bi se mogao iskoristiti u potencijalnom sudskom procesu. Ručna ekstrakcija se smatra najjednostavnijom vrstom ekstrakcije podataka iz mobilnih uređaja. Ne zahtijeva dodatna stručna znanja za upravljanje procesom ekstrakcije. Može se provoditi samo ako je mobilni uređaj otključan jer u protivnom istraživač ne može doći do željenog sadržaja. Moguće ju je provesti na svim vrstama mobilnih uređaja, uz uvjet da su otključani, i nisu potrebni dodatni kablovi, [11].

Prednost ručne ekstrakcije je ta da ju je moguće upotrijebiti gotovo na svakom mobilnom uređaju, od kojeg god proizvođača on bio. Glavna prednost je jednostavnost uporabe, tj. rukovanja jer ne zahtijeva dodatno osposobljavanje, [9].

Nedostatak kod ručne ekstrakcije podataka je taj što se ne može pristupiti svim podacima, a to za bitnije forenzičke istrage nije prihvatljivo. Podložna je problemima koji se javljaju prilikom očitavanja podataka jer proces nije dovoljno usklađen i adekvatan. Također, nedostatak su strani jezici koji mogu biti ne razumljivi za ispitivača koji provodi istragu, a razlog tomu je što ručna ekstrakcija ne pruža platformu na svim jezicima. Problem može također biti i neispravan ili oštećen mobilni uređaj ili tipka, jer ako postoji oštećenje postoji mogućnost da određene funkcije neće raditi i forenzičko ispitivanje neće biti moguće. Nedostatak je također što se ručnom ekstrakcijom ne može očuvati integritet uređaja i ne može se pristupiti obrisanim podacima, [9].

### 3.1.2. Logička ekstrakcija

Logička ekstrakcija uključuje povezivanje mobilnog uređaja s forenzičnim dodatnim hardverom ili forenzičnom radnom stanicom putem USB (engl. *Universal Serial Bus*) kabela,

RJ-45 (engl. *Registered Jack 45*) kabela, infracrvene tehnologije ili *Bluetooth* tehnologijom. To je vrsta ekstrakcije koja kopira podatke s logičkih jedinica za pohranu na mobilni uređaj. Nakon spajanja mobilnog uređaja, računalo pokreće naredbu i šalje je prema uređaju, a zatim naredba biva interpretirana od strane procesora uređaja. Nakon toga traženi podaci primaju se iz memorije uređaja i šalju natrag prema forenzičkoj radnoj stanici. Kasnije, ako ispitivač želi može pregledati podatke, [10].

Većina trenutno dostupnih forenzičkih alata radi na ovoj razini ekstrakcije podataka. Logička ekstrakcija se uglavnom odvija preko tvorničkog sučelja koje je ugradio proizvođač, a služi za sinkronizaciju podataka s osobnim računalom što je u većini slučajeva USB (engl. *Universal Serial Bus*) kabel, [12].

Logička ekstrakcija ne zauzima veliki prostor za pohranu prikupljenih podataka. U slučaju da nema korisnih podataka za sudski proces, zbog kojeg se ujedno i vrši analiza mobilnog uređaja, prelazi se na druge vrste ekstrakcija, [6].

Prednosti logičke ekstrakcije su brzina, tj. proces ekstrakcije ne traje dugo. Nije kompliciran za korištenje, nudi ekstrakciju različitih informacija, veći broj nego što je to kod ručne ekstrakcije. Podržava velik broj stranih jezika, tako da tu predstavlja olakšanje i poboljšanje u odnosu na ručnu ekstrakciju. Ima mogućnost ponavljanja što je od velike važnosti, [12].

Jedan od nedostataka logičke ekstrakcije je da može izmijeniti ili preskočiti određene podatke (npr. ne pročitani SMS). Za razliku od ručne ekstrakcije, ovdje se podrazumijeva veliki broj kablova. Logička ekstrakcija ne prikuplja podatke koji su izbrisani jer se takvi podaci ne prikazuju u mapama mobilnih uređaja, odnosno logička ekstrakcija ne prikuplja podatke s dijela memorije koji nije dodijeljen. Također, nije u mogućnosti zaobići zaključan ili zaštićen uređaj, [9].

### 3.1.3. Datotečna ekstrakcija

U odnosu na količinu prikupljenih podataka, između logičke i fizičke nalazi se datotečna ekstrakcija. Ona obuhvaća sve datoteke koje su pohranjene na određenoj lokaciji u mobilnom uređaju koje se smatraju zauzetima. Njome je moguće vidjeti raspored sustava datoteka mobilnog uređaja, povijest Internet preglednika, koje sve aplikacije su instalirane na uređaju, SMS poruke i ostale zapise. Datotečna ekstrakcija do podataka u mobilnom uređaju dolazi putem SQL naredbi. Pri zapisivanju podataka na memoriju samog uređaja, adresa memorije smatrat će se zauzetom sve dok korisnik mobilnog uređaja ne odluči izbrisati podatak. Ako se korisnik odluči na brisanje, to neće značiti brisanje podatka već njegove adrese. Datotečna ekstrakcija ne može doći do podataka ako je prethodno memorija formatirana, [13].

Postupak forenzičke analize datoteka ima za cilj prepoznati vrstu sadržaja datoteke, tj. program, bazu podataka, tekst, sliku, audio, video. Zatim, u datoteci je potrebno pronaći i ekstrahirati metapodatke, one koji opisuju datoteku, autora, vrijeme nastanka i mjesto nastanka. U datoteci je se također moraju pronaći ostale „nevidljive“ informacije kao što su obrisani sadržaji (npr. za vrijeme uređivanja teksta), privremeni sadržaji (npr. indeksi, tablice, itd) te ostatke prijašnjih datoteka (koje su zauzimale isti prostor), [14]. Datoteke se mogu jednostavno kopirati korištenjem alata poput „cp“ ili „mv“. Moguće je kopirati čitave datoteke ili samo dijelove. U slučaju da se kopiraju samo dijelovi, kopiraju se samo blokovi bajta koji su se promijenili, [15].

## 3.2. Fizička, JTAG i chip-off ekstrakcija podataka

Sljedeće tri metode ekstrakcije podataka su zahtjevnije od prethodnih. One podrazumijevaju veća ulaganja u hardver i softver, veću razinu stručnog znanja, obuke itd.

### 3.2.1. Fizička ekstrakcija

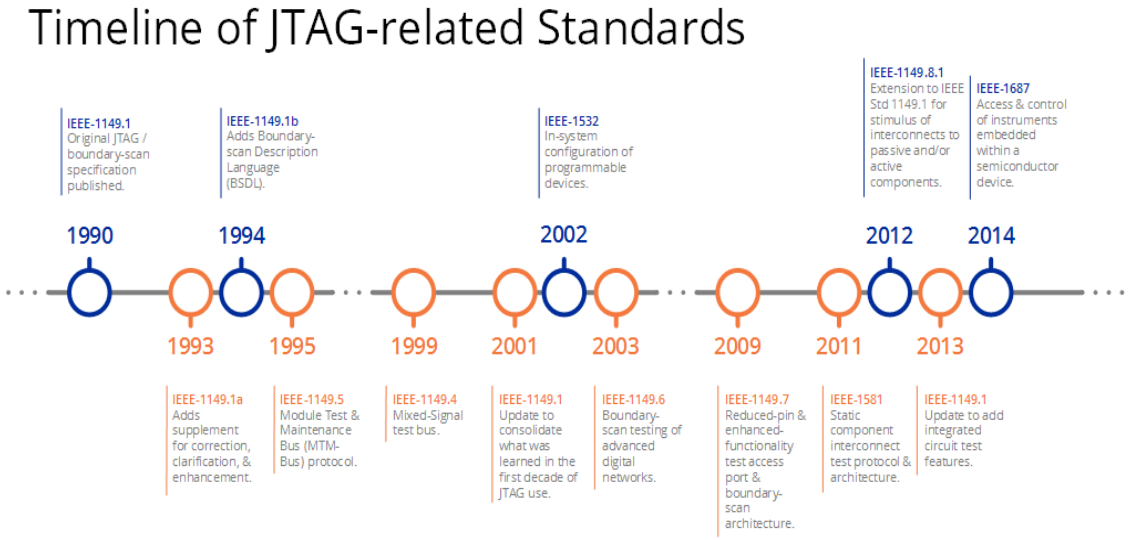
Fizička ekstrakcija postiže se spajanjem uređaja s forenzičnom radnom stanicom i guranjem nepotpisanog koda ili pokretačkog sustava za podizanje sustava u mobilni uređaj i upućivanje mobilnog uređaja da izbaci memoriju s mobilnog uređaja na računalo. Budući da je rezultirajuća slika osnovna slika u binarnom formatu, potrebna je tehnička stručnost za analizu. Proces je jeftin, pruža više podataka ispitivačima i omogućuje oporavak izbrisanih datoteka s uređaja koji nije raspodijeljen na većini uređaja, [14].

Ukoliko je potrebna kompletna forenzička analiza, upotrebljava se fizička ekstrakcija. Fizička ekstrakcija koristi napredne metode izdvajanja fizičke bit-po-bit slike *flash* memorije mobilnog uređaja. Prednost ove tehnike u odnosu na logičku ekstrakciju je što se kopira ne samo dodijeljeni, nego i nedodijeljeni prostor memorije, tj. uz postojeće podatke kopiraju se i oni izbrisani i odbačeni, [16].

Fizička ekstrakcija je jedna od najzahtjevnijih metoda dobave podataka jer je potrebno zaobilaziti sigurnosne mehanizme koji omogućuju samo uređaju na kojem je medij pohranjen manipulaciju podacima. To je osnovni razlog zašto je nedostupna u besplatnim alatima, a dostupna je u profesionalnim alatima te zahtjeva veliki stupanj tehničkog znanja. Vrši se preko USB (engl. *Universal Serial Bus*) kabela ili neke druge veze s uređajem, [6].

## 3.2.2. Ekstrakcija JTAG metodom

JTAG (engl. *Joint Test Action Group*) je udruga elektroničkih industrija osnovana 1985. godine radi razvijanja metode provjere dizajna i ispitivanja tiskanih pločica nakon izrade. Utvrdili su poseban ulaz za otklanjanje pogrešaka vezanih uz procesore koji ne zahtijevaju pristup sistemskim adresama i podatkovnim sabirnicama čiji je naziv IEEE 1149.1, [17]. Nekoliko godina kasnije, 1993. godine uvedena je nova revizija standarda pod nazivom 1149.1a, koja je razjašnjavala, ispravila i poboljšala originalnu verziju. Dodatna dopuna, 1149.1b, obavljena je 1994. godine kako bi dodala standardni jezik za opisivanje graničnog jezika, postavljajući način brzog, automatiziranog razvoja testova i potičući kontinuirano usvajanje velikih proizvođača elektronike diljem svijeta. Pouke koje su naučene iz svih verzija su usvojene u jedan osnovni standard 2001. godine u IEEE-1149.1-2001. Kako su nove aplikacije JTAG-a otkrivene, razvijeni su novi standardi kako bi se proširile mogućnosti JTAG-a. Standardi kao što su IEEE-1149.5 koji je služio za testiranje i održavanje i IEEE-1149.4 koji je služio za ispitivanje mješovitog signala, 1999. godine bili su zadovoljeni s niskim stopama adaptacije i nisu bili toliko korišteni. IEEE-1149.6 standard je uveden 2003. godine i postao je standard mnogi ICT-ovcima. Na kraju IEEE-1149.7 objavljen je 2009. godine kako bi se riješio potreba za JTAG sustavima s malim brojem pinova te je sada standard u gotovo svakom mikrokontroleru, [18].




**Slika 4:** Razvoj JTAG-a, [18]

JTAG implementira standarde za instrumente na čipu u automatizaciji elektroničkog dizajna kao komplementarni alat za digitalnu simulaciju. Određuje upotrebu posebnog pogrešnog porta koji implementira sučelje za serijski komunikacijski sustav za nisko-nadzemni pristup bez potrebe za izravnim vanjskim pristupom adresi sustava i podatkovnim sabirnicama. Sučelje se povezuje s priključkom za testiranje na čipu (TAP) koji implementira protokol za pristup skupu testnih registara koji prikazuju razine logičkih čipova i mogućnosti

uređaja različitih dijelova. Standarde JTAG-a produžili su mnogi proizvođači poluvodičkih čipova sa specijaliziranim izvedbama kako bi pružili specifične značajke dobavljača, [19].

Način ekstrakcije podataka JTAG metodom je ne-destruktivna metoda ekstrakcije podataka iz uređaja koja se koristi kada tradicionalna forenzika zakaže. JTAG se koristi kada je uređaj zaključan uzorkom ili lozinkom, kada je utor za prijenos podataka nedostupan ili kada je uređaj fizički oštećen ili djelomično uništen. Ova razina ekstrakcije pristupačna je i prikladna za uporabu za razne osobe, uključujući policiju, odvjetnike, fizičke osobe i institucije, [19]. U većini slučajeva kako bi se ekstrakcija provela potrebno je ukloniti bateriju mobilnog uređaja kako bi se sam uređaj mogao rastaviti te kako bi se moglo pristupiti procesoru, a za tu radnju potrebno je koristiti vanjsko napajanje. Kako bi se omogućilo serijsko sučelje, potrebno je fizički se spojiti na pinove procesora. Pinovi služe za stvaranje nove forenzičke slike na kojoj se temelji daljnja forenzička analiza, [16].

JTAG sučelje, zajednički poznato kao TAP (engl. *Test Access Port*) koristi sljedeće signale koji podržavaju rad graničnog skeniranja:

- TCK (engl. *Test Clock*) – taj signal sinkronizira rad unutrašnjih operacija uređaja
- TMS (engl. *Test Mode Select*) – ovaj se uzorak uzorkuje na usponu ruba TCK da bi se odredilo sljedeće stanje
- TDI (engl. *Test Data In*) – predstavlja podatke koji se prebacuju u logiku uređaja za testiranje ili programiranje. Uzorkuje se na uzlaznom rubu TCK.
- TDO (engl. *Test Data Out*) – predstavlja podatak koji se prebacuje iz logike programiranja ili programiranja uređaja i vrijedi na padajućem rubu TCK.
- TRST (engl. *Test Reset*) – dodatni pin koji, ako je dostupan, može resetirati kontroler, [19]

JTAG metoda ima mnogo prednosti od kojih treba izdvojiti pristup podacima koji su izbrisani. Također, omogućuje ekstrakciju skrivenih podataka u uređaju što je vrlo česti slučaj kod kriminalaca koji pokušavaju prikriti trag zločina. Najveća prednost je korištenje vlastitih registara koja minimalizira mogućnost korumpiranja podataka tijekom procesa ekstrakcije. Zaobilazi lozinke, uzorke i sve sustave zaštite na razini grafičkog sučelja uređaja, [17].

Kao što posjeduje velike prednosti, tako ima i mnoge nedostatke. Problem je što zahtijeva pretvorbu podataka, što može odužiti proces ekstrakcije. Neki alati su proizašli iz hakerskih zajednica što otvara mogućnost zlouporabe istih. Ograničena je određeni broj proizvođača koji pružaju podršku za ovu metodu i nije ista za svaki uređaj. Zahtjevna je metoda jer je potrebna dodatna oprema i veliki broj kablova. Postupak je spor jer je potrebno pažljivo rukovati s procesorom i pinovima, [9].

### 3.2.3. Chip-off ekstrakcija

*Chip-off* je metoda ekstrakcije podataka kod koje se prikupljanje podataka vrši direktno s memorijskog čipa uređaja. Na ovoj razini, čip se fizički uklanja iz uređaja i čitač čipa ili drugi uređaj koristi se za izdvajanje podataka pohranjenih na njemu. Ova metoda tehnički je zahtjevnija jer se u mobilnim uređajima koriste brojni čipovi. Proces je skup i zahtijeva znanje na razini hardvera jer uključuje de-lemljenje i zagrijavanje memorijskog čipa, [20]. Osposobljavanje je potrebno za uspješno izvlačenje chip-off ekstrakcije. Nepravilni postupci mogu oštetiti memorijski čip i učiniti sve podatke nečitljivima. Kad je moguće, preporučuje se da se druge razine ekstrakcije pokušaju prije chip-off metode jer ova metoda je destruktivna u prirodi. Također, informacije koje izlaze iz memorije su u osnovnom formatu i moraju se analizirati, dekodirati i tumačiti. Chip-off metoda je poželjnija u situacijama u kojima je važno očuvati stanje memorije točno onako kako postoji na uređaju. Također je jedina opcija kada je uređaj oštećen, ali memorijski čip je netaknut. Uključuje fizičko uklanjanje *flash* memorije s uređaja nad kojim se vrši forenzička analiza. Nakon uklanjanja *flash* memorije, počinje ekstrakcija slike uređaja za što se koristi čitač memorije uređaja. Za svaku vrstu memorije koriste se drugi upravljački programi, koji već postoje ili se na novo programiraju što može biti vrlo zahtjevno, [1].

Čipovi na uređaju često se čitaju pomoću JTAG (engl. *Joint Test Action Group*) metode. JTAG metoda uključuje povezivanje s testnim pristupnim priključcima (TAP-ovima) na uređaju i upućivanje procesora na prijenos neobrađenih podataka pohranjenih na memorijskim čipovima, [20].

Prednosti *chip-off* ekstrakcije podataka su što može dobaviti sve vrste podataka iz memorije uređaja i što radi sa svim vrstama memorije. Također zaobilazni sve sigurnosne mehanizme osim enkripcije podataka, ali i to se može riješiti tako da se direktno iz memorije sazna enkripcijski ključ. Pruža bolji prikaz događanja u samom uređaju. Zadržava integritet podataka i pruža mogućnost ekstrakcije podataka iz oštećenog uređaja, [9].

Kod *chip-off* ekstrakcije podaci ne moraju biti blizu jedni drugima što može otežati i usporiti proces ekstrakcije. Također je problem što se može oštetiti čip prilikom ekstrakcije i podaci mogu biti izgubljeni. Zahtijeva velika ulaganja u opremu, za razliku od JTAG metode. U usporedbi s JTAG metodom, *chip-off* se čini lošijim izborom zato što nije moguće probiti zaštitu mobilnog uređaja, [20].

## 3.3. Ostale metode ekstrakcije

### 3.3.1. Flasher Box

*Flasher Box* (FB) je jedna od metoda ekstrakcija podataka koja se koristi ako prijašnje navedene metode nisu dostupne, tj. ukoliko se traži jeftinije rješenje. Alternativno je rješenje forenzičke analize koje može pomoći u prevladavanju ograničenja komercijalnih alata u pitanju troškova. Kutije su povezane s računalom preko USB-a i mobilnog uređaja koji se analiziraju putem posebnih kabela koji na kutiji obično implementiraju standardni RJ-45 (engl. *Registered Jack 45*) utor. Na strani mobilnog uređaja kabeli mogu koristiti JTAG kontakte ili servisne priključke. Kao i kod komercijalnih alata potreban je niz posebnih kabela, ali za razliku od njih, oni se mogu kupiti po potrebi s različitih internetskih prodajnih mjesta. Ovi su uređaji izvorno razvijeni za pružatelje mobilnih uređaja i trgovine, uglavnom na azijskim i ruskim tržištima. Neke od njihovih sposobnosti za koje se koriste nisu sasvim legalne. Oni mogu otključati mobilne uređaje koji su ograničeni od strane operatera, uređaje koji imaju SIM (eng. *Subscriber Identity Module*) ograničenja i starije uređaje s IMEI ograničenjima. Najvažnije za forenzičku analizu je sposobnost čitanja *flash* memorije mobilnog uređaja na fizičkoj razini, stvarajući ono što se naziva „fizička“ kopija, koja može imati najpotpuniji dokaz, uključujući i izbrisani sadržaj, [21].

Prednosti *Flasher Box*-a su da potpuno i pouzdano omogućuje razumijevanje svake aktivnosti kroz ekstrakciju i analizu *hex-dump*-a. Izbrisani podaci iz mobilnog uređaja mogu se dohvatiti i iščitati. Nad oštećenim uređajima i uređajima bez baterije se također može provesti forenzička analiza. Velika prednost je cijena, koja je neusporedivo manja u odnosu na komercijalne metode ekstrakcije, [22].

Veliki nedostatak ove metode je opasnost za integritet podataka zato što ova metoda nije bila zamišljena kao sredstvo za forenzičku analizu. Neke izvedbe su tehnički zahtjevne i komplicirane za uporabu. Problem je i taj što nije moguće utvrditi integritet podataka nakon ekstrakcije podataka. Ujedno to što je cijena mala predstavlja i sigurnosni problem jer je tako lako dostupna običnim osobama koje ga mogu nabaviti, [22].

### 3.3.2. Micro Read

To je postupak koji uključuje ručno gledanje i tumačenje podataka vidljivih na memorijskom čipu. Ispitivač koristi elektronski mikroskop i analizira fizičke ulaze na čip, a zatim prevodi status vrata na 0 i 1 kako bi se odredili rezultirajući ASCII znakovi. Cijeli proces je dugotrajan i skup i zahtijeva veliko znanje i obuku na flash memoriji i datotečnom sustavu. Također, metoda je jako spora i zahtijeva složenu tehničku opremu (elektronski mikroskop), te uz to je potreban određen tim stručnjaka kako bi se provela. Zbog ekstremnih tehničkih zadataka koji su uključeni u mikročitanje, bilo bi pokušano samo za slučajeve

visokog profila koji su ekvivalentni krizi nacionalne sigurnosti nakon što su iscrpljene sve druge tehnike ekstrakcije. Proces se rijetko izvodi i nije dobro dokumentiran u ovom trenutku, a isto tako, trenutno ne postoje komercijalni alati za izvođenje mikročitanja. *Micro Read* također zahtijeva visoku razinu poznavanja građe uređaja koji se pregledava. Ovo je metoda koja je napuštena jer su tijekom vremena metode nižih razina poboljšane te su se one počele više koristiti i smanjile su potrebu za korištenjem ove metode. Dakle, metoda je dosta zastarjela i loša je, ali prednost joj je da može izdvojiti sve podatke iz memorije uređaja i daje najbolju sliku o tome što se događa u uređaju, [1].

### 3.3.3. Ekstrakcija podataka uređaja s njegove sigurne kopije

Ova metoda ekstrakcije podataka je jedna od najmanje zastupljenih u IK okruženju. Sigurna kopija uređaja nalazi se u računalstvu u oblaku (engl. *Cloud Computing*). Spremišta podataka u oblaku predstavljaju virtualni zlatni rudnik za potencijalne dokaze u forenzičkoj istrazi. Jedni od najpoznatijih spremišta podataka u oblaku su *Dropbox*, *Google Drive, iCloud Drive, Facebook, Twitter, Instagram,* a spremište podataka je i e-mail poslužitelj koji koristi IMAP protokol, kao što su *AOL*, *Google*, *Yahoo* itd. Sigurna kopija predstavlja kopiju uređaja i njegovih podataka koji se pohranjuju na oblak, a iz te sigurne kopije je potrebno vršiti ekstrakciju, [23].

Problem predstavlja virtualizirano okruženje računalstva u oblaku u kojemu se do podataka dolazi na puno teži način nego je to slučaj kod klasične ekstrakcije podataka. Problem može predstavljati i to što svi uređaji i udaljeni serveri nisu na istim lokacijama, pa je do podataka doći teže. Za uspješnu ekstrakciju potrebno je poznavati i mrežni zapis, kojim se utvrđuje kada je podatak stigao na *Cloud*, a ne samo podatke. Problem predstavlja i to što nema komercijalnih alata kojima bi se omogućila ekstrakcija podataka s *Cloud*-a. Prednost ove vrste pohrane podataka je sigurnost i tajnost lokacije podataka, a što se tiče ekstrakcije podataka, prednost je što se može doći do podataka nekog mobilnog uređaja bez poznavanja njegove lokacije i stanja, [23].

# 4. Svrha i korištenje alata forenzičke analize

Forenzički alati su u stalnom razvoju kako bi pružili prikladan način ekstrahiranja određenih podataka s različitih mobilnih uređaja, tipično logički putem kabela, infracrvene mreže i Bluetooth veze ili fizički putem kabela ili JTAG-a. Svi komercijalni alati funkcioniraju na sličan način, a to je: slanje naredbi mobilnom uređaju i snimanje odgovora koji sadrže informacije pohranjene u memoriji uređaja. Informacije koje se mogu ekstrahirati ovim metodama ovise o mehanizmu veza i modelu uređaja, [24].

## 4.1. Svrha alata

Alati se koriste za analizu digitalnih podataka i često za pronalaženje dokaza da je netko počinio ili nije počinio zločin. Budući da se alat za forenzičku analizu može predstavljati kao dokaz u sudskom procesu, mora ispunjavati određene zakonske zahtjeve, [25]. Alati su namijenjeni za pomoć osoblju za sigurnost, policiji i pravnim istražiteljima u prikupljanju, čuvanju i ispitivanju podataka koji se odnose na neprikladne i ilegalne aktivnosti poput zloupotrebe e-pošte i Interneta, prijevare, neovlaštenog otkrivanja korporativnih informacija, krađe intelektualnog vlasništva itd. Digitalni forenzički alati obično nude tri glavne mogućnosti: stjecanje, skupljanje i očuvanje. Za izbor najboljeg alata uključuju se sljedeće funkcionalnosti: potpuna povezanost sa zakonom, sposobnost čuvanja relevantnih podataka, integracija i mogućnost upravljanja predmetima, [26].

Logični sustavi za ekstrakciju podataka stupaju u interakciju s operacijskim sustavom uređaja za tu ekstrakciju podataka. Kao takav, postoje ograničenja za ekstrakciju informacija, a dostupne su samo informacije relevantne za operativni sustav. Informacije koje su potencijalno relevantne u forenzičkoj istrazi možda neće biti ekstrahirane; informacije kao što su izbrisane stavke neće se ekstrahirati. Mobilni uređaji uglavnom imaju podatke koji se gotovo uvijek mogu ekstrahirati , kao što su telefonski imenik, zapisnici poziva, SMS-i i fotografije, no dodatne informacije nisu zajamčene. Ograničenje na ove oblike aplikacija je da se oslanja na pretpostavku da se desktop aplikacija i istražitelj pretpostavljaju da logika telefona ne mijenja druge dijelove memorije telefona. Međutim, ova se pretpostavka ne može provjeriti bez izvornog koda i shema softvera i hardvera, koji su rijetko, ako i ikad, javno dostupni, [24].

Forenzički alati mogu se također podijeliti na hardverske i softverske alate, [27]:

- **Hardverski alati**: Dizajnirani su prvenstveno za ispitivanja uređaja za pohranu i nastoje zadržati sumnjive uređaje kako bi se očuvala cjelovitost dokaza.
- **Softverski alati**: Većina softverskih alata, tj. aplikacija je višenamjenska i može obavljati različite zadatke u jednoj aplikaciji. Neki od njih mogu obraditi više uređaja istovremeno ili upravljati različitim operacijskim sustavima. Softverski alati mogu steći i analizirati digitalne dokaze prikupljene sa sumnjivog uređaja.

## 4.2. Uporaba alata tijekom faza forenzičke analize

Općenito, cilj digitalne forenzičke analize je identificirati digitalne dokaze za istragu. Istraga tipično koristi i fizičke i digitalne dokaze sa znanstvenom metodom kako bi se izveli ispravni zaključci. Kao što je u prethodnom poglavlju objašnjeno, digitalna forenzika se dijeli u 3 glavne faze: ekstrakcija, analiza i prezentacija, [25].

Faza akvizicije ili ekstrakcije štedi stanje digitalnog sustava tako da ga se kasnije može analizirati. Neki od primjera su analogno uzimanje fotografija, otisaka prstiju itd. Kao i u fizičkom svijetu, nepoznato je koji će se podaci koristiti kao digitalni dokaz, pa je cilj ove faze spasiti sve digitalne vrijednosti. Alati koji se koriste u ovoj fazi su namijenjeni za kopiranje podataka s osumnjičenikovog uređaja za pohranu na pouzdani uređaj. Ovi alati moraju modificirati osumnjičeni uređaj što je manje moguće i kopirati sve podatke, [25].

Faza analize preuzima stečene podatke i pregledava ih kako bi identificirala dijelove dokaza. U ovoj fazi se traže tri glavne vrste dokaza, a to su: dokazi koji podupiru zadanu teoriju, iskustvo dokaza, tj. ono što proturječi određenoj teoriji i dokazi o neovlaštenim prijelazima, tj. oni koji se ne mogu povezati s bilo kojom teorijom. Ova faza uključuje ispitivanje sadržaja datoteke i mape te oporavak izbrisanih sadržaja. Alati u ovoj fazi analizirat će datotečni sustav za popis imenika i imena izbrisanih datoteka, izvođenje izbrisanih datoteka i prikazivanje podataka u najkorisnijem obliku. Ova faza treba koristiti točnu kopiju izvornika, što se može provjeriti izračunavanjem kontrolnog zbroja MD5 (engl. *Checksum*). Važno je da forenzički alati u ovoj fazi pokazuju sve podatke, [25].

Faza prezentacije temelji se na politici i zakonu, u odnosu na prethodne faze u kojima dominiraju tehnička pitanja. Ova faza predstavlja zaključke i odgovarajuće dokaze iz istrage. Forenzički alati u ovoj fazi nemaju aktivnu ulogu, već se, zahvaljujući njima i njihovom prikupljanju podataka, analiziraju ti prikupljeni podaci, [25].

## 4.3. Zahtjevi alata za forenzičku analizu

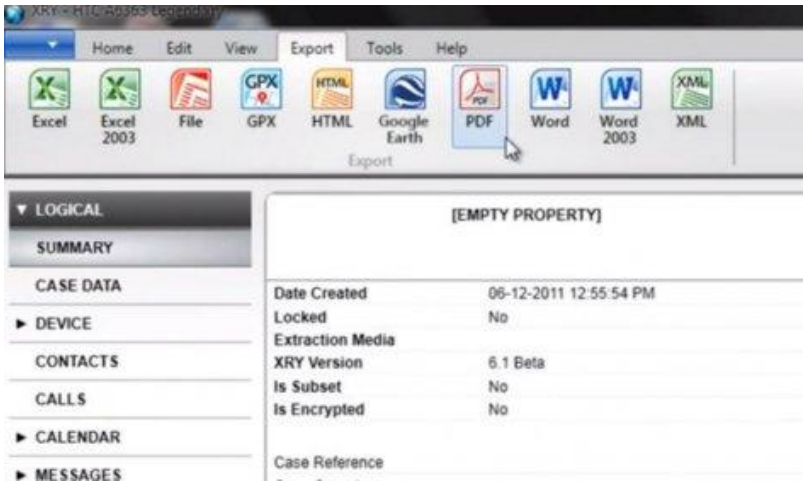
1. **Upotreba:** Riješiti problem složenosti (podatke u najmanjem obliku teško je analizirati) tako da alati moraju dati podatke na sloju apstrakcije i formatu koji pomaže istražitelju. Minimalno, istražitelj mora imati pristup slojevima apstrakcije koji su definirani kao granični slojevi.
2. **Opsežnost:** Kako bi se utvrdili i dokazni i poticajni dokazi, istražitelj mora imati pristup svim izlaznim podacima u danom sloju apstrakcije.
3. **Točnost:** Da bi se riješio problem pogreške (slojevi apstrakcije uvode pogreške u konačni proizvod) alati moraju osigurati da su izlazni podaci točni i da se izračunava margina pogreške kako bi se rezultati mogli interpretirati na odgovarajući način.
4. **Determinističnost:** Da bi se osigurala točnost alata, uvijek se mora proizvoditi isti izlaz kada se daje skup pravila i ulaznih podataka.

5. **Verifikacija:** Kako bi se osigurala točnost alata, treba biti u mogućnosti provjeriti rezultate. To se može obaviti ručno ili pomoću drugog i nezavisnog alata. Stoga je potrebno da se izlaz može provjeriti.
6. ***Read-Only*:** Iako ovaj zahtjev nije nužan, očito je visoko preporučena značajka. Budući da priroda digitalnih medija omogućuje jednostavnu kopiju podataka, kopije se mogu napraviti prije korištenja alata koji mijenja izvornik. Za potvrdu rezultata, što je uvjet, potrebna je kopija unosa, [28].

## 4.4. Popis najčešće korištenih alata

Postoji nekoliko komercijalnih forenzičkih alata specifično dizajniranih za prikupljanje podataka s mobilnih uređaja. U ovom odlomku će se opisati neki od najpopularnijih:

- **MicroSystemation XRY**: Jedan je od vodećih alata na tržištu u ekstrakciji podataka s mobilnih uređaja. XRY je digitalni forenzički alat za forenziku mobilnih uređaja, osmišljen od strane švedske tvrtke Micro Systemation koja se bavi analizom i oporavkom podataka s mobilnih uređaja. Sastoji se od hardverskog uređaja koji omogućuje povezivanje telefona s računalom i softver za izdvajanje podataka. XRY je dizajniran tako da oporavlja sadržaj uređaja na forenzički način tako da se korisnik može osloniti na sadržaj podataka. Tipično se koristi u građanskim/krivičnim istraživanjima, obavještajnim operacijama, usklađenosti podataka i slučajevima elektroničkog otkrivanja. Omogućava i logičke (izravnu komunikaciju s operativnim sustavom) i fizičke preglede (zaobilazeći operacijski sustav). Logički oporavak podataka je bolje podržan na više uređaja, ali zato fizički nudi mogućnost povratka više izbrisanih informacija kao što su tekstualne poruke SMS poruke, slike, zapisi o pozivima itd, [29].




**Slika 5**: MicroSystemation XRY, [30]

- **Cellebrite UFED**: UFED (Universal Forensic Extraction Device) je samostalni, prijenosni uređaj za logičko stjecanje podataka s mobilnih uređaja. Dizajniran je u Izraelu od strane tvrtke Cellebrite. UFED može izdvojiti, dešifrirati i analizirati sve vrste multimedijskih sadržaja, SMS i MMS poruke, pozivne brojeve, elektronske serijske brojeve (engl. *Electronic Serial Numbers*, ESN), IMEI (engl. *International Mobile Equipment Identity*) i podatke o SIM lokaciji. Podržava sve mobilne protokole, a može se povezati i s različitim datotečnim sustavima operacijskih sustava kao što su iOS, Android OS, BlackBerry, Symbian, Windows Mobile i Palm. Podržava i fizičku i logičku ekstrakciju, a fizičkom omogućuje da se izbrisani podaci oporave, da dešifrira šifrirane podatke i dobije informacije iz mobilnih aplikacija zaštićenih zaporkom, kao što su Facebook, Skype, WhatsApp i lozinke spremljene u pregledniku, [31].


**Slika 6**: Cellebrite UFED, [31]

- **Logicube CellDEK**: Sustav dizajniran za prikupljanje podataka s mobilnih uređaja i drugih malih uređaja poput GPS prijamnika. CellDEK provodi logičku ekstrakciju podataka putem USB-a, infracrvene mreže i Bluetooth veze. Omogućuje jednostavnu identifikaciju mobilnih uređaja i PDA (engl. *Personal Digital Assistant*). Kada se identificira ciljani uređaj, omogućen je izbor povezivanja. Program za odabir „pametnih“ priključnica odabire odgovarajući priključak, a nakon što se izabere, bilježi sve pohranjene podatke putem te odabrane metode povezivanja. Izvodi ekstrakciju podataka kao što su vrijeme i datum poziva, serijski brojevi uređaja, birani brojevi, primljeni pozivi, imenik, SMS, kalendar itd, [32].

**Slika 7**: Logicube CellDEK , [32]

- **iXAM**: Sustav za forenzičku analizu koji je posebno dizajniran za Apple iPhone i Apple iPod Touch. IXAM dobiva podatke putem USB sučelja, ali ima punu fizičku

ekstrakciju podataka. Osigurava stjecanje mali broj uređaja od strane jednog proizvođača. Obično može oporaviti sljedeće podatke: informacije o uređaju i korisnicima (ESN, IMEI, SIM, popis poziva, SMS/MMS poruke, kontakte itd.), e-mail račune i informacije o web-u (e-mail, e-mail računi, internetski kolačići, internetska povijest, preuzimanja sadržaja itd.) i podatke o uređaju (slikovne, video i audio datoteke, lokacije na karti itd.), [33].


**Slika 8**: iXAM, [34]

- **MOBILedit! Forensic**: Još jedan alat za prikupljanje podataka logičkom ekstrakcijom. Ima sposobnost generiranja izvješća na bilo kojem jeziku. Sposobnost stvaranja određenih predložaka za određene funkcije također je funkcija MOBILedit! Forensic alata. Ti predlošci se mogu stvoriti u alatima kao što su MS Word i mnogi drugi uređivači teksta. MobilEdit! će pročitati te predloške i umetati u njega sve podatke prikupljene s uređaja. To znači da nema potrebe za unošenjem ili izvozom podataka sa SIM kartica ili uređaja, [35].


**Slika 9**: MOBILedit! Forensic, [36]

# 5. Izvori podataka terminalnih uređaja za potrebe forenzičke analize

Mobilni terminalni uređaji se razlikuju iz perspektive obnavljanja podataka i analize. Svojom povećanom funkcionalnošću i rastućim spremištima podataka, mobilni uređaji postaju analogni računalima s posebnim funkcijama (uglavnom kao kanal za komunikaciju i pristup Internetu). Održavanje svih različitih datotečnih sustava, formata podataka i izvora podataka na mobilnim uređajima trajni je izazov. Međutim, velika prednost mobilnih uređaja iz forenzičke perspektive je ta da oni mogu sadržavati izbrisane podatke čak i nakon što ih pojedinac pokuša prikazati nepovratnima. Osnovni razlog za to postojanje izbrisanih podataka na mobilnim uređajima je uporaba Flash memorijskih čipova za pohranu podataka. Flash memorija je fizički otporna od utjecaja visoke temperature i tlaka, što ju čini teže uništivom. Osim toga, Flash memorija ima ograničen broj zapisa i može se izbrisati samo dio po dio, a ne sve od jednom, a mobilni uređaji općenito čekaju da se dio ispuni prije brisanja podataka. Nadalje, mobilni uređaji upotrebljavaju algoritme za uravnoteženo korištenje Flash memorije. Kako bi se pristupilo i obnavljalo starim izbrisanim kopijama, potrebno je stjecati potpunu kopiju fizičke memorije. Zbog svih prikupljanja, izdvajanja i analize mobilni uređaji predstavljaju odličan izvor digitalnih dokaza i mogu pružiti uvid nedostupnim podacima s drugih uređaja. Dodatno, osobna priroda uređaja olakšava utvrđivanje posljednjih koraka za povezivanja uređaja s pojedincem, [37].

## 5.1. Funkcionalnosti mobilnih terminalnih uređaja

Mobilni terminalni uređaji su dinamički sustavi koji predstavljaju izazove iz forenzičke perspektive. Osim toga, novi modeli mobilnih uređaja se razvijaju na globalnoj razini, a neki stručnjaci kažu da se pet novih telefonskih modela izdaje svaki tjedan. Sve veći broj i raznovrsnost mobilnih uređaja otežava razvoj jednog procesa ili alata za rješavanje svih mogućih događaja. Nadalje, postoje određeni razlozi za očuvanje mobilnih uređaja kao izvora dokaza. Većina mobilnih uređaja današnjice su mrežni uređaji kojima se slanje i primanje podataka odvija putem telekomunikacijskih sustava, WiFi tehnologija i Bluetooth-a. Digitalni dokazi se u mobilnim uređajima mogu potpuno izgubiti jer su osjetljivi na preknjiženje novih podataka ili daljinskim naredbama koje prima putem bežičnih mreža. Osim toga, radi izdvajanja informacija potrebno je komunicirati s uređajem, često mijenjanjem stanja sustava. Kao i kod bilo kojeg računala, interakcije s mobilnim uređajem mogu uništiti ili mijenjati postojeće dokaze, [24].

Mobilni uređaji su jednostavna računala s CPU-om (engl. *Central Processing Unit*), memorijom, baterijama, ulaznim sučeljima kao što su tipkovnica ili mikrofon i izlaznim sučeljima poput zaslona ili slušalice. Podaci u memoriji uglavnom su fokus forenzičkog pregleda, ali potrebno je razumijevanje ulaznih i izlaznih komponenti za pristup tim podacima. U nekim slučajevima može biti dovoljno ručno upravljati uređajem i čitati informacije sa zaslona. Međutim, da biste oporavili izbrisane podatke ili izvršili napredniji

pregled, potrebni su specijalno dizajnirani alati za sučelje s uređajem. U nekim situacijama dovoljno je ekstrahirati i prikupljati specifične informacije od interesa s mobilnog uređaja putem kabela priključenog na priključak za podatke, ali u drugim okolnostima potrebno je izravno priključiti specijalizirani konektor na matičnu ploču kako bi stekli sve informacije potrebne za određeni slučaj. Ponekad je potrebno poznavati način kako se podaci pohranjuju na ručnim uređajima za stjecanje svih raspoloživih digitalnih dokaza iz ručnih uređaja bez da se mijenjaju i prevode u čitljivi oblik. Na primjer, postavljanje mobilnog uređaja na postolje i sinkroniziranje s računalom za dobivanje informacija s uređaja neće kopirati sve podatke i čak ni uništiti digitalne dokaze. Mobilni uređaji koriste radio valove za komuniciranje preko mreža s različitim frekvencijama i standardnim komunikacijskim protokolima. Dva od najčešće korištenih mobilno komunikacijskih protokola su GSM i CDMA. Druga uobičajena tehnologija koja se koristi u SAD-u i nekim drugim zemljama jest IEN, [5].

Mobilni uređaji u istrazi razlikuju se ovisno o kaznenim djelima koja se istražuju, mogućnosti mobilnog uređaja i načina na koji se ona upotrebljava. Podaci povezani s mobilnim telefonima nalaze se na brojnim lokacijama; Ugrađena memorija, memorijska kartica, SIM kartica itd. Prilikom ispitivanja nisu sve od navedenih komponenti raspoložive i dostupne, a u nekim slučajevima može postojati i više SIM kartica. Nisu svi uređaji izrađeni jednaki, a ono što je moguće ekstrahirati iz uređaja ovisi o njegovim mogućnostima. Osnovni podaci o uređaju zajednički su u velikoj većini potrošača mobilnih telefona, dok dokazna vrijednost pametnog telefona proširuje ovu osnovnu funkcionalnost i povezane informacije. S obzirom na širok raspon mogućih funkcionalnosti, kada se radi o određenom mobilnom uređaju u nekom slučaju, preporučljivo je utvrditi njegovu punu funkcionalnost kako biste dobili bolji uvid u vrste digitalnih dokaza koje može sadržavati. Dokument proizvođača može pružiti te informacije, a tu su i web stranice koje katalogiziraju mogućnosti mobilnih uređaja. Očekuje se da mobiteli minimalno sadrže imenik, registre poziva, SMS poruke koje se još nazivaju i tekstualne poruke, [24].

Digitalni podaci su odvojeni vremenom i udaljenosti od događaja koje predstavljaju. Zapisna datoteka koja bilježi mrežne aktivnosti povijesni je zapis događaja koji se dogodio na raznim mjestima na svijetu. Čak i pri pregledu mrežnog prometa dolazi do kašnjenja između aktivnosti koja je generirala promet i prikaza podataka na monitoru. Osim toga, mreže se sastoje od slojeva koji obavljaju različite funkcije od prenošenja elektroničkih impulsa preko mrežnih kabela do prikazivanja podataka u obliku koji računalni programi mogu tumačiti. Na primjer, referentni model otvorenog sustava povezivanja (OSI) dijeli mreže na sedam slojeva. Svaki sloj apstrakcije skriva složenost donjeg sloja i pruža novu priliku za pogrešku i gubitak, [37].

## 5.2. Digitalni dokaz

Dokazom se naziva sve ono što razdvaja hipotezu od neosnovane tvrdnje. Dokazi mogu potvrditi ili oboriti hipotezu, pa je njihov integritet bitan u njihovom prihvaćanju,

odnosno poricanjem pred sudom. Digitalni dokaz je informacija uskladištena ili prenošena u digitalnoj formi koja se koristi u sudskim postupcima. Digitalna forma po svojoj prirodi podrazumijeva da se radi o nekom elektronskom ili magnetnom uređaju, pa to mogu biti podaci u radnoj memoriji, na tvrdom disku, *flash* karticama, ali i podaci koji se nalaze u prijenosu, tj. transmisiji kao što su radio valovi, [38].

### 5.2.1. Forma digitalnog dokaza

Digitalni dokaz nije jednostavan pojam i nije nešto što ljudi mogu na prvi pogled protumačiti. U doslovnom smislu, digitalni dokaz je niz nula i jedinica koje neki uređaj pretvara u oblik razumljiv ljudima, koji ga onda mogu koristiti u sudskim slučajevima, [39].

Računalna forenzika više je zainteresirana za formu nego funkciju izvora digitalnog dokaza pa su tako digitalni dokazi klasificirani prema skladištenju podataka na, [38]:

- **Privremena forma digitalnog dokaza**: klasičan primjer ove forme je RAM memorija koja bez eksternog izvora napajanja se briše.
- **Nestalna forma**: za ovu vrstu forme karakteristično je to da postoji neki interni izvor napajanja poput baterije. Kao i kod privremene forme ukoliko bi se izvadila baterija, informacije bi bile izgubljene. Primjer nestalne forme je CMOS ili RAM na prijenosnom računalu koji ima napajanje na bateriju.
- **Polustalna forma**: karakteristike polustalne ili semipermanentne forme je da se radi o čvrstom mediju koji se može promijeniti. Primjeri su hard disk, disketa, CD, DVD, memorijska kartica.
- **Stalna forma**: stalna ili permanentna forma jest ROM memorija.

Računalni forenzičar mora biti dobro upoznat sa svakom od navedenih formi kako bi izbjegao probleme prilikom izvlačenja podataka. Istražitelj mora veliku količinu podataka svesti na optimalnu veličinu, [39].

### 5.2.2. Analiza digitalnih dokaza

Metoda analize ovisi o tipu forenzičke istrage koja se provodi: računalna, mrežna, forenzika elektroničke pošte itd. Forenzička slika, tj. digitalni dokaz je zapravo jedan dokument, a takav format omogućuje jednostavnu pretragu ključnih riječi kako bi se pronašle informacije od značaja ili pregledalo umanjene sličice koje se nalaze na originalnom disku, [39].

Nakon ispravnog kreiranja forenzičke slike, istražitelju koji provodi analizu nad njom ostaje velika količina podataka, od koje neistraženi dio može sadržavati informacije važne za

istragu. Ručna pretraga dokument po dokument u većini slučajeva nije praktična i adekvatna zbog dugog trajanja, preporučuje se sljedeća strategija pregleda podataka, [39]:

- **Postavljanje pitanja i promatranje**: ukoliko istražitelj nije uključen u slučaj od samog početka, mora prikupiti osnovne informacije, činjenice i elemente slučaja, što se očekuje od istrage i na što se sumnja. Kada prikupi te osnovne informacije, preporučuje se razgovor s nadređenim i osumnjičenim osobama u slučaju, kako bi se smanjila pretraga po podacima.
- **Strategija pretrage mora uključivati liste ključnih riječi i traženih pojmova**: ovisno o značaju slučaja, može biti dovoljna samo pretraga slika, elektroničke pošte ili mrežnog prometa.
- **Pregled digitalnih dokaza odvija se prema strategiji razvijenoj u prošlom koraku**: kako se nailazi na nove dokaze ključne se riječi ili lokacije traženja mogu mijenjati. Tragovi mogu voditi do lokacija ili dokaza.
- **Formulacija objašnjenja, interpretacija pronađenih dokaza, te izvlačenje zaključaka**: istražiteljeva je zadaća objasniti što i kako se dogodilo, a što nije.
- **Preispitivanje zaključaka i metoda**: uzimajući u obzir pronađene dokaze, poželjno je preispitati metode i rezultate, te moguće propuste.
- **Izvještaj o zaključcima i pronađenim dokazima**

Niti jedan alat za analizu ne može interpretirati digitalne dokaze ili doći do traga koji spaja dokaze s elementima slučaja, upravo to je glavna zadaća istražitelja.

Forenzički se softver može koristiti za strukturiranje upita i kategorizaciju rezultata, no završni rezultat ovisi naravno o istražitelju. Forenzički istražitelj postavlja upite nad forenzičkom slikom sustava na strukturirani način. Iznimke su slučajevi kada se trebaju pregledati male količine podataka ili istražitelj na raspolaganju ima neograničenu količinu vremena. Efektivnost upita postavlja se boljim poznavanjem i razumijevanjem elemenata slučaja, karakteristika zločina te uključenih sudionika. U nekolicini elektroničkih poruka samo nekoliko njih sadrži važne informacije, pa tako i ako forenzički istražitelj pronađe veliki broj važnih informacija, ne može biti siguran da ih je pronašao sve, stoga se pretraga i istraživanje mora provoditi racionalno i logično. Strategije pretrage podataka često se osporavaju stoga se preporučuje detaljno dokumentirati svaki korak, protokole pretrage, procedure, liste pretrage i objasniti razloge poduzimanja određenih koraka. Pretraga po ključnim riječima također može biti problematična, zbog toga što se za pronalazak određenih informacija mora postaviti dovoljno precizan upit, ali u istu ruku dovoljno općenit, kako se ne bi izuzelo povezane podatke. Pretrage se moraju provoditi u više navrata kako bi se dobio što točniji rezultat, s modifikacijama lista pretraživanja, [40].

## 5.3. Značajke ekstrakcije podataka

Jedno od temeljnih pravila digitalne forenzike jest da se nad originalnim podacima ne smiju provoditi nikakve analize već se nad istima stvara identična kopija kako se ne bi oštetilo ili uništilo originalne podatke. Stvaranje forenzičke kopije naziva se dobavljanje ili akvizicija. Forenzička kopija naziv je za krajnji, tj. završni produkt forenzičkog prikupljanja informacija iz uređaja. Forenzička kopija naziva se i *bitstream* kopija ili *bitstream* slika zato što predstavlja identičnu bit-po-bit kopiju originalnih podataka, datoteke, slike, fotografije itd. U praksi se stvara nekoliko forenzičkih kopija u slučaju da se nešto dogodi podacima koji se obrađuju. Prikupljanje podataka nije isto što i kopiranje podataka s jednog medija na drugi. Kopiranjem se ne mogu očuvati datumi i vremenske oznake, dok se kod prikupljanja ti nedostaci ne pojavljuju, [5].

Postoji nekoliko načina izrade slike, korištenjem specijaliziranog softvera, [39]:

- **Zrcalna kopija**: ovaj način očuvanja dokaza temelji se na metodi hvatanja (engl. *Capture*) ili kopiranja svih podataka na disk, kako bi se stvorila neprobojna zrcalna kopija (engl. *Mirror image*) kopiranog diska. *Mirror image* može, ali ne i nužno, predstavljati identičnu kopiju originala zbog toga što se ona općenito koristi kao sigurnosna kopija (engl. *Backup*), a u zahtjevnim situacijama *mirror image* ne tretira se kao forenzička kopija.
- **Sektor-po-sektor kopija (*bitstream*)**: ova metoda je naprednija zato što započinje na početku diska te kopira svaki bit, jedinice i nule, sve do kraja, bez ikakve promjene i brisanja podataka. Kopiraju se svi dijelovi, pa tako i neiskorišteni i nelocirani zbog toga što se na njima često nalaze izbrisani podaci.

Vrlo je važno razlikovati nekoliko pojmova koji se vrlo često koriste kao sinonimi, što pri svakodnevnom korištenju računala ne predstavlja problem, no prilikom forenzičke analize razlike su velike, a pravi primjer toga je razlika između *bitstream* kopije i kopije. Vrlo je važno razlikovati sljedeće, [39]:

- **Kopija**: uključuje samo informacije o datotekama, ne i o *slack* ili nelociranom prostoru, također nisu očuvane vremenske oznake.
- **Pričuvna kopija (engl. *Backup*)**: datoteke kopirane za buduću restauraciju, služe kao sigurnosna kopija, a vrlo često se može i nazivati sigurnosnom kopijom.
- **Slika (engl. *Image*)**: kopija podataka cijelog diska kreirana zbog dupliciranja ili restauracije.
- **Kopija bit-po-bit (*engl. Bitstream kopija*)**: egzaktna replika svih sektora.

Dobavljanje podataka na forenzički prihvatljiv način temelj je svake forenzičke istrage. Ako se taj korak ne obavi prema određenim pravilima, svi kasniji pronalasci, kao i otkriveni dokazi i informacije mogu se odbaciti zbog nepravilnog dobavljanja kopija originalnih podataka. Osnovni problem prilikom izrade odgovarajuće forenzičke kopije je da se prilikom pokušaja kopiranja podaci na neki način promijene. Oprema koja se koristi za

dupliciranje podataka ovisi o mediju s kojeg se ti podaci trebaju kopirati. Uobičajeni postupak uključuje dokumentaciju svih načinjenih koraka prilikom dobave podataka. Generalizirani format procesa dobave podataka može se podijeliti na nekoliko koraka, [24]:

1. Određivanje tipa medija na kojem se radi.
2. Pronalazak odgovarajućeg alata.
3. Prijenos podataka: koristeći odgovarajuću opremu prenose se podaci na sterilni medij, pritom koristeći alat kojim je moguće potvrditi integritet podataka, te njihovu autentičnost.
4. Autentificiranje i provjera integriteta prenesenih podataka provjerom *checksum-a* i *hash* vrijednosti.
5. Stvaranje radne kopije forenzičke kopije. U praksi, originalnim podacima pristupa se jednom, forenzičkoj kopiji dva puta, a radnoj kopiji koliko god je puta potrebno prilikom istrage. Razlog izrade duplikata kopije jest potreba za radnom kopijom koju se obrađuje i koju se u slučaju gubitka ili uništenja podataka jednostavno može zamijeniti bez daljnjeg kompromitiranja originalnih podataka. Izradi duplikata pristupa se kao da je forenzička kopija originalni skup podataka.

Prilikom dobavljanja podataka s uređaja na uređaj, kao platforma za izvlačenje podataka na uređaj istražitelja koristi se posebno računalo, tj. uređaj. Za takav način dobave podataka koriste se dvije metode spajanja kabelima, [39]:

- **Paralelni**: najsporija metoda, no najbolja, uključuje izravno spajanje uređaja s uređajem.
- **Mrežni**: nešto brža metoda , spaja računalo na mrežu istraživačkog računala LAN kabelom.

Ograničavajući faktor obje metode je količina podataka koja se može prenijeti u jedinici vremena. Obje metode korisne su prilikom pregleda materijala, i traženja bitnih dokaza, no općenito ih se ne isplati koristiti za kopiranje podataka većih od 50GB, [39].

### 5.3.1. Provjera integriteta sačuvanih podataka

Digitalne podatke vrlo je jednostavno mijenjati u forenzičkim postupcima, bitno je utvrditi kako se podaci nakon dobavljanja i analize nisu mijenjali. Ako forenzička slika nije autentificirana, može se dogoditi da se svi dokazi prikupljeni s nje ne mogu uzeti u obzir. Kako bi se takve situacije izbjegle koriste se razni alati kao što su FTK Imager ili ENCase prilikom stvaranja forenzičke kopije. Navedeni programi sastavljaju izvještaj koji uključuje dva digitalna otiska prstiju koji se nazivaju MD5 i SHA1 *hash* vrijednosti, pomoću kojih se mogu identificirati i autentificirati prikupljeni podaci. *Hash* vrijednosti omogućuju matematičko dokazivanje kako su dokazi i njihovi duplikati identični. Ako se duplikat mijenja, *hash* vrijednosti im se više neće poklapati. Autentifikacijom elektroničkih dokaza utvrđuje se dodatno i jeli računalo s kojeg su podaci prikupljeni bilo ispravno i u funkcionalnom stanju, [5].

Ponekad *hash* vrijednosti ne odgovaraju zbog tehničkih razloga, od kojih su najčešći, [39]:

- Medij s kojega se dobavljaju podaci se počinje kvariti te softver nije u mogućnosti ispravno prenijeti podatke s jednog medija na drugi, stoga *hash* vrijednosti ne odgovaraju.
- Korištena oprema nije ispravna: originalni medij je ispravan, kao i ciljni medij, no transportni medij nije.

### 5.3.2. Prikupljanje ranjivih podataka

Računalna forenzika fokusirana je na istraživanje, razvoj i implementaciju odgovarajućih alata i metodologija za prikupljanje, pohranu i očuvanje osjetljivih podataka ostavljenih na medijima za pohranu. Osobe koje prve imaju pristup istraživanom uređaju (mrežni i sustavski administratori, policijski istražitelji), općenito reagiraju na sigurnosni incident tako da isključuju i osiguravaju uređaje. Nakon isključivanja, prikupljaju se svi postojani podaci s medija za pohranu podataka. Isključivanje uređaja onemogućuje prikupljanje ranjivih podataka. Postoje mnogi *open source* alati koji omogućuju izvlačenje ranjivih podataka s računala, no većina ih je specifično dizajnirana za prikupljanje samo dijelova ranjivih podataka, ovisno o njihovoj lokaciji i tipu, [7].

Ranjivi podaci su pohranjeni u memoriji sustava (registrima, *cache* memoriji, radnoj memoriji itd.) i gube se ako uređaj nije spojen na izvor napajanja ili se resetira. Ranjivi podaci prikupljaju se radi otkrivanja razloga zašto uređaj ne radi normalno, ako se primijeti neuobičajeno ponašanje korisnika, odnosno ako je prekršeno neko sigurnosno pravilo ili dobivena obavijest od strane zaštitne stijene ili IDS-a (engl. *Intrusion detection system*). Prva reakcija na sigurnosni incident određenog uređaja trebalo bi biti prikupljanje ranjivih podataka, te analiza rezultata kako bi se utvrdio daljnji slijed događaja, [39].

Postojani podaci nalaze se na tvrdim diskovima i ostalim medijima za trajnu pohranu podataka i obično se ne gube kada se računalo ugasi ili resetira.

Prilikom prikupljanja postojanih podataka, kontaminaciju je moguće izbjeći pridržavanjem i korištenjem provjerenim metodama te korištenjem alata koji stvaraju bit-po-bit kopiju podataka i generiraju *checksum* zbog provjere integriteta i autentifikacije kopije podataka. Prilikom prikupljanja ranjivih podataka, teže je izbjeći kontaminaciju, zbog toga što sami korišteni alati i njihove procedure mogu promijeniti datume i vremena pristupa podacima, koristiti zajedničke povezne biblioteke, izazvati pokretanje zlonamjernih računala ili resetiranja računala. Bit-po-bit kopiju ranjivih podataka očito nije moguće izraditi, no korištenjem provjerenih alata moguće je prikupiti podatke i rekonstruirati reprezentaciju trenutnog stanja istraživanog uređaja, [24].

### 5.3.3. Prikupljanje skrivenih podataka

Prikriveni ili prerušeni podaci predstavljaju izazov svakom forenzičkom istražitelju. Zajednički naziv za takve podatke je nevidljivi digitalni dokazi. Istraživač mora otkriti pokušaje prikrivanja, te doći do skrivenih podataka, time svrstavajući ovaj dio računalne forenzike u jedan od najzahtjevnijih, [39].

Cilj skrivanja podataka jest prikrivanje poruke, a to se postiže koristeći jedan ili više sljedećih načina, [5]:

- **Nevidljivi podaci**: primjer je da je poruka sakrivena u prostoru tvrdog diska kojem operacijski sustav nema pristup.
- **Prerušeni podaci**: primjer je da je poruka sakrivena u objektu ili stvari koja izgleda nebitno, odnosno nepovezano kako bi poruka ostala skrivena
- **Nečitljivi podaci**: primjer je kriptiranje, tj. poruku ne može pročitati nitko osim onoga kome je namijenjena, a primaoc ima ključ i zna na koji način pročitati poruku.

Postoji vrlo velik broj raznih načina skrivanja podataka, a za njihov pronalazak nužno je koristiti razne alate i metode. Forenzički istražitelj zasniva se na pokazateljima kako je netko koristio metodu sakrivanja, [39].

## 5.4. Izvori podataka

Proizvođači mobilnih uređaja obično nude sličan skup značajki i upravljanja informacijama, uključujući aplikacije za upravljanje osobnim informacijama (engl. *Personal Information Management*, PIM), poruke, e-poštu i pregledavanje web-a. Skup značajki i mogućnosti razlikuje se ovisno o razdoblju u kojem je uređaj izrađen, izmjenama koje su napravljene za određenog davatelja usluga te svim izmjenama ili aplikacijama koje je instalirao korisnik. Potencijalni dokazi o tim uređajima mogu uključivati sljedeće stavke: datum/vrijeme, jezik i ostale postavke, informacije o kalendaru, imenik/podatke o kontaktima, SMS poruke, fotografije, e-poštu, zapisnike poziva, audio/video snimke, podatke o lokaciji itd. U nastavku će izvori podataka biti detaljnije objašnjeni. Stavke koje se nalaze na uređaju ne ovise samo o značajkama i mogućnostima mobilnog uređaja, već i o podatkovnim i glasovnim uslugama na koje je korisnik pretplaćen. Na primjer, prepaid telefonska usluga može isključiti mogućnost za multimedijske poruke, elektroničku poštu i pregledavanje web-a. Slično tomu, pretplata na ugovore može selektivno isključiti određene vrste usluga, [7].

### 5.4.1. SIM kartica

*Subscriber Identity Module* (SIM) je neophodni dio svakog mobilnog uređaja, a upotrebljava se s GSM i iDEN mrežama. Omogućava korisnicima prebacivanje podataka kao što su imenik i poruke, te korisničke autentifikacije među mobilnim uređajima. Korisnik, naravno, može mijenjati svoje mobilne uređaje, a da ga se i dalje može pronaći korištenjem SIM kartice. Kako bi se izbjeglo kontaminiranje dokaza ne preporučuje se pristupanje mobilnom uređaju korištenjem druge SIM kartice. Kloniranje SIM kartica korištenjem forenzičkih alata najsigurniji je način pristupanja mobilnom uređaju. Svaka SIM kartica zaštićena je PIN brojem (engl. *Personal Identification Number*), čija je zadaća ne samo zaštita podataka na kartici, već i samom uređaju. PIN broj dužine je od četiri do osam znamenki, te provodi sigurnosnu opciju blokiranja uređaja ako se unese pogrešan PIN određen broj puta, a taj broj je najčešće tri. Nakon blokiranja, mobilni uređaj se otključava PUK brojem (engl. *PIN Unblocking Key*), a ako se kojim slučajem nekoliko puta unese i krivi PUK broj, uređaj se više ne može odblokirati, [39].

SIM kartica sadrži sljedeće, [41]:

- Mikroprocesor (CPU)
- Programsku memoriju (ROM)
- Memoriju podataka (EPROM ili EEPROM)
- Serijski komunikacijski modul

SIM kartica je čip koji je zapravo UICC(engl. *Universal Integrated Circuit Card*), tj. univerzalni integrirani krug, a predstavlja pametnu karticu koja pomaže uređajima kao što su mobilni uređaji, Set Top Box-ovi i sl. pri ostvarivanju konekcije s najbližim mrežnim tornjem za komunikacijske svrhe, [39].

Forenzika SIM kartice bitan je dio forenzike mobilnih uređaja. Informacije koje SIM kartica može pružiti forenzičaru može biti ključna za istragu. Dobivanje i pristup SIM kartici dozvoljava mnoštvo informacija koje je osumnjičenik prenio preko mobilnog uređaja, a koje mogu biti od značaja za promatrani slučaj. Općenito, neki od tih podataka mogu pomoći istražitelju odrediti, [41]:

- Telefonske brojeve upućenih/primljenih poziva
- Kontakte
- Pojedinosti o SMS-u (vrijeme, datum, primatelj itd.)
- SMS tekst (sama poruka)

Neke dodatne informacije koje davatelji usluga mogu pohraniti su:

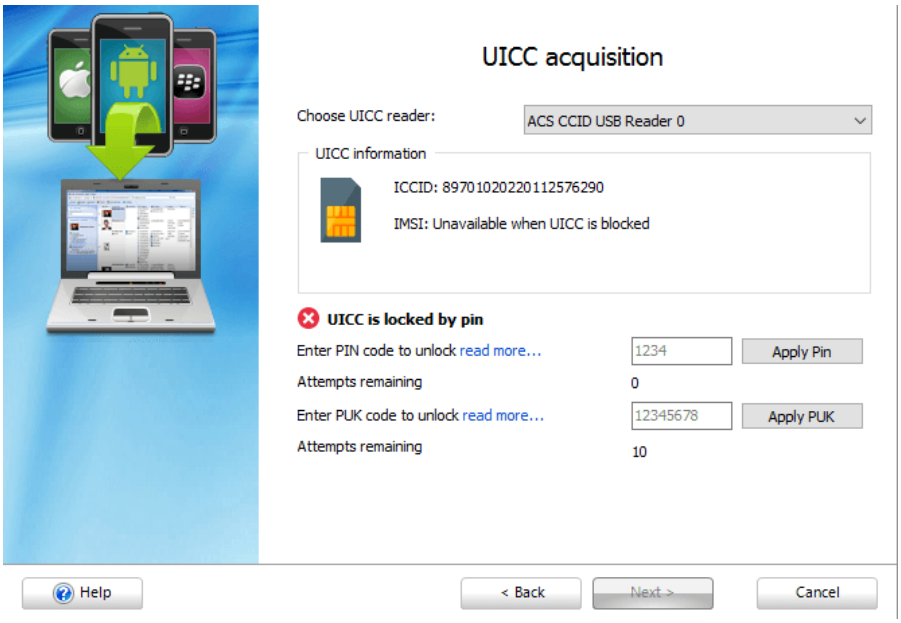
- Baza podataka korisnika
- Zapisi o detaljima poziva (engl. *Call Detail Records,* CDR)
- Registar domaćih korisnika (eng. *Home Location Register,* HLR)

Mreže za mobilne telefone raspoređene su u lokacijska područja. Svaka lokacija prepoznata je po jedinstvenom identifikacijskom broju koji se naziva „Informacije o jedinstvenom identifikacijskom broju“ (engl. *Location Area Information*, LAI). LAI je pohranjen na SIM kartici te prepoznaje i prima uslugu od najbližeg mobilnog tornja. Kada mobilni telefon mijenja lokacijska područja, novi LAI se nalazi na popisu prethodnih LAI-a. Kada je mobilni telefon isključen i dok se ponovo pokreće, može se pretražiti popis svih LAI-a koji su pohranjeni, a tako otkriti i koji se trenutno koristi, odnosno na kojem lokacijskom području je uređaj. Ovo je vrlo velika prednost za forenzičke istražitelje jer pri pregledavanju SIM kartice, oni mogu dobiti opću ideju gdje se geografski nalazi SIM kartica. Također, daje im informacije o prethodnoj lokaciji, odnosno gdje je telefon bio, [41].

Organizacija datotečnog sustava SIM kartice se sastoji od, [39]:

- **Glavna datoteka (engl. *Master File*, MF)**: korijen organizacije datotečnog sustava. Sadrži sve elementarne datoteke.
- **Podređena datoteka (engl. *Dedicated File*, DF)**: podređeni direktoriji glavnoj datoteci koji sadrže privržene i elementarne datoteke.
- **Elementarna datoteka (engl. *Elementary File*, EF)**: ovo su datoteke koje sadrže različite vrste podataka, što može biti niz bajtova podataka, niz zapisa s fiksnom veličinom ili fiksni skup zapisa s fiksnom veličinom koji se koriste ciklički.

SIM kartice predstavljaju tehnički pametne kartice koje sadrže ugrađeni EEPROM memorijski čip. EEPROM čip u pametnim karticama je isti uređaj za *flash* memoriju koji su prisutni u običnim pogonima, kao što su SSD-ima. Stoga je moguće oporaviti podatke s drugih uređaja s elektroničkim memorijskim čipovima. Problem nastaje kada su SIM kartice u oštećenom stanju i bivaju neprepoznatljive uređajima za ekstrakciju SIM kartica. Prije ekstrakcije SIM kartice, potrebno ju je očistiti, [41].




**Slika 10**: Prikaz ekstrakcije SIM kartice, [42]

### 5.4.2. Lokacija

Sposobnost određivanja lokacije mobilnih uređaja tijekom razdoblja istraživanja je vrlo snažna istraživačka sposobnost. Neki mobilni uređaji bilježe lokaciju staničnih tornjeva koje su kontaktirali, a pruža i povijesni zapis o mjestu boravka korisnika tijekom određenog razdoblja. Uređaji s GPS-om mogu sadržavati i ostatke prošlih lokacija i mapa koje mogu biti korisne u istrazi. Osim toga, podaci EXIF-a (engl. *Exchangeable Image File Format*) ugrađenih u digitalne fotografije mogu dodati dodatnu dokaznu vrijednost, pružajući datum i vrijeme stvaranja fotografije, vrstu uređaja upotrijebljenog za njegovu izradu i potencijalno GPS koordinate gdje je fotografija snimljena. GPS također može pružiti i funkcionalnost mapiranja i stoga pružiti forenzičkim istražiteljima putne točke, planirane destinacije i preuzete puteve, [24].

Postoje dvije kategorije informacija koje većina GPS jedinica može pružiti ispitivačima. Prva je informacija o razini sustava, a to su podaci koje sam uređaj bilježi, neovisno o korisniku. Drugi su podaci stvoreni od strane korisnika, tj. zahtijeva interakciju korisnika kako bi se snimili. Ove dvije vrste informacija mogu se razdvojiti na još manje dijelove/elemente. Unutar podataka o razini sustava postoje zapisne točke i zapis tragova. Kada je uređaj uključen i prepoznaje dovoljno satelita, počet će zapisivati zapisne točke samostalno. Ove točke bilježe podatke o lokaciji i prate ih u unaprijed određenom intervalu, iako mnogi uređaji omogućuju korisniku da kreira zapisne točke u određenim vremenskim intervalima po izboru. Osim toga, korisnici uglavnom ne mogu mijenjati podatke o točkama, [43].

Zapis je samo popis svih snimljenih podataka, navedenih redoslijedom snimanja. Korisnici mogu koristiti evidenciju zapisnika kako bi se vratili koraci i krenuli natrag na prethodnu lokaciju, naravno, ako je to potrebno. U smislu forenzičke upotrebe, ispitivači mogu koristiti zapisnik puta kako bi prikazali jasan put gdje se GPS uređaj nalazio i u kojem trenutku. U kaznenim istragama, takve informacije mogu se upotrijebiti kako bi se utvrdilo gdje i kada je zločin počinjen, [44].

Što se tiče podataka stvorenih korisnikom, postoje putne točke i rute. Putne točke su lokacije koje korisnici moraju samostalno unijeti u uređaj, što se može učiniti tako da prikvače lokaciju na kojoj su bili, a zatim odaberu točku od interesa, tj. lokaciju od interesa. Putne točke mogu se ponovo pronaći u budućnosti uz pomoć GPS-a kao vodiča.Kao što se može očekivati, ruta je u osnovi ekvivalentna putna točka dnevnika staza. Putem rute korisnici se mogu kretati do međutočaka u bilo kojem redoslijedu koji samostalno biraju. Nakon što korisnik stvori rutu, GPS će ih voditi na svaku sljedeću putnu točku i automatski prijeći na sljedeću putnu točku, [43].

Iako svi ovi podaci mogu biti korisni forenzičarima, općenito postoji razlika između podataka o razini sustava i podataka koji su stvorili korisnici. S obzirom na to da uređaj sam snima podatke o razini sustava, to može pomoći dokazati da je netko bio na određenoj lokaciji ili barem dokazuje da je uređaj bio na određenoj lokaciji. S druge strane, korisnički podaci

mogu pomoći pri dokazivanju namjere, jer zahtijeva da netko unese podatke. U kaznenoj istrazi to bi pomoglo dokazati da netko namjerava ići na određeno mjesto, [24].

Uređaji s GPS funkcionalnosti mogu sadržavati neke ili sve od navedenih podataka, [44]:

- Zapisnici tragova
- Putne točke
- Rute
- Pohranjene lokacije: dom, posao, dječji vrtić itd.
- Sigurnosnu lokaciju
- Nedavne adrese
- Zapisnike poziva
- Povijest uređaja
- Video, Fotografije, Audio

### 5.4.3. E-pošta

Elektronička pošta koristi se kao dokazni materijal u većini civilnih i kriminalnih forenzičkih istraga. Elektronička pošta širi se vrlo velikom brzinom, te jednostavno može završiti na računalu korisnika kojem nije namijenjena. Elektronička pošta zasnovana na Internet poslužiteljima vrlo često je od velike koristi za forenzičku istragu, [39].

Svaka elektronička pošta šalje se kao niz paketa veličine bajta. Prilikom transporta na mreži, svaki od tih paketa sadrži sljedeće elemente, [45]:

- **Izvorišnu adresu**: IP adresu računala pošiljatelja, osim u slučaju kada je ta IP adresa prikrivena.
- **Odredišnu adresu**: IP adresu računala na koje se ta poruka treba poslati.
- **Payload**: podatke ili poruku.

Usmjerivači prosljeđuju pakete prema svojim tablicama usmjeravanja sve do krajnjeg odredišta. Za prijenos e-pošte koristi se osnovni protokol aplikacijskog sloja – SMTP (engl. *Simple Mail Transfer Protocol*), a prilikom prijenosa koristi se pouzdana veza. SMTP zahtijeva da svaka poruka bude u sedmobitnom obliku, [39].

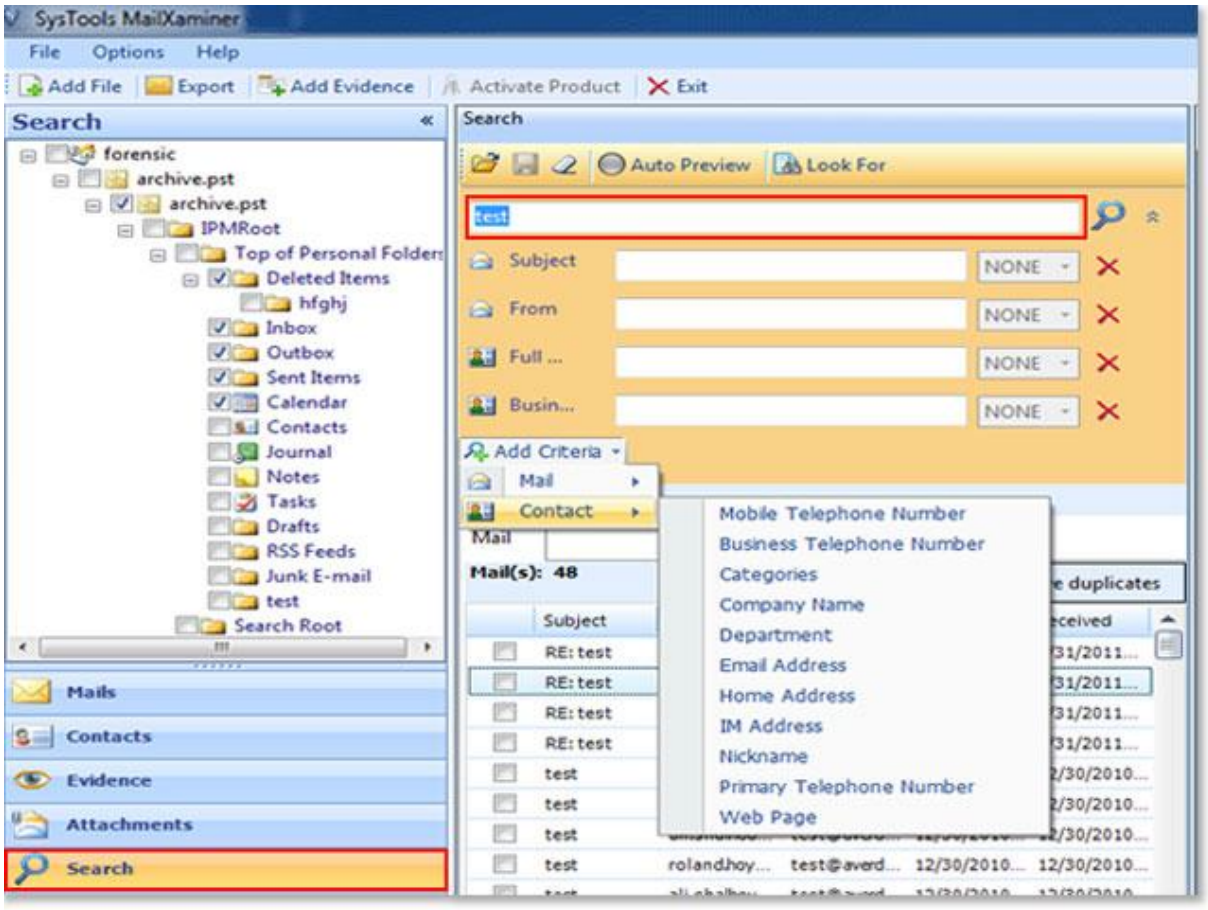
Elektronička pošta sastoji se od dva osnovna dijela: zaglavlja i tijela poruke. Iz zaglavlja se može saznati izvorišna i odredišna adresa, tj. adresa pošiljaoca i primaoca, a tijelo poruke sadrži tekst poruke. Kako istražitelj zapravo ne može vjerovati osnovnim informacijama u zaglavlju, mora proširiti informacije koje se prikazuju u njemu. Prošireno zaglavlje sadrži mnogo više informacija nego je usmjerivačima potrebno da dostave poruku do svog odredišta. Najkorisnija informacija u proširenom zaglavlju je IP adresa izvora, odnosno domene. Pomoću IP adrese izvora, moguće je ući u trag pošiljaocu poruke. Prvi

poslužitelj e-pošte kroz koji e-poruka prođe dodjeljuje joj jedinstveni identifikacijski broj, te ukoliko istražitelj pristupi dnevnicima poslužitelja prije nego li se tražene informacije prebrišu. Moguće je pratiti stvarno vrijeme i smjer prolaska poruke kroz mrežu. Osim pregleda osnove poruke, tj. zaglavlja i tijela poruke, potrebno je provjeriti i ostale potencijalne izvore informacija, [45]:

- Privitke s ekstenzijama kao što su .doc, .xls ili slike.
- Ljude koji su navedeni u CC (engl. *Carbon Copy*) ili BCC (engl. *Blind Carbon Copy*) poljima.
- Ljude kojima je poruka proslijeđena.
- Originalnu poruku ili niz poruka na koje je ova odgovor, ili odgovor na istraživanu poruku.

Za osobnu komunikaciju često se koriste Web servisi za elektroničku poštu, kao što su Google, Hotmail, Yahoo. Ovi servisi koriste se bez uporabe softvera klijenata elektroničke pošte, no zapravo predstavljaju klijent/poslužitelj sustav. *Web mail* sustav predaju e-poruku koristeći SMTP protokol, a dohvaća pomoću POP ili IMAP protokola. Web pošta se ne sprema na lokalni uređaj, osim ako to korisnik ne zatraži. Pristup računu e-pošte na poslužitelju ili dobava podataka o korisničkom računu od strane pružatelja usluga znatno smanjuje posao forenzičkom istražitelju. Ako pristup nije dozvoljen ili mu je teško prići, do *web mail* poruka može se doći i pregledom radne i *cache* memorije. Kada korisnik provjerava poruke, ili sastavlja novu, operacijski sustav sačuva podatke s ekrana, pogotovo ako korisniku treba duže vrijeme da sastavi poruku. Najbolja mjesta za traženje *web mail* poruka na lokalnom uređaju su, [39]:

- Područje privremenih datoteka kao što su sustavski *swap* prostor ili *cache* memorija.
- Nealociran prostor, nakon brisanja privremenih datoteka i dokumenata.




**Slika 11**: Prikaz ekstrakcije e-pošte, [46]

## 5.4.4. Digitalna kamera

Mnogi mobilni uređaji, tj. njihove kamere sadrže dokaze o zločinu ili podupiru vremensku liniju ljudi povezanih sa zločinom. Važno je shvatiti da mobilni uređaji, digitalni fotoaparati i drugi digitalni foto uređaji često koriste FAT 32 ili ext 3 datotečni sustav koji djeluje kao mali tvrdi disk. To znači da ako uređaj ima bežičnu, infracrvenu ili Bluetooth mogućnost, osoba je mogla tajno staviti sliku na taj uređaj. Razlučivost ili shema slike mogu dokazati da kamera ili mobilni uređaj možda nisu mogli snimiti fotografiju, [47].

Forenzička analiza digitalnih slika može se uglavnom podijeliti u dvije grane: prepoznavanje i identifikacija izvora slike. Uspjeh forenzike digitalnih kamera ovisi o značajkama tehnika kojima se forenzika provodi. Značajke koje se koriste za prepoznavanje modela digitalne kamere izvedene su iz razlika između tehnika obrade slike i komponenti koje se koriste. Najveći problem s ovim pristupom je da različiti modeli digitalnih fotoaparata koriste komponente malog broja proizvođača, a algoritmi koji se koriste također su vrlo slični među modelima iste marke. Za tu svrhu se mogu uspostaviti četiri vrste tehnika: sustav leća, filter boja (engl. *Color Filter Array*, CFA), karakteristike slike i nepravilnosti senzora.

Tehnike bazirane na temelju značajki slike koriste se kao skup značajki izvađenih iz sadržaja slike kako bi se utvrdio izvor, [48].

Skup značajki koji se koriste u forenzici digitalne kamere ovise o prirodi njihova dobivanja, a to su, [47]:

1. **Značajke buke**: Jedan od ciljeva je dobiti niz značajki koje omogućuju razlikovanje različitih vrsta uređaja. Da bi se to omogućilo, prvo se uzima u obzir da digitalni fotoaparati koriste dvodimenzionalni senzor polja, dok većina skenera koristi senzor linearnog polja. U slučaju skenera, linearni raspored senzora se pomiče kako bi se generirala cjelovita slika pa se očekuje da će se naći redovitost buke senzora unutar redaka skenirane slike. S druge strane, nema razloga pronaći periodičnost buke senzora unutar stupaca skenirane slike. U slučaju digitalnih fotoaparata ova vrsta buke periodičnosti ne postoji. Ta se razlika može koristiti za razlikovanje različitih vrsta uređaja. Temelji se na ekstrakciji buke.
2. **Značajke boja**: Konfiguracija CFA filtara, raznih algoritama i tehnika obrade boja znače da signali u grupama boja mogu sadržavati tretmane i specifične uzorke. Kako bi se utvrdile razlike u značajkama boja za različite modele fotoaparata, potrebno je ispitati statistiku prvog i drugog reda snimljenih slika.
    - **Prosječna vrijednost piksela**: Ova se mjera provodi za svaki RGB (engl. *Red Green Blue*) kanal.
    - **Paralelni par između RGB grupa**: Ova mjera izražava činjenicu da ovisno o strukturi kamere, korelacija između različitih boja se može mijenjati.
    - **Centar za raspodjelu grupa boja**: Ova se mjera izračunava za svaku skupinu zasebno. Prvo, izračunava se ukupni broj piksela za svaku vrijednost boje, dobivajući vektor s 256 komponenata. Zatim, uz ove izračunate vrijednosti, dobivaju se zbrojevi susjednih vrijednosti.
    - **Energetski omjer između parova RGB**: Ova značajka ovisi o postupku ispravljanja bijelih točaka fotoaparata.
3. **IQM (engl. *Image Quality Metrics*)**: Različiti modeli fotoaparata stvaraju slike različite kvalitete. Postoje razlike u svjetlini slike, oštrine ili boje kvalitete. Te razlike predlažu niz značajki mjernih podataka koji nam pomažu razlikovati izvor slike. Postoje različite kategorije IQM-a:mjerenja temeljena na razlikama piksela, mjerenja na temelju korelacije, mjerenja na temelju spektralne udaljenosti. Za dobivanje ovog skupa mjernih podataka osim originalne slike potrebna je i filtrirana slika u kojoj se smanjuje buka izvorne slike za obavljanje različitih izračuna. Za to se koristi Gaussov filtar koji omogućuje izvođenje zaglađivanja slike. Nakon što se jezgra dobije, normalizira se tako da zbroj svih njegovih komponenata bude jednak 1. To je neophodno za dobivanje glatke slike, ali s istim bojama kao izvorna. Normalizacija se vrši podjelom svake komponente zbrojem vrijednosti svih komponenti.
4. **Značajke valova**: Može se reći da je buka senzora na digitalnom fotoaparatu kao otisak prsta na ljudskom biću. Kako bi se identificirao izvor akvizicije, potreban je algoritam koji omogućuje izlučivanje buke senzora i drugih metoda koji omogućuje da se dobiju značajke otisaka prstiju kako bi se klasificirale i identificirale.

Digitalna kamera sadrži mnoštvo podataka kao što su, [48]:

- Datum i vrijeme snimljene fotografije/videozapisa
- Lokaciju snimljene fotografije/videozapisa
- Veličinu snimljene fotografije/videozapisa itd.

### 5.4.5. Web preglednici

Internet koriste gotovo svi, uključujući i osumnjičene pod istragom. Osumnjičenik može koristiti web preglednik za prikupljanje podataka, sakrivanje svojih zločina ili traženje novih metoda zločina. Pretraživanje dokaza koji su ostavljeni aktivnošću pregledavanja Interneta obično je ključna komponenta digitalnih forenzičkih istraga. Gotovo svaki pokret koji osumnjičeni čini prilikom korištenja web preglednika ostavlja trag na uređaju. Stoga, kada istražitelj analizira uređaj osumnjičenog, ovaj dokaz može pružiti korisne informacije. Nakon preuzimanja podataka kao što su predmemorija, povijest, kolačići i popisi za preuzimanje s uređaja sumnjivca, moguće je analizirati ove dokaze za posjećene web stranice, vrijeme i učestalost pristupa te ključne riječi pretraživača koje koristi sumnjivac. Postoje istraživačke studije i alati koji se odnose na analizu log datoteka web preglednika, a neki od njih dijele zajedničke karakteristike. Prvo, ove studije i alati usmjereni su na određeni web preglednik ili određenu dnevničku datoteku iz određenog web preglednika. Mnoge vrste web preglednika pružaju internetske usluge i danas, tako da jedan korisnik može istovremeno koristiti i usporediti različite vrste web preglednika. Iz tog razloga, obavljanje različite analize za svaki web preglednik nije prikladan način za otkrivanje dokaza o kriminalnoj aktivnosti korisnika putem Interneta. Štoviše, nije dovoljno istražiti jednu datoteku dnevnika iz jednog preglednika jer se dokazi mogu proširiti na nekoliko dnevnika. Najčešće korišteni web preglednici su Internet Explorer, Mozilla Firefox, Google Chrome, Safari i Opera, [49].

Forenzika web preglednika uključuje sve podatke koji se mogu otkriti o korisnikovoj aktivnosti na Internetu, od e-mail poruka (u slučaju da se koristio web klijent za pristup sandučiću elektroničke pošte), preuzetih datoteka, kronološkog popisa posjećenih stranica, pa do lozinki za razne web stranice. S obzirom na to da se računala danas uglavnom koriste baš zbog mogućnosti povezivanja na Internet i razmjenu podataka sa svijetom, ovo područje je jako bitno za istražitelje. Dok korisnik posjećuje stranice na Internetu, njegov preglednik pohranjuje sve podatke o posjetama u određene datoteke na korisnikovom računalu (npr. index.dat za Internet Explorer). Web forenzičari prilikom istrage moraju obratiti pažnju na više elemenata kroz koje mogu saznati različite stvari o korisniku, a to su, [50]:

- Webmail (web based e-mail),
- Povijest posjećenih stranica (engl. *Browsing History*),
- *Cookies*,
- Ključne riječi (engl. *Keywords*) korištene u pretragama,
- Preuzete / pokrenute datoteke,

- Lozinke,
- Podaci koje je korisnik upisivao u formulare (kućice).

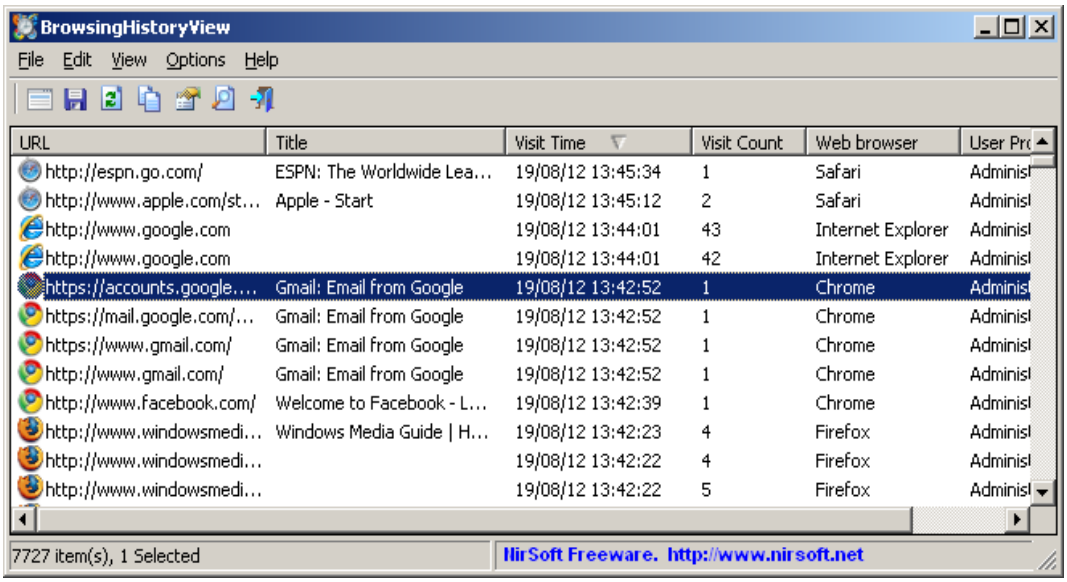
Postojeće studije i alati nisu dovoljno snažni da se koriste za forenziku web preglednika. U takvoj situaciji potrebna je napredna metodologija za prevladavanje nedostataka postojećih istraživanja i alata. Naime, sljedeći zahtjevi smatraju se neophodnima, [51]:

1. Integrirana analiza višestrukih web preglednika
2. Analiza vremenske linije koja pomaže istražitelju da utvrdi aktivnost osumnjičenog u ispravnoj vremenskoj zoni.
3. Izdvajanje značajnih informacija vezanih uz digitalnu forenziku, kao što su riječi za pretraživanje i aktivnost korisnika.
4. Dekodiranje kodiranih riječi na određenom URL-u, a budući da kodirane riječi nisu čitljive, oni otežavaju istragu.
5. Oporavak izbrisanih podataka o web pregledniku, jer sumnjivac može izbrisati podatke dnevnika web-preglednika kako bi uništio dokaze.

Alati za analizu datoteka zapisnika web preglednika koji postoje danas ciljaju određeni web preglednik ili određene informacije. Ovaj pristup može dovesti do pogrešnih zaključaka u digitalnoj forenzičkoj istrazi. *Cacheback* i *Encase* su dostupni alati za istraživanje raznih web preglednika i mogu analizirati široki raspon informacija. Međutim, *Encase* ne pruža integriranu analizu nekoliko različitih web preglednika. To olakšava istražitelju otkrivanje dokaza o aktivnostima ako osumnjičeni koristi različite web preglednike tijekom zločina. Pomoću drugog alata *Cacheback* moguće je provesti integriranu analizu različitih web preglednika, ali ovaj alat koristi jednostavan postupak parsiranja za analizu datoteka predmemorije i povijesti, [49].

Korisnici izvode različite aktivnosti s web preglednikom, kao što su pronalaženje informacija, e-pošta, kupovina, vijesti, online bankarstvo, bloganje itd. Stoga bi forenzički istražitelji trebali biti u mogućnosti analizirati aktivnosti korisnika prilikom provođenja istrage. Posebno su važne informacije o pretraživanju riječi koje se mogu koristiti za analizu aktivnosti prikupljanja podataka. Osim toga, ako korisnik koristi više web preglednika, informacije koje se generiraju iz različitih web preglednika moraju se analizirati na istoj vremenskoj skali, [51].

Podaci koji se najčešće pretražuju su oni iz povijesti preglednika:




**Slika 12**: Prikaz ekstrakcije iz povijesti web preglednika, [52]

### 5.4.6. SMS

SMS (engl. *Short Message Service*) je usluga koju mobilni uređaji mogu koristiti za slanje kratkih poruka između uređaja. SMS poruka se općenito nazivaju tekstualnim porukama, a u današnje vrijeme se lagano gube radi novih internetskih usluga sličnih SMS-u, [53].

SMS komunikacijsko okruženje omogućuje visoku razinu anonimnosti u usporedbi s komunikacijom lice u lice. Kriminalci mogu zloupotrijebiti ovu anonimnost u svoju korist. Prevalencija SMS-a u društvenim i poslovnim komunikacijama zajedno s potrebom za vizualnom anonimnošću opravdava neposrednu potrebu istražiteljima da snažno razmotre SMS podatke za digitalne dokaze. U istraživanju, malo je pažnje posvećeno analizi SMS-a za uporabu u istraživanjima. Trenutačno ne postoje softverski paketi od dobavljača koji obavljaju analizu podataka SMS-a putem jezičnih tehnika, iako je to potrebno. Analiza podataka pomoću jezičnih tehnika odigrava ključnu ulogu u procesiranju i pripajanju pojedinaca kroz atribuciju autora, [54].

Većina sadašnjih forenzičkih alata izvlače podatke s mobilnog uređaja u tekstualnu datoteku. SMS poruke u mobilnom uređaju pohranjuju se sa svojim sadržajem i atributima. Međutim, ovi alati izvode ekstrakciju u različitim formatima datoteka. Tekstualne datoteke mogu biti razgraničene tablicom, zarezima itd. Istraživači su zaključili da bi *Post-Hox* alat za analizu SMS podataka trebao biti sposoban unositi različite formate tekstualnih datoteka bez značajnijeg napora. Glavni problem koji postoji u izgradnji forenzičnog alata za mobilne uređaje jest taj da oni ne sadrže alate i tehnike jezične analize. Te probleme potrebno je riješiti kako bi se SMS mogao učinkovitije koristiti kao izvor digitalnih dokaza. Problem je također što niti jedan forenzički alat ne uzima u obzir analizu SMS poruka prema postizanju sposobnosti prepoznavanja autora SMS poruka, [53].

Budući da je SMS stekao popularnost širom svijeta, mobilni operatori pružaju korisnicima mogućnost slanja tekstualnih poruka na više jezika. Ovo može biti problematično kada se bavi atribucijom autora, budući da su sustavi dodjele autora najviše ovisni o jeziku. Da bi se riješio taj problem, proučavan je pristup temeljen na N-gramu za atribuciju autora u radu koji je autor objavio. Većina ljudi koristi SMS u velikoj količini, pa se može primijetiti da ljudi ne pišu SMS poruke kao što pišu e-poštu ili neke druge oblike pisane komunikacije. Zbog ograničene veličine SMS poruka ljudi su počeli zamjenjivati riječi s brojevima. Na primjer riječ „forgot“ se zamjenjuje sa „4got“ u SMS porukama. To je problem jer jezične tehnike pronalaženja glagola i imenica ovise o karakteristikama engleskog jezika koje se izgube u korištenju takvih skraćenih riječi. Zatim postaje važno da se ove skraćenice pretvaraju natrag u odgovarajuće predmete koji mogu otkriti informacijski ključ za slučaj, [54].

U slučajevima pravih istraga, bilo bi korisno identificirati predmet ili značenje SMS poruka jer bi pomoglo razjasniti namjeru promatranog subjekta. Prvi korak u tom smjeru je otkrivanje imenica i glagola koji čine ove poruke, budući da imenice pružaju objekt interesa, a glagoli mogu potpisivati akcije koje je želio autor. Analiza podataka ne može biti korisna bez pružanja adekvatne sposobnosti za izvješćivanje rezultata u tekstualnim ili grafičkim oblicima. Ove metode izvješćivanja korisne su kada istražitelji pretražuju podatke za dokaz. Većina forenzičkih alata pruža tehnike izvještavanja jer je to važan korak u forenzičkom procesu. Međutim, ti izvještaji nisu opsežni i ne razmatraju analizu SMS poruka. Da bi se ubrzao postupak forenzičke analize mobilnog uređaja, važno je osposobiti istraživače da mogu generirati izvješća i grafikone na SMS-u, [53].

### 5.4.7. Pozivi

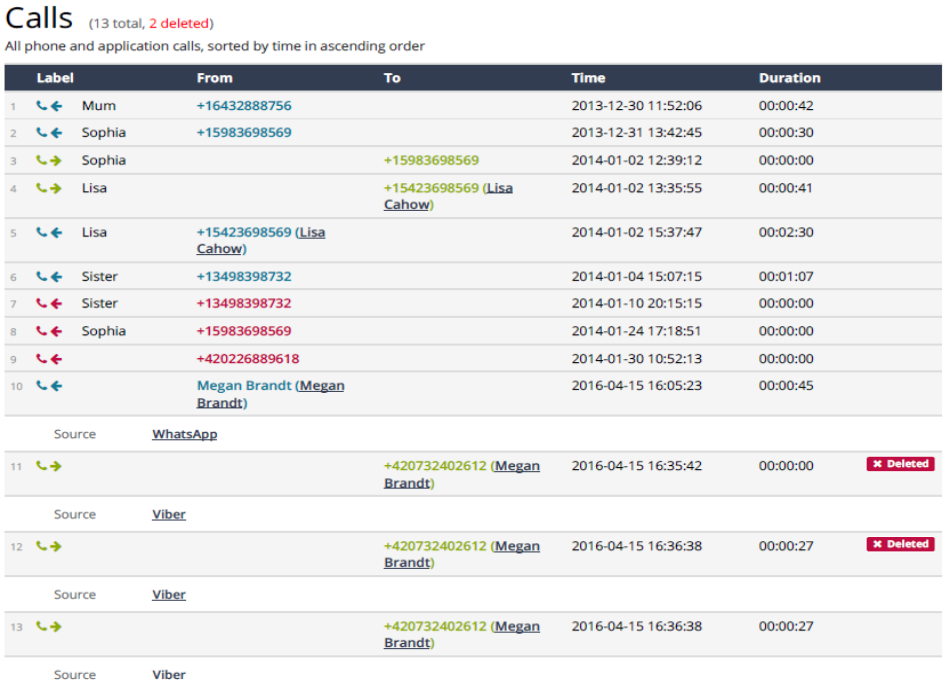
Budući da gotovo svi koriste mobilni uređaj, vrlo je djelotvorno moći vidjeti aktivnosti zapisnika poziva osumnjičenika kako bi dobili potencijalne tragove zločina. Zapisnici poziva dolaze iz dva različita izvora. Jedan je od samog mobilnog uređaja osumnjičenog, a drugi od dnevnika koji se vode kod telekom operatora ili pružatelja mobilne mreže. Iako zapisnici poziva u mobilnom uređaju oduzetog sumnjivca mogu otkriti važne pojedinosti, možda neće biti pouzdani jer bi uređaj korisnika mogao izbrisati zapise poziva. Međutim, zapisnici poziva koji se vode kod telekom operatora su vrlo pouzdani. Prema zakonu, svi telekom operatori moraju održavati automatske zapise poziva svakog od svojih klijenata. Taj mehanizam se automatizira uz pomoć softvera u prostorijama telekomunikacijskog operatora. Softver koristi pojedinosti o pozivu kako bi generirao račune klijentima, vodio evidenciju zapisa itd., [55].

Na svaki poziv korisnika uređaja, softver za naplatu kod telekom operatera pohranit će pojedinosti o pozivu, kao što su broj mobitela pozivatelja i broj mobitela primatelja, njihove IMEI brojeve, pojedinosti o tornju u kojima oba razgovaraju, datum i vrijeme početka poziva, trajanje poziva, itd. Ove pojedinosti koriste telekom operatori za obavljanje naplate svakog poziva i praćenje korisničke mreže korisnika. U bitnim forenzičkim slučajevima, odvjetnička

agencija ili vlada mogu zatražiti detaljan zapisnik poziva osumnjičene osobe od telekom operatora. Taj zahtjev treba biti pravni i mora se dobiti pravni poredak od viših dužnosnika. Osim, ako je telekom operator zadržao pravo uskraćivanja otkrivanja zapisnika poziva svojih korisnika. Zapisnici poziva su privatne evidencije o aktivnostima korisnika i telekom operatori služe za čuvanje povjerljivosti tih evidencija s izuzetkom objavljivanja zakonskih agencija na vlasti prema zakonu. Zapisnici poziva dobiveni od telekom operatora bili bi u obliku baze podataka ili formata datoteka MS-Excel. Ovi podaci mogu biti vrlo veliki i ručna istraga po tim podacima može biti vrlo veliki napor za forenzičke istražitelje. Kako pravni slučajevi trebaju biti pravovremeno riješeni, važno je da istražiteljske agencije koriste softver koji pomaže istražitelju da brzo i točno provede analizu, [39].

Iz zapisa poziva na mobilnom uređaju može se doći do vrlo bitnih podataka koji mogu razriješiti razne slučajeve u forenzičkoj istrazi, a neki od njih su, [55]:

- Datumi i vremena poziva
- Trajanje poziva
- Učestalost uspostave poziva
- Broj pozivatelja
- Favorite, odnosno koji se korisnici najčešće kontaktiraju
- Preslušavanje obavljenog razgovora
- Otkrivanje identiteta korisnika pomoću glasa itd.



Calls (13 total, 2 deleted)

All phone and application calls, sorted by time in ascending order

| | Label | From | To | Time | Duration | |
|---|---|---|---|---|---|---|
| 1 | Mum | +16432888756 | | 2013-12-30 11:52:06 | 00:00:42 | |
| 2 | Sophia | +15983698569 | | 2013-12-31 13:42:45 | 00:00:30 | |
| 3 | Sophia | | +15983698569 | 2014-01-02 12:39:12 | 00:00:00 | |
| 4 | Lisa | | +15423698569 (Lisa Cahow) | 2014-01-02 13:35:55 | 00:00:41 | |
| 5 | Lisa | +15423698569 (Lisa Cahow) | | 2014-01-02 15:37:47 | 00:02:30 | |
| 6 | Sister | +13498398732 | | 2014-01-04 15:07:15 | 00:01:07 | |
| 7 | Sister | +13498398732 | | 2014-01-10 20:15:15 | 00:00:00 | |
| 8 | Sophia | +15983698569 | | 2014-01-24 17:18:51 | 00:00:00 | |
| 9 | | +420226889618 | | 2014-01-30 10:52:13 | 00:00:00 | |
| 10 | | Megan Brandt (Megan Brandt) | | 2016-04-15 16:05:23 | 00:00:45 | |
| | Source | WhatsApp | | | | |
| 11 | | | +420732402612 (Megan Brandt) | 2016-04-15 16:35:42 | 00:00:00 | Deleted |
| | Source | Viber | | | | |
| 12 | | | +420732402612 (Megan Brandt) | 2016-04-15 16:36:38 | 00:00:27 | Deleted |
| | Source | Viber | | | | |
| 13 | | | +420732402612 (Megan Brandt) | 2016-04-15 16:36:38 | 00:00:27 | |
| | Source | Viber | | | | |

**Slika 13**: Prikaz ekstrakcije iz poziva, [56]

### 5.4.8. Društvene mreže

Postoji jako puno dokaza o lokalnom uređaju koji pristupa društvenim medijima i samim poslužiteljima društvenih medija. Cusack i Son su 2012. godine otkrili da, iako postoje brojni alati za izdvajanje dokaza iz društvenih medija, funkcionalnost se uvelike razlikuje, a najbolji rezultati mogu ovisiti o onome što istraživač posebno traži, kao što su prijave ili zapisnici za razgovor. Zawoad i Hasan, 2013. godine primjećuju da postoje kritički forenzički problemi s *cloud*-om, kao što su fizička nepristupačnost, podaci brojnih pojedinaca koji se miješaju i problemi s lancem skrbništva, gdje je mjesto poslužitelja nepoznato. Delport, Kohn i Olivier su 2011. istražili višestruke metode za izoliranje podataka iz oblaka za ekstrakciju, s mješovitim rezultatima sličnim Cusackovom i Sonovom pokušaju na društvenim medijima, [57].

Istraživanja su se usredotočila na izravnu vezu ili aplikaciju gdje korisnici unose određeni stupanj podataka, ali često završavaju dijeljenje više od namjeravanih zbog metapodataka i korporativnog pretraživanja podataka. Na primjer, Facebook koristi ciljane oglase na temelju korisničkih podataka i Google nudi slične oglase analizom sadržaja Gmail-a. Međutim, druge usluge mogu prikupljati, sastavljati i mijenjati osobne podatke neizravno, kao što su aplikacije koje traže dopuštenje za pokretanje određenih podataka. Takve neizravne usluge, poput igara ili GPS alata, također bi mogle pružati slične informacije u svrhu istrage i vjerojatno predstavljaju novi put za digitalne dokaze koji se kreću naprijed, [58].

Znanstveno istraživanje uključilo je i istraživanje artefakata ostavljenih društvenim mrežnim mjestima na računalnim sustavima i alatima koji pomažu u vađenju tih artefakata. Budući da su mnoge aplikacije za društveno umrežavanje integrirane u nove pametne telefone, u slučajevima koji uključuju društvene mreže, forenzični ispitivači mogu pronaći odgovarajuće dokaze o smartphoneu osumnjičenog. Forenzički pregled iPhone 3GS-a (putem logičke akvizicije) pokazao je da se baza podataka povezana s Facebook aplikacijom pohranjuje na memoriju uređaja. Baza podataka pohranjuje podatke za svakog prijatelja na popisu, uključujući njihova imena, ID brojeve i telefonski broj. Dva druga direktorija povezana s programom Twitter također se mogu pronaći. Ovi imenici pohranjuju podatke o podacima o Twitter računu, privitcima poslanim s tweetovima s datumom i vremenskim vrijednostima. Forenzički pregled logičke slike Android telefona prikazuje da su osnovne informacije o Facebook prijateljima pohranjene u bazama podataka kontakata (contacts.db) jer uređaj sinkronizira Facebook-ove ažurirane statuse kontakta s telefonskim imenikom. Također, Android uređaj pohranjuje Twitter lozinke i Twitter ažuriranja koja se izvode putem Twitter aplikacije u običnom tekstu, [57].

Ovisno o prirodi istrage, nadležnosti i stupanj do kojeg socijalni umreživač surađuje s policijom, pružatelj usluga može biti prikladniji izvor digitalnih dokaza o korištenju društvenog umrežavanja pametnog telefona. Međutim, istraga pametnog telefona ima dvostruku vrijednost. Često je korisno potkrijepiti dokaze iz različitih izvora, kao npr. od pružatelja usluga, a zatim s pametnog telefona. Štoviše, posebno u doba sveprisutnih mobilnih internetskih veza, mnoge tradicionalne telefonske usluge (kao što su tekstualne poruke)

pružaju se putem društvenih mrežnih mjesta putem svojih aplikacija za pametne telefone, [58].

### 5.4.9. Memorijske kartice

Kapacitet pohrane memorijske kartice kreće se od 128 MB na više. Kao tehnološki napredak, takvi mediji postaju fizički manji i nude veće gustoće pohranjivanja. Izmjenjivi mediji proširuju kapacitet pohrane mobilnih uređaja koji omogućuju pojedincima pohranu dodatnih datoteka izvan ugrađenog kapaciteta uređaja i dijeljene podataka između kompatibilnih uređaja, [7].

Neki alati za forenziku mogu ekstrahirati sadržaj memorijskih kartica, iako mnogi i ne. Ako je stjecanje, tj. dobava podataka logična, izbrisani podaci koji se nalaze na kartici neće se vratiti. Srećom, takvi mediji mogu se tretirati slično prijenosnom disku i analizirati pomoću konvencionalnih forenzičkih alata uz upotrebu vanjskog čitača medija, [59].

Fizička akvizicija podataka prisutnih na uklonjivim medijima omogućuje ispitivačima potencijal za pretraživanje sadržaja medija i potencijalno oporavak izbrisanih datoteka. Jedan od nedostataka je taj da podatak mobilnih uređaja, kao što su tekstualne SMS poruke, može zahtijevati ručno dekodiranje ili zaseban alat za dekodiranje kako bi se interpretiralo. Ozbiljnije pitanje je da značajke sadržaja uključene u karticu mogu blokirati oporavak podataka. Na primjer, BlackBerry uređaji pružaju korisniku mogućnost šifriranja podataka koji se nalaze na prijenosnom mediju povezanom s mobilnim uređajem, [7].

# 6. Anketni upitnik – osviještenost korisnika o prikupljanju podataka terminalnih uređaja

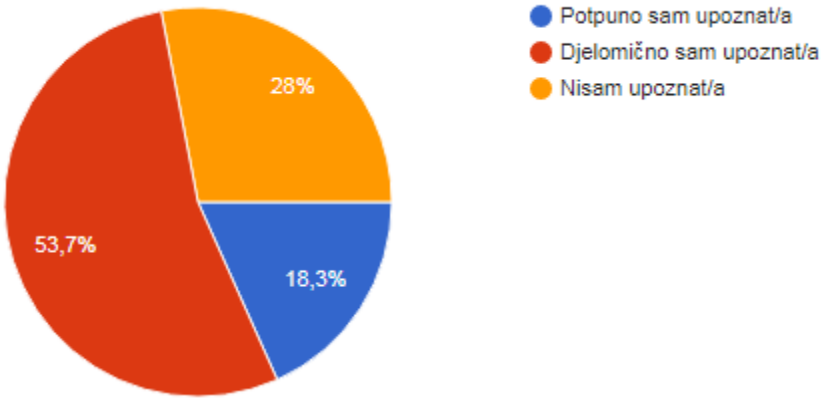
Istraživanje o osviještenosti korisnika o prikupljanju podataka terminalnih uređaja za potrebe završnog rada provelo se elektronskim putem, a istraživanje je bilo sastavljeno od 15 pitanja vezanih uz navedenu tematiku uz dodatna dva pitanja koja ispituju spol i starost.

Istraživanje se provelo nad 82 ispitanika, od čega je 80.5% (66 ispitanika) bilo muškog spola, a 19.5% (16 ispitanika) ženskog spola. Najviše ispitanika je u dobnoj granici od 18-24 godine, njih 52, zatim 15 ispitanika je u dobnoj granici od 24-30 godina, 30-40 godina ima 8 ispitanika, dok najmanje zastupljene dobne granice u istraživanju su one ispod 18 godina (4 ispitanika) i ona iznad 40 godina (3 ispitanika).

Cilj anketnog upitnika bio je provjeriti koliko su korisnici mobilnih terminalnih uređaja svjesni pojma forenzičke analize i što se forenzičkom analizom može ekstrahirati iz njihovih uređaja.

U nastavku slijede pitanja anketnog upitnika popraćena grafikonima

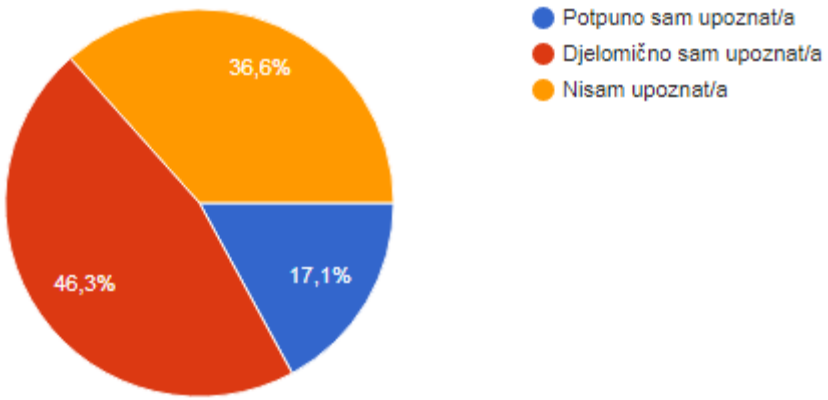
**Koliko ste upoznati s pojmom forenzička analiza?**




**Grafikon 1**: Pojam forenzičke analize

Iz grafikona 1 vidljivo je da je većina ispitanika djelomično upoznata s pojmom forenzičke analize, njih 44 (53.7%) što i ne čudi jer se pojam forenzičke analize mobilnih uređaja sve češće pojavljuje u javnosti. Njih 23 (28%) nije uopće upoznato s pojmom forenzičke analize te u sljedećim pitanjima će se to odraziti na osviještenost o ekstrahiranju podataka iz mobilnih uređaja. Potpuno je upoznato 15 ispitanika, a to su vjerojatno ispitanici koji se bave ICT tematikom.

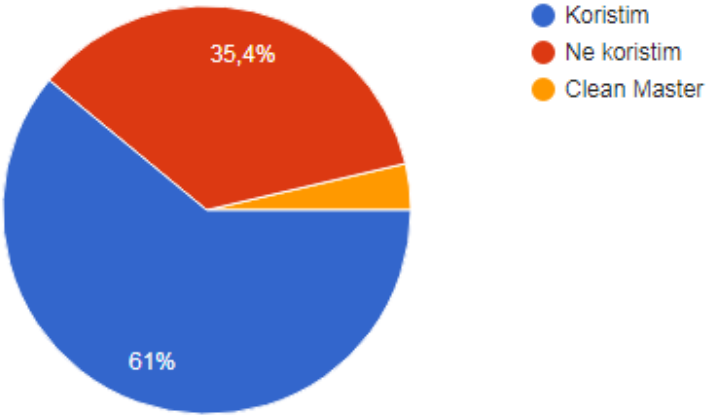
**Koliko ste upoznati s pojmom ekstrakcija podataka?**




**Grafikon 2**: Pojam ekstrakcije podataka

Za razliku od grafikona 1, u ovom grafikonu je osviještenost korisnika o samom pojmu manja. Ekstrakcija podataka je pojam puno više vezan uz ICT tematiku nego forenzička analiza pa i ne čudi da su rezultati istraživanja ovakvi. Naime, opet je najviše ispitanika koji su djelomično upoznati s pojmom ekstrakcije podataka, njih 38 (46,3%), zatim slijede ispitanici koji nisu upoznati s pojmom, njih 30 (36,6%), a 14 ispitanika (17,1%) je potpuno upoznato s pojmom ekstrakcije podataka.

**Koristite li antivirusni program ili neki drugi oblik zaštite mobilnog uređaja? (ako da, navesti koji)**

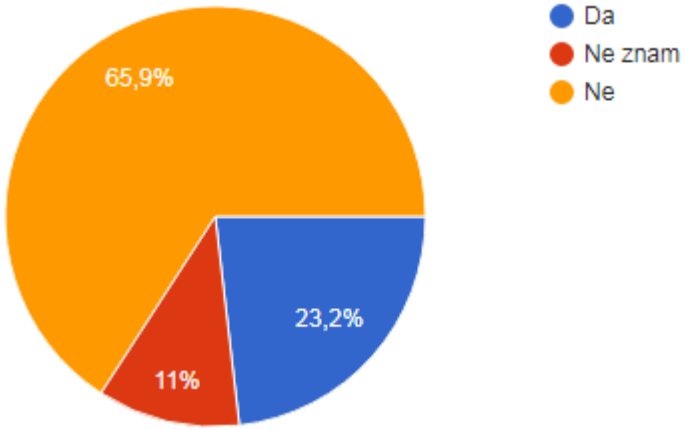



**Grafikon 3**: Prikaz korištenja antivirusnog programa

Iz grafikona 3 vidljivo je da većina korisnika razumije opasnosti koje vrebaju prilikom posjećivanja raznih Internetskih stranica pa koriste antivirusni program kako bi preventivno djelovali u tu svrhu, to čini njih 50 (61%). Pomalo je zabrinjavajuće da čak 29 ispitanika

(35,4%) ne koristi nikakav način zaštite njihovih mobilnih uređaja. Mali dio korisnika koristi program Clean Master za sigurnost njihovih uređaja, njih 3 (3,6%).

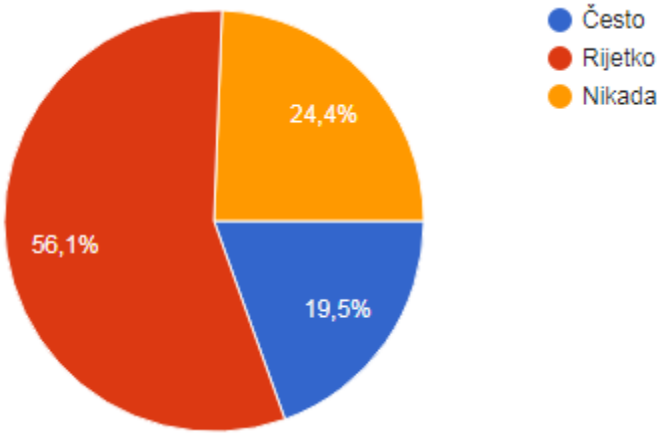
**Smatrate li da se ručno (samostalno) izbrisani podaci u potpunosti brišu s vašeg mobilnog uređaja i da se njima više ne može pristupiti ni na jedan način?**




**Grafikon 4**: Svijest korisnika o brisanju podataka s mobilnih uređaja

Grafikon 4 prikazuje da većina ispitanih osoba razumije da se samostalno izbrisani podaci ne brišu u potpunosti s mobilnog uređaja i da se do njih može doći na neki način, što je vrlo pozitivno. To smatra njih 54 (65,9%), dok 19 ispitanika (23,2%) smatra da se podaci u potpunosti brišu s uređaja. Njih 9 (11%) ne zna ili nije sigurno da se podaci brišu u potpunosti.

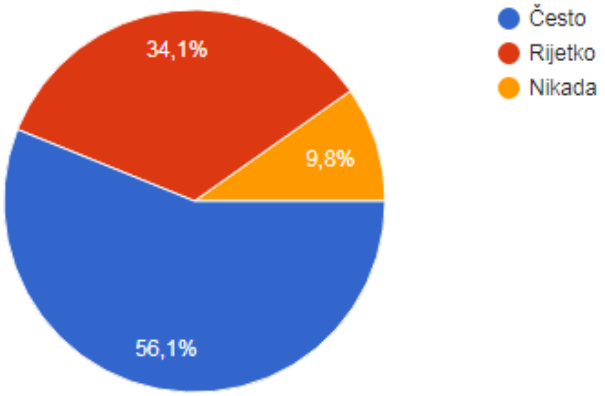
**Koliko često mijenjate lozinke vaših računa (Facebook, Google, ostale aplikacije) na mobilnom uređaju?**




**Grafikon 5**: Mijenjanje lozinki raznih korisničkih računa

Grafikon 5 pokazuje da veliki dio ispitanika rijetko mijenja lozinke svojih računa, što nije pohvalno. To smatra 46 ispitanika (56,1%), što znači da nisu svjesni da se do njihovih lozinki na mobilnom uređaju može doći lako jer se pohranjuju svaki put kada ih korisnik unese. Još veći problem je u 20 ispitanika (24,4%) koji nikada ne mijenjaju svoje lozinke. Mali dio ispitanika je svjestan mogućih problema ako se lozinke ne mijenjaju i ažuriraju često, njih 16 (19,5%).

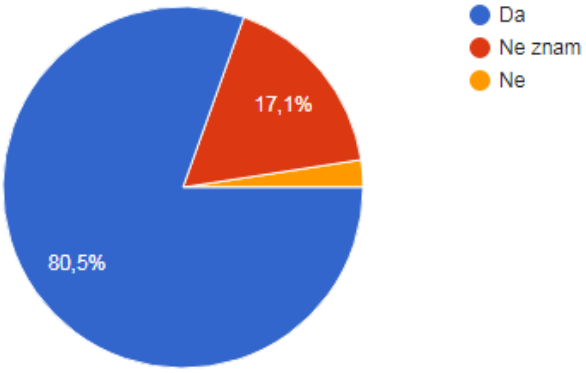
**Koliko često ažurirate aplikacije na vašem mobilnom uređaju?**




**Grafikon 6**: Učestalost ažuriranja aplikacija na mobilnom uređaju

U grafikonu 6 prikazana je učestalost ažuriranja aplikacija, koja je također bitna za sigurnost mobilnog uređaja, jer u određenim aplikacijama ostaju pohranjene aktivnosti korisnika i ako se ne ažuriraju često može doći do otkrivanja raznih korisničkih podataka. Ovaj grafikon pokazuje da većina korisnika često ažurira aplikacije, njih 46 (56,1%) te da su svjesni mogućih problema ako se aplikacije ne ažuriraju redovito. Rijetko ažurira 28 ispitanika (34,1%), a nikada 8 ispitanika (9,8%).

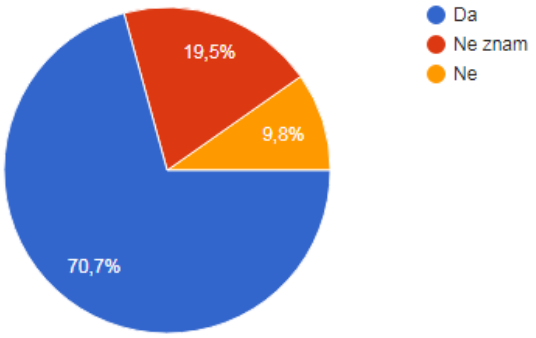
**Smatrate li da podaci iz mobilnih uređaja, tj. digitalni dokazi mogu biti korisni u otkrivanju raznih kriminalnih djela?**




**Grafikon 7**: Osviještenost korisnika o digitalnim dokazima kao pomoć u otkrivanju kriminalnih djela

Grafikon 7 pokazuje da većina ispitanika, odnosno njih 66 (80,5%) misli da podaci iz mobilnih uređaja mogu biti bitni u otkrivanju raznih kriminalnih djela, što je i točno. O tome se jako puno piše na raznim Internetskim stranicama i ovakvi rezultati su očekivani. Njih 14 (17,1%) nije sigurno da digitalni podaci mogu biti korisni u otkrivanju kriminalnih djela, a njih 2 (2,4%) smatra da digitalni dokazi nisu korisni u otkrivanju kriminalnih djela.

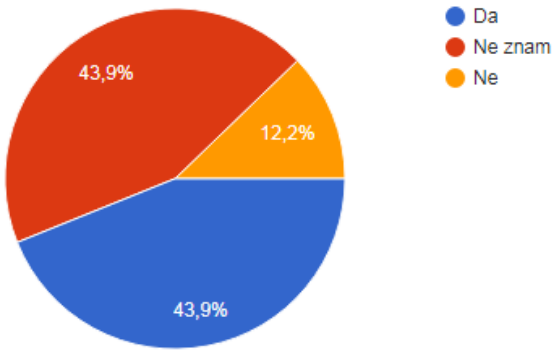
**Smatrate li da se forenzičkom analizom SIM kartice mobilnog uređaja može doći do: telefonskih brojeva upućenih/primljenih poziva, kontakata, pojedinostima o SMS-u (datum, vrijeme, primatelj, itd.), SMS teksta (sama poruka)?**




**Grafikon 8**: Osviještenost korisnika o digitalnim dokazima iz SIM kartice

Grafikon 8 pokazuje malo iznenađujuće rezultate jer veliki broj korisnika je svjestan da se forenzičkom analizom može doći do gore navedenih podataka. To je očito rezultat širenja računalnih tehnologija, što je vrlo dobro. Njih čak 58 (70,7%) smatra da se forenzičkom analizom može doći do mnogo podataka koje sadrži SIM kartica. Njih 16 ne zna može li se doći do navedenih podataka, jer vjerojatno nisu upoznati s pojmom forenzička analiza. 8 ispitanika (9,8%) smatra da se ne može doći do navedenih podataka.

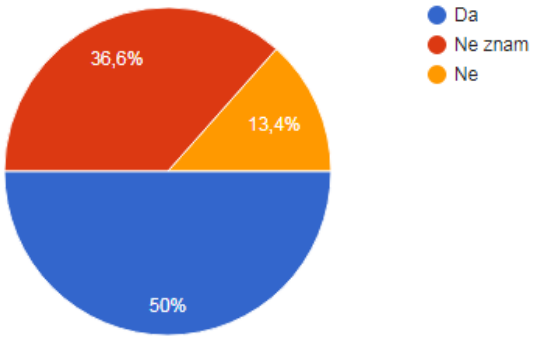
**Smatrate li da se forenzičkom analizom lokacije mobilnog uređaja može doći do: zapisnika tragova, putnih točaka, ruta, pohranjenih lokacija (dom, posao, dječji vrtić, itd.), sigurnosnih lokacija, nedavnih adresa, zapisnika poziva, povijesti uređaja, multimedijskih podataka)?**




**Grafikon 9**: Osviještenost korisnika o digitalnim dokazima iz lokacije mobilnog uređaja

Grafikon 9 prikazuje da su ispitanici podijeljeni u razmišljanju s lokacijom mobilnog uređaja i podacima koje ona sadržava. Lokacija mobilnog uređaja jedan je od najvećih izvora podataka i često se koristi za otkrivanje kriminalnih djela, a to smatra 36 ispitanika (43,9%), dok isto toliko ispitanika nije sigurno da se forenzičkom analizom može doći do navedenih podataka. 10 ispitanika (12,2%) smatra da se forenzičkom analizom lokacije ne može doći do podataka koji su od velikog značaja za otkrivanje kriminalnih djela.

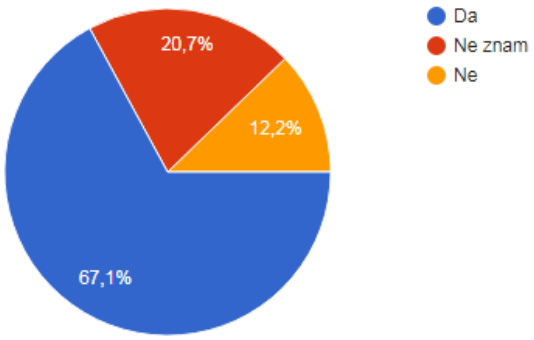
**Smatrate li da se forenzičkom analizom elektroničke pošte može doći do: izvorišne/odredišne IP adrese, privitaka s ekstenzijama (.doc, .xls, itd.), osoba koje su navedene u CC ili BCC poljima, osoba kojima je poruka proslijeđena, originalne poruke?**




**Grafikon 10**: Osviještenost korisnika o digitalnim dokazima iz elektroničke pošte

Za razliku od prethodnog grafikona, grafikon 10 pokazuje da su ispitanici više svjesni mogućih digitalnih dokaza kada se radi o elektroničkoj pošti. Razlog tomu je možda što više koriste elektroničku poštu nego lokaciju mobilnog uređaja. Pola od ukupnih ispitanika, njih 41 (50%) smatra da se do navedenih podataka može doći forenzičkom analizom. 30 ispitanika (36,6%) nije sigurno ili ne zna da se do podataka može doći forenzičkom analizom, a njih 11 (13,4%) smatra da se do podataka ne može nikako doći.

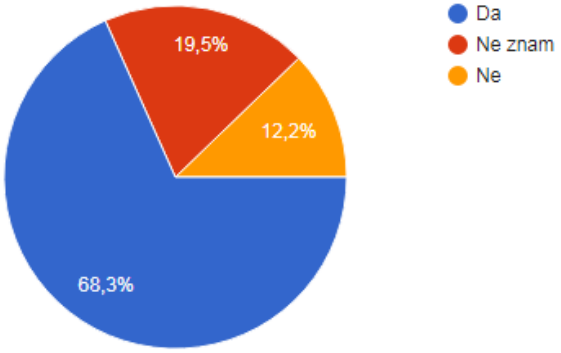
**Smatrate li da digitalna kamera mobilnog uređaja osim fotografija i videozapisa sadrži podatke kao što su: datum i vrijeme snimljene fotografije/videozapisa, lokaciju snimljene fotografije/videozapisa, veličinu snimljene fotografije/videozapisa?**




**Grafikon 11**: Osviještenost korisnika o digitalnim dokazima iz digitalne kamere

Grafikon 11 prikazuje osviještenost ispitanika o nevidljivim podacima koje skriva digitalna kamera mobilnog uređaja. Forenzičkom analizom digitalne kamere može se doći do različitih podataka, a to smatra 55 ispitanika (67,1%). Mnogi kriminalni slučajevi riješeni su uz pomoć gore navedenih podataka digitalne kamere. 17 ispitanika (20,7%) ne zna može li se do navedenih podataka doći forenzičkom analizom, a 10 ispitanika (12,2%) smatra da se do podataka ne može doći.

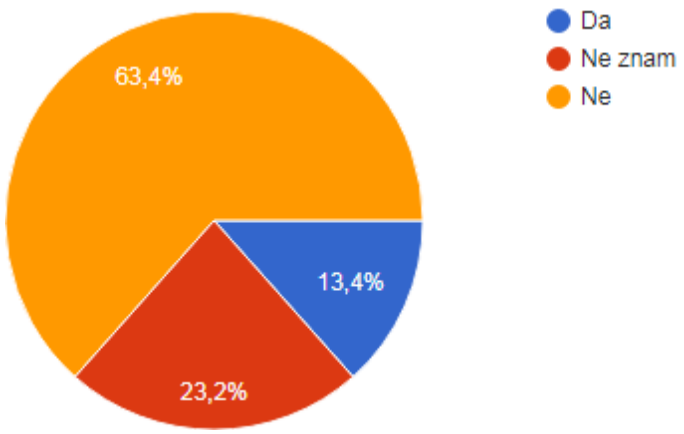
**Smatrate li da se forenzičkom analizom poziva mobilnih uređaja može doći do: datuma i vremena poziva, trajanja poziva, učestalosti uspostave poziva, broja pozivatelja, favorita (odnosno koji se korisnici najčešće kontaktiraju), preslušavanja obavljenog razgovora, otkrivanja identiteta korisnika pomoću glasa?**




**Grafikon 12**: Osviještenost korisnika o digitalnim dokazima iz poziva mobilnog uređaja

U grafikonu 11 vidljivo je da je većina ispitanika svjesna do čega se sve može doći forenzičkom analizom poziva, odnosno njih 56 (68,3%). Zapisnici poziva sadržavaju vrlo bitne dokaze kojima se mogu otkriti kriminalne radnje. Loše je što 10 ispitanika (12,2%) smatra da se do podataka ne može doći i da smatraju da je njihova privatnost zajamčena. 16 ispitanika ne zna, ili nije sigurno može li se doći do podataka.

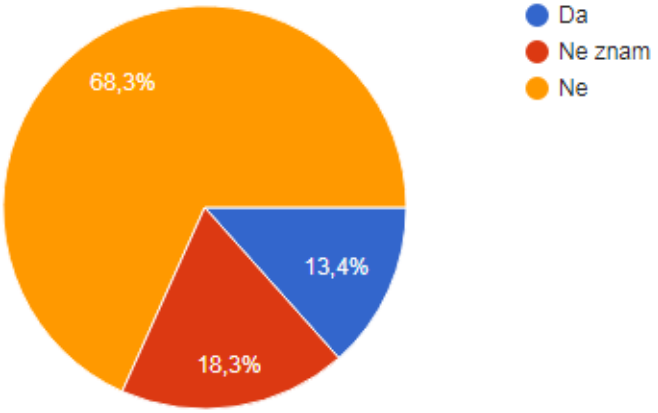
**Smatrate li da elementi (Webmail, povijest posjećenih stranica, Cookies (kolačići), ključne riječi korištene u pretragama, preuzete/pokrenute datoteke, lozinke, podaci koje je korisnik upisivao u formulare) na web preglednicima čuvaju vašu privatnost?**




**Grafikon 13**: Osviještenost korisnika o sigurnosti na web preglednicima

Grafikon 13 pokazuje da su korisnici vrlo svjesni nesigurnosti web preglednika i web stranica. Podaci koje korisnik upisuje u web preglednike, a i lozinke, ostaju pohranjene na njima i do njih je forenzičkom analizom vrlo lako doći. 52 ispitanika (63,4%) je u pravu i smatra da web preglednici ne čuvaju privatnost korisnika. Njih 19 (23,2%) ne zna, a 11 (13,4%) smatra da elementi web preglednika čuvaju privatnost korisnika.

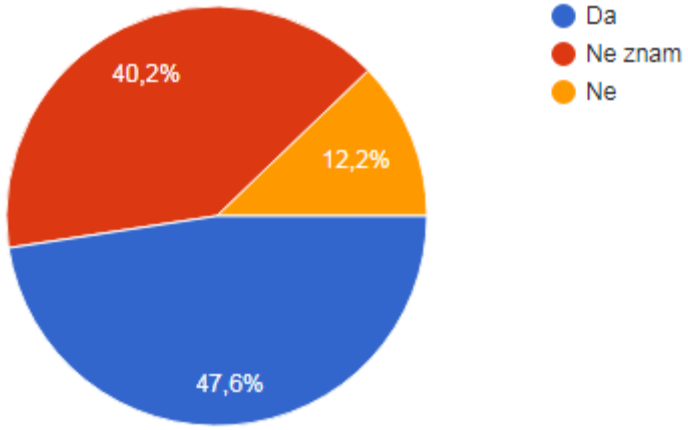
**Smatrate li da aplikacije društvenih mreža (Facebook, Twitter, itd.) čuvaju vašu privatnost?**




**Grafikon 14**: Osviještenost korisnika o sigurnosti društvenih mreža

U grafikonu 14 ispitano je smatraju li ispitanici da aplikacije društvenih mreža čuvaju privatnost korisnika. Kao što je bilo i za očekivati, većina njih smatra da ne čuvaju privatnost, njih 56 (68,3%). Razlog tomu je što su računi korisnika na društvenim mrežama često pod napadima i provalama. 15 (18,3%) ispitanika ne zna čuvaju li aplikacije društvenih mreža privatnost korisnika, dok 11 ispitanika (13,4%) smatraju da aplikacije društvenih mreža čuvaju privatnost korisnika.

**Smatrate li da se postupkom forenzičke analize mogu prikupiti gotovo svi digitalni podaci iz mobilnog uređaja?**




**Grafikon 15**: Osviještenost korisnika o prikupljanju svih digitalnih podataka iz mobilnog uređaja

Grafikon 15 prikazuje statistiku na zadnje pitanje istraživanja. Da se forenzičkom analizom mobilnog uređaja može doći do svih podataka, smatra 39 ispitanika (47,6%). Da se ne može doći do svih podataka, smatra 10 ispitanika (12,2%), a njih 33 (40,2%) ne zna. Dakle, zaključno ovim pitanjem može se utvrditi da je većina ispitanika svjesna pojma i značaja forenzičke analize.

# 7. Zaključak

Forenzička analiza mobilnih terminalnih uređaja u sve većem je porastu, jer računalne i mobilne tehnologije svakim danom napreduju. Broj kriminalnih djela povezanih s mobilnim i računalnim tehnologijama, također je svakim danom sve veći. U tu svrhu moraju se razvijati obrambene tehnologije, tj. načini kako će se ta kriminalna djela spriječiti i kako će se otkriti osoba koja je počinila zločin. Forenzička analiza tu djeluje kao najmoćnije sredstvo otkrivanja identiteta osumnjičenika. Također, može se zaključiti da pojam ekstrakcije podataka se sve više koristi, jer je pojam povezan s forenzičkom analizom. Forenzička analiza mobilnih terminalnih uređaja dugotrajan je proces jer može ovisiti o puno vanjskih faktora, kao što su operativni sustav, stanje uređaja, softver uređaja itd.

Za pravilnu provedbu forenzičke analize, potrebno je da je forenzički istražitelj dobro obučen za rad na određenom forenzičkom alatu i da je dobro upoznat sa slučajem koji istražuje. Alati za forenzičku analizu u prvom redu služe za olakšavanje u prikupljanju, čuvanju i ispitivanju podataka koji mogu biti od velikog značaja za eventualne sudske procese. Također, mogućnosti alata su proporcionalne njegovoj vrijednosti, a to znači da su zahtjevniji i skuplji alati mnogo bolji od jeftinih ili besplatnih, što je i logično.

Provedbom forenzičke analize nad mobilnim terminalnim uređajem, može se doći do ogromnog broja podataka vezanih uz korisnika. Izvori podataka, tj. digitalni dokazi dobivaju se pravilnom ekstrakcijom podataka. Ti digitalni dokazi, vrlo često se upotrebljavaju u sudskim procesima, jer otkrivaju podatke o aktivnostima korisnika. Forenzička analiza mobilnih terminalnih uređaja može se provoditi gotovo nad svim izvorima podataka, a većina njih je opisana u ovome radu.

Nad 82 ispitanika provedeno je istraživanje o osviještenosti korisnika o prikupljanju podataka terminalnih uređaja i rezultati su uglavnom očekivani. Iz istraživanja može se zaključiti da je svijest korisnika o sigurnosti mobilnih uređaja i mogućim digitalnim dokazima vrlo dobra, iako ima nedostataka. Dobro je to što većina korisnika smatra da se forenzičkom analizom može doći do podataka koji mogu biti od velikog značaja za sudske procese, ali loše je to što nekolicina ispitanika ne zna što je ustvari forenzička analiza i ekstrakcija podataka. Istraživanje je pokazalo da se forenzička analiza mora razvijati i biti što češći pojam u javnosti kako bi svijest korisnika o mogućim izvorima podataka s njihovih mobilnih uređaja bila još veća.

# Literatura


[1]URL:https://www.packtpub.com/mapt/book/Application%20Development/9781783288311/1/ch01lvl1sec09/mobile-phone-evidence-extraction-process (pristupljeno: travanj 2017.)

[2]URL:https://pdfs.semanticscholar.org/0d15/132439fc1de82724dd06effff5a782eefeac.pdf (pristupljeno travanj 2017.)

[3]URL:http://www.infosecurityeurope.com/__novadocuments/83665?v=635652368156170000 (pristupljeno travanj 2017.)

[4]URL:https://www.techopedia.com/definition/27805/digital-forensics (pristupljeno: travanj 2017.)

[5]Casey, E.: *Digital forensic and ivestigation*, USA, 2009.

[6]URL: http://icsa.cs.up.ac.za/issa/2014/Proceedings/Full/34_Paper.pdf (pristupljeno: travanj 2017.)

[7]URL:http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf (pristupljeno: travanj 2017.)

[8]URL:http://resources.infosecinstitute.com/mobile-forensics-investigation-process-model/#gref (pristupljeno: travanj 2017.)

[9]URL:https://www.nist.gov/sites/default/files/documents/forensics/2-Brothers-NIST-2014_Slides-23-Pages-2.pdf (pristupljeno: travanj 2017.)

[10]URL:http://airccse.org/journal/jcsit/0611csit02.pdf (pristupljeno: travanj 2017.)

[11]Alghafli, K.A., Jones, A., Martin, T.A.: *Forensic data acquisition methods for mobile phones*, London, 2012.

[12]URL:https://www.cclgroupltd.com/mobile-device-forensics-data-acquisition-types/ (pristupljeno: travanj 2017.)

[13]URL:http://www.cellebrite.com/Pages/file-system-extraction-of-mobile-data (pristupljeno: travanj 2017.)

[14]URL:https://www.fer.unizg.hr/_download/repository/RacFor-Dokumenti-Handouts-v13-pp.pdf (pristupljeno: travanj 2017.)

[15]URL:https://wiki.open.hr/wiki/Backup (pristupljeno: travanj 2017.)

[16]URL:http://detektiv-mreza.hr/hr/specijalnost/forenzika-mobilnih-uredaja-1 (pristupljeno: travanj 2017.)

[17]URL:https://standards.ieee.org/findstds/standard/1149.1-2013.html (pristupljeno: svibanj 2017.)

[18]URL:http://www.corelis.com/education/What-Is-JTAG.htm (pristupljeno: svibanj 2017.)

[19]URL:https://www.xjtag.com/about-jtag/jtag-a-technical-overview/ (pristupljeno: svibanj 2017.)

[20]URL:http://www.binaryintel.com/services/jtag-chip-off-forensics/chip-off_forensics/ (pristupljeno: svibanj 2017.)

[21]URL:http://www.studioag.pro/en/2011/10/le-flasher-box-per-lanalisi-forense-dei-cellulari/ (pristupljeno: svibanj 2017.)

[22]URL:http://www.forensicmag.com/product-release/2010/07/flasher-boxes-back-basics-mobile-phone-forensics (pristupljeno: svibanj 2017.)

[23]URL:https://www.linkedin.com/pulse/forenzi%C4%8Dka-analiza-mobilnih-ure%C4%91aja-miroslav-klarica (pristupljeno: svibanj 2017.)

[24]URL: https://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf (pristupljeno: kolovoz 2017.)

[25]URL:http://www.digital-evidence.org/papers/opensrc_legal.pdf (pristupljeno: kolovoz 2017.)

[26]URL:http://www.csoonline.com/article/2117658/investigations-forensics/rules-of-evidence---digital-forensics-tools.html (pristupljeno: kolovoz 2017.)

[27]URL:https://www.dhs.gov/sites/default/files/publications/Digital-Forensics-Tools-TN_0716-508.pdf (pristupljeno: kolovoz 2017.)

[28]URL:http://www.digital-evidence.org/papers/dfrws_define.pdf (pristupljeno: kolovoz 2018.)

[29]URL:https://www.msab.com/products/xry/ (pristupljeno: kolovoz 2017.)

[30]URL:http://img.informer.com/screenshots/3450/3450217_1_4.png (pristupljeno: kolovoz 2018.)

[31]URL: https://www.cellebrite.com/en/solutions/pro-series/ (pristupljeno: kolovoz 2017.)

[32]URL:http://www.diament.pl/diament/lc/celldek.html (pristupljeno: kolovoz 2017.)

[33]URL: https://wikileaks.org/spyfiles/docs/FORENSICTELECOMMUNICATIONS-2011-iXAMZeroFore-en.pdf (pristupljeno: kolovoz 2017.)

[34]URL:http://www.yuikee.com.hk/photos/Page27/P0019264.jpg (pristupljeno: kolovoz 2017.)

[35]URL: http://forensicswiki.org/wiki/MOBILedit! (pristupljeno: kolovoz 2017.)

[36]URL: http://mobiledit.mobiledit.com/img/mails/mef1.jpg (pristupljeno: kolovoz 2017.)

[37]URL:https://pdfs.semanticscholar.org/35d7/b7386ee91fc4576966259daf360b4754c1d0.pdf?_ga=2.92825179.718869684.1501156263-1854761517.1501156263 (pristupljeno: srpanj 2017.)

[38]URL:https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A163/datastream/PDF/view (pristupljeno: srpanj 2017.)

[39]URL:http://sigurnost.zemris.fer.hr/ostalo/2010_marceta/Diplomski.htm#_Toc261209076 (pristupljeno: srpanj 2017.)

[40]URL:https://www.academia.edu/27667604/Osnovne_karakteristike_digitalnih_dokaza (pristupljeno: srpanj 2017.)

[41]URL:https://www.omicsonline.org/open-access/forensic-importance-of-sim-cards-as-a-digital-evidence-2157-7145-1000322.pdf (pristupljeno: srpanj 2017.)

[42]URL:https://i0.wp.com/www.digitalforensicscorp.com/blog/wp-content/uploads/2017/05/Fig006-2.png?resize=665%2C455&ssl=1 (pristupljeno: srpanj 2017.)

[43]URL:https://www.gillware.com/forensics/gps-forensics (pristupljeno: srpanj 2017.)

[44]URL:http://guardian-forensics.com/gps-forensics/ (pristupljeno: srpanj 2017.)

[45]URL:https://www.systoolsgroup.com/email-forensics.html (pristupljeno: srpanj 2017.)

[46]URL:http://www.seoclick.com/images/search-email-evidence.gif (pristupljeno: srpanj 2017.)

[47]URL:https://www.researchgate.net/publication/300715450_New_Technique_of_Forensic_Analysis_for_Digital_Cameras_in_Mobile_Devices (pristupljeno: srpanj 2017.)

[48]URL:http://www.securitymagazine.com/articles/79807-digital-camera-forensics (pristupljeno: srpanj 2017.)

[49]URL:http://security.lss.hr/images/dokumenti/lss-pubdoc-2010-11-004.pdf (pristupljeno: srpanj 2017.)

[50]URL:http://www.cis.hr/WikiIS/doku.php?id=web_forenzika (pristupljeno: srpanj 2017.)

[51]URL:https://www.dfrws.org/sites/default/files/session-files/paper-advanced_evidence_collection_and_analysis_of_web_browser_activity.pdf (pristupljeno: srpanj 2017.)

[52]URL: http://www.nirsoft.net/utils/browsinghistoryview.png (pristupljeno: srpanj 2017.)

[53]URL:http://www.forensicswiki.org/wiki/SMS (pristupljeno: srpanj 2017.)

[54]Goel, S.: *Digital Forensis and Cyber Crime*, New York, 2009.

[55]URL: https://www.irjet.net/archives/V3/i7/IRJET-V3I7375.pdf (pristupljeno: srpanj 2017.)

[56]URL:https://static1.squarespace.com/static/574d60aef85082d3b6cb20d2/57c826fc29687f29e695aa16/57c826fd6b8f5bbd1033cf86/1472734975289/calls.png (pristupljeno: srpanj 2017.)

[57]URL: https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf (pristupljeno: srpanj 2017.)

[58]URL: http://digitalcommons.newhaven.edu/cgi/viewcontent.cgi?article=1016&context=electricalcomputerengineering-facpubs (pristupljeno: srpanj 2017.)

[59]URL:http://www.acquireforensics.com/services/data/memory-card.html (pristupljeno: srpanj 2017.)

# Popis kratica

| | |
|---|---|
| ASCII | (American Standard Code for Information Interchange) američki standard za razmjenu informacija |
| ASTM | (The American Society of Testing Materials) američko društvo za ispitivanje materijala |
| BCC | (Blind Carbon Copy) primatelji skrivenog e-maila |
| CC | (Carbon Copy) primatelji e-maila |
| CD | (Compact Disc) medij za pohranu koji koristi optički zapis za snimanje podataka |
| CDMA | (Code Division Multiple Access) kodna raspodjela kanala |
| CDR | (Call Detail Records) zapisi o detaljima poziva |
| CFA | (Color Filter Array) filter boja |
| CMOS | (Complementary Metal Oxide Semiconductor) tehnologija za izradu analognih i digitalnih mikroelektričnih sklopova |
| CPU | (Central Processing Unit) središnja procesorska jedinica |
| DF | (Dedicated File) podređena datoteka |
| DVD | (Digital Versatile Disc) optički disk koji se koristi za visokokvalitetno pohranjivanje informacija |
| EEPROM | (Electricaly Erasable Programmable Read Only Memory) električno izbrisiva programibilna ispisna memorija |
| EF | (Elementary File) elementarna datoteka |
| EPROM | (Erasable Programmable Read Only Memory) izbrisiva programibilna ispisna memorija |
| ESN | (Electronic Serial Number) elektronski serijski broj |
| EXIF | (Exchangeable Image File Format) format koji specificira formate za multimedijske sadržaje |
| FAT | (File Allocation Table) računalni datotečni sustav |
| FB | (Flasher Box) kutija za bljeskanje |
| FTK | (Forensic ToolKit) alat za forenzičku analizu |

| | |
|---|---|
| GPS | (Global Positioning System) američki navigacijski satelitski sustav |
| HLR | (Home Location Register) registar domaćih korisnika |
| HTCIA | (High Technology Crime Investigation Association) udruga za istraživanje visokog kriminala |
| IACIS | (International Association of Computer Investigative Specialists) grupni naziv za organizacije posvećene digitalnoj forenzici |
| IBM | (International Business Machines) američka računalna tvrtka, jedna od najrazvijenijih |
| ICT | (Information and Communication Technology) informacijsko-komunikacijska tehnologija |
| IDEN | (Integrated Digital Enhanced Network) mobilna telekomunikacijska tehnologija koja koristi kompresiju govora i višestruki pristup vremenskoj podjeli |
| IDS | (Intrusion Detection System) uređaj ili softver koji upravlja mrežom |
| IEEE | (Institute of Electrical and Electronics Engineers) svjetska organizacija za napredovanje računalnih tehnologija |
| IMAP | (Internet Message Access Protocol) protokol za preuzimanje elektronske pošte preko Interneta |
| IMEI | (International Mobile Equipment Identity) međunarodni broj mobilne opreme |
| IQM | (Image Quality Metrics) različite kvalitete slike |
| JTAG | (Joint Test Action Group) udruga elektroničkih industrija za razvijanje metode provjere dizajna i ispitivanja tiskanih pločica nakon izrade |
| LAI | (Location Area Information) podaci o lokacijskom području |
| LAN | (Local Area Network) lokalna mreža |
| MF | (Master File) glavna datoteka |
| MMS | (Multimedia Messaging Service) usluga slanja poruka koja uključuje multimedijske sadržaje |
| MTU | (Mobilni Terminalni Uređaj) krajnji uređaji u kojima se vrši pretvorba različitih vidova informacije u električne signale prilagođene za prijenos komunikacijskim kanalom, i obrnuto |

| | |
|---|---|
| OS | (Operativni sustav) skup osnovnih sustavnih programa koji upravljaju sklopovljem računala |
| OSI | (Open Systems Interconnection) model za otvoreno povezivanje sustava |
| PDA | (Personal Digital Assistant) uređaji koji olakšavaju svakodnevne aktivnosti |
| PIM | (Personal Information Management) aplikacije za upravljanje osobnim informacijama |
| PIN | (Personal Identification Number) tajna brojčana lozinka koja služi kao autentifikacija mobilnih uređaja |
| POP | (Post Office Protocol) protokol za prijenos e-pošte |
| PUK | (PIN Unblocking Key) zaštitni kod koji se koristi ako se nekoliko puta unese krivi PIN |
| RAM | (Random Access Memory) memorija s nasumičnim pristupom |
| RGB | (Reed Green Blue) osnovni kanal za prosječnu vrijednost piksela |
| RJ-45 | (Registered Jack 45) kabel koji se koristi u strukturnom kabliranju |
| ROM | (Read Only Memory) memorija iz koje se podaci mogu samo čitati |
| SIM | (Subscriber Identity Module) modul za identifikaciju pretplatnika |
| SMS | (Short Message Service) usluga slanja kratkih tekstualnih poruka |
| SMTP | (Simple Mail Transfer Protocol) protokol aplikacijskog sloja za prijenos e-pošte |
| SQL | (Structured Query Language) računalni jezik za upravljanje bazama podataka |
| SSD | (Solid State Drive) uređaj za pohranu podataka koji koristi integrirane krugove |
| TAP | (Test Access Point) priključna točka na čipu |
| TCK | (Test Clock) signal za sinkronizaciju rada unutrašnjih operacija uređaja |
| TDI | (Test Data In) signal za testiranje ili programiranje |
| TDO | Test Data Out) signal koji se prebacuje iz logike programiranja ili programiranja uređaja |
| TMS | (Test Mode Select) signal koji određuje sljedeće stanje |
| TRST | (Test Reset) signal koji može resetirati kontroler |

| | |
|---|---|
| UFED | (Universal Forensic Extraction Device) samostalni prijenosni uređaj za logičko stjecanje podataka s mobilnog uređaja |
| UICC | (Universal Integrated Circuit Card) univerzalni integrirani krug |
| URL | (Uniform Resource Locator) ujednačeni lokator sadržaja |
| USB | (Universal Serial Bus) tehnološko rješenje za komunikaciju računala s vanjskim uređajima |

# Popis slika

# Popis grafikona