

# Forenzički pristup zaštiti djece žrtava kaznenih djela

Djeca žrtve kaznenih djela predstavljaju jednu od najranjivijih skupina u kaznenopravnom sustavu. U takvim slučajevima, forenzički pristup omogućuje precizno i zakonito prikupljanje dokaza bez dodatnog ugrožavanja djetetove sigurnosti i dostojanstva. Kao policijski inspektor s dugogodišnjim iskustvom, svjedočim koliko je važna stručna i osjetljiva obrada svakog digitalnog traga. Cilj ove prezentacije je približiti forenzičku praksu stručnjacima koji sudjeluju u zaštiti djece, kako bismo zajedno djelovali učinkovitije i odgovornije. Iskustva iz prve ruke i stvarni primjeri iz prakse (uz zaštitu identiteta) pomoći će vam razumjeti složenost i važnost ovog posla koji svakodnevno obavljamo.

**D Denis**

**Rukavina**

Policijski





# Uvod: Zašto je dječja zaštita prioritet?

Zaštita djece je postao jedan od najvažnijih prioriteta modernog društva, posebice zbog alarmantnog porasta internetskih prijetnji i različitih oblika digitalnog zlostavljanja. Djeca provode sve više vremena na internetu, često bez adekvatnog nadzora i svijesti o opasnostima koje vrebaju.

**21%**

**Prijavljenih slučajeva**

Vezano uz digitalne platforme i online zlostavljanje

**78%**

**Porast slučajeva**

U posljednjih pet godina

**63%**

**Roditelja**

Nije svjesno digitalnih prijetnji kojima su izložena njihova djeca

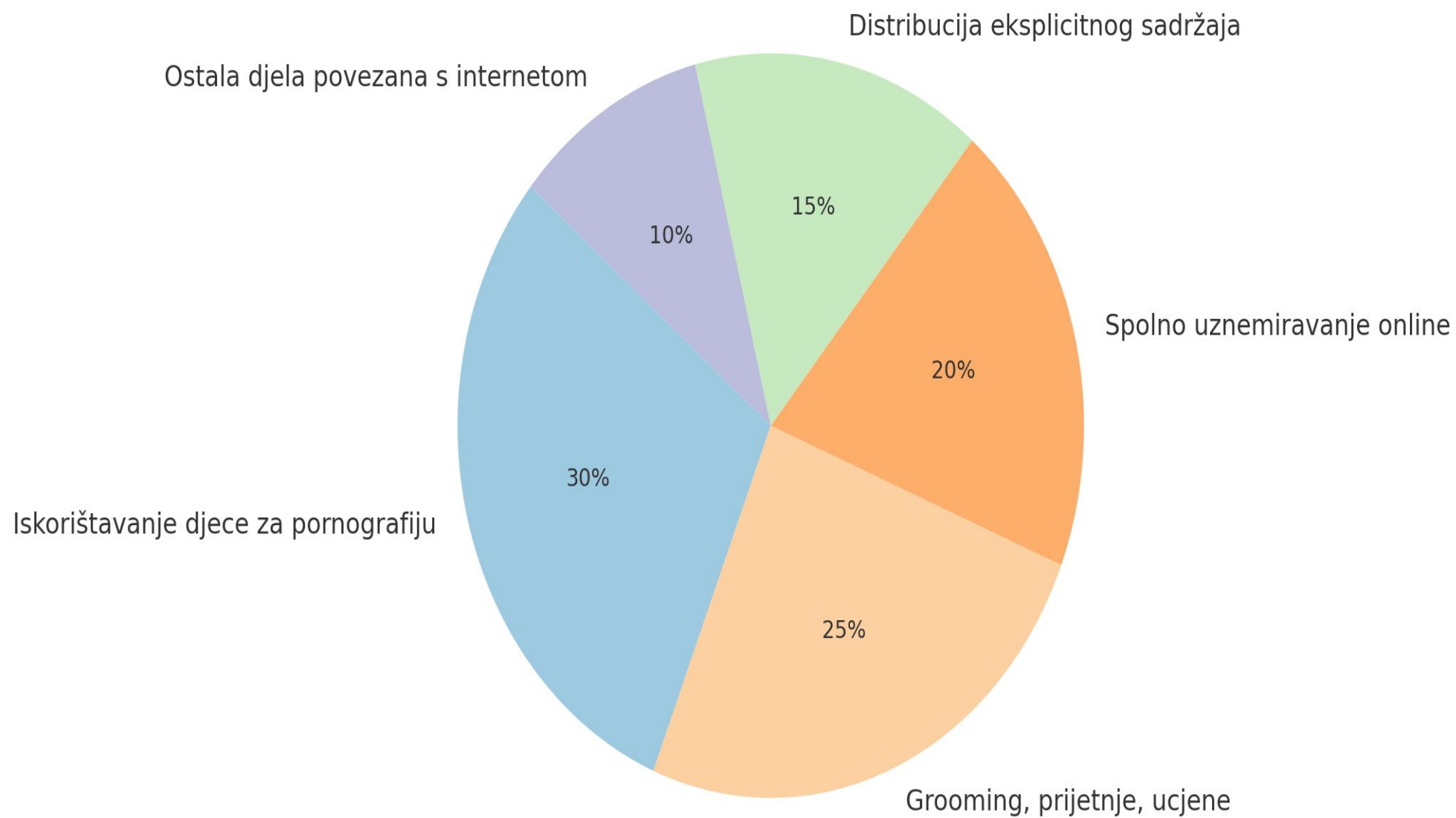
**40 - 50%**

**Kaznenih djela nad djecom putem digitalnih platformi ili uključuje digitalne dokaze**  
Ova brojka uključuje: online zlostavljanje,

seksualno iskorištavanje, prijetnje, grooming, ucjene, kao i distribuciju eksplicitnog sadržaja.

Naša istraživanja pokazuju da roditelji često precjenjuju svoju sposobnost zaštite djece u digitalnom okruženju, dok istovremeno podcjenjuju vještine manipulatora i predatora koji ciljano pristupaju djeci.

### Procijenjena raspodjela online kaznenih djela nad djecom u RH (2024.)



#### Najčešći oblici:

- Iskorištavanje za pornografiju (30%)
- Grooming, prijetnje i ucjene (25%)
- Spolno uznemiravanje online (20%)
- Distribucija eksplicitnog sadržaja (15%)
- Ostala djela povezana s internetom(10%)

# Uloga policijskog inspektora u zaštiti djece

Uloga policijskog inspektora u zaštiti djece je višedimenzionalna, osobito kad je riječ o slučajevima nasilja, zlostavljanja i kibernetičkog kriminaliteta. U koordinaciji s drugim institucijama, uvijek imajući u fokusu najbolji interes djeteta radi se kriminalističko istraživanje - **prikupljanje dokaza** i zaštita žrtve.



## Zaprimanje prijave

Od građana, škole, socijalnih službi ili automatizirane detekcije (osobno, e-mailom, pismeno)



## Inicijalna istraga

Procjena hitnosti i težinu prijave, prikupljanje dokaza, utvrđivanje identiteta, uključivanje DO I CZSS



## Multidisciplinarni pristup

Koordinirano djelovanje više institucija (osim spomenutih zdravstvo, škole, sudovi)



## Zaštitne mjere

Trenutne akcije za osiguranje sigurnosti djeteta

Ključni dio rada je analiza uloge policijskog inspektora u prikupljanju i obradi digitalnih dokaza te provođenju forenzičke istrage nad maloljetnim žrtvama, uz istovremenu zaštitu njihovih prava i dobrobiti kroz suradnju s drugim stručnjacima sustava zaštite djece.



## Hijerarhijska piramida zaštitnih mjera

### Psihološka podrška

Stručna pomoć djetetu u suočavanju s traumom.

### Hitne mjere CZSS-a

Brza reakcija CZSS-a za sigurnost djeteta.

### Privremeni smještaj djeteta

Smještaj djeteta na sigurno, uz stručni nadzor.

### Zabrana kontaktiranja

Počinitelju se zabranjuje svaki oblik kontakta.

### Zabrana približavanja

Zabrana dolaska u blizinu žrtve ili ustanove.

### Udaljenje počinitelja

Fizičko udaljenje iz djetetove okoline (dom, škola).

Te mjere se donose brzo, kako bi dijete bilo fizički i emocionalno zaštićeno dok postupak traje

# Najčešći oblici ugrožavanja djece

U svojoj praksi susrećem različite oblike ugrožavanja djece, pri čemu digitalno okruženje stvara nove oblike zlostavljanja koji se brzo razvijaju. Najčešći su cyberbullying (digitalno vršnjačko nasilje), grooming (mamljenje djece u svrhu seksualnog iskorištavanja) te različiti oblici seksualnog iskorištavanja.

## Cyberbullying

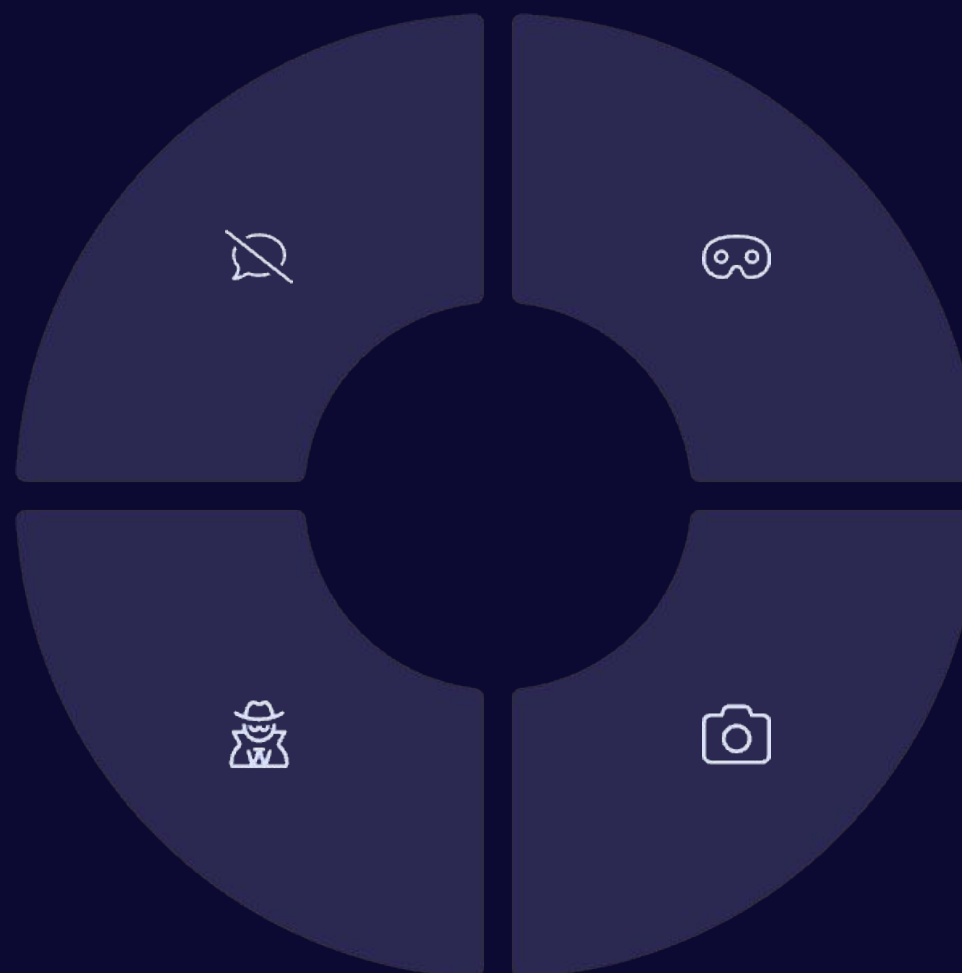
Sustavno uznemiravanje putem društvenih mreža, poruka i aplikacija

- Najčešće među vršnjacima
- Teško dokazivo zbog brisanja dokaza

## Identitetska prijevара

Korištenje dječjih podataka za lažno predstavljanje

- Stvaranje lažnih profila
- Pristupi osjetljivim podacima



## Grooming

Manipulativno stvaranje "prijateljstva" s ciljem seksualnog iskorištavanja

- Dugotrajna izgradnja povjerenja
- Često uključuje lažne profile

## Seksting i iznuda

Iznuđivanje i dijeljenje intimnih fotografija maloljetnika

- Brzo širenje sadržaja
- Teške psihološke posljedice



# Cyberbullying (digitalno vršnjačko nasilje)

Cyberbullying predstavlja sustavno uznemiravanje djeteta putem društvenih mreža, poruka i aplikacija. Najčešći primjeri takvog ponašanja uključuju izrugivanje, javno sramoćenje, širenje laži i manipulaciju slikama.



## Primjer iz Hrvatske

U Slavoniji je učenica osnovne škole bila izložena konstantnom vrijeđanju putem razredne WhatsApp grupe, uz manipulaciju njezine fotografije i dijeljenje po Instagramu. Podnesena je kaznena prijava zbog sumnje na povredu djetetovih prava.



## Tragičan slučaj Megan Meier

U SAD-u je slučaj 13-godišnje Megan Meier tragično završio samoubojstvom nakon što je bila žrtva lažnog profila koji je koristila odrasla susjeda kako bi ju emocionalno destabilizirala. Ovaj slučaj doveo je do promjena u zakonodavstvu nekoliko saveznih država.



# Grooming (digitalno zavođenje djece)

Grooming je proces manipulacije i izgradnje "prijateljstva" s djetetom s ciljem seksualnog iskorištavanja.

Karakterizira ga dugotrajno dopisivanje, izgradnja povjerenja i korištenje lažnih identiteta.



## Početni kontakt

Počinitelj uspostavlja kontakt predstavljajući se kao vršnjak ili osoba od povjerenja.



## Izgradnja povjerenja

Kroz mjesecе komunikacije gradi se lažni odnos povjerenja s djetetom.



## Manipulacija

Počinja traženje osobnih informacija i slanje neprimjerenog sadržaja.



## Pokušaj susreta

Krajnji cilj je često organiziranje fizičkog susreta s djetetom.

U Osijeku je 37-godišnji muškarac putem Instagrama kontaktirao 15-godišnju djevojčicu, predstavljajući se kao vršnjak. Nakon uspostavljanja povjerenja, počeo je slati neprimjerene poruke i pokušao dogovoriti susret. U Velikoj Britaniji, grooming bande koriste društvene mreže poput Snapchata i TikToka kako bi stupile u kontakt s djecom.

# Sexting i iznuda

## (sexortion)

Sexting i iznuda odnose se na dijeljenje intimnih fotografija maloljetnika, često pod ucjenom. Obilježja uključuju brzo širenje sadržaja, anonimni pritisak i psihološki šok kod žrtava.

### Početni kontakt i manipulacija

Počinitelj uspostavlja kontakt i gradi povjerenje, često kroz laskanje i manipulaciju.

### Dijeljenje intimnog sadržaja

Žrtva je nagovorena ili prisiljena na dijeljenje intimnih fotografija ili videozapisa.

### Ucjena i širenje sadržaja

Počinja ucjena za novac ili dodatni sadržaj, uz prijetnje širenjem materijala.

### Psihološke posljedice

Žrtve često pate od depresije, samopovlačenja ili pokušaja suicida.

U Splitu je 14-godišnji dječak bio žrtva sextortiona nakon što je nepoznatoj osobi putem Snapchata poslao fotografije – počinitelj je tražio novac i prijetio objavom. Tragičan slučaj 17-godišnje Rehtaeh Parsons iz Kanade, koja je počinila samoubojstvo nakon širenja fotografija seksualnog napada među vršnjacima, pokrenuo je važne zakonodavne promjene.



# Identitetska prijevvara (krađa digitalnog identiteta)

Identitetska prijevvara podrazumijeva korištenje osobnih podataka djeteta za lažno predstavljanje ili manipulaciju. Primjeri uključuju krađu profila, korištenje tuđih slika i stvaranje lažnih identiteta u svrhu napada na drugo dijete.

## Primjer iz Hrvatske

U Zagrebu su srednjoškolci stvorili lažni TikTok profil koristeći stvarne fotografije kolege, putem kojeg su vrijeđali druge učenike. Policija i škola su reagirali preventivno, a roditelji su obaviješteni.

## Primjer iz Njemačke

Identificirani su slučajevi u kojima su odrasli stvarali lažne profile koristeći fotografije djece kako bi stupili u kontakt s drugim maloljetnicima. Slučajevi su povezani s međunarodnim iskorištavanjem djece.

## Napomena

Identitetska prijevvara sve se češće događa u školskim okruženjima, a djeca nerijetko ne shvaćaju ozbiljnost ili kaznenu prirodu tih radnji.

# Prikupljanje digitalnih dokaza: Osnove

Digitalni dokazi predstavljaju temelj modernih istraga u zaštiti djece. Naši podaci pokazuju da čak 83% slučajeva uključuje neki oblik digitalnih tragova. Od presudne je važnosti pravilno prikupljanje ovih dokaza kako bi se očuvala njihova pravna valjanost.

## Mobilni uređaji

- Poruke, fotografije, aplikacije
- Podaci o lokaciji
- Povijest poziva
- Skriveno ili izbrisane datoteke

## Računala

- Povijest pregledavanja
- Spremljene datoteke
- Programi za komunikaciju
- Dnevnicu aktivnosti

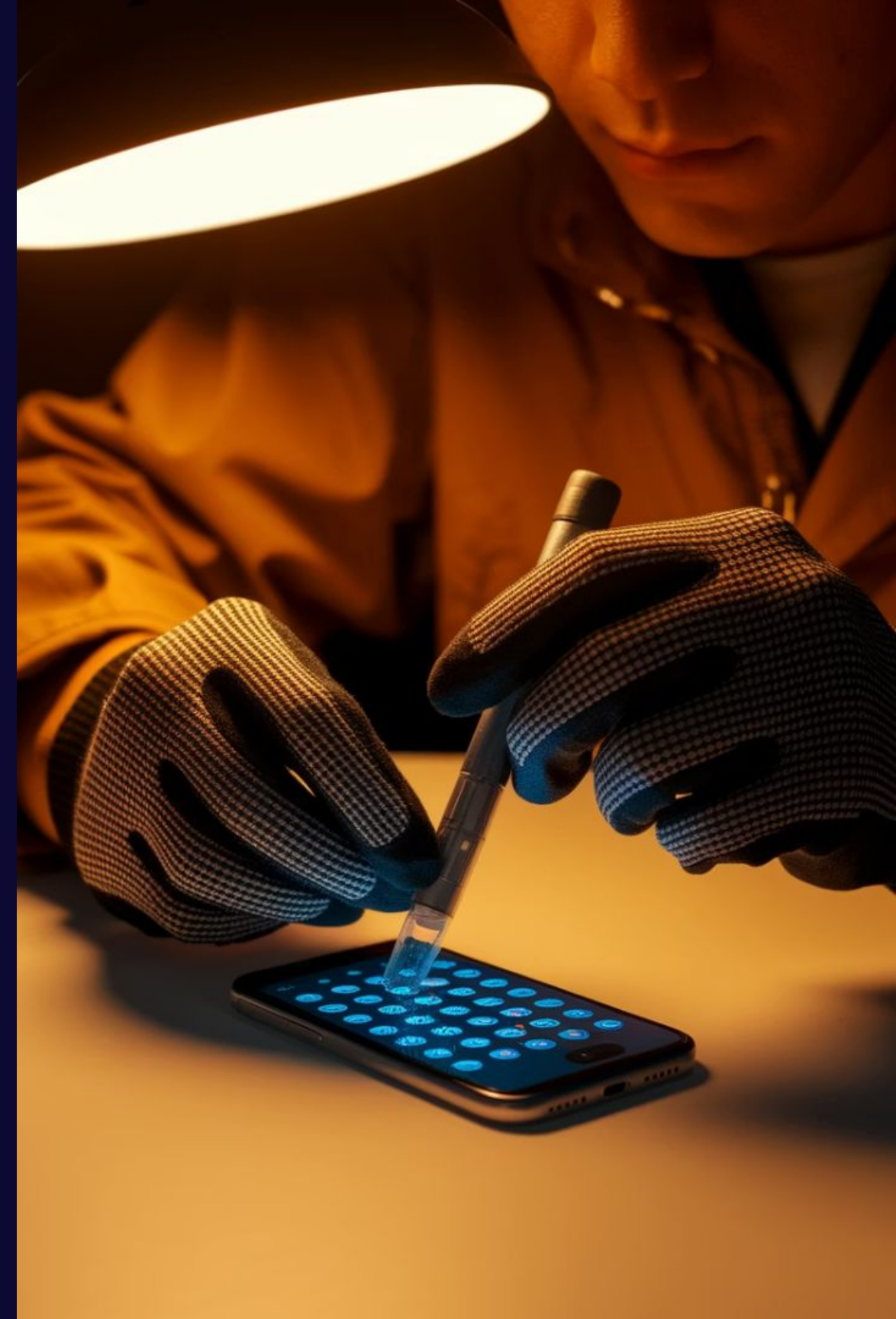
## Društvene mreže

- Javne i privatne komunikacije
- Kronologija aktivnosti
- Kontakti i veze
- Podaci o profilu

## Cloud servisi

- Spremljene fotografije i videozapisi
- Dijeljeni dokumenti
- Sigurnosne kopije poruka
- Podaci o pristupu

Kod prikupljanja digitalnih dokaza vrijedi pravilo "prvo što je sigurno" - prioritet je osiguravanje dokaza koji bi mogli biti najbrže izgubljeni, poput podataka u RAM memoriji ili privremenih datoteka.



# Alati i tehnike digitalne forenzike

Suvremena digitalna forenzika oslanja se na specijalizirane softverske alate koji omogućuju oporavak, analizu i prezentaciju digitalnih dokaza. Ovi alati moraju biti redovito ažurirani kako bi pratili brzinu tehnoloških promjena i novih metoda sakrivanja tragova.



## Forenzička akvizicija

Stvaranje točne kopije originalnih podataka bez ikakvih izmjena



## Dubinska analiza

Pretraga izbrisanih podataka, privremenih datoteka i skrivenih informacija



## Analiza metapodataka

Izvlačenje informacija o vremenu, lokaciji i uređaju iz digitalnih datoteka



## Vizualizacija povezanosti

Mapiranje komunikacijskih obrazaca i veza između osumnjičenih

Posebno su važni alati za oporavak izbrisanih poruka i fotografija, koji često otkrivaju ključne dokaze. Naša jedinica koristi kombinaciju komercijalnih (Cellebrite UFED, Cellebrite Physical Analyser, Magnet Axiom, EnCase, FTK) i open-source alata (Autopsy) kako bismo osigurali sveobuhvatnu analizu.

# Alati za otključavanje i brute force pristup uređajima

## BlackKey - Specijalizirani alat za forenziku

BlackKey je razvijen od BlackBag Technologies, danas dio Cellebrite grupacije.

Fizičkim spajanjem na uređaj omogućuje probiranje zaštita poput PIN-ova i uzoraka.

Koristi brute-force napade sistemskim isprobavanjem svih mogućih kombinacija.

Na starijim Android uređajima pokazuje posebnu učinkovitost zbog sigurnosnih propusta.



# GrayKey - Specijalizirani alat za iOS uređaje

## Funkcionalnosti

Razvijen od tvrtke Grayshift iz SAD-a, specijaliziran za probijanje iOS uređaja.

- Fizičko povezivanje s uređajem
- Zero-day exploit metode zaobilaznja zaštite
- Brute force napadi na lozinke

## Primjena

Primarno ga koriste sigurnosne agencije i policijske snage.

- Široka primjena u SAD-u i Ujedinjenom Kraljevstvu
- Ekstrakcija podataka bez znanja vlasnika
- Probijanje enkripcije bez ostavljanja tragova



# Poznati slučajevi u Europi i svijetu

Regija	Forenzički alati	Primjeri slučajeva
Europska unija	EnCase, XRY, Nuix	Operation Rescue, Project Childhood
SAD	FTK, BlackBag, Magnet AXIOM	Operation Safety Net, Innocent Images
Azija	UFED, Belkasoft, AccessData	Operation Blackwrist, Project VIC
Australija	Cellebrite, X-Ways, SANS SIFT	Task Force Argos, Operation Molto

# Europska Unija - Operativni uspjesi

## Operation Rescue

Jedna od najvećih međunarodnih akcija protiv dječje pornografije i digitalnog iskorištavanja.

- Razbijanje internetske zajednice s desecima tisuća članova
- Spašeno više od 230 djece
- Uhićeno gotovo 200 osumnjičenika diljem svijeta

## Project Childhood

Inicijativa za suzbijanje seksualnog iskorištavanja djece u turističkim destinacijama.

- Jačanje zakonskih okvira
- Edukacija lokalnih zajednica
- Podizanje kapaciteta policije za istrage i procesuiranje

## Koordinirana prevencija

EU osigurava resurse za kontinuiranu zaštitu djece.

- Financiranje specijaliziranih jedinica
- Prekogranična razmjena podataka
- Harmonizacija zakonodavstva među državama članicama

# Sjedinjene Američke Države

## Operation Safety Net

Proaktivna inicijativa za pronalazak nestale djece u Ohiju.

- Suradnja lokalne policije i američke službe maršala
- Fokus na djecu izloženu riziku trgovine ljudima
- Trenutačna zaštita i pomoć pronađenim maloljetnicima

## Innocent Images

FBI-jev specijalizirani program protiv online zlostavljanja.

- Razbijanje međunarodnih mreža dječje pornografije
- Identifikacija i procesuiranje počinitelja
- Edukativne kampanje o digitalnoj sigurnosti

## Tehnološki napredak

Kontinuirano ulaganje u digitalne forenzičke alate.

- Sustavi za prepoznavanje žrtava i počinitelja
- Napredni algoritmi za pretraživanje dark weba
- Međuagencijska razmjena podataka

# Azija i Australija

## Operation Blackwrist

Međunarodna akcija protiv kriminalne mreže na dark webu.

- Suradnja policijskih snaga Tajlanda, Australije i SAD-a
- Spašeno više desetaka djece
- Razbijanje organizirane mreže zlostavljača

## Project VIC

Globalna inicijativa za borbu protiv seksualne eksploatacije.

- Napredne tehnologije za identifikaciju žrtava
- Brza razmjena podataka među agencijama
- Učinkovitije procesuiranje počinitelja

## Task Force Argos



Specijalizirana jedinica australske policije.

- Infiltracija u mreže zlostavljača
- Praćenje kriminalnih aktivnosti na internetu
- Međunarodna suradnja u kompleksnim slučajevima

## Operation Molto



Velika nacionalna akcija protiv online zlostavljanja.

- Identifikacija stotine počinitelja
- Preko tisuću podignutih optužnica
- Spašavanje djece iz opasnih okruženja

# Hrvatska - Operativni uspjesi

Hrvatska policija kontinuirano sudjeluje u međunarodnim akcijama protiv seksualnog iskorištavanja djece.

## Operacija Stream / KidFlix (2025.)

Ugašena darknet platforma s gotovo dva milijuna korisnika. Provedena dva kriminalistička istraživanja i uhićen jedan počinitelj u Hrvatskoj.

## Operacija Fenris (2023.)

Akcija protiv dijeljenja sadržaja putem peer-to-peer mreža. Identificirano pet počinitelja koji su dijelili preko 46.000 datoteka zlostavljanja.



## Operacija Mozaik (2024.)

Koordinirana akcija s EUROPOL-om i regionalnim policijama. Identificirano 63 osumnjičenih koji su preko društvenih mreža zlorabljivali djecu.

# Zakonitost i lanac čuvanja digitalnog dokaza

Zakonitost digitalnih dokaza temelji se na strogom pridržavanju protokola o lancu čuvanja dokaza. Svaki propust u dokumentiranju tko je, kada i zašto imao pristup digitalnom dokazu može rezultirati njegovom neprihvatljivošću na sudu, čime se ugrožava cijeli slučaj.



Uz standardne mjere osiguranja fizičkih dokaza, posebno je izazovno osigurati lanac čuvanja za digitalne dokaze pohranjene u oblaku, gdje dokazi često prelaze državne granice i različite pravne sustave.

# Izazovi: Enkripcija, anonimizacija, dark web

Moderni kriminalci sve više koriste napredne tehnološke metode za prikrivanje tragova. Suočavamo se s jakom enkripcijom, anonimnim mrežama i komunikacijom putem dark weba, što značajno otežava otkrivanje i procesuiranje počinitelja kaznenih djela na štetu djece.

Izazov	Opis problema	Metode rješavanja	Uspješnost
Jaka enkripcija	24% zaplijenjenih uređaja koristi naprednu enkripciju cijelog diska	Forenzički zaobilazni mehanizmi, sudski nalozi	42% uspješno otključanih
Anonimne mreže	Korištenje VPN-a, Tor mreže i proxy servera	Suradnja s davateljima usluga, napredne metode praćenja	35% uspješne identifikacije
Dark web	Skrivene stranice i forumi za razmjenu ilegalnog sadržaja	Infiltracija, praćenje kriptovalutnih transakcija	28% uspješnih akcija
Samouništavajuće poruke	Aplikacije koje automatski brišu sadržaj nakon čitanja	Forenzičko oporavljanje iz cache memorije	53% djelomično uspješno

Napredak u dekriptiranju i forenzičkim alatima donosi optimizam, ali utrka između sigurnosnih tehnologija i kriminalnih metoda predstavlja stalni izazov za istražitelje u digitalnoj forenzici.

# Postupanje prema maloljetnim žrtvama: Etički principi

Pristup maloljetnim žrtvama zahtijeva posebnu osjetljivost i stručnost. Naš rad vodi se etičkim principima koji stavljaju dobrobit djeteta na prvo mjesto. Svaki razgovor i postupak prilagođavamo dobi, zrelosti i emocionalnom stanju djeteta, uz maksimalno izbjegavanje retraumatizacije.



## Najbolji interes djeteta

Svaka odluka i postupak mora prvenstveno služiti dobrobiti djeteta, čak i kad to komplicira istragu



## Prilagođena komunikacija

Korištenje jezika i pristupa prilagođenog dobi i razumijevanju djeteta, bez sugestivnih pitanja



## Minimalna intervencija

Ograničavanje broja razgovora i postupaka na minimum potreban za zaštitu i dokazivanje



## Multidisciplinarni pristup

Obvezna suradnja sa stručnjacima za mentalno zdravlje i dječju psihologiju tijekom cijelog procesa

Posebnu pažnju pridajemo stvaranju sigurnog okruženja za dijete tijekom cijelog postupka. To uključuje posebno opremljene prostorije za razgovor, mogućnost prisutnosti osobe od povjerenja i fleksibilnost u vremenskom rasporedu kako bi se dijete osjećalo što ugodnije.

# Prva intervencija i razgovor s djetetom

Prvi kontakt s djetetom žrtvom često određuje uspjeh cijelog postupka. Razgovor s djetetom provodi se uz prisutnost stručnjaka - psihologa ili socijalnog radnika - u posebno opremljenim prostorijama koje pružaju osjećaj sigurnosti. Koristimo NICHD (National Institute of Child Health and Human Development) protokol koji strukturira razgovor na način koji maksimizira dobivanje točnih informacija uz minimalan stres. NICHD protokol za forenzičko ispitivanje djece – koristi se u mnogim zemljama, uključujući i Hrvatsku, kao model za strukturirane, nenasilne razgovore s djecom žrtvama kaznenih djela.

## Uvodna faza i izgradnja povjerenja

Početak razgovora o neutralnim temama, objašnjavanje uloga prisutnih osoba, postavljanje osnovnih pravila razgovora (dopušteno je reći "ne znam" i ispraviti odraslu osobu).

Iz iskustva ističemo važnost strpljenja tijekom ovog procesa - dijete često treba vrijeme i nekoliko razgovora prije nego što može u potpunosti artikulirati traumatična iskustva. Forenzički pristup počinje u trenutku kada dijete kaže prvu rečenicu – jer sve što dijete ispriča može voditi do digitalnih tragova koji su ključni za kazneni postupak. Zato pristup mora biti strukturiran, nenametljiv i osjetljiv, u skladu s NICHD protokolom.

## Vježba narativnog pamćenja

Traženje od djeteta da opiše neki nedavni pozitivan događaj kako bi se uvježbalo slobodno pripovijedanje prije prelaska na teške teme.

## Fokusirani razgovor o događaju

Postupno uvođenje teme zlostavljanja, korištenje otvorenih pitanja, izbjegavanje sugestivnih pitanja, dopuštanje djetetu da svojim riječima opiše što se dogodilo.

## Dokumentiranje i zaključivanje

Audiovizualno snimanje razgovora, vraćanje na neutralne teme na kraju, informiranje djeteta o sljedećim koracima na njemu razumljiv način.

# Zaštita privatnosti i identiteta

## žrtve

Zaštita privatnosti maloljetnih žrtava nije samo etička odgovornost već i zakonska obveza. Dijete koje je već pretrpjelo zlostavljanje ne smije dodatno patiti zbog izlaganja javnosti ili curenja osjetljivih informacija. Naši protokoli osiguravaju maksimalnu zaštitu identiteta kroz cijeli pravosudni proces.

### Zakonska ograničenja

- Zabrana objavljivanja identiteta maloljetne žrtve
- Ograničen pristup spisima i dokazima
- Zatvorena ročišta bez prisutnosti javnosti
- Stroge kazne za curenje informacija

### Postupanje s dokumentacijom

- Šifriranje osobnih podataka u dokumentima
- Sigurno pohranjivanje materijala
- Kontrolirani pristup elektroničkim zapisima
- Uništavanje nepotrebnih kopija

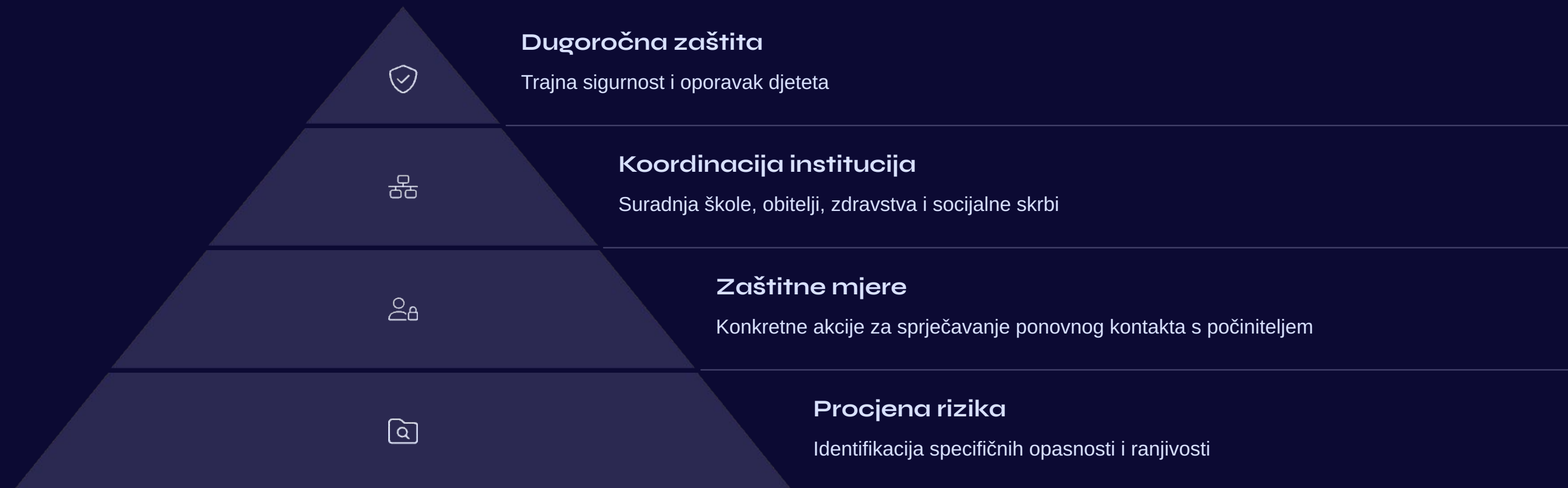
### Digitalna zaštita

- Enkripcija svih digitalnih dokaza
- Zaštićeni komunikacijski kanali
- Uklanjanje metapodataka iz slika
- Anonimizacija u digitalnoj forenzici

Poseban izazov predstavlja balansiranje između zaštite privatnosti djeteta i prikupljanja neophodnih dokaza, pogotovo u slučajevima kada su dokazi izrazito osobne prirode, poput fotografija ili video zapisa zlostavljanja. U takvim slučajevima primjenjujemo stroge protokole rukovanja i ograničavamo pristup samo najneophodnijim stručnjacima.

# Izrada sigurnosnog plana za dijete

Nakon identifikacije žrtve i početne intervencije, ključno je izraditi sveobuhvatni sigurnosni plan koji će dijete zaštititi od daljnje viktimizacije. Takav plan razvijamo kroz procjenu rizika i koordinaciju s relevantnim institucijama, pri čemu se uzimaju u obzir specifične okolnosti svakog djeteta.



Sigurnosni plan mora biti prilagodljiv i redovito ažuriran kako se mijenjaju okolnosti. Za djecu žrtve digitalnog zlostavljanja, plan često uključuje i digitalne sigurnosne mjere - promjene lozinki, privremeno uklanjanje profila na društvenim mrežama, instalaciju sigurnosnih aplikacija te edukaciju o digitalnoj zaštiti.

Posebna pažnja posvećuje se psihološkoj podršci djetetu, uključujući redovite terapijske sesije i praćenje emocionalnog stanja kako bi se na vrijeme uočile i adresirale posljedice traumatskog iskustva.

# Uloga roditelja/skrbnika u forenzičkom postupku

Roditelji ili skrbnici imaju dvojak uлогу u forenzičkom postupku - kao ključni izvori informacija i kao primarna podrška djetetu. Međutim, ponekad se suočavamo s izazovima kada su roditelji prestrašeni, preopterećeni ili u rijetkim slučajevima, umiješani u zlostavljanje. Naš pristup roditeljima temelji se na transparentnoj komunikaciji uz jasno definirana ograničenja.

## Prava roditelja/skrbnika

- Informacije o postupku i napretku istrage
- Prisutnost tijekom medicinskih pregleda
- Sudjelovanje u odlukama o sigurnosnom planu
- Pristup psihološkoj podršci i savjetovanju
- Pravna pomoć i zastupanje interesa djeteta

## Ograničenja

- Ne mogu biti prisutni tijekom forenzičkog intervjua
- Ograničen pristup detaljima iskaza i dokazima
- Ne smiju utjecati na iskaz djeteta
- U slučaju sumnje na umiješanost, moguće potpuno isključenje
- Podložni procjeni sposobnosti zaštite djeteta

Roditelje educiramo o važnosti njihove uloge u oporavku djeteta, pružajući im smjernice kako razgovarati s djetetom o traumatičnom iskustvu, kako prepoznati znakove traume i kada potražiti dodatnu stručnu pomoć. Naglašavamo da je njihova emocionalna reakcija ključna - dijete ne smije osjećati krivnju ili odgovornost za ono što mu se dogodilo ili za posljedice koje postupak ima na obitelj.

# Zakonski okvir RH i EU

Pravni okvir koji usmjerava naš rad u zaštiti djece obuhvaća nacionalno i europsko zakonodavstvo. Poznavanje ovih propisa ključno je za osiguravanje zakonitosti postupanja i maksimalne zaštite prava djeteta. Hrvatski zakonodavni okvir usklađen je s direktivama EU, ali postoje i specifičnosti našeg sustava.



## Zakon o kaznenom postupku

Definira posebne uvjete ispitivanja maloljetnih osoba, uključujući obveznu prisutnost stručnjaka, ograničen broj ispitivanja i mogućnost audiovizualnog snimanja iskaza kao dokaza na sudu bez ponovnog svjedočenja.



## Kazneni zakon

Sadrži strože kazne za kaznena djela na štetu djece, široku definiciju seksualnog iskorištavanja koja uključuje i digitalne oblike zlostavljanja te specifična kaznena djela vezana uz internet.



## Zakon o sudovima za mladež

Regulira postupke kada su djeca žrtve kaznenih djela, uz posebna pravila o hitnosti postupka, zaštiti privatnosti i obvezi specijalizacije svih stručnjaka uključenih u postupak.



## Direktiva 2011/93/EU

Europska direktiva o suzbijanju seksualnog zlostavljanja i iskorištavanja djece koja zahtijeva harmonizaciju kaznenog prava, preventivne mjere i posebna pravila za istragu i procesuiranje.

Posebno je važna implementacija Direktive 2011/93/EU koja je donijela značajne promjene u pristupu digitalnim dokazima i međunarodnoj suradnji u slučajevima koji prelaze granice država članica.

# Izazovi: Ograničeni rokovi za naloge za pretragu uređaja

Zakonodavni okvir (ZKP čl. 263. i 264.) propisuje vremenski ograničene naloge za pretragu digitalnih uređaja, često samo 72 sata.



# Tehnička složenost i zaštita uređaja

Najnoviji pametni telefoni poput iPhonea koriste napredne sustave zaštite koji uključuju:

- FaceID/TouchID biometrijske metode
- Secure Enclave hardversku enkripciju
- Zaštitu od neovlaštenog pristupa podacima

Za probijanje ovih zaštita potrebni su specijalizirani alati koji često nisu dostupni svim policijskim upravama.



## Problem pristupa

Skupe forenzičke alate (UFED Premium, GrayKey) posjeduju samo centralizirane institucije.



## Vremensko ograničenje

Čekanje na specijalizirane timove često premašuje zakonske rokove od 72 sata.



## Posljedice

Gubitak ključnih dokaza i otežano procesuiranje počinitelja kaznenih djela.

# Ovisnost o suradnji s globalnim digitalnim platformama

Pristup digitalnim dokazima često ovisi o suradnji s tehnološkim divovima.



# Zakonske zapreke u digitalnim istragama

## Sukob zakona i istražne prakse

GDPR i zaštita privatnosti često su u sukobu s potrebama hitne istrage digitalnog sadržaja.

Zakon o sudovima za mladež zahtijeva specijalizirane stručnjake

- U manjim sredinama nedostaju specijalizirani kadrovi
- Odgode postupka često rezultiraju gubitkom ključnih dokaza



# Noviteti i izmjene iz prakse (2022. – 2025.)

Zakonodavni okvir i praktične smjernice za zaštitu djece kontinuirano se razvijaju kao odgovor na nove izazove. Posljednje tri godine donijele su značajne promjene u pristupu digitalnim dokazima i postupanju prema žrtvama, s tendencijom povećanja učinkovitosti i brzine reakcije na prijave zlostavljanja.



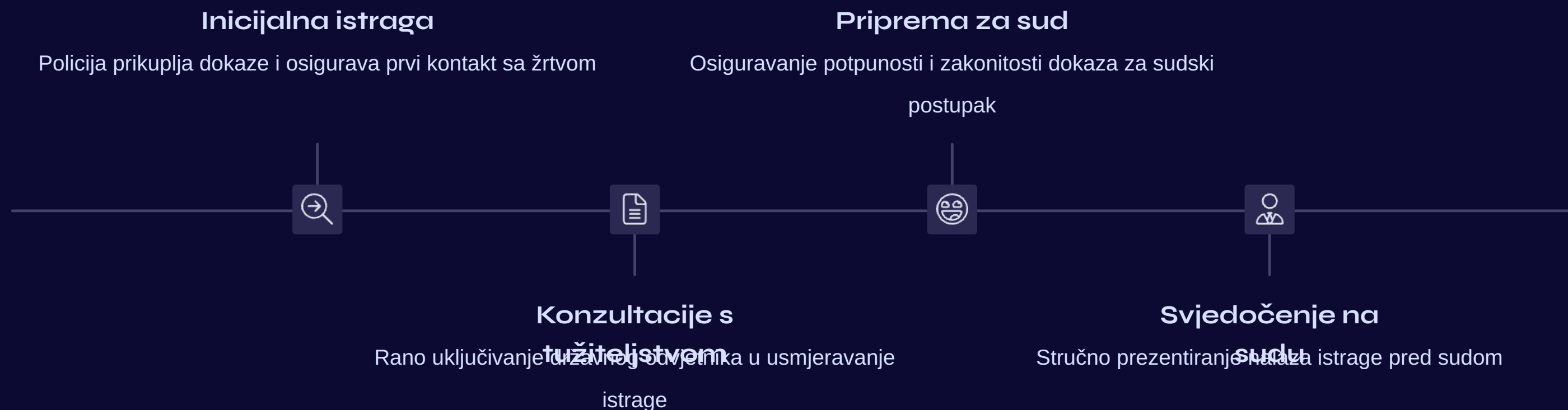
Najznačajniji noviteti uključuju obvezno izvješćivanje svih online platformi o potencijalnom dječjem seksualnom zlostavljanju, uvođenje strožih kazni za digitalne oblike zlostavljanja i uspostavljanje linije za prijavu neprimjerenog sadržaja. Također, implementirani su novi protokoli za brzu reakciju na prijave, koji omogućuju pokretanje istrage unutar 24 sata od prijave.

U tijeku je i digitalizacija cijelog procesa upravljanja dokazima, s implementacijom naprednih sustava za pohranu i obradu digitalnih dokaza koji značajno ubrzavaju forenzičku analizu i povećavaju mogućnost identifikacije počinitelja.

# Suradnja s državnim odvjetništvom i

## sudovima

Uspješna zaštita djece ključno ovisi o koordiniranoj suradnji između policije, državnog odvjetništva i sudova. Naša uloga kao policijskih inspektora ne završava prikupljanjem dokaza – aktivno sudjelujemo kroz cijeli pravosudni proces, od izrade optužnice do svjedočenja na sudu.

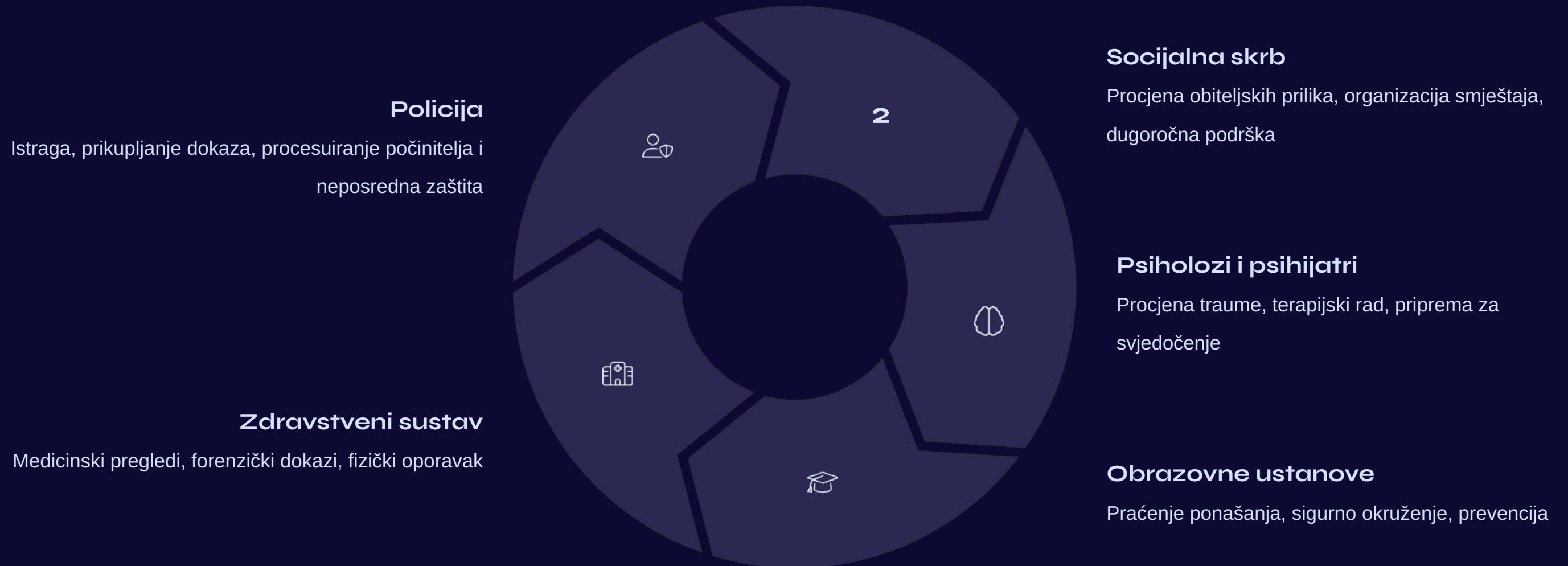


Rano uključivanje državnog odvjetništva u istragu pokazalo se kao najbolja praksa, jer omogućuje usmjeravanje istrage prema prikupljanju upravo onih dokaza koji će biti najvažniji za uspješno procesuiranje. Posebno je važna naša uloga u pripremi dokaza u formi prihvatljivoj sudu, uz detaljnu dokumentaciju lanca čuvanja dokaza i metoda analize.

Kao policijski inspektori često svjedočimo na sudu o prikupljenim dokazima, metodama istrage i stručnim interpretacijama digitalnih dokaza, posebno kada se radi o složenim tehničkim aspektima koje sud treba razumjeti za pravedno odlučivanje.

# Važnost multidisciplinarnе suradnje

Zaštita djece je kompleksan zadatak koji nadilazi mogućnosti bilo koje pojedinačne institucije. Uspješni slučajevi gotovo uvijek uključuju blisku suradnju između različitih stručnjaka koji donose svoja specifična znanja i perspektive. Naša policijska jedinica zato aktivno razvija i održava formalne i neformalne mreže suradnje.



Ključni izazov u multidisciplinarnoj suradnji često je koordinacija različitih protokola postupanja i usklađivanje prioriteta različitih struka, što zahtijeva visoku razinu komunikacijskih vještina od voditelja slučaja.

# Uključivanje nevladinih i međunarodnih organizacija

Osim državnih institucija, ključnu ulogu u zaštiti djece imaju specijalizirane nevladine organizacije i međunarodne agencije. One često donose dodatnu ekspertizu, resurse i globalne perspektive koje nadopunjuju nacionalne kapacitete, posebno u složenim slučajevima s međunarodnim elementima.



## UNICEF

Kroz svoje programe za zaštitu djece, UNICEF pruža stručnu podršku, financira edukacije i razvija standarde postupanja. Njihova globalna mreža omogućuje razmjenu najboljih praksi i podržava razvoj nacionalnih kapaciteta za forenzičku zaštitu djece.

Prekogranična suradnja postala je neophodna u doba digitalnog zlostavljanja gdje počinitelji često djeluju iz drugih država. INTERPOL-ova baza podataka o seksualnom iskorištavanju djece (ICSE) omogućuje identifikaciju žrtava i počinitelja na globalnoj razini kroz usporedbu digitalnih otisaka slika i videozapisa.



## Europol

EC3 (European Cybercrime Centre) pri Europolu specijaliziran je za borbu protiv seksualnog iskorištavanja djece na internetu. Koordinira međunarodne istrage, identificira žrtve i pruža analitičku podršku nacionalnim policijama u složenim slučajevima.



## Centar za nestalu i zlostavljano djecu

Vodeća hrvatska nevladina organizacija koja upravlja nacionalnom prijavnom linijom za neprimjereni online sadržaj, provodi edukacije i pruža psihosocijalnu podršku žrtvama i obiteljima. Njihova tehnička ekspertiza dopunjuje policijske kapacitete.

# Europol – EC3 i digitalna analiza

- 🏢 EC3 – European Cybercrime Centre: Specijalizirani odjel Europola za koordinaciju slučajeva seksualnog iskorištavanja djece putem interneta
- 💻 ICSE baza podataka: Omogućuje prepoznavanje ilegalnog materijala i povezivanje žrtava i počinitelja kroz digitalnu analizu
- 🔍 Napredna analitika: Koristi AI i Big Data algoritme za otkrivanje obrazaca i povezivanje lažnih profila
- 🌐 Suradnja s RH: MUP i Centar "Ivan Vučetić" koriste Europolovu analitičku podršku pri većim međunarodnim istragama
- 🔧 Forenzička podrška: Pruža pristup specijaliziranim alatima za dešifriranje i otključavanje uređaja državama s ograničenim resursima

# UNICEF – podrška u digitalnim istragama

## Edukacija i forenzika

UNICEF financira razvoj NICHD protokola za forenzičko ispitivanje djece.

Razvija digitalne materijale za razgovor s djecom žrtvama.

- E-learning alati za policijske službenike
- Simulacije stvarnih slučajeva
- Obrasci za dokumentiranje digitalnog nasilja

## Materijalna podrška

Održava kapacitete policije i CZSS-a kroz edukacije.

U nekim zemljama financira pristup forenzičkim alatima.

- Cellebrite za ekstrakciju podataka
- EnCase za forenzičku analizu
- Specijalizirani alati za dešifriranje za slabije razvijene zemlje

## Međunarodna suradnja

Djeluje kroz ICSE sustav za identifikaciju žrtava.

Povezuje stručnjake iz različitih zemalja.

- Suradnja s INTERPOL-om
- Partnerstvo s Internet Watch Foundation
- Razmjena praksi i znanja

# Preporuke za daljnje unaprjeđenje sustava

Unatoč značajnom napretku posljednjih godina, sustav zaštite djece u Hrvatskoj još uvijek ima prostor za unaprjeđenje. Temeljem iskustava iz prakse, identificirao sam nekoliko ključnih područja gdje su potrebna dodatna ulaganja i institucionalne promjene.



## Stalna edukacija stručnjaka

Potrebno je sustavno ulaganje u specijalizaciju i kontinuiranu edukaciju svih stručnjaka u lancu zaštite. Tehnologija i metode zlostavljanja brzo se mijenjaju, zahtijevajući redovito ažuriranje znanja i vještina.

Posebno naglašavam potrebu za većim brojem specijaliziranih stručnjaka u svim dijelovima sustava, od policijskih istražitelja do dječjih psihologa i socijalnih radnika. Bez dovoljno educiranih profesionalaca, i najbolji protokoli i tehnologija neće dati željene rezultate u zaštiti djece.



## Digitalna infrastruktura

Unaprjeđenje tehnoloških kapaciteta za brzu forenzičku analizu i pohranu velikih količina digitalnih dokaza. Trenutni resursi često ne odgovaraju rastućem broju i kompleksnosti digitalnih istraga.



## Jačanje međusektorske suradnje

Formaliziranje protokola suradnje između svih institucija, s jasnim odgovornostima i vremenskim okvirima. Trenutan sustav često ovisi o individualnim odnosima umjesto o institucionalnim mehanizmima.



## Proaktivno online djelovanje

Povećanje kapaciteta za proaktivno otkrivanje online zlostavljanja kroz napredne tehnologije i specijalizirane jedinice. Trenutno se većina slučajeva otkriva tek nakon prijave.

# Zaključak i poziv na odgovornost

Forenzička zaštita djece predstavlja jedan od najvažnijih i najizazovnijih aspekata rada pravosudnog sustava. Kao policijski inspektori, svjedočimo kako kvalitetna forenzika često predstavlja ključnu razliku između uspješnog procesuiranja počinitelja i propuštene prilike za zaštitu djeteta.



## Forenzika kao ključ pravde

Pravilno prikupljeni i analizirani dokazi osiguravaju da počinitelji odgovaraju za svoje postupke, a žrtve dobiju zasluženu pravdu i podršku



## Odgovornost svih dionika

Zaštita djece nije samo zadatak policije - zahtijeva aktivno sudjelovanje roditelja, obrazovnih institucija, zdravstvenog sustava i cijelog društva



## Prevenција kroz edukaciju

Podizanje svijesti o digitalnim rizicima i učenje djece o sigurnom ponašanju online je prva linija obrane protiv zlostavljanja

Odgovornost za zaštitu djece leži na svima nama. Kao stručnjaci, imamo profesionalnu dužnost kontinuirano unaprjeđivati svoje vještine i znanja.

Kao građani, imamo moralnu obvezu prijaviti svaku sumnju na zlostavljanje. Kao društvo, imamo kolektivnu odgovornost stvoriti okruženje u kojem se dječji glas čuje i poštuje.

Svaki uspješno riješen slučaj, svako dijete koje dobije potrebnu zaštitu i podršku, potvrđuje važnost našeg zajedničkog djelovanja. Pozivamo sve dionike da nam se pridruže u ovoj najvažnijoj misiji - stvaranju sigurnog okruženja za odrastanje svakog djeteta.