STRUČNI ČLANAK

UDK: 343.98
Primljeno: siječanj 2018.

NIKOLA PROTRKA*, DAVOR HRESTAK*

Provođenje kriminalističkih istraživanja korištenjem P2P računalnih mreža

Sažetak

U radu se opisuje kriminalistička analiza prije i tijekom kriminalističkog istraživanja kažnjivih ponašanja i otkrivanja kaznenih djela na P2P (Peer to Peer) računalnim mrežama s posebnim osvrtom na dječju pornografiju. Također se opisuju načini dijeljenja i preuzimanja datoteka kroz P2P računalne mreže te mogućnosti iskorištavanja mreže za kriminalna ponašanja. Napravljen je pregled softverskih alata kojima se mogu istraživati takva zabranjena ponašanja te su pojašnjeni smjerovi kriminalističkog istraživanja korištenjem takvih alata, posebno za otvorene P2P, a posebno za zatvorene P2P računalne mreže. Prikazan je primjer prediktivne analize fotografija kroz generičke nazive, a koje mogu biti zanimljive analitičarima i istražiteljima prilikom kriminalističke analize ili istraživanja.

Ključne riječi: *P2P, računalna mreža, kriminalistička analiza, dječja pornografija.*

UVOD

Svjedoci smo činjenice da razvojem tehnologije, ponajprije informatike, te nezaustavljivim širenjem interneta veliki dio naših života seli u digitalni svijet. Prema zadnjim podacima, 3.731.973.423[1] ljudi na svijetu ima pristup internetu, što znači da 49,6 % ljudske populacije dio svojih života provodi na *mreži svih mreža.* Ako pogledamo Europu, koje smo i mi dio, postotak stanovništva s pristupom internetu još je i veći te iznosi 77,4 %[2]. Neminovno je da uza sve dobre strane koje internet nosi, dolaze i loše. Tako se putem interneta mogu naručiti

* Nikola Protrka, univ. spec. inf., viši predavač na Visokoj policijskoj školi u Zagrebu.
** Davor Hrestak, struč. spec. crim., policijski službenik, Policijska uprava zagrebačka.

[1] Internet UsageStatistics, dostupno na http://www.internetworldstats.com/stats.htm

[2] Ibid.

ubojstva, kupiti oružje i droga ili razmjenjivati dječja pornografija. Nepobitna je činjenica da se veliki dio kriminalnih aktivnosti iz stvarnog svijeta preselio u virtualni svijet gdje je puno teže istražiti i dokazati takva ponašanja, jer tu više ne postoje državne granice i ne postoji udaljenost koju treba fizički prijeći. Radnju kaznenog djela moguće je počiniti na jednom kraju svijeta, a posljedica će se ostvarivati na drugom kraju svijeta. Kroz rad će se pokušati naći odgovor na pitanje gdje se u svemu tome trenutačno nalazi hrvatska policija, prije svega vezano uz kriminalistička istraživanja na *Peer to Peer* računalnim mrežama (P2P).

Istraživanje kažnjivih ponašanja na računalnim sustavima i mrežama još uvijek predstavlja novo poglavlje u kriminalističkim istragama, a naročito su mistificirana istraživanja kažnjivih ponašanja na *Peer to Peer* računalnim mrežama za koja je osposobljen tek mali broj policijskih službenika. Iako se zlouporabom korištenja *Peer to Peer* mreža može počiniti cijeli niz kaznenih djela, u radu će fokus biti stavljen na istraživanje kaznenih djela iz domene spolnog zlostavljanja i iskorištavanja djece, ponajprije istraživanje kaznenih djela, iskorištavanje djece za pornografiju, opisanih u članku 163. Kaznenog zakona. *Peer to Peer* mreže postale su idealan medij za distribuciju dječje pornografije koji ne prepoznaje državne granice niti druge fizičke prepreke zbog čega će se posebna pažnja u radu posvetiti istraživanju baš takvih kaznenih djela te će se pokušati skrenuti pozornost na masovnost tih kaznenih djela koja prolaze dosta nezamijećeno ispred policije i državnog odvjetništva.

1. *PEER TO PEER* RAČUNALNE MREŽE

Peer to peer (P2P) je oznaka za vrstu komunikacije unutar računalne mreže. Uobičajen način komunikacije u mrežama je klijent – poslužitelj, gdje klijenti komuniciraju samo s poslužiteljem i od njega preuzimaju podatke. Za razliku od takvog načina dijeljenja podataka u P2P mrežama ne postoje centralizirani poslužitelji - serveri, već su svi sudionici ravnopravni. Svi imaju jednaka prava uzimanja i davanja podataka te svi sudionici dijele svoje resurse (tu se radi o prostoru na tvrdim diskovima i radnoj memoriji i procesorskom vremenu). Razmjena podataka trebala se odvijati izravno između računala spojenih na mrežu, što i jest osnovna ideja P2P mreža. Jednu od vodećih zasluga za razvoj P2P mreža svakako ima i Napster[3], koji se smatra prvim P2P sustavom, a koji je služio izravno za razmjenu glazbe između korisnika na internetu. Nakon Napstera, nastale su mnoge druge P2P mreže za razmjenu podataka kao što su Gnutella, eDonkey, BitTorrent, Gigatribe i sl.[4].

1.1. Otvorene P2P računalne mreže i alati za istraživanje kažnjivih ponašanja

Pod otvorene P2P mreže možemo svrstati Gnutellu, eDonkey, Ares, BitTorrent i druge koje svim korisnicima koji koriste kompatibilni softver omogućavaju pridruživanje mreži i nesmetano dijeljenje i preuzimanje datoteke. P2P mrežu čini grupa računala povezanih preko određenog protokola i mreža se mijenja svaki put kada se pojedini sudionici priključe ili isključe s mreže. Za sudjelovanje u P2P mreži i za dijeljenje datoteka jedan od preduvjeta je

[3] Napster, dostupno na https://en.wikipedia.org/wiki/Napster

[4] *Peer to peer,* dostupno na https://hr.wikipedia.org/wiki/Peer_to_peer

i stvaranje dijeljenih mapa na računalu u kojima se nalaze datoteke koje korisnik namjerava dijeliti s drugima. Sama ideja P2P mreža je u dijeljenju tako da nitko ne može samo preuzimati datoteke, već mora i dijeliti svoje datoteke pohranjene na računalu. Kako bi ostali korisnici mogli znati koje datoteke korisnik želi dijeliti, softver sastavlja popis koji prikazuje sve dijeljene datoteke spremljene u dijeljenoj mapi te indeksira datoteke prema ključnim riječima kako bi ih bilo moguće pretraživati. Popisi dijeljenih i indeksiranih datoteka najčešće se nalaze na serveru za indeksiranje, *Ultrapeer* – računalu, koje ne sadrži dijeljene datoteke, već ostalim korisnicima dijeli popise na kojem računalu se nalazi koja datoteka. Računala na kojima se nalaze dijeljene datoteke nazivaju se *peer* računala ili *host*. Da bi računala na P2P mreži mogla međusobno komunicirati i razmjenjivati podatke moraju biti označena na jedinstven način kako bi se mogla međusobno razlikovati. Svako računalo koje pristupa mreži tj. mrežni uređaj preko kojeg se računalo spaja na mrežu, dobiva svoju jedinstvenu IP adresu koja se može usporediti s telefonskim brojem jer jednoznačno obilježava korisnika te se može utvrditi kome je koja IP adresa u određenom trenutku bila dodijeljena. Drugi važan podatak za uspostavu komunikacije na P2P mreži su portovi. Da bi moglo doći do razmjene paketa podataka na mrežnom uređaju moraju biti otvoreni određeni portovi kroz koje računalo prima pakete podataka. P2P programi komuniciraju preko IP adresa i portova[5] te tako točno znaju gdje trebaju isporučiti određene pakete podataka. Problem s IP adresama je taj što se korisnicima dodjeljuju dinamičke IP adrese koje se mijenjaju svaka 24 sata. Da bi se računala na mreži mogla raspoznati, većina P2P softvera generira GUID – *Globally Unique Identifier*[6] koji omogućuje identifikaciju računala i nakon promjene IP adrese. GUID se može promijeniti nadogradnjom P2P softvera ili deinstalacijom i ponovnom instalacijom što često koriste korisnici koji žele prikriti svoje ilegalne djelatnosti na mreži.

Vrlo važna funkcija za funkcioniranje P2P mreža je *hash*[7], a radi se o jedinstvenom sažetku svake datoteke. Prilikom pretraživanja dijeljenih datoteka prema ključnim riječima P2P klijent nalazi datoteku i započinje s preuzimanjem, ali istovremeno i dalje pretražuje mrežu u potrazi za datotekama koje imaju isti *hash* kako bi mogao paralelno preuzimati datoteke ili nastaviti s preuzimanjem ako dođe do prekida veze s računalom s kojeg je počeo preuzimati traženu datoteku.

U kriminalističkim istraživanjima *hash* ima veliku vrijednost jer se prema njemu datoteke koje sadrže dječju pornografiju klasificiraju kao takve i moguće ih je otkriti bez obzira na to pod kojim se nazivom dijele na mreži. Preimenovanje datoteke ne utječe na promjenu *hash* vrijednosti, ali svaka promjena sadržaja pa i ona od jednog bita[8] u potpunosti mijenja *hash* vrijednost.

---

[5] Primjer IP adrese i porta 172.16.254.1:6346 gdje 172.16.254.1 označava IP adresu, a 6346 broj otvorenog porta.

[6] GUID – jedinstveni globalni identifikator je 128-bitni broj koji se koristi za identifikaciju podataka u računalnim sustavima.

[7] *Hash* - Sažetak - Jednosmjerni proces koji pretvara ulazni sadržaj bilo koje veličine na izlaz kao poruku kontrolnog zbroja fiksne veličinu, zove se rezime-sažetak poruke (*messagedigest*), ili samo sažetak. Ovaj proces nije reverzibilan, te nije moguće stvoriti izmjene u poruci ili izmijeniti podatke sažetka a da promjene ostanu usklađene. Jedna vrsta zaštite koja se koristi za digitalni potpis u PGP mehanizmu kriptiranja.

[8] Akronim od BinaryDigIT, najmanja jedinica binarnog zapisa, sadržaj može biti '0' ili '1'.

1.2. Softverski alati za pretraživanje P2P mreža

P2P mreže grubo možemo podijeliti na mreže namijenjene za VoIP i *online chat* te mreže za razmjenu datoteka, kao što su Gnutela, eDonkey, BitTorrent, Gigatribe i sl. Predmet policijskog interesa su mreže za razmjenu datoteka zato što je takve mreže moguće pratiti kao otvorene izvore, a one najčešće i služe za razmjenu zabranjenog sadržaja poput dječje pornografije. U sklopu međunarodne suradnje, hrvatskoj policiji dostupno je više softverskih alata na temelju kojih mogu pratiti i analizirati otvorene izvore te tako otkrivati počinitelje kaznenih djela na P2P mrežama.

Shareaza je P2P klijent koji ima mogućnost preuzimanja datoteka iz više mreža kao što su BitTorrent, eDonkey, Gnutella, Gnutella2. U izvorni kod *Shareaze* ugrađeni su filtri sadržaja koji onemogućuju preuzimanje sadržaja klasificiranog kao pornografija, dječja pornografija, kao i sadržaja zaštićenog s Digital rights management (DRM). Za potrebe policijskog korištenja izvorni kod *Shareaze* je izmijenjen tako da onemogućuje bilo kakvo dijeljenje datoteka, već je moguće samo pretraživanje i preuzimanje datoteka koje drugi korisnici P2P mreža nude na dijeljenje. Filtri sadržaja su za razliku od originalne *Shareaze* u *Shareaze* LE promijenjeni tako da blokiraju sav sadržaj osim ciljanih datoteka klasificiranih kao dječja pornografija, čime se omogućuje pronalaženje sadržaja i korisnika koji distribuiraju zabranjeni materijal. Isto tako ugrađeni su posebni filtri koji omogućuju praćenja isključivo IP adresa određene države. Tako se korištenjem *Shareaze* LE mogu pratiti IP adrese dodijeljene hrvatskim korisnicima. Softver prepoznaje *hash* vrijednosti datoteka koje sadrže pedofilski sadržaj što je vrlo bitan podatak kod provođenja istrage, jer *hash* potpisuje datoteku na jedinstven neponovljiv način te onemogućuje osumnjičenika da se brani tvrdeći da datoteke koje je on distribuirano nisu sadržavale pedofilski sadržaj. Usporedbom *hash* vrijednosti datoteke koju je osumnjičeni nudio na dijeljenje i datoteke pedofilskog sadržaja koja se nalazi u policijskim bazama podataka, nedvojbeno se može utvrditi da je to baš ta datoteka.

Phex RoundUp je verzija javno dostupnog *Gnutella* klijenta *Phex* koji je modificiran za provođenje kriminalističkih istraživanja dječje pornografije na P2P mreži Gnutella. Sam program ima slične mogućnosti kao i prethodno opisana Shareaza LE tako da omogućuje pristup podacima o preuzimanju i korisniku, kao što su IP adresa, naziv datoteke, veličina datoteke, *hash* vrijednost, GUID. Isto tako program omogućava pretraživanje i filtriranje sadržaja prema ključnim riječima, vrstama datoteke, prema IP adresi ili državi korisnika. Alat može prikazivati rezultate pretraživanja po ključnoj riječi i prije izravnog spajanja na računalo koje dijeli datoteke, jer pronalazi popise datoteka koji se nalaze na *Ultra-peer* računalu i koji samo upućuje na računalo na kojem se nalaze dijeljene datoteke.

eMule RoundUp je modificirana verzija *eMule* klijenta namijenjenog za pretraživanje i dijeljenje datoteka na P2P mreži eDonkey. Slično kao i Phex RoundUp i Shareaze LE, eMule RoundUp je modificiran tako da omogućuje pretraživanje i skidanje dječje pornografije s mreže eDonkey. Posjeduje mogućnost pretraživanja prema ključnim riječima, *hash* vrijednostima, IP adresama. Osim mogućnosti pretraživanja datoteka, *eMule RoundUp* ima mogućnost i preuzimanja ciljanih datoteka. Kako P2P mreže funkcioniraju na međusobnom dijeljenju datoteka i zahtijevaju od korisnika da dijele svoje datoteke, *eMule RoundUp* ima implementiranu funkciju lažnog dijeljenja datoteka. Navedena funkcija simulira dijeljenje i prikazuje da se datoteka preuzima, a u stvarnosti se ne dijeli sadržaj. Vrlo važna funkcija koju posjeduje *eMule RoundUp* je mogućnost izrade snimki zaslona čime se dokumentiraju svi

postupci tijekom pretraživanja i preuzimanja datoteka koje sadrže dječju pornografiju. Osim toga program stvara i log zapise što je također vrlo važna stavka prilikom dokazivanja da su određene datoteke dijeljene od strane točno određenog klijenta ili da je datoteka preuzeta isključivo od jednog klijenta, tj. da se nije radilo o višestrukom preuzimanju.

Ares Tools RoundUp je skup alata namijenjen za pretraživanje P2P mreže Arest, tj. za otkrivanje i preuzimanje datoteka s dječjom pornografijom. Skup programa funkcionira slično kao i prethodno opisani programi te ima mogućnost pretraživanja mreže u potrazi za datotekama dječje pornografije i preuzimanje takvih datoteka koje bi se mogle koristiti kao dokaz u kaznenom postupku. *Ares Tools RoundUp* se sastoji od nekoliko samostalnih alata; RU Ares alata za pretraživanje, RU Ares alata za upravljanje slučajevima, LA Ares klijent (Downloader) i Ares preglednika (Viewer). RU Ares alat za pretraživanje omogućava pretraživanje prema ključnoj riječi, pretragu indeksiranih ključnih riječi te pretragu *hash* vrijednosti. Nakon pronalaženja sumnjivih datoteka uz pomoć RU Ares alata za upravljanje slučajevima, povlače se podaci u korisničko sučelje programa odakle se ciljane datoteke mogu preuzeti alatom LA Ares klijent. Na kraju procesa moguće je Ares preglednikom istražiti detalje o svakoj pojedinačnoj ciljanoj IP adresi kao i nazive datoteka, opise, datume, vrijeme, broj djelomičnih preuzimanja te broj dovršenih preuzimanja. Ares preglednik također omogućuje generiranje automatskog elektroničkog .html izvješća te zapisivanje logova o preuzimanju datoteka.

U okviru kriminalističke analize dječje pornografije od važnijih alata potrebno je još spomenuti *GnuWatch, Spectre2 IRC LE, Torrential Downpour, TiPS* koji su namijenjeni otvorenim P2P mrežama, a svi oni imaju slične karakteristike i mogućnosti koje se svode na to da omogućuju pretraživanje mreže prema ključnim riječima, *hash* vrijednostima, prema GUID-u ili IP adresi te nude mogućnost preuzimanja ciljanih datoteka isključivo od samo jednog korisnika. Navedeni alati također ne dozvoljavaju dijeljenje vlastitih datoteka. Svim opisanim alatima zajedničko je to da rade s otvorenim P2P mrežama kojima može pristupiti svaki korisnik koji ima instaliran odgovarajući softver.

1.3. Zatvorene ili privatne *Peer to peer* mreže i alati za istraživanje kažnjivih ponašanja

Osim otvorenih P2P mreža postoje i zatvorene mreže kojima ne može pristupiti svaki korisnik. Jedan od najčešće korištenih mreža za distribuciju dječje pornografije je *GigaTribe* koji korisnicima omogućuje dijeljenja datoteka samo za pozvane korisnike. *GigaTribe* osim osnovnih funkcija koje imaju i druge mreže posjeduje nekoliko funkcija koje omogućuju veću privatnost. Korisnici koji žele dijeliti datoteke samo s određenim prijateljima imaju mogućnost kreirati kontakt-listu (do 500 prijatelja) nakon čega samo ti prijatelji s kontakt-liste imaju pristup njihovim dijeljenim mapama s time da se prijatelji međusobno ne vide nego vide samo dijeljene mape u kojima se mogu nalaziti sve vrste datoteka neovisno o njihovoj veličini, što je izvrsna platforma za dijeljenje zabranjenog sadržaja. Još jedna mogućnost koja ide u prilog dijeljenju zabranjenog sadržaja jest i mogućnost kriptiranja sa 256-bitnom enkripcijom koja je praktički neprobojna tako da nitko osim ovlaštenih primatelja ne može vidjeti kakav se sadržaj dijeli. Unutar samog programa korisnicima je omogućeno slanje instant-poruka čime je otvoren i kanal za sigurnu komunikaciju. Korisnici također mogu pristupiti svojim dijeljenim mapama s bilo kojeg mjesta na svijetu preko *web* preglednika

što im omogućuje manipuliranje datotekama, brisanje ili zaključavanje lozinkom. Datoteke se u mreži razmjenjuju izravno između dvaju korisnika, a na serverima *GigaTribe* ne ostaju nikakvi zapisi o prijenosu datoteka, tako da je praktički nemoguće pratiti povijest dijeljenja datoteka. Da bi se još više pojačala privatnost i anonimnost *GigaTribe* omogućava skrivanje IP adresa računala koja razmjenjuju datoteke te im za identifikaciju na mreži dodaje jedinstveni niz brojeva. Zbog svih tih karakteristika koje omogućuju anonimnost i privatnost *GigaTribe* je postala jedna od omiljenijih P2P mreža za osobe koje razmjenjuju ilegalni materijal, u prvom redu dječju pornografiju, jer je izrazito teško pratiti promet na takvoj mreži. (Miller R., 2014.)

1.4. Alati za istraživanje kažnjivih ponašanja na zatvorenim *Peer to Peer* mrežama

Kao što je bilo riječi u uvodnom dijelu, *GigaTribe* je zatvorena P2P mreža koja svojim korisnicima omogućuje stvaranje privatnih P2P mreža unutar kojih nesmetano mogu dijeliti sve vrste zabranjenog sadržaja, ponajprije dječje pornografije. U cilju otkrivanja takvih počinitelja i spašavanja djece, američki FBI, tj. njegov posebni odjel *Innocent Images Operations Unit* razvio je posebne protokole i softver namijenjen upravo za istraživanje dječje pornografije na P2P mreži *GigaTribe.* S obzirom na odredbe licenčnog ugovora nije moguće javno iznositi način funkcioniranja i mogućnosti softvera, ali može se načelno reći na koji način funkcioniraju istrage na *GigaTribe* P2P mrežama.

Kako se radi o privatnim mrežama, istražitelji imaju dvije mogućnosti pristupa takvim mrežama. Prva mogućnost je kreiranje lažnog profila na kojem se istražitelj predstavlja kao pedofil koji nudi razmjenu pedofilskog sadržaja. Nakon kreiranja profila istražitelj čeka da ga se pozove u zatvorenu mrežu i da se od njega zatraži dijeljenje sadržaja, a on zauzvrat dobiva pristup njihovim dijeljenim datotekama. Druga mogućnost pristupa privatnoj mreži je preuzimanje identiteta poznatog počinitelja, koji je za vrijeme kriminalističkog istraživanja ustupio svoj virtualni identitet policijskim istražiteljima, omogućujući im da se priključe na privatnu mrežu uz pomoć posebnog softvera.

U svakom slučaju, nakon pristupanja mreži bilo pod lažnim identitetom, bilo pod preuzetim identitetom, policijskom istražitelju je zabranjeno dijeliti datoteke s dječjom pornografijom, već može samo prikupljati informacije o članovima mreže i datotekama koje dijele.

2. ISTRAŽIVANJE KAZNENIH DJELA KORIŠTENJEM P2P MREŽA

Istraživanje kažnjivih ponašanja na računalnim mrežama ili sustavima, posebice na P2P mrežama, nedvojbeno još uvijek spada u domenu kojom se hrvatska policija ne bavi sustavno niti su takva istraživanja dovoljno eksploatirana kao mogući izvori saznanja o počinjenom kaznenom djelu. U praksi, a i u stručnim raspravama, kao izvori saznanja o počinjenom kaznenom djelu najčešće se navodi prijava oštećenog. Tako D. Škrtić u svom stručnom radu navodi: "Prikupljanje dokaza, u pravilu kreće nakon prijave kaznenog djela ili nakon utvrđivanja osnova sumnji da je osoba nad kojom se provodi kriminalističko istraživanje zbog kaznenih djela spolne zlouporabe djece, uključujući i djecu mlađu od petnaest godina ili kaznenih djela počinjenih uporabom informacijsko-komunikacijske tehnologije, počinila i

kaznena djela spolnog zlostavljanja i iskorištavanja djeteta. Radi potvrde osnova sumnje, policija uvijek može, radi sprječavanja i otkrivanja kaznenih djela, primijeniti ovlast provjere uspostavljanja telefonskih kontakata i od davatelja telekomunikacijskih usluga zatražiti provjeru istovjetnosti, trajanja i učestalosti kontakta određenih telekomunikacijskih adresa. (D. Škrtić, 2013:1165).″

S takvom konstatacijom slaže se i Ivica Kokot koji u svom preglednom znanstvenom radu navodi: "Do saznanja o kaznenim djelima spolnog iskorištavanja djece na računalu ili računalnoj mreži policijski službenici dolaze ili proaktivnim postupanjem u sprječavanju i otkrivanju kaznenih djela ili obavljajući svakodnevne policijske poslove. Proaktivno postupanje sastoji se prije svega u senzibiliziranju društva za pojave konkretnog kaznenog djela i povećanju spremnosti na prijavu počinjenih kaznenih djela." (I. Kokot, 2015:247).

Oba autora uz prijavu kaznenog djela od strane oštećenog spominju i postupanje policije u skladu sa Zakonom o policijskom poslovima i ovlastima (NN 76/09., 92/14.) prije svega referirajući se na ovlast iz članka 68. Provjera uspostavljanja elektroničke komunikacije, što može biti izvor saznanja o počinjenom kaznenom djelu, ali jako rijetko i samo kada već postoje saznanja da određena osoba ili osobe čini kaznena djela putem računalnih mreža. Razlog tome je što se provjera uspostavljanja elektroničke komunikacije većim dijelom odnosi na telefonski promet, a iz toga je moguće vidjeti jedino s kime je osumnjičeni ostvarivao telefonsku komunikaciju i lokaciju na kojoj se nalazio u to vrijeme. Provjerom uspostavljanja elektroničke komunikacije nikako se ne može utvrditi je li potencijalni osumnjičeni razmjenjivao ili distribuirao bilo kakav ilegalni sadržaj putem računalnih ili P2P mreža, a pogotovo se ne može na temelju provjere uspostavljanja elektroničke komunikacije iz grupe ljudi izdvojiti osoba za koju bi se moglo reći da postoje osnove sumnje da se bavi počinjenjem takvih kaznenih djela. Jedini dio provjere uspostavljanja elektroničke komunikacije koji može doprinijeti otkrivanju kažnjivih ponašanja na mreži jest utvrđivanje podatka kome je u određenom trenutku bila dodijeljena određena IP adresa, ali iz toga također nije moguće vidjeti kakav se sadržaj razmjenjivao preko te IP adrese.

U stručnim raspravama spominju se i druge policijske ovlasti, najčešće prikrivene policijske radnje, promatranje, klopka i zasjeda[9]. Te radnje definitivno daju rezultate u istraživanju klasičnog kriminaliteta, ali nikako nisu prikladne za istraživanje kriminaliteta i kriminalnih ponašanja na računalnim mrežama. Određene uspjehe u otkrivanju i dokazivanju počinjenja kaznenih djela na računalnim mrežama moguće je ostvariti primjenom posebnih dokaznih radnji kojima se privremeno ograničavaju određena ustavna prava građana, na temelju pisanog i obrazloženog naloga suca istrage[10]. Tu se ponajprije misli na posebnu dokaznu radnju presretanje, prikupljanje i snimanje računalnih podataka[11] iako i tu postoje određena ograničenja. Naime, za primjenu posebnih dokaznih radnji, tj. za dobivanje naloga za provedbu posebnih dokaznih radnji moraju postojati osnove sumnje da je određena osoba počinila kazneno djelo za koje se mogu odrediti posebne dokazne radnje[12] te moraju postojati okolnosti koje ukazuju na to da se izvidi kaznenih djela ne bi mogli provesti na drugi način ili bi to bilo moguće samo uz nerazmjerne poteškoće. U takvoj situaciji pretpostavlja se da je

[9] Članak 80. Zakona o policijskim poslovima i ovlastima, NN 92/14.

[10] Članak 332. Zakona o kaznenom postupku, NN 145/13.

[11] Članak 332. stavak 1. točka 2. Zakona o kaznenom postupku, NN 145/13.

[12] Članak 334. Zakona o kaznenom postupku, NN 145/13.

policija već otkrila da je određena osoba počinitelj kaznenih djela i potrebno je prikupiti dokaze na temelju kojih će se voditi kazneni postupak, što znači da se tako ne otkrivaju kaznena djela i počinitelji već se radi o sljedećem stadiju postupka kada se prikupljaju formalni dokazi bitni za vođenje kaznenog postupka. Što se tiče prijavljivanja počinjenja kaznenih djela od strane oštećenih, smatra se da se radi o manjem broju kaznenih djela koja se tako otkrivaju zato što se najveći dio kaznenih djela počinjenih putem P2P odnosi na nuđenje, činjenje dostupnim, distribuciju, pribavljanje za sebe ili drugoga, prodaju, davanje, prikazivanje ili posjedovanje zabranjenih materijala, što znači da u najvećem broju slučajeva oštećeni nisu ni svjesni svog položaja. Isto tako, s obzirom na međunarodni karakter kaznenih djela počinjenih putem P2P mreža, gdje se primjerice medijski materijali dječje pornografije proizvode na jednom kraju svijeta, a umnožavaju, distribuiraju i razmjenjuju na drugom kraju svijeta, nemoguće je da oštećeni uopće zna da se distribuiraju takvi sadržaji.

Svjesnost da se protiv takvih kažnjivih ponašanja koja imaju međunarodni karakter teško boriti jer je mogućnost umnožavanja, distribucije i prikrivanja ilegalnih materijala praktički neograničena, primorala je policijske organizacije diljem svijeta da promijene svoje metodologije rada i da se prilagode novom takozvanom *cyber* okruženju, gdje će u virtualnom svijetu otkrivati kažnjiva ponašanja. Neminovno je da se i hrvatska policija morala prikloniti tom trendu te je pogotovo na polju istraživanja kaznenih djela iz domene spolnog zlostavljanja i iskorištavanja djeteta pokrenuta obuka policijskih istražitelja i nabavka opreme potrebne za istraživanje kaznenih djela počinjenih putem P2P mreža.

Ministarstvo unutarnjih poslova se još 2009. godine u sklopu programa pretpristupne pomoći Europske komisije priključilo u projekt ″Izgradnja kapaciteta u području suzbijanja seksualnog iskorištavanja i seksualnog zlostavljanja djece te pružanja pomoći policije ranjivim žrtvama kriminaliteta″[13], čiji je cilj bilo jačanje kapaciteta tijela kaznenog progona. Za vrijeme provođenja projekta od 2011. do travnja 2013. ostvarena je suradnja s policijskim službenicima iz Ujedinjenog Kraljevstva Velike Britanije i Sjeverne Irske koji su održali radionice na kojim su prezentirani načini počinjenja kaznenih djela na štetu djece te prenesena znanja o načinu provođenja istraga i korištenja otvorenih izvora na internetu. Krajem 2013. godine u Budimpešti na International Law Enforcement Academy održan je seminar FBI-a na kojem su sudjelovali predstavnici hrvatske policije, a na kome su proširena znanja o istraživanju kaznenih djela na štetu djece korištenjem P2P mreža.

Korištenjem prethodno opisanih programskih rješenja policijski službenici prikupljaju podatke o datotekama koje osumnjičeni nudi na dijeljenje i daljnju distribuciju na P2P mreži, vremenu kada je datoteke nudio na dijeljenje te IP adresama s kojih su datoteke nuđene na dijeljenje. Na temelju tih prikupljenih saznanja sastavlja se izvješće kao osnova za pokretanje kriminalističkog istraživanja. Na temelju takvog izvješća, s obzirom na to da se radi o kaznenom djelu koje se progoni po službenoj dužnosti, policija ima ovlast iz članka 68. Zakona o policijskim poslovima i ovlastima izvršiti provjeru uspostavljanja elektroničke komunikacije te od telekomunikacijskog operatera dobiva podatak kome je bila dodijeljena IP adresa preko koje su distribuirane datoteke klasificirane kao dječja pornografija, što je dovoljno za poduzimanje dokazne radnje pretrage doma i drugih prostorija. Prilikom pretrage, osim oduzimanja

[13] Izvješće o ocjenjivanju sedmog kruga uzajamnih ocjenjivanja pod nazivom ″Praktična provedba i djelovanje europskih politika o sprečavanju kiberkriminaliteta i borbi protiv njega″ – izvješće o Hrvatskoj (2017), dostupno na http://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/hr/pdf

računala, posebnu pozornost treba posvetiti traženju i drugih medija za pohranu podataka, poput vanjskih, prijenosnih tvrdih diskova, memorijskih stikova, optičkih medija, memorijskih kartica ali i drugih elektroničkih uređaja koji u sebi imaju ugrađenu mogućnost pohrane podataka. Posebnu pažnju potrebno je obratiti i na pronalaženje zabilješki s korisničkim imenima i lozinkama servisa za pohranu podataka u oblaku. Takvi servisi su vrlo prikladni za čuvanje ilegalnog sadržaja jer se nalaze na serverima koji su locirani diljem svijeta, a moguć im je pristup s bilo kojeg računala i u slučaju potrebe brisanje svih podataka.

Prednosti tog smjera kriminalističkog istraživanja leže u tome da policijski službenici s osumnjičenim ne dolaze ni u kakav kontakt do samog trenutka uhićenja i provođenja pretrage računala tako da osumnjičeni ni u jednom trenutku ne može znati niti posumnjati da su njegove ilegalne aktivnosti pod nadzorom policije, a samim time smanjuje se i mogućnost da će uništiti ili sakriti ilegalni materijal koji posjeduje.

Kroz praksu su se pokazali i nedostaci takvog načina istraživanja, a to je prije svega pronalaženje elektroničkih dokaza, tj. materijala s dječjom pornografijom. Osim na računalu s kojeg se putem P2P klijenata na distribuciju nudi sadržaj dječje pornografije, takve datoteke mogu biti spremljene i skrivene na drugim medijima za pohranu podataka, što je ponekad jako teško pronaći i otkriti. Osumnjičenici često, ne samo zbog straha od policije nego i od straha od ukućana, takve datoteke pohranjuju na razne medije kao što su prijenosni diskovi (HDD ili SSD), memorijski stikovi, optički mediji, memorijske kartice. Svi ti mediji imaju mogućnost kriptiranja, što u današnje doba ne traži preveliku razinu informatičkog znanja korisnika. Podatke na prijenosnom mediju, kao i na tvrdom disku računala, moguće je vrlo lako kriptirati 128- ili 256-bitnom AES enkripcijom pomoću alata BitLocker[14] koji je već sastavni dio operativnog sustava Windows. Tako kriptiranim podacima nije moguće pristupiti zbog čega postoji velika mogućnost da se protiv osumnjičenog uopće ne pokrene kazneni postupak.

Uza sve to problem predstavlja i pohrana u oblaku *(Cloud storage).* Radi se o mjestima za pohranu podataka na dislociranim, međusobno povezanim serverima kojima se pristupa putem interneta. Podaci pohranjeni u oblaku predstavljaju poseban izazov za istražitelje jer se serveri najčešće nalaze u drugim zemljama i nisu u nadležnosti hrvatskog pravosuđa. Iako postoje forenzični alati koji su kreirani za pretraživanje podataka u oblaku, oni mogu funkcionirati samo ako je aplikacija *Cloud* servisa instalirana na računalo i povezana s oblakom. Ako se podacima pristupa preko internetskog preglednika, za svako spajanje je potrebno korisničko ime i lozinka. Bez suradnje osumnjičenika ti podaci postaju praktički nedostupni. S druge strane ne postoji ni mogućnost blokiranja podataka koji se nalaze u oblaku, jer im korisnik može pristupiti s bilo kojeg računala povezanog s internetom i obrisati ih.

Što se tiče broja kriminalističkih istraživanja započetih na temelju praćenja prometa na P2P mrežama, može se reći da je Policijska uprava zagrebačka, Služba općeg kriminaliteta, u zadnjih pet godina provela više takvih uspješnih kriminalističkih istraživanja, ali s obzirom na to da se statistički ne prati na koji način su inicirana istraživanja, ne može se dati niti statistički pregled i usporedba kako za Policijsku upravu zagrebačku, tako ni za druge policijske uprave.

Drugi način kriminalističke analize jest taj da se iskoriste mogućnosti softvera i da se od počinitelja preuzmu datoteke klasificirane kao dječja pornografija. Sam se tijek preuzi-

[14] https://technet.microsoft.com/en-us/library/cc732774(v=ws.11).aspx

manja dokumentira korak po korak te se takve datoteke kasnije mogu koristiti na sudu kao dokaz da je počinitelj distribuirao dječju pornografiju na P2P mreži. Za takvo postupanje policije postoji zakonsko uporište u članku 12. Zakona o policijskim poslovima i ovlastima (NN 76/2009.), koji kaže da "Glavni ravnatelj ili osoba koju on ovlasti, u skladu sa zakonom, može pisanim nalogom odrediti prikrivanje policijskog posla. Prikrivanje se može odnositi na pravni posao, pravnu i fizičku osobu, tijelo državne vlasti i *sredstva komuniciranja*." Usprkos tome do sada se nije postupalo tako jer je neslužbeni stav Državnog odvjetništava da ne postoji sudska praksa u takvim predmetima i nije do kraja definirano postupanje policije i način fiksiranja takvih dokaza zbog čega se nastavilo s praksom da se kaznena djela istražuju na prvoopisani način gdje je popis dijeljenih datoteka dječje pornografije dovoljan za pokretanje izvida i provođenja dokaznih radnji u cilju otkrivanja počinitelja kaznenog djela iskorištavanje djece za pornografiju. Za razliku od Hrvatske, druge zemlje, ponajprije Sjedinjene Američke Države, koriste takve načine kriminalističkog istraživanja te je u presudama njihovih sudova dokumentirano da prihvaćaju preuzete datoteke dječje pornografije kao dokaz u sudskom postupku.

Još uvijek prevladava mišljenje kako su dječja pornografija i pedofilija nešto što se događa negdje daleko u nekim drugim zemljama, a kod nas se samo sporadično distribuiraju slike zlostavljane djece. S druge strane, kad se u popisima dijeljenih datoteka klasificiranih kao dječja pornografija nađu stotine fotografija koje nisu označene kao dječja pornografija a nazivi tih datoteka su *DSC_003456, DSC_003457, DSC_003460 ili IMG_20150204-0112, IMG_20150204-0114, IMG_20150204-0118*, vrijeme je da se promijeni mišljenje i da se shvati da se zlostavljanje djece događa i kod nas bez obzira na to koliko mi to ne želimo priznati.

Analizom naziva fotografije DSC_003456 otkriva se da se radi o izvornoj fotografiji koja nije preuzeta s neke *web* stranice ili društvene mreže već je riječ o izvornoj fotografiji preuzetoj s nekog od fotoaparata tipa Nikon ili Olympus, ili s nekog pametnog telefona koji kao prefiks svake fotografije stavljaju oznaku "DSC", a u nastavku je redni broj fotografije snimljen tim uređajem. Slična stvar je i s nazivom fotografije IMG_20150204-0112, gdje fotoaparat ili pametni telefon kao prefiks naziva datoteke stavlja "IMG", dok drugi dio naziva "_20150204" predstavlja datum snimanja fotografije, a treći dio "_0112" predstavlja redni broj fotografije snimljene toga dana. Nameće se pitanje zašto bi netko tko dijeli stotine fotografija i filmova klasificiranih kao dječja pornografija u istu dijeljenu mapu stavio fotografije sa svoga fotoaparata ili mobitela, ako one nemaju nikakve veze s dječjom pornografijom. Jedini je logički zaključak da se na tim fotografijama također nalaze slike zlostavljane djece, ali za razliku od ostalih fotografija ove su najvjerojatnije fotografirane na našem području, koje je slikao naš zlostavljač.

3. ZAKLJUČAK

U posljednjih 20 godina razvoj znanosti, tehnologije i informatike u tolikoj mjeri utječe na razvoj cjelokupnog društva i života da je to neusporedivo s bilo kojim prijašnjim razdobljem u ljudskoj povijesti. Činjenica je da se širenjem interneta i ostalih naprednih tehnologija brišu državne granice te se otvara jedan novi virtualni svijet u kojem je bezbroj prilika za zaradu i bogaćenje. Kako živimo u kapitalističkom sustavu gdje je najveća vrijednost imovina i novac, ljudi ne prežu od zabranjenih ponašanja ni u tom virtualnom svijetu, gdje postoji i puno veća mogućnost za kriminalna ponašanja nego u stvarnome svijetu, jer mehanizmi djelovanja policije i pravosuđa još uvijek nisu razvijeni do granica kao u stvarnome svijetu. Kriminalci to dobro znaju i koriste situaciju kako bi se na lak način domogli novca. Razvijene zemlje prepoznale su taj problem i sve više sredstava ulažu u nabavljanje tehnologije i obučavanje policijskih službenika za borbu protiv kriminalnih ponašanja na računalnim sustavima i mrežama. Problem leži u tome što kriminalna ponašanja u virtualnom svijetu ne poznaju državne granice, dok su nacionalna zakonodavstva i djelovanje policije itekako vezani uz državne granice tako da počinitelji kaznenih djela i zabranjenih ponašanja često ostaju izvan dohvata snaga reda. Taj problem su uvidjele mnoge razvijene zemlje zbog čega su i spremne podijeliti svoje resurse i znanje s manje razvijenima kako bi se zajednički borili protiv te nove vrste kriminala. Postavlja se pitanje koliko je hrvatska policija organizacijski i materijalno spremna prihvatiti takve izazove i koliko se uopće radi na suzbijanju i otkrivanju kažnjivih ponašanja na računalnim sustavima i mrežama. Kroz rad je dat pregled alata i mogućnosti koji su dostupni za istraživanje kriminalnih ponašanja na P2P mrežama. Svi ti alati su besplatni i prilagođeni osnovnim znanjima informatike, tako da za korištenje spomenutih alata nisu potrebni informacijski stručnjaci već se njima mogu služiti prosječno obrazovani i vješti policijski službenici.

Da bi se pokrenula kriminalistička istraživanja na P2P mrežama, ponajprije istraživanje iskorištavanja djece za pornografiju, potrebno je s obzirom na to da baza podataka i pristup softveru za takva istraživanja postoji, organizacijski ustrojiti grupu policijskih službenika koja će se specijalizirati za takva istraživanja i kojima će se profesionalna karijera razvijati u tome smjeru. Isto tako, potrebno je usmjeriti tehničke službe da osiguraju resurse, da pruže potporu i omoguće uvjete za kvalitetno provođenje kriminalističkih istraživanja. Zbog toga je potrebno čim prije organizacijski i tehnički krenuti u sustavna istraživanja kriminalnih ponašanja na računalnim sustavima i mrežama jer se veliki dio zabranjenih ponašanja preselio u virtualno okruženje i policija mora biti spremna pratiti korak s razvojem novih trendova.

LITERATURA

1. *Internet Usage Statistics* (2017). Dostupno na http://www.internetworldstats.com/stats.htm
2. *Kazneni zakon.* NN 125/11., 144/12., 56/15., 61/15.
3. Kokot, I. (2015). *Temeljne odrednice kriminalističkih postupanja u vezi sa sadržajem spolnog iskorištavanja djece na računalnom sustavu ili mreži u Republici Hrvatskoj*. Zagrebačka pravna revija, 4 (2), 231.-259. Dostupno na: http://hrcak.srce.hr/159400
4. Miller, R. *Istrage na P2P mrežama.* Obuka istražitelja dječje pornografije, International Law Enforcement Academy, Budimpešta, 27. 1. 2014. [predavanje i prezentacija].
5. *Peer to peer*, dostupno na https://hr.wikipedia.org/wiki/Peer_to_peer
6. Škrtić, D. (2013). *Mamljenje djeteta za zadovoljenje spolnih potreba uporabom informacijsko-komunikacijske tehnologije.* Zbornik Pravnog fakulteta Sveučilišta u Rijeci, 34 (2), 1139.-1170. Dostupno na http://hrcak.srce.hr/119419
7. Vijeće Europske unije, *Izvješće o ocjenjivanju sedmog kruga uzajamnih ocjenjivanja pod nazivom "Praktična provedba i djelovanje europskih politika o sprečavanju kiberkriminaliteta i borbi protiv njega" – izvješće o Hrvatskoj* (2017). Dostupno na http://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/hr/pdf
8. *Zakon o kaznenom postupku.* NN 152/08., 76/09., 80/11., 121/11., 91/12., 143/12., 56/13., 145/13., 152/14.
9. *Zakon o policijskim poslovima i ovlastima.* NN 76/09., 92/14.
10. *Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu.* NN 9/02.

Summary

Nikola Protrka, Davor Hrestak

Criminal Investigations Using P2P Computer Networks

The paper describes criminal analysis before and during criminal investigation of criminal behaviour and detection of criminal offences on P2P (Peer to Peer) computer networks with special focus on child pornography. It also describes the ways of sharing and downloading files through P2P computer networks and how those networks could be misused for criminal behaviour. It provides an overview of software tools that can be used for investigations of criminal behaviour and explains the directions that criminal investigations can take if such tools are used, both as regards open and close P2P networks. The paper provides an example of predictive analysis of photographs, which might be interesting to analysts and investigators during criminal analysis or investigation, through generic names.

Key words: P2P, computer network, criminal analysis, child pornography.