CARNET

Pregled protokola za privatnost DNS prometa

CERT.hr-PUBDOC-2022-1-406

CERT.hr

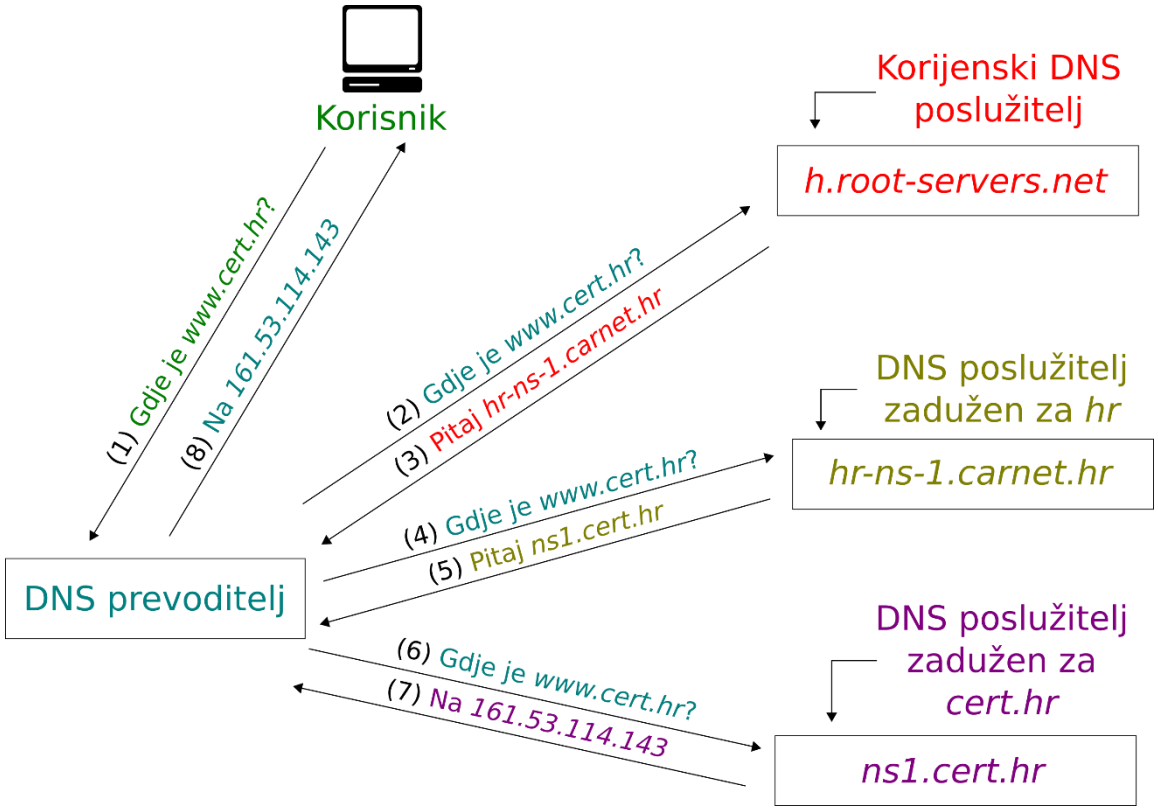
Sadržaj

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

DNS (engl. *Domain name System*) je sustav koji prevodi ljudima razumljive i lako pamtljive nazive domena (npr. *www.cert.hr*) u brojčane IP adrese koje računala trebaju za mrežnu komunikaciju (npr. *161.53.114.143*).

Taj se proces naziva DNS prevođenje (engl. *DNS resolution*) i ilustriran je na slici 1:



Slika 1 DNS prevođenje

Osim što su domene ljudima lakše pamtljive, korištenje domena smanjuje i ovisnost o nepromjenjivosti IP adresa (npr. ako dođe do promjene IP adrese, jednostavno se ažurira DNS zapis s novom IP adresom o čemu korisnici ne moraju biti obaviješteni).

Pri prevođenju, računalo prvo provjerava svoju DNS priručnu memoriju (engl. *DNS cache*), ako nema zapis šalje upit svojem *prevoditelju* (engl. *resolver*). Korisnici većinom koriste prevoditelj svog pružatelja internetskih usluga, ali postoje brojni drugi poslužitelji kao npr. *Google Public* DNS (IP adrese: 8.8.8.8 i 8.8.4.4) ili *Cloudfare* DNS (IP adrese: 1.1.1.1 i 1.0.0.1).

Prevoditelj pokušava odgovoriti na zahtjev koristeći svoju priručnu memoriju, a u slučaju da ne pronalazi odgovor pokušava ga naći kod odgovarajućih DNS poslužitelja, prateći hijerarhiju prostora domenskih imena. Primjer postupka prevođenja domene *www.cert.hr* prikazan je detaljno u nastavku:

```
(1) Učitavam popis vršnih poslužitelja:


-> a.root-servers.net (198.41.0.4)
-> b.root-servers.net (192.228.79.201)
-> c.root-servers.net (192.33.4.12)
-> d.root-servers.net (128.8.10.90)
-> e.root-servers.net (192.203.230.10)
-> f.root-servers.net (192.5.5.241)
-> g.root-servers.net (192.112.36.4)
-> h.root-servers.net (128.63.2.53)
-> i.root-servers.net (192.36.148.17)
-> j.root-servers.net (192.58.128.30)
-> k.root-servers.net (193.0.14.129)
-> l.root-servers.net (199.7.83.42)
-> m.root-servers.net (202.12.27.33)


(2) Šaljem upit na "h.root-servers.net" (nasumično odabran
među ponuđenim poslužiteljima)


Primljen odgovor - DNS poslužitelji za "hr" su:
-> pch.carnet.hr (204.61.216.90)
-> hr-ns-1.carnet.hr (161.53.160.100)


(3) Šaljem upit na "hr-ns-1.carnet.hr" (nasumično odabran među
ponuđenim poslužiteljima)


Primljen odgovor - DNS poslužitelji za "cert.hr" su:
-> ns2.cert.hr (161.53.114.135)
-> ns1.cert.hr (161.53.114.134)


(4) Šaljem upit na "ns1.cert.hr" (nasumično odabran među
ponuđenim poslužiteljima)


Primljen odgovor:
-> Odgovor: Zapis tipa A za www.cert.hr = 161.53.114.143
```

DNS poruke šalju se u otvorenom, nešifriranom obliku i kao takve ih mogu prisluškivati svi koji imaju pristup mrežnom prometu korisnika, primjerice pružatelji internetskih usluga (engl. *Internet Service Providers*, ISP) te ponekad i drugi korisnici spojeni na istu lokalnu mrežu.

Informacije iz DNS poruka otkrivaju koje web stranice korisnici posjećuju (ali ne i precizne aktivnosti koje korisnici na web stranicama obavljaju), **te i općenito koje sve ostale usluge na internetu koriste** (npr. usluge e-pošte, pozadinski servisi mobilnih aplikacija, videokonferencijski alati i sl.). Činjenica da je DNS promet nezaštićen može dovesti do značajnih ugroza privatnosti, npr. u svibnju 2020. godine procurilo je više od tri milijarde snimljenih DNS upita korisnika jednog tajlandskog pružatelja internetskih usluga [1].

Kao što primjerice postoje načini za zaštitu HTTP prometa i poruka e-pošte, s vremenom je postalo jasno da je važno zaštititi i privatnost DNS prometa, te su s tim ciljem osmišljeni i implementirani razni protokoli koji će biti opisani u nastavku ovog dokumenta.

Kako ne bi bilo zabune, prije detaljnijeg objašnjavanja problema i rješenja za privatnost DNS-a, potrebno je razjasniti razliku između privatnosti DNS prometa (teme ovog dokumenta) i autentičnosti DNS odgovora. Privatnost DNS prometa se odnosi na problem prisluškivanja DNS prometa koji nije šifriran, čime se ugrožava privatnost korisnika. Autentičnost DNS odgovora odnosi se na zaštitu od lažiranja DNS odgovora kojima bi se korisnika moglo preusmjeriti na drugu web stranicu ili internetsku uslugu od one koju je htio posjetiti.

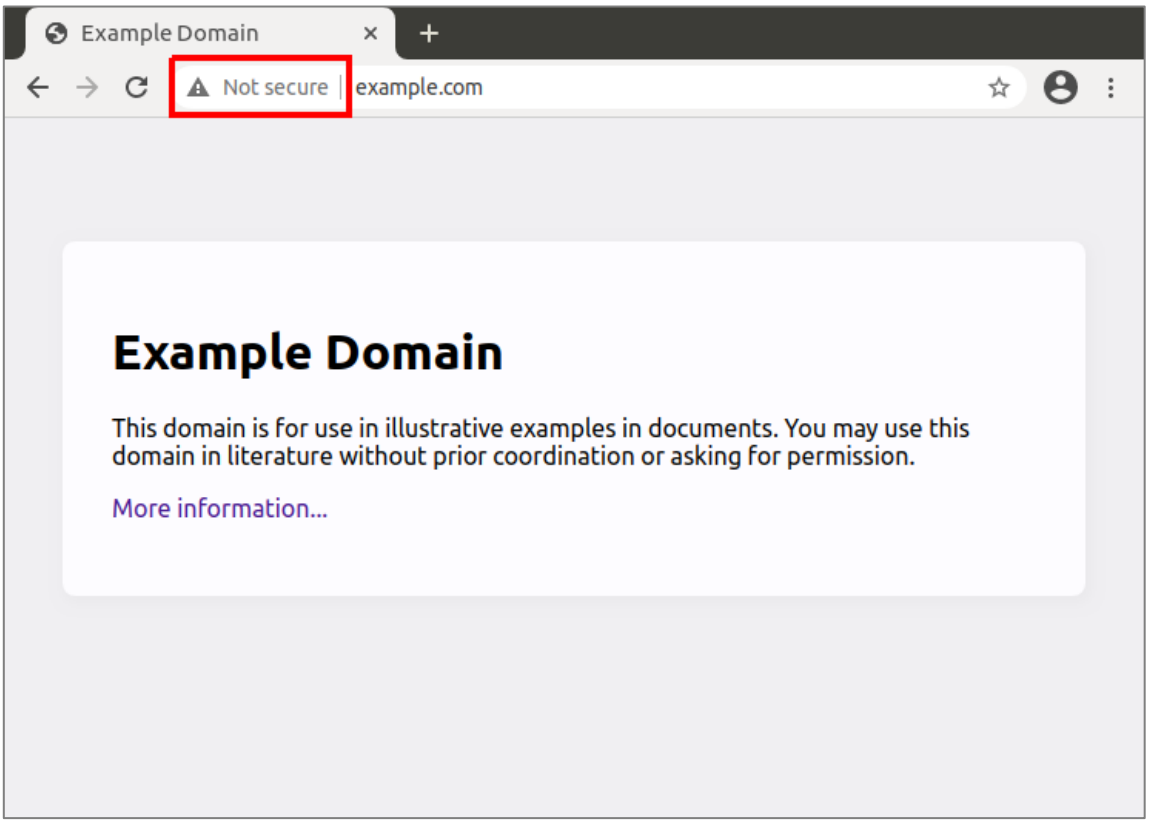
Za razliku od HTTP prometa kod kojega HTTPS rješava i problem privatnosti i problem autentičnosti, zbog distribuirane arhitekture DNS-a nije praktično osigurati i privatnost i autentičnost DNS poruka jednim rješenjem. Kod DNS-a, korisnici komuniciraju s DNS prevoditeljima, koji su zapravo posrednici te ni sami ne znaju odgovor na DNS upit, a tek krajnji DNS poslužitelji, koji nemaju izravan doticaj s korisnicima, mogu dati autentičan DNS odgovor. Zato, zaštita (kriptiranje) komunikacije s DNS prevoditeljima ne jamči autentičnost DNS odgovora. Rješenje problema autentičnosti DNS odgovora je DNS proširenje zvano DNSSEC. Detaljnije informacije o problemu i rješenju za autentičnost DNS odgovora dostupne su u dokumentu Nacionalnog CERT-a: „DNSSEC“.

2 Privatnost DNS prometa

Kada je riječ o rješenju za privatnost mrežnog prometa, prva pomisao je često HTTPS – protokol za šifriranje i zaštitu HTTP prometa. HTTPS je riješio probleme privatne i sigurne komunikacije koju dotadašnji protokol HTTP nije podržavao. Uvođenjem i primjenom HTTPS-a zahtjevi koje korisnik šalje i odgovori koje dobiva od poslužitelja su šifrirani i mrežni promatrač ih više ne može prisluškivati.

Svijest o privatnosti korisničkih podataka prilikom korištenja interneta postala je sve veća te su se osim HTTPS-a razvile i sigurne verzije ostalih protokola, npr. često korištene mobilne aplikacije za razmjenu poruka (*WhatsApp*, *Telegram*, *Signal*...) imaju mogućnost slanja šifriranih poruka.

No, iz aktivnosti osiguravanja privatnosti mrežnog prometa, dugo je bio isključen DNS protokol, dijelom zbog tehničkih izazova i dijelom zbog manjka svijesti. Za razliku od neprestanog upozoravanja korisnika da moraju paziti da pristupaju web stranicama putem HTTPS-a (kao što je prikazano na slici 2, i sami web preglednici upozoravaju korisnika kada se ne koristi HTTPS), privatnost DNS-a dugo je bila u sporednom planu.



Slika 2 Web preglednik otežava posjećivanje stranice koja ne osigurava privatnost [2]

Ako korisnik primjerice posjeti web stranicu *Facebooka* (koja koristi siguran HTTPS protokol i šifrira svu komunikaciju), nitko neće moći vidjeti HTTP zahtjeve koje korisnik šalje i odgovore koje dobiva, tj. nitko neće moći vidjeti aktivnosti koje korisnik obavlja na *Facebooku*, profile koje posjećuje ni poruke koje šalje.

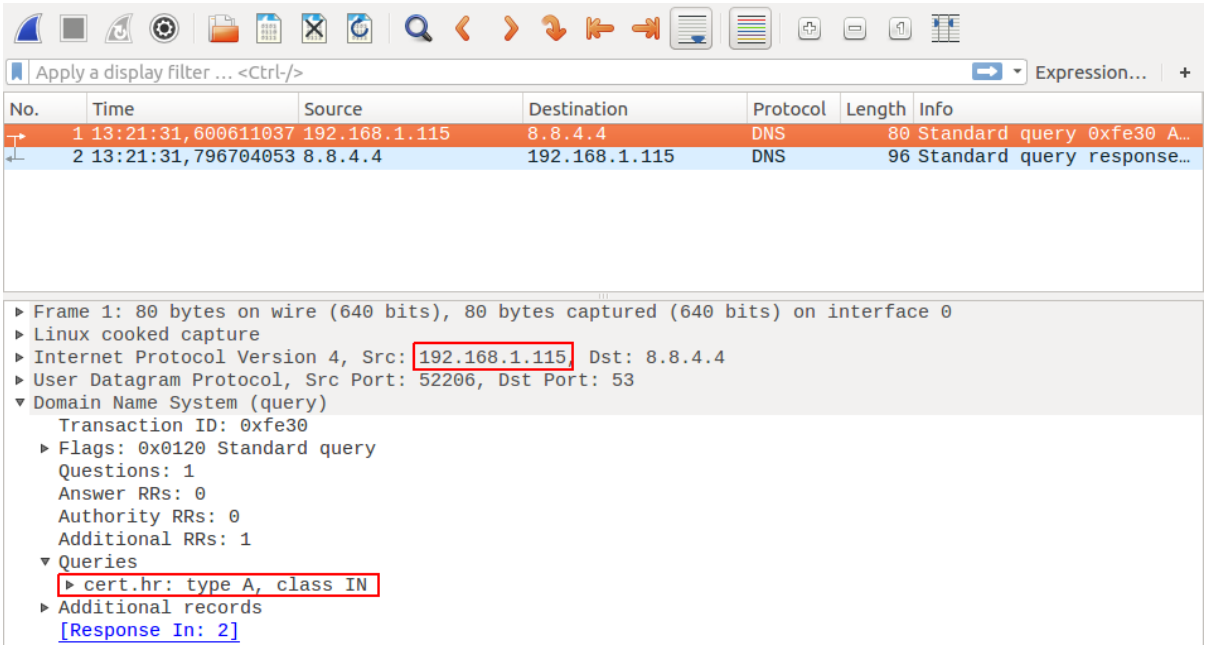
Ali, informacija da je korisnik posjetio *Facebook* stranicu poznata je prvenstveno zbog DNS upita kojim komunikacija započinje, a koji nije šifriran i vidljiv je:

- DNS prevoditeljima,
- pružatelju internetskih usluga (engl. *Internet Service Provider*, ISP),
- usmjerivačima (engl. *routers*) na koje DNS zahtjev nailazi na putu do odredišta i
- svakom tko prisluškuje mrežu.

Kako bi se očuvala korisnikova privatnost, informacije o tome koje je stranice korisnik posjećivao trebale bi ostati tajne, tj. trebao bi ih imati samo DNS prevoditelj (engl. *resolver*) kojemu vjerujemo da ne zloupotrebljava podatke o domenskim imenima koje smo posjetili.

Za sve ostale nabrojane sudionike komunikacije (osim DNS prevoditelja) ne postoji opravdan razlog da vide sadržaj DNS upita. DNS prevoditelj u konačnici mora vidjeti zahtjev jer ne može odgovoriti na pitanje ako ne zna koje je pitanje. Ako korisnika brinu i namjere DNS prevoditelja, moguće je sakriti identitet od njega (primjerice slanjem DNS zahtjeva preko mreže anonimnosti Tor) kako ne bi mogao povezati DNS upite s korisnikom.

Klijent (korisnik) šalje uobičajeni nešifrirani DNS upit putem UDP protokola i priključka (engl. *port*) 53. Podržano je slanje DNS zahtjeva i preko TCP protokola, ali ono se iznimno koristi samo za veće poruke. DNS upit sastoji se od više polja, ali za privatnost su najbitniji QNAME (puni naziv domene kojoj korisnik želi pristupiti) i IP adresa korisnika preko kojih se može povezati koji je korisnik pregledavao koje web stranice, odnosno na koje usluge na internetu se spajao. Primjer snimljenog nezaštićenog DNS upita, s istaknutom IP adresom korisnika (u ovom primjeru privatnom IP adresom) te nazivom tražene domene, može se vidjeti na slici 3.



Slika 3 Nezaštićen DNS upit

Dok se iz DNS prometa ne mogu prepoznati precizne aktivnosti na posjećenoj stranici ili internetskoj usluzi, može se općenito zaključiti koji se programi koriste i koje se stranice posjećuju. Pristup tim podacima nije zanimljiv samo pružateljima internetskih usluga te marketinškim tvrtkama koje se bave profiliranjem korisnika i ciljanim oglašavanjem, već i zlonamjernim pojedincima, u procesu pripreme za napad.

Prisluškivanje DNS prometa možemo podijeliti na dva slučaja:

- **prisluškivanje između klijenta i prevoditelja**
  U ovom se slučaju zna točna IP adresa korisnika koji je poslao DNS upit.

- **prisluškivanje između prevoditelja i DNS-poslužitelja**
  U ovom se slučaju zna samo da skup korisnika, npr. korisnici određenog pružatelja internetskih usluga, šalju DNS zahtjeve.

Postoji i mogućnost da sam prevoditelj ne poštuje privatnost svojih korisnika, već da nekako zloupotrebljava podatke o DNS upitima svojih korisnika. Naravno, prevoditelj se može promijeniti, ali teško je znati zaslužuje li neki drugi prevoditelj naše povjerenje. Kao što je i prethodno spomenuto, ako korisnik ne vjeruje DNS prevoditelju, onda može na neki način (npr. pomoću mreže anonimnosti Tor) sakriti svoj identitet prilikom slanja DNS upita.

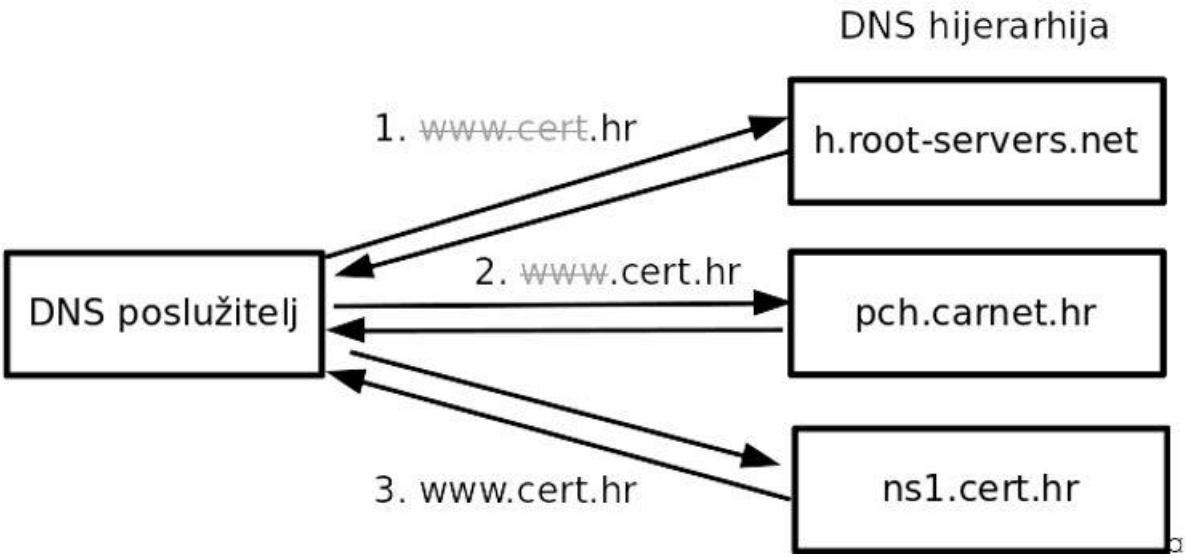
QNAME minimizacija, DNS *over* TLS, DNS *over* HTTPS i *DNSCrypt* neka su od tehničkih rješenja koja ograničavaju curenje podataka ili u potpunosti šifriraju DNS promet te tako osiguravaju veću privatnost DNS prometa. Navedena rješenja bit će opisana u nastavku ovog dokumenta.

2.1 QNAME minimizacija

QNAME minimizacija opisana je u standardu RFC 7816 kao jedna tehnika poboljšanja privatnosti u DNS protokolu [3]. Bitno je naglasiti da QNAME minimizacija ne rješava problem privatnosti DNS protokola u potpunosti, već samo djelomično ublažava posljedice.

QNAME minimizacija oslanja se na činjenicu da je privatnost manje ugrožena ako prenosimo manje podataka. QNAME minimizacija postiže poboljšanje u privatnosti DNS protokola tako da smanjuje količinu podataka koju DNS prevoditelj šalje DNS poslužiteljima.

Umjesto da se šalje potpuno ime svakom DNS poslužitelju, šalje mu se samo dio imena koji odgovara hijerarhijskoj poziciji DNS poslužitelja. Primjer QNAME minimizacije prikazan je na slici 4.



Slika 4 Primjer Q-NAME minimizacije

Glavna prednost QNAME minimizacije je potpuna kompatibilnost s postojećim DNS protokolom te se zbog toga može vrlo lagano implementirati u postojeću infrastrukturu. Isto tako, budući da se implementira na razini DNS prevoditelja, korisnici ne moraju ništa konfigurirati.

Mana QNAME minimizacije je činjenica da promet i dalje ostaje nešifriran te je prisluškivanje i dalje moguće. Komunikacija između korisnika i prevoditelja se ne mijenja te kao takva nema nikakva poboljšanja u smislu privatnosti, a komunikacija između prevoditelja i poslužitelja ima ograničena poboljšanja.

2.2 DNS over TLS

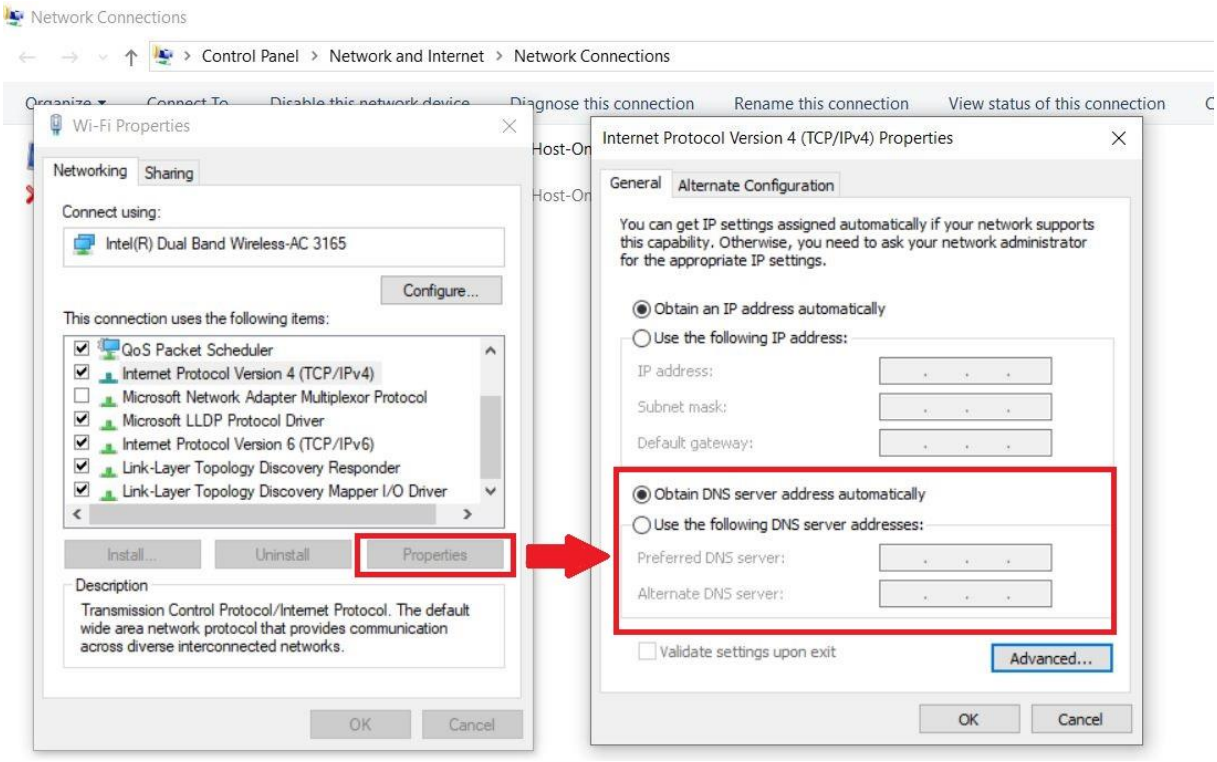
DNS preko TLS-a (engl. *DNS over Transport Layer Security* ili *DNS over TLS*, skr. DoT, RFC 7858) je protokol koji za prijenos DNS upita koristi sigurni transportni sloj (kao i npr. HTTPS) te na taj način šifrira i sprječava prisluškivanje DNS prometa [4].

Osiguravanje privatnosti sigurnim transportnim slojem već je viđeno i na nekim drugim protokolima:

- HTTP (tcp/80) → HTTPS (tcp/443)
- SMTP (tcp/25) → SMTPS (tcp/465)
- IMAP (tcp/143) → IMAPS (tcp/993)
- te u ovom slučaju: **DNS (tcp/53 ili udp/53) → DoT (tcp/853)**

Umjesto uobičajenog protokola UDP i priključka 53 koje koristi DNS, DoT koristi protokol TCP i priključak 853. Kako bi se mogao koristiti DoT (a i ostali sigurni DNS protokoli), i klijent i prevoditelj ga moraju podržavati.

U postavkama računala spojenog na mrežu uobičajeno je konfigurirano korištenje automatski postavljenog DNS prevoditelja (putem protokola DHCP), kao što je prikazano na slici 5.



Slika 5 Podrazumijevane (engl. *default*) postavke računala

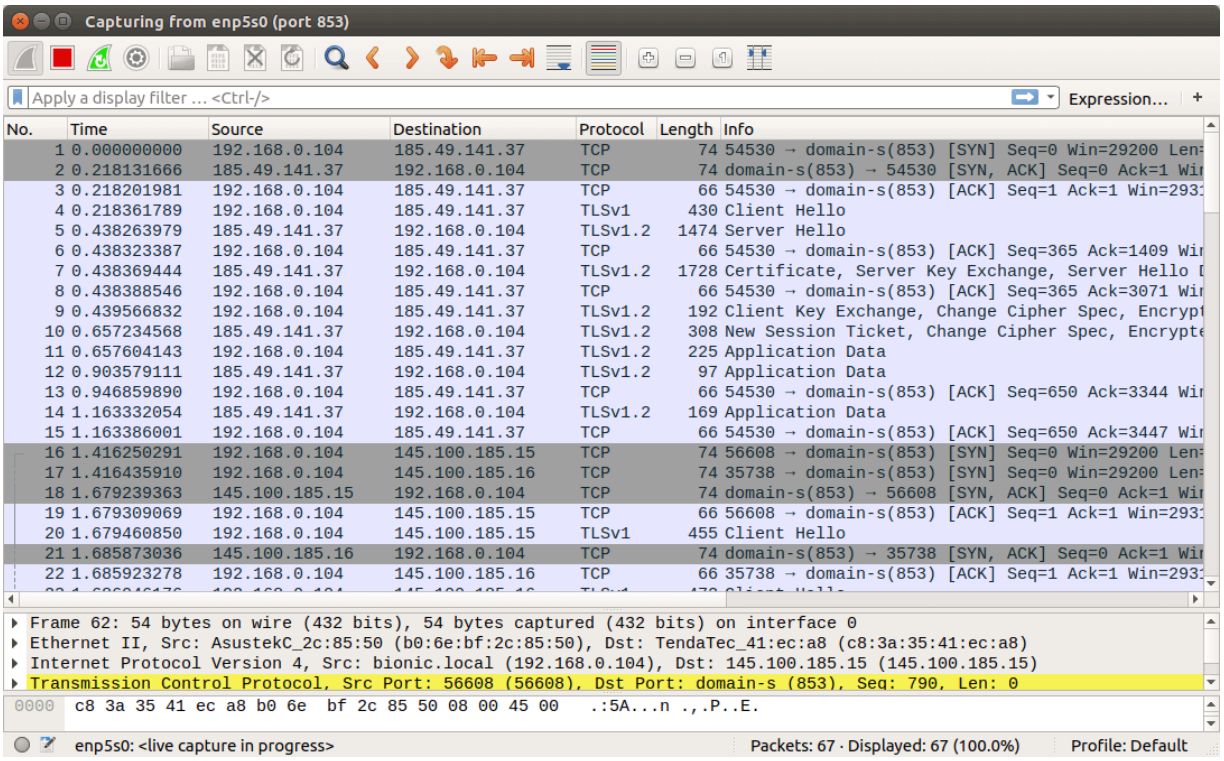
To najčešće dovodi do toga da korisnik koristi DNS prevoditelj od svog pružatelja internetskih usluga.

Umjesto automatske dodjele DNS prevoditelja, korisnici mogu i ručno konfigurirati korištenje točno određenog DNS prevoditelja. Trenutno su popularni alternativni DNS prevoditelji od tvrtki Google (adrese 8.8.8.8 i 8.8.4.4), Cloudflare (adrese 1.1.1.1 i 1.0.0.1), OpenDNS/Cisco (adrese 208.67.222.222 i 208.67.220.220) itd. Napredni korisnici često ručno konfiguriraju neki od takvih DNS prevoditelja, što znači da će njihovo računalo uvijek poslati svoj DNS zahtjev tim prevoditeljima, a ne prevoditeljima njihovog pružatelja internetskih usluga.

DoT je prvenstveno namijenjen korištenju između korisničkog računala i DNS prevoditelja, gdje je opasnost za privatnost DNS prometa najveća. Preduvjet za korištenje DoT-a je odabir DNS prevoditelja koji podržava taj protokol. Mnogi javni DNS prevoditelji podržavaju DoT, uključujući Google DNS i Cloudflare DNS.

Kod razmjene DNS poruka putem DoT-a, veza se uspostavlja preko poznatog priključka (engl. *well-known port*) 853, klijent i prevoditelj stvaraju TLS sjednicu (engl. TLS *session*) te tako osiguravaju kanal i razmjenjuju poruke.

Na slici 6 prikazana je snimka DoT prometa. Iz sadržaja mrežnog prometa se ne može iščitati DNS upit kojeg klijent šalje, moguće je samo otkriti tko komunicira (korisnik i DNS prevoditelj) te da je korišteni protokol DoT (zbog korištenja priključka 853).



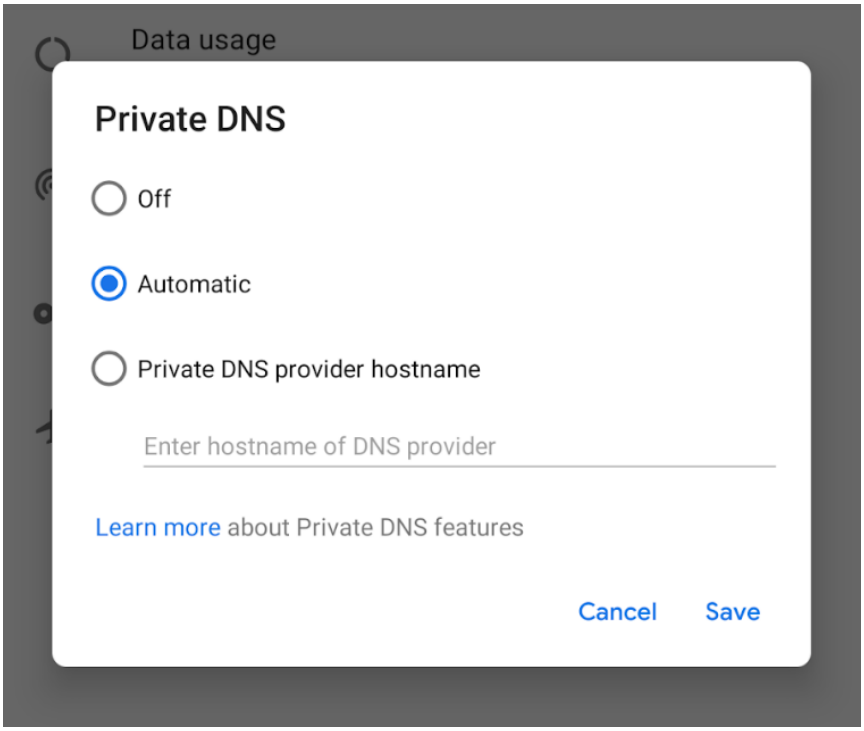
Slika 6 DoT promet usnimljen alatom Wireshark

Iako je promet šifriran, činjenica da se promet prema poznatom priključku (u ovom slučaju 853) može jednostavno blokirati vatrozidom (engl. *firewall*) omogućuje određenim institucijama ili državnim režimima da lako spriječe korištenje ovog protokola kako bi natjerali korisnike da koriste uobičajeni, nešifrirani DNS protokol.

Još neki nedostaci u usporedbi s običnim DNS-om su činjenica da stvaranje i održavanje TLS sjednica zahtjeva dodatne resurse, pogotovo sa strane prevoditelja koji istovremeno komuniciraju s velikim brojem klijenata, te činjenica da softverska podrška za DoT sa strane klijenata nije ugrađena u operacijski sustav Microsoft Windows ni u starije verzije drugih operacijskih sustava.

Potpora za DoT ugrađena je u operacijski sustav Android (od verzije 9, prikazano na slici 7), u Linux distribucije kroz paket *systemd-resolved* (od verzije 239) te u operacijske sustave iOS (od verzije 14) i macOS (od verzije *Big Sur*).

Na operacijskom sustavu Microsoft Windows se za sada mora koristiti odvojena implementacija koje se mora ručno instalirati. Jedna od najpoznatijih implementacija je *Stubby* koja podržava *Windows, Linux* i *macOS*.



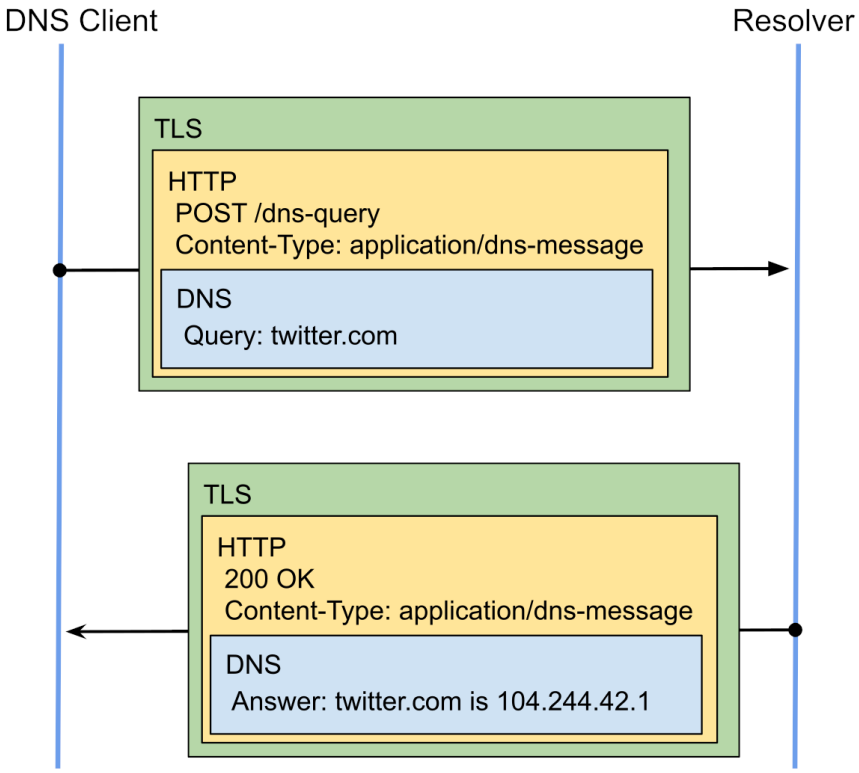
Slika 7 Konfiguracijsko sučelje za DoT (pod nazivom *Private DNS*) na operacijskom sustavu Android 9 (izvor)

2.3 DNS over HTTPS

DNS preko HTTPS-a (engl. *DNS over HTTPS*, skr. DoH, RFC 8484), isto kao DoT, u potpunosti šifrira DNS promet i tako osigurava privatnost [5].

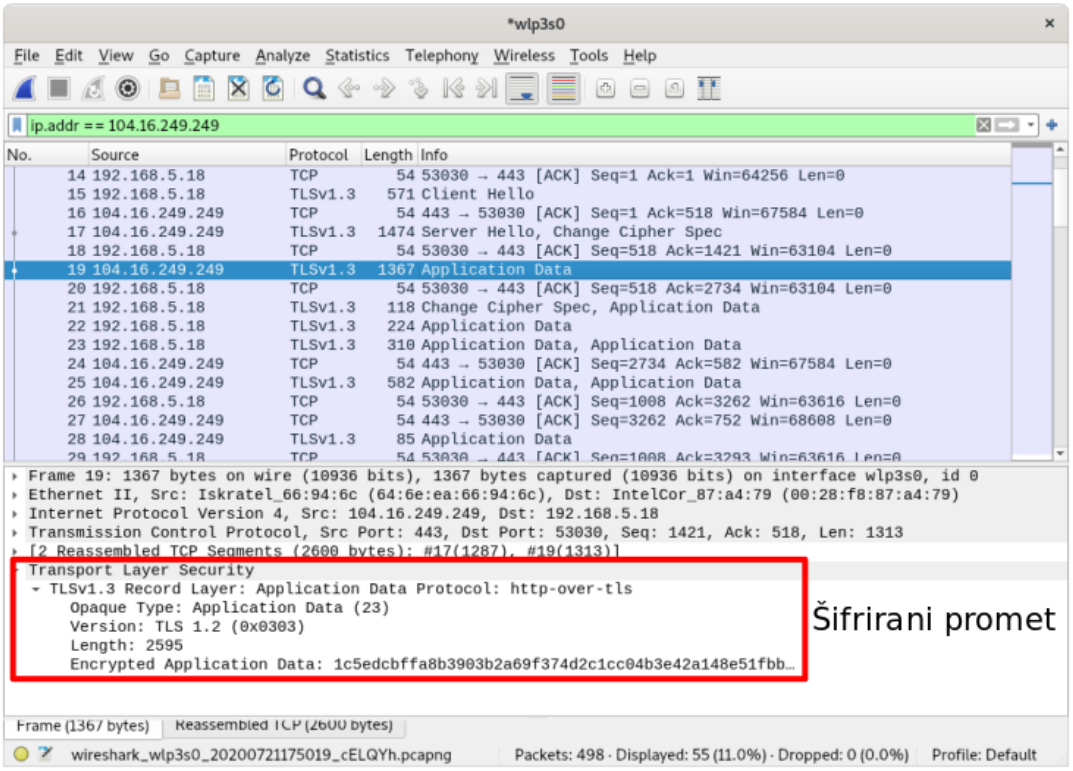
DoH je sličan DoT-u, ali umjesto uspostavljanja izravne TLS veze koristi HTTPS protokol (koji interno koristi TLS). Jedna od glavnih razlika između ova dva proširenja DNS protokola je što DoT koristi jedinstven poznati priključak (853) dok DoH koristi priključak 443, isto kao i protokol HTTPS. Za DoH, korištenje istog priključka kao i protokol HTTPS dovodi do boljeg uklapanja DNS prometa u sveprisutni HTTPS promet. Drugim riječima, DoH promet je teže uočiti i blokirati jer nalikuje na uobičajeni HTTPS promet, što je dobra vijest za korisnike koji ne žele da se njihov DNS promet nadzire ili blokira.

Na slici 8 prikazan je pojednostavljeni primjer slanja upita i primanja odgovora protokolom DoH.



Slika 8 DoH slanje DNS zahtjeva i primanje odgovora [6]

Mrežna snimka DNS upita i odgovora preko DoH-a prikazana je na slici 9. Kao i kod DoT-a, iz mrežnog prometa ne možemo zaključiti za koju je domenu korisnik poslao upit. Uz to, jedini razlog zašto možemo naslutiti da je to DNS upit je zato što je moguće prepoznati da je IP adresa s kojom korisnik komunicira javno poznata IP adresa DoH prevoditelja (u ovom slučaju, to je IP adresa prevoditelja *mozilla.cloudflare-dns.com*). Kada bi se koristio DoH prevoditelj koji na istoj domeni ima i web stranicu, bilo bi izrazito teško iz mrežnog prometa uopće zaključiti da se radi o DNS upitu i odgovoru.



Slika 9 Snimljeni DoH promet

Mana protokola DoH su dodatno utrošeni resursi koji proizlaze ne samo iz stvaranja i održavanja TLS sjednica, nego i zbog HTTP zaglavlja koji se prenose.

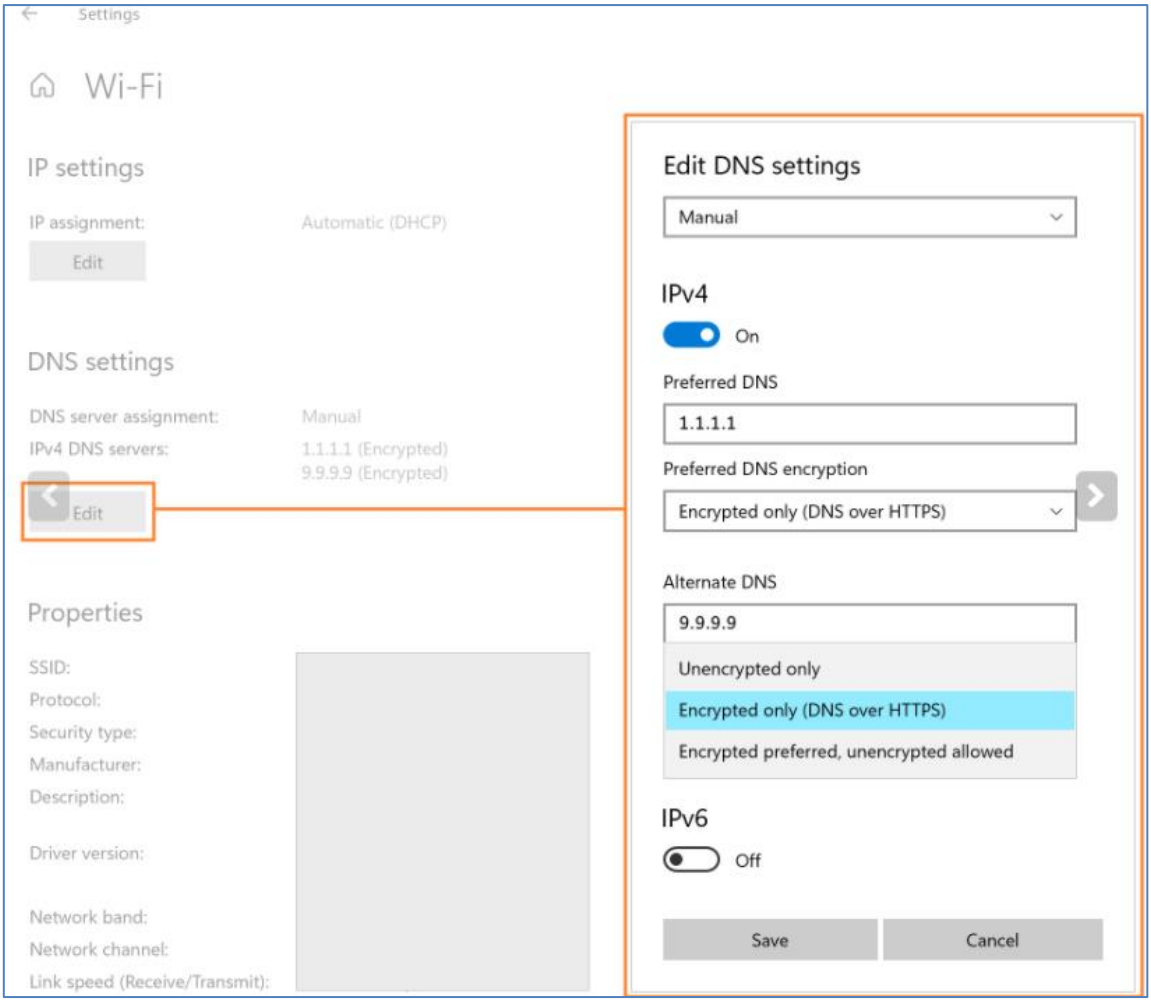
Kao i u slučaju DoT-a, da bi se DoH mogao koristiti, i DNS prevoditelj i klijent ga moraju podržavati. Slično kao i za DoT, mnogi javni DNS prevoditelji imaju podršku za DoH, uključujući Google DNS, Cloudflare DNS i OpenDNS.

Sa strane klijenta, na razini operacijskih sustava, podrška za DoH ugrađena je u iOS (od verzije 14) i macOS (od verzije *Big Sur*), a podrška u operacijskom sustavu Microsoft Windows je trenutno u razvoju za Windows 10, tj. trenutno je dostupna u testnoj verziji (*Windows Insider Preview*, prikazano na slici 10). Windows 11 podržava DoH. Na ostalim operacijskim sustavima (Android i Linux distribucije) potrebno je instalirati zaseban softver za korištenje DoH-a, primjerice *dnscrypt-proxy* koji podržava više različitih protokola, uključujući i DoH.

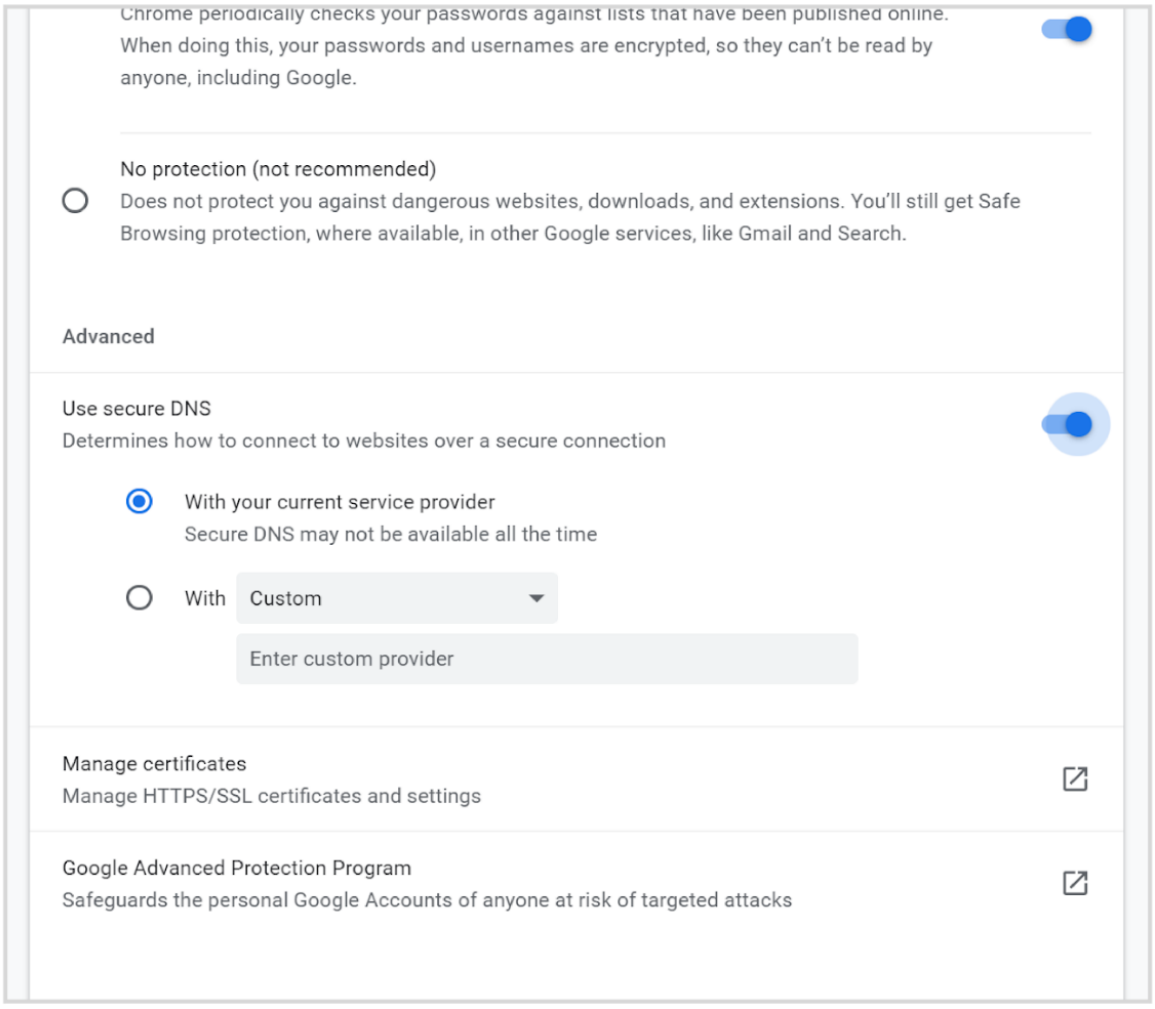
Implementacija i podrška za korištenje DoH-a danas je dostupna i u svim najčešće korištenim web preglednicima (*Firefox*, *Google Chrome*, *Microsoft Edge*). Web preglednici ne samo da su počeli podržavati implementaciju DoH-a, već su ih neki od njih (*Firefox* i *Google Chrome*) počeli i podrazumijevano koristiti u određenim slučajevima. Primjerice, *Firefox* automatski koristi DoH (pomoću posebnog Cloudflare DNS prevoditelja) za korisnike u SAD-u, dok *Google Chrome* automatski koristi DoH ako ga trenutno konfigurirani DNS prevoditelj podržava.

Korištenje DoH-a na razini web preglednika znači da će biti zaštićen samo DNS promet kojega je inicirao web preglednik, no prednost je lakoća korištenja, tj. trenutno je najlakši način za korištenje DoH-a upravo korištenje kroz web preglednik. Slike 11 i 12 prikazuju

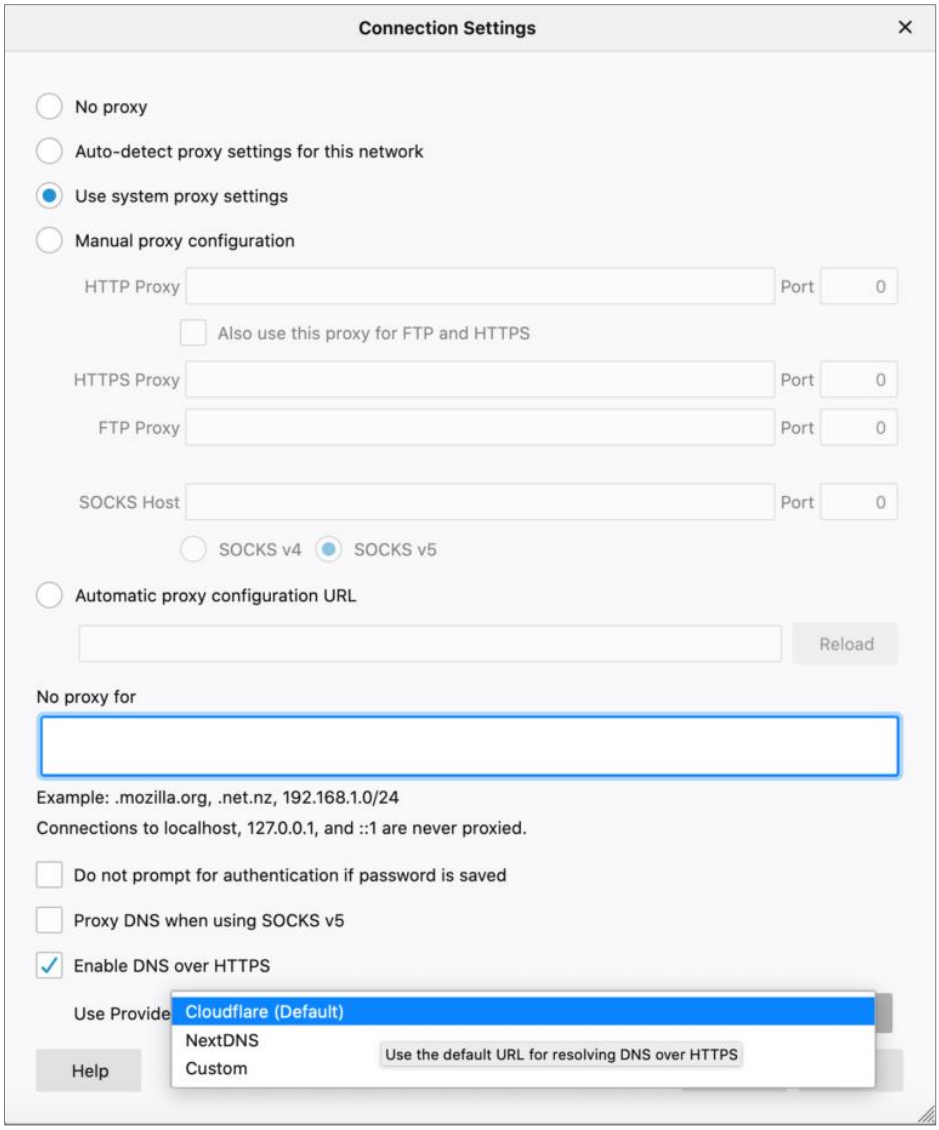
konfiguracijsko sučelje DoH-a u postavkama web preglednika *Google Chrome* i *Mozilla Firefox*.



Slika 10 Konfiguracija DoH-a u testnoj (Insider Preview) verziji Windowsa (izvor)



Slika 11 Konfiguracija DoH-a u postavkama web preglednika Google Chrome (izvor)



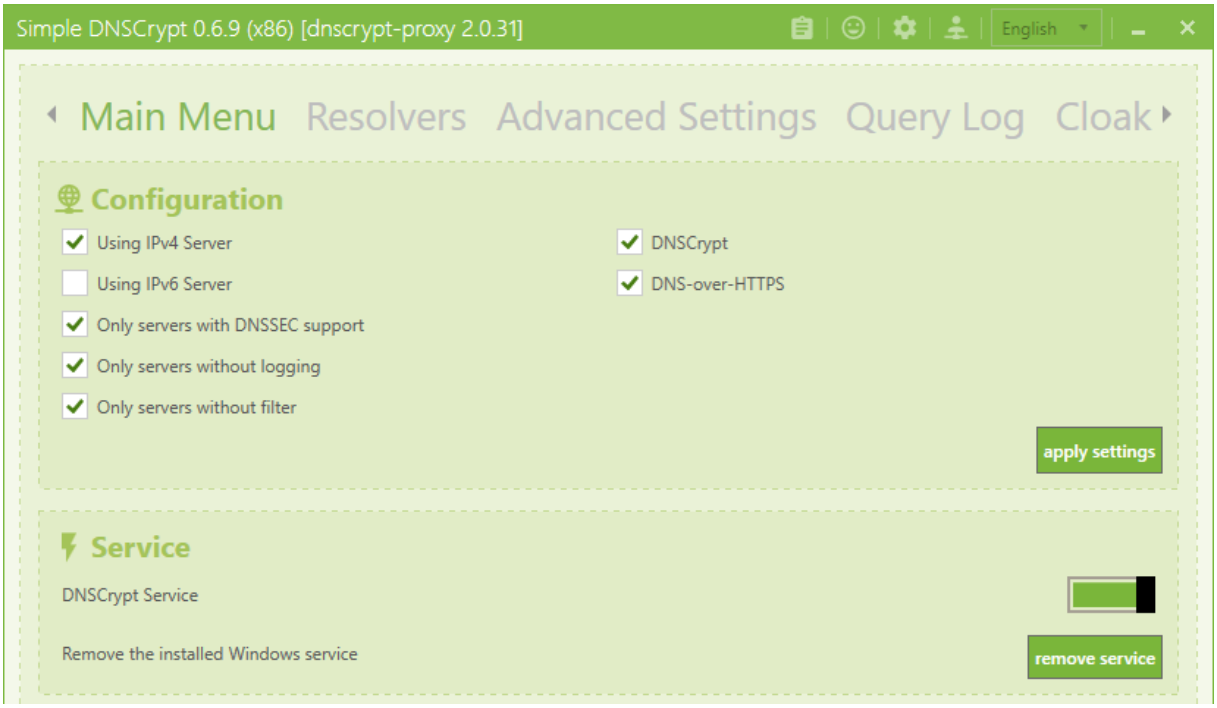
Slika 12 Konfiguracija DoH-a u postavkama web preglednika Mozilla Firefox (izvor)

2.4 DNSCrypt

DNSCrypt je još jedan protokol koji šifrira komunikaciju između DNS klijenta i DNS prevoditelja te na taj način sprječava prisluškivanje DNS zahtjeva i odgovora [7]. Protokol DNSCrypt može koristiti UDP ili TCP protokol te koristi priključak 443 (isti kao HTTPS i DoH). Također, DNSCrypt podržava i način rada sličan radu mreže anonimnosti Tor za anonimno slanje DNS upita i primanje DNS odgovora [8].

Kao što i web stranica projekta DNSCrypt navodi, u usporedbi DNSCrypta s rješenjima poput DoT-a i DoH-a [9], sva navedena rješenja (DNSCrypt, DoT, DoH i neka druga manje korištena rješenja) u praksi nude sličnu zaštitu, pa je korisnicima zato kompatibilnost s postojećim alatima i infrastrukturom jedan od glavnih kriterija odabira. Za razliku od DoT-a i DoH-a, DNSCrypt nije standardiziran na razini IETF-a, tj. nema svoj RFC standard. Podrška za DNSCrypt nije ugrađena ni u jedan često korišteni operacijski sustav ili web preglednik, tako da je za korištenje DNSCrypta trenutno potrebno instalirati zaseban softver na svim često korištenim platformama.

Najpopularnija implementacija DNSCrypt klijenta je *dnscrypt-proxy*, ona je dostupna za instalaciju i korištenje na svim najčešće korištenim operacijskim sustavima. Uz podršku za protokol DNSCrypt, *dnscrypt-proxy* podržava i protokol DoH te podržava korištenje Tor-a, SOCKS posrednika ili DNSCryptovog sustava anonimiziranih DNS upita i odgovora (*Anonymized DNS*) za anonimnost pri korištenju DNS protokola. Za operacijski sustav Microsoft Windows, dostupan je i alat *Simple DNSCrypt* koji, kroz grafičko sučelje, omogućava jednostavnu konfiguraciju alata *dnscrypt-proxy* (prikazano na slici 13).



Slika 13 Konfiguracija DNSCrypta ili DoH-a na operacijskom sustavu Windows pomoću alata Simple DNSCrypt (izvor)

3 Zaključak

Skoro svako korištenje weba (i interneta općenito) započinje DNS upitom. Zahvaljujući DNS-u, ljudi ne moraju pamtiti IP adrese, već se DNS protokolom automatski pronalazi IP adresa povezana s domenskim imenom.

Iako raste svijest oko problema privatnosti mrežne komunikacije, tek su se nedavno pojavila praktična, gotova rješenja za zaštitu privatnosti DNS prometa, prvenstveno temeljena na protokolima DNS over HTTPS (DoH), DNS over TLS (DoT) i DNSCrypt.

DoT, DoH i DNSCrypt nude sličnu razinu zaštite, te je korištenje bilo kojega od ta tri protokola značajno unaprjeđenje privatnosti u usporedbi s korištenjem običnog, nešifriranog DNS-a. Osim privatnosti i sigurnosti, jedan od glavnih faktora koji će utjecati na korištenje navedenih protokola je njihova podrška na strani klijenta, tj. korisnika.

DoH je podržan u često korištenim web preglednicima, te je u nekim slučajevima i podrazumijevano (engl. *default*) uključen. Dostupan je i u operacijskim sustavima iOS i macOS, a sad je dostupan i za Windows 11. Korisnici koji na jednostavan način žele isprobati neki od protokola za privatnost DNS prometa mogu lako uključiti DoH u svom web pregledniku i tako zaštititi veliki dio svog DNS prometa.

Za korisnike koji žele otići korak dalje i zaštititi sav svoj DNS promet, potrebno je:

1. Konfigurirati korištenje jednog od opisanih protokola za privatnost DNS prometa na svojem kućnom usmjerivaču (engl. *router*) kako bi se zaštitio DNS promet svih uređaja koji su stalno spojeni na kućnu mrežu (stolna računala, pametni televizori i sl.).

   Napredni kućni usmjerivači, primjerice oni temeljeni na Linux distribuciji OpenWRT, imaju podršku za sve od opisanih protokola za DNS privatnost. Uključivanje protokola za DNS privatnost na razini kućnog usmjerivača znači da će svi uređaji na kućnoj mreži koji koriste automatske (DHCP) postavke efektivno biti zaštićeni.

2. Konfigurirati korištenje jednog od opisanih protokola za privatnost DNS prometa na svim uređajima koji se koriste i izvan kućne mreže (pametni telefoni, prijenosna računala i sl.), kako bi oni bili zaštićeni i kada se ne nalaze u kućanstvu.

   Pod pretpostavkom da se koristi relativno nova verzija operacijskog sustava, trenutno je lako uključiti DoT ili DoH na pametnim telefonima (Android i iOS) te na računalima s operacijskim sustavom macOS i Linux. Ubuduće će biti lako kroz postavke uključiti DoH i na razini operacijskog sustava Windows (dostupno za Windows 11), no do tada je na te uređaje potrebno instalirati zaseban softver (npr. *Simple DNSCrypt*) za korištenje nekog od protokola za privatnost DNS prometa.

U sljedećoj tablici se nalazi trenutni pregled (s kraja 2021. godine) podrške za protokole privatnosti DNS prometa na često korištenim operacijskim sustavima i web preglednicima:

	DoT	DoH	DNSCrypt
Microsoft Windows	potrebno je ručno instalirati zaseban softver za podršku, npr. *Stubby*	dostupno za Windows 11; dostupno u testnoj verziji (*Windows Insider Preview*); u suprotnom, potrebno je ručno instalirati zaseban softver za podršku, npr. *Simple DNSCrypt*	potrebno je ručno instalirati zaseban softver za podršku, npr. *Simple DNSCrypt*
macOS	dostupno od verzije *Big Sur*	dostupno od verzije *Big Sur*	potrebno je ručno instalirati zaseban softver za podršku, npr. *dnscrypt-proxy*
Linux	podržano kroz *systemd-resolved* od verzije 239	potrebno je ručno instalirati zaseban softver za podršku, npr. *dnscrypt-proxy*	potrebno je ručno instalirati zaseban softver za podršku, npr. *dnscrypt-proxy*
Android	podržano od verzije 9 (*Pie*)	potrebno je ručno instalirati zaseban softver za podršku, npr. *Nebulo*	potrebno je ručno instalirati zaseban softver za podršku, npr. *InviZible Pro*
iOS	podržano od verzije 14	podržano od verzije 14	potrebno je ručno instalirati zaseban softver za podršku, npr. *DNSCloak*
Google Chrome	nema podrške	podržano od verzije 78	nema podrške
Mozilla Firefox	nema podrške	podržano od verzije 62	nema podrške

Uz privatnost prometa, još jedan problem DNS-a je autentičnost DNS odgovora. Rješenje tog problema, DNSSEC, kompatibilno je s DoT-om, DoH-om i DNSCryptom, tako da oprezni korisnici mogu koristiti DNSSEC zajedno s jednim od protokola za privatnost DNS prometa. Za korisnike koji ne žele samostalno konfigurirati DNSSEC, samo korištenje DoT-a, DoH-a ili DNSCrypta već daje jednu razinu garancije da su primljeni DNS odgovori

autentični, pod pretpostavkom da korišteni DNS prevoditelj koristi DNSSEC (tj. provjerava potpise) i da korisnik vjeruje da prevoditelj ne mijenja DNS odgovore.

4 Reference

1. **xxdesmus.** Rainbowtabl.es. [Mrežno] svibnja 2020. [Citirano: 20. rujna 2020.] https://rainbowtabl.es/2020/05/25/thai-database-leaks-internet-records/.

2. **K, Tim.** What Is The "Not Secure" Warning In Google Chrome? *Byte Bite bit.* [Mrežno] [Citirano: 20. rujna 2020.] https://bytebitebit.com/1788/not-secure-warning-google-chrome/.

3. **Bortzmeyer, Stephane.** RFC7816 - DNS Query Name Minimisation to Improve Privacy. [Mrežno] [Citirano: 19. siječnja 20218.] https://tools.ietf.org/html/rfc7816.

4. **Hu, Zi, i dr.** RFC7858 - Specification for DNS over Transport Layer Security (TLS). *IETF*. [Mrežno] svibanj 2016. [Citirano: 19. siječnja 2021.] https://tools.ietf.org/html/rfc7858.

5. **Hoffman, Paul i McManus, Patrick.** RFC8484 - DNS Queries over HTTPS (DoH). *IETF*. [Mrežno] listopad 2018. [Citirano: 19. siječnja 2021.] https://tools.ietf.org/html/rfc8484.

6. **Wu, Peter.** DNS Encryption Explained. *Cloudflare.* [Mrežno] 29. listopada 2019. [Citirano: 25. rujna 2020.] https://blog.cloudflare.com/dns-encryption-explained/.

7. **Jensen, Tommy.** Windows Insiders gain new DNS over HTTPS controls. [Mrežno] 29. lipnja 2021. [Citirano: 2. studenog 2021.] https://techcommunity.microsoft.com/t5/networking-blog/windows-insiders-gain-new-dns-over-https-controls/ba-p/2494644.

8. **DNSCrypt.** DNSCrypt version 2 - Official Project Home Page. [Mrežno] [Citirano: 19. siječnja 2021.] https://dnscrypt.info/.

9. —. Anonymized DNS · DNSCrypt/dnscrypt-proxy Wiki. *GitHub.* [Mrežno] [Citirano: 19. siječnja 2021.] https://github.com/DNSCrypt/dnscrypt-proxy/wiki/Anonymized-DNS.

10. —. DNSCrypt - FAQ - DNSCrypt vs DoH. [Mrežno] [Citirano: 21. siječnja 2021.] https://dnscrypt.info/faq.

11. **Fisher, Dennis.** Google Makes DNS Over HTTPS Default in Chrome By Dennis Fisher . *Decipher.* [Mrežno] 20. svibnja 2020 . [Citirano: 20. rujna 2020.] https://duo.com/decipher/google-makes-dns-over-https-default-in-chrome.

12. **DNSCrypt.** dnscrypt-proxy. *Github.* [Mrežno] [Citirano: 20. rujna 2020.] https://github.com/DNSCrypt/dnscrypt-proxy.