

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

Covid-tracker

Tehnička dokumentacija

Verzija 1.0

Studentski tim: Adam Ban
Marko Filipović
Marino Rabuzin
Hrvoje Rom

Nastavnik: doc. dr. sc. Ante Đerek

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

Sadržaj

1.	Problematika i ciljevi projekta	3
2.	Načelo rada aplikacija za praćenje kontakata	4
3.	Razvoj aplikacije za praćenje kontakata temeljena na Googleovom API-u	5
4.	Sigurnosna analiza službene hrvatske aplikacije za praćenje kontakata Stop COVID-19	5
4.1	Izgradnja i instalacija aplikacije iz izvornog koda	5
4.2	Dekompajliran izvršni kod aplikacije i analiza	7
4.3	Praćenje internetskog prometa	8
4.4	Otpornost aplikacije na MITM napad pomoću Android uređaja	9
4.5	Otpornost aplikacije na MITM napad pomoću Apple uređaja	10
5.	Zaključci i preporuke	20
6.	Literatura	21

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

1. Problematika i ciljevi projekta

Prošlo je godinu dana od prve zabilježene zaraze korona virusom¹, u prosincu 2019. u Wuhanu (Kina). Virus se brzo proširio svijetom i uveo nas u dugotrajno razdoblje svjetske pandemije i borbe sa novom i slabo poznatom bolešću. Dok su vlade i svjetski vođe vodili borbu s virusom informiranjem javnosti, provođenjem mjera poput fizičkog distanciranja, nošenjem maski, uvođenjem lockdowna i slično, tehnološka zajednica te sigurnosni stručnjaci su radili na tehnološki podržanom praćenju kontakata i pravovremenom obavješćavanju korisnika da su bili u kontaktu s virusom. Nekoliko znamenitih primjera su Google/Apple Exposure Notification², SwissCovid App³, te DP-3T⁴ protokol za praćenje kontakata. Uspješnost korištenih rješenja je upitna s obzirom na ograničene mjere kojima su vlade promovirale i poticale korištenja navedenih rješenja, što pokazuje činjenica da je android verziju hrvatske aplikacije preuzelo oko 50 tisuća korisnika. Jedan od mogućih razloga slabe korištenosti aplikacije je nepovjerenje korisnika u rad aplikacije te posljedično očuvanje privatnosti i tajnosti kontakata. Cilj našeg projekta bio je implementirati gotovo rješenje za praćenje kontakata u vlastitu aplikaciju uz testiranje funkcionalnosti te analizirati i usporediti sigurnosna svojstva prezentiranih rješenja i stvarnih implementacija na korisničkim uređajima.

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

2. Načelo rada aplikacija za praćenje kontakata

Trenutno korištena rješenja⁵ temelje se na razmjeni podataka između korisnika aplikacije putem bluetooth odašiljača. Korisnik nakon instalacije aplikacije mora odobriti korištenje bluetootha za odašiljanje vlastitih nizova podataka. Te nizove podataka, nazovimo ih "ključevima", osluškuju drugi uređaji i pohranjuju u vlastitu memoriju uređaja. Aplikacija periodički povlači ključeve zaraženih korisnika sa centralnog poslužitelja i uspoređuje ih sa ključevima u vlastitoj memoriji. Kada pronađe poklapanje obavještava korisnika ili koristi to poklapanje za izračunavanje rizika za korisnika. Korisnik tad zna da je bio u kontaktu sa zaraženom osobom i može se samoinicijativno izolirati i tako spriječiti daljnje širenje virusa. Korisnici koji su zaraženi virusom mogu svoje ključeve prenijeti na udaljeni poslužitelj koji će ih onda podijeliti ostalim korisnicima. Tajnost kontakata očuvana je zbog činjenice da poslužitelj ne zna kome je podijelio ključeve te kojem je korisniku aplikacija dojavila da je bio u kontaktu sa "zaraženim" ključevima. Postoje varijacije na sam postupak jer je različitim algoritmima moguće dodatno zaštititi privatnost korisnika i smanjiti količinu podataka koja se izmjenjuje između korisnika i poslužitelja, npr. razmjenom "seedova" za generiranje ključeva umjesto razmjene svih generiranih ključeva. Dežurna zdravstvena organizacija mora zaraženom korisniku uz pozitivan test generirati verifikacijski ključ koji koristi prilikom prijenosa zaraženih ključeva na poslužitelj. Poslužitelj ne smije moći preko verifikacijskog koda identificirati osobu koja prenosi ključeve, već bi tu informaciju smjela znati samo dežurna zdravstvena organizacija. Trenutna rješenja se oslanjaju na dobru volju i savjest korisnika jer rade ispravno samo pod pretpostavkom da korisnici drže aplikaciju aktivnom na uređaju te da će podijeliti sa drugim korisnicima da su bili pozitivni jednom kad im test to potvrdi.

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

3. Razvoj aplikacije za praćenje kontakata temeljena na Googleovom API-u

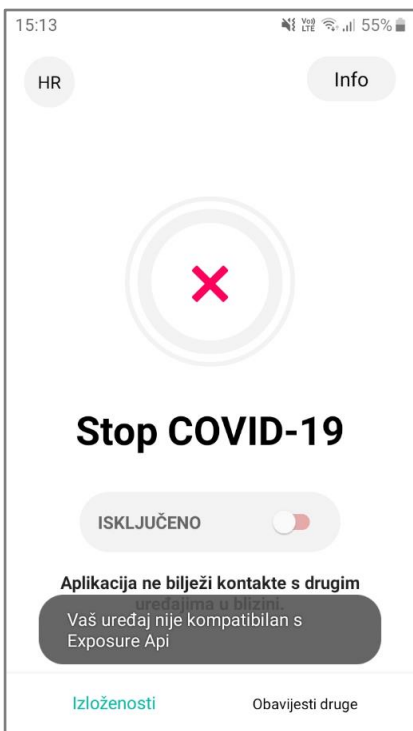
Nakon uvodnog upoznavanja sa problematikom zadatka i informiranja o postojećim rješenjima, započeli smo s pokušajem implementacije u vlastitu aplikaciju. Nakon izgradnje postojeće aplikacije iz izvornog koda i instalacije na uređaj došli smo do zaključka da aplikacija ne radi. Dodatno smo istražili i zaključili da je Googleov Exposure API otvoren i dostupan za razvoj samo "allowedlisted" računima tj. javnim zdravstvenim ustanovama koje su odlučile surađivati sa Googleom. Isprobana su druga rješenja no nismo ih uspjeli implementirati. S obzirom da je vlastito implementiranje praćenje kontakata vrlo zahtjevan problem odlučeno je da ćemo odustati od tog dijela projekta i posvetiti se analizi službene hrvatske aplikacije.

4. Sigurnosna analiza službene hrvatske aplikacije za praćenje kontakata Stop COVID-19

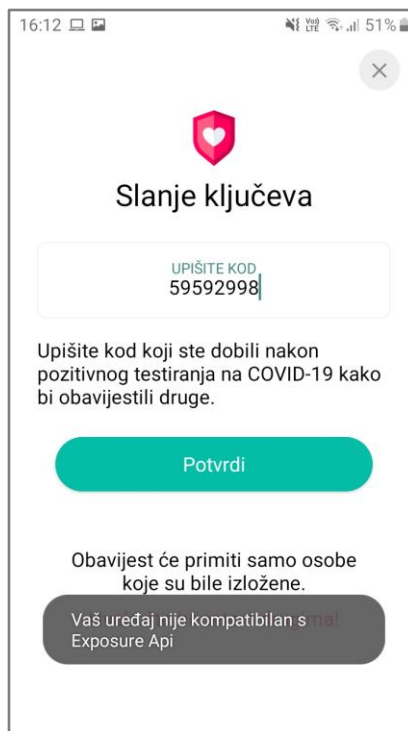
4.1 Izgradnja i instalacija aplikacije iz izvornog koda

Izvorni kod aplikacije dostupan je udaljenom repozitoriju GitHub-a⁶. Svaki korisnik može besplatnim alatima sam izgraditi izvršni kod aplikacije i instalirati ju na uređaj. Korištenjem Android Studia⁷ i podešavanjem gradle postavki, lako je izgraditi aplikaciju i instalirati ju na uređaj. Aplikacija izgrađena iz izvornog koda izgleda i ponaša se identično kao i aplikacija instalirana sa Google Play Store-a⁸, no ukoliko pokušamo pokrenuti praćenje kontakata ili pokušamo unijeti verifikacijski kod, aplikacija će nas obavijestiti da uređaj nije kompatibilan s Exposure Api-jem (Googleov Exposure Notification Api)(Slike 1.1 i 1.2). To se događa jer, kao što smo ranije naveli, Exposure Api je dostupan samo Googleovim partnerima u javnom zdravstvu⁹. Takav oblik zaštite pristupa api-ju vjerojatno je uveden kako bi se spriječila zlouporaba otvorenosti koda i umanjile mogućnosti instalacije krivotvorenih verzija službenih aplikacija koje bi ugrožavale zdravlje, sigurnost i privatnost korisnika. Na slikama 2.1 i 2.2 vidimo očekivano ponašanje aplikacije.

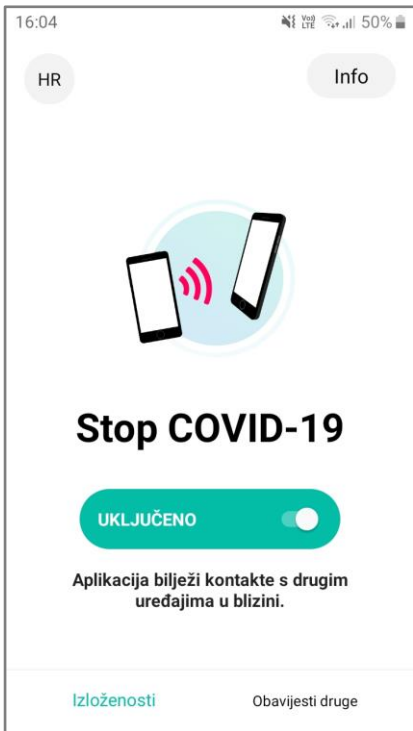
Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021



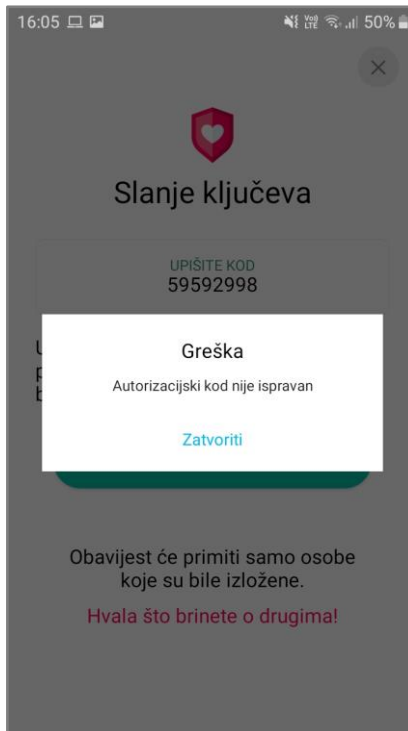
Slika 1.1 Prikazuje početna stranica aplikacije kada je isključen API



Slika 1.2 Prikazuje sučelje na kojem se šalju ključevi



Slika 2.1 Prikazuje početnu stranicu aplikaciju kada je uključen API



Slika 2.2 Prikazuje poruku ako se upiše krivi kod

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

4.2 Dekompajliran izvršni kod aplikacije i analiza

Otvorenost koda se često spominje u kontekstu sigurnosti programske podrške i u pravilu indicira da programska potpora radi ono za što se reklamira, bez tajnih motiva i skrivenih procesa, prateći pravila sigurnosti po dizajnu. Kako bi se uvjerali da aplikacija radi ono za što se reklamira, potrebno je prevesti izvršni kod u izvorni i usporediti ga sa službenim izvornim kodom dostupnim na GitHub-u. Izvršni kod Android aplikacija pakira se u apk datotečni format koji se zatim može lako prenositi i instalirati na android uređaje. Mi smo preuzeli apk datoteku, instalirali je na android uređaj kako bi provjerili je li to ta aplikacija te radi li. Nakon što smo se uvjerali da je apk datoteka valjana, korištenjem programa jadx¹⁰ i njegovog grafičkog sučelja dekompileirali smo ju i dobili dekompileiran izvorni kod aplikacije. Usporedbom s kodom s GitHub-a, došli smo do zaključka da aplikacija ne radi ništa što nebi trebala, struktura projekta i klase su identične i ulazno/izlazna točka aplikacije pokazuje na isti centralni poslužitelj kao i referentni kod. Programski kod je malo drugačiji, no te razlike ostvaruju istu funkcionalnost kao što pokazuje primjer sa slike 3.1 gdje je crveno označen referentni izvorni kod, a zeleno dekompileiran izvorni kod. Vidimo da razlika vjerojatno proizlazi iz načina na koji je kod optimiran prilikom prevođenja.

```

33
34 private static void setupGlobalEnvironment() {
-   globalEnvironment = new GlobalEnvironment();
-
-   if (isProduction()) {
-       globalEnvironment.globalURL = mInstance.getString(R.string.global_url);
-   } else {
-       globalEnvironment.globalURL = mInstance.getString(R.string.global_url_test);
-   }
35+   GlobalEnvironment globalEnvironment2 = new GlobalEnvironment();
36+   globalEnvironment = globalEnvironment2;
37+   globalEnvironment2.globalURL = mInstance.getString(R.string.global_url);
38 }
39

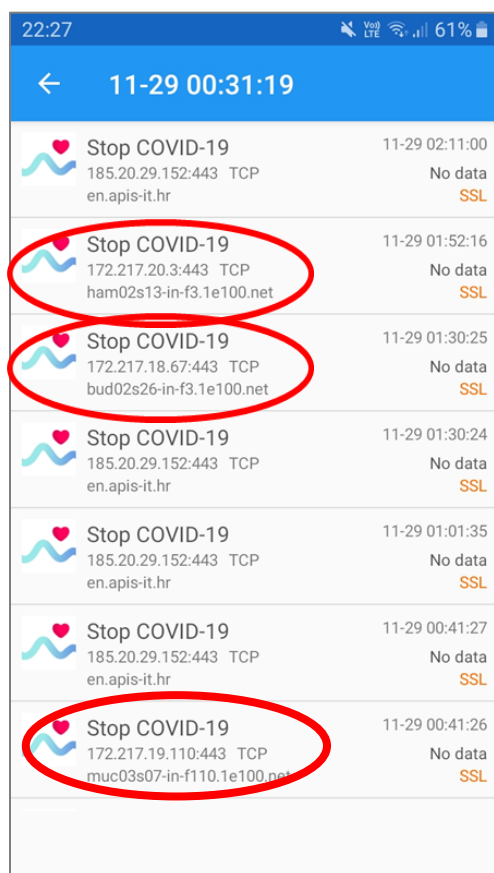
```

Slika 3.1 Prikazuje razliku dekompileiranih kodova

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

4.3 Praćenje internetskog prometa

Prema navodima, aplikacija bi trebala komunicirati samo s centralnim poslužiteljem. U slučaju hrvatske aplikacije za praćenje kontakata to je poslužitelj tvrtke APIS-IT¹¹ s IP-adresom 185.20.29.152. APIS-IT je tvrtka zadužena za implementaciju i održavanje hrvatske verzije aplikacije za praćenje kontakata. U izvornom kodu sa GitHub-a i dekompileiranom izvornom kodu definirana je ista adresa centralnog poslužitelja. No željeli smo se uvjeriti da aplikacija komunicira samo s tim poslužiteljem. Prvo smo snimali internetski promet koristeći aplikaciju Packet Capture¹², ona nam omogućuje da zabilježimo s kojim poslužiteljima komunicira odabrana aplikacija. Zabilježila je komunikaciju s APIS-serverom, ali i s drugim nepoznatim poslužiteljima (Slika 4.1). Za ostale poslužitelje se ispostavilo da pripadaju Google-u i da se vjerojatno koriste u sklopu Google Play Service-ova koje je bilo neophodno prihvatiti za korištenje aplikacije za praćenje kontakata.



App Icon	App Name	IP Address	Port	Protocol	Data	Security	Time
Stop COVID-19	Stop COVID-19	185.20.29.152	443	TCP	No data	SSL	11-29 02:11:00
Stop COVID-19	Stop COVID-19	172.217.20.3	443	TCP	No data	SSL	11-29 01:52:16
Stop COVID-19	Stop COVID-19	172.217.18.67	443	TCP	No data	SSL	11-29 01:30:25
Stop COVID-19	Stop COVID-19	185.20.29.152	443	TCP	No data	SSL	11-29 01:30:24
Stop COVID-19	Stop COVID-19	185.20.29.152	443	TCP	No data	SSL	11-29 01:01:35
Stop COVID-19	Stop COVID-19	185.20.29.152	443	TCP	No data	SSL	11-29 00:41:27
Stop COVID-19	Stop COVID-19	172.217.19.110	443	TCP	No data	SSL	11-29 00:41:26

Slika 4.1 Prikazuje praćenje prometa aplikacije

Željeli smo istražiti sadržaj internetskog prometa te smo, koristeći alat Wireshark¹³ i osobno računalo kao Wi-Fi Hotspot, snimali internetski promet aplikacije. Prema specifikaciji, očekivani promet bi trebao sadržavati: periodično preuzimanje ključeva s poslužitelja, lažno slanje vlastitih ključeva, te pravo slanje vlastitih ključeva (posljednje nije moguće provjeriti bez valjanog verifikacijskog koda).¹⁴ Aplikacija inicira komunikaciju s poslužiteljem svakih 20-ak minuta, sadržaj paketa je zaštićen na transportnom sloju te nije moguće iz sadržaja paketa odrediti svrhu komunikacije, ali vidljive su različite duljine sadržaja paketa pa iz toga zaključujemo da je zabilježen promet kakav smo i očekivali.

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

4.4 Otpornost aplikacije na MITM napad pomoću Android uređaja

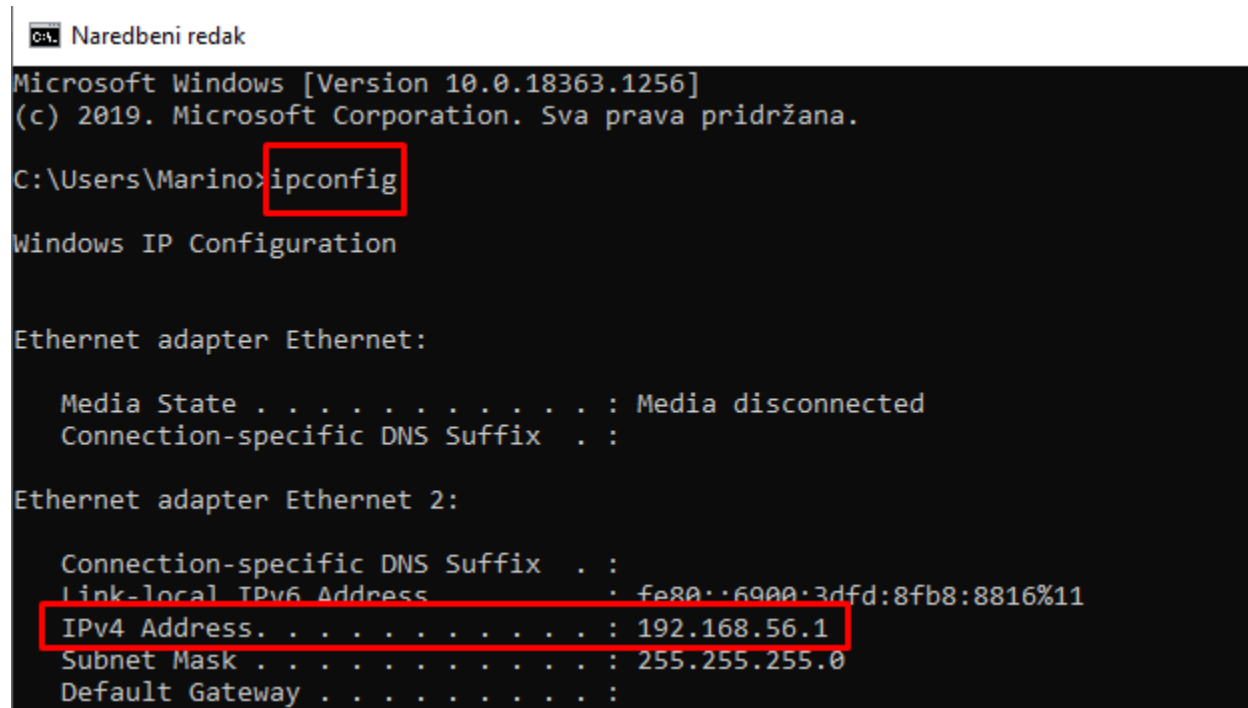
S obzirom da je promet zaštićen na transportnom sloju, pokušali smo doći do sadržaja paketa koristeći Man In The Middle¹⁵ napad. Ne ulazeći u detalje same zaštite, čitatelju je potrebno znati da u MITM napadu, MITM software gledajući sa strane poslužitelj glumi korisnika, a sa strane korisnika glumi poslužitelj i, koristeći vlastite certifikate, pokušava zavarati korisnika da ustvari komunicira sa pravim poslužiteljem i zavarava poslužitelj da komunicira direktno s korisnikom te bilježi sadržaj paketa kako bi se mogao analizirati.

Koristeći alate Fiddler¹⁶ ili mitmproxy¹⁷ postavljamo proxy poslužitelj na našem osobnom računalu, zatim je na mobilnom uređaju potrebno postaviti računalo kao proxy poslužitelj. Mobilni uređaj "ne vjeruje" proxy-u i internetski promet ne putuje preko njega. Potrebno je na mobilni uređaj instalirati certifikat odabranog alata. Na Android mobilnim uređajima, nakon dodavanja certifikata, moguće je pokrenuti internet preglednik i obavljati pretraživanje na internetu te je sav taj promet vidljiv u proxy software-u, no ostale aplikacije ne rade i ne snima se njihov promet. Razlog tome je što od Android Nougat-a nadalje nijedna aplikacije ne vjeruje korisničkim certifikatima. Rješenje tog problema je da modificiramo sam kod aplikacije, odnosno u manifest dodamo da vjeruje korisničkim certifikatima, no nakon izgradnje i instalacije na uređaj pri pokušaju korištenja aplikacija će nas obavijestiti s porukom da uređaj nije kompatibilan s Exposure API-jem te ponovo nije moguće zabilježiti promet te aplikacije. Iz svega zaključujemo da je aplikacija sigurna od MITM napada.

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

4.5 Otpornost aplikacije na MITM napad pomoću Apple uređaja

Potrebne stvari za ispitivanje otpornosti aplikacije **Stop COVID – 19** pomoću MITM napad za početak su spajanje samog Apple uređaja na računalo preko pristupne točke. Tako će se dobiti efekt čovjeka u sredini kojeg će u ovom slučaju glumiti odabrano računalo na kojeg se Apple uređaj spojio. Kako bio spojili Apple uređaj potrebno je pronaći IP adresu samog računala tj. izvršavanjem **ipconfig** naredbe u naredbenom retku računala:



```

C:\Users\Marino>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

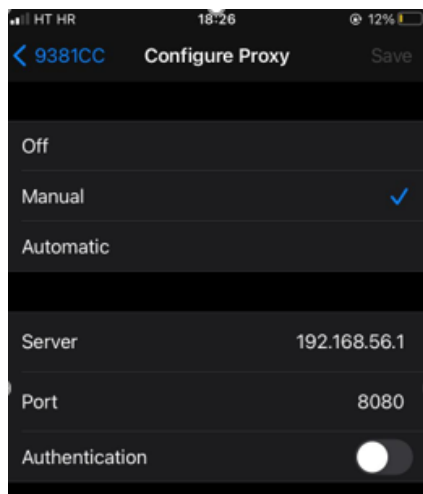
    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::6900:3dfd:8fb8:8816%11
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

```

Slika 4.2 Slika prikazuje rezultata izvršavanja naredbe ipconfig

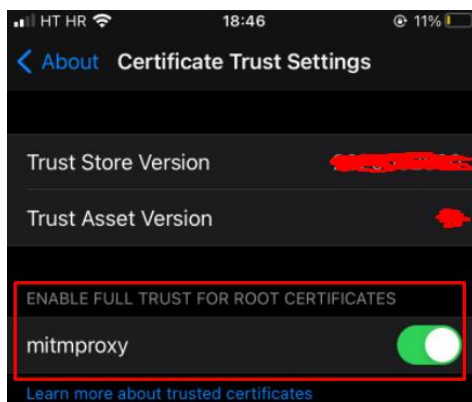
Nakon što je IP adresa računala poznata moramo konfigurirati proxy Apple uređaj. Konfiguracija proxya na Apple uređajima radi se u postavkama samog uređaja. Pritiskom na **Settings** → **Wi-fi** → pritisak na trenutnu spojenu vezu (pristupna točka računala) → **Configure Proxy** prikaz je na slici 4.3. Kada se otvorilo sučelje sa slike 4.3 tada se popunjavaju podaci tj. **Server** što predstavlja prema kojem uređaju ćemo kreirati proxy, a to je IP adresa računala na kojeg je Apple uređaj spojen te **Port** na kojem će se osluškivati promet.

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021



Slika 4.3 Prikazuje sučelje koje se otvara pritiskom na *Configure proxy*

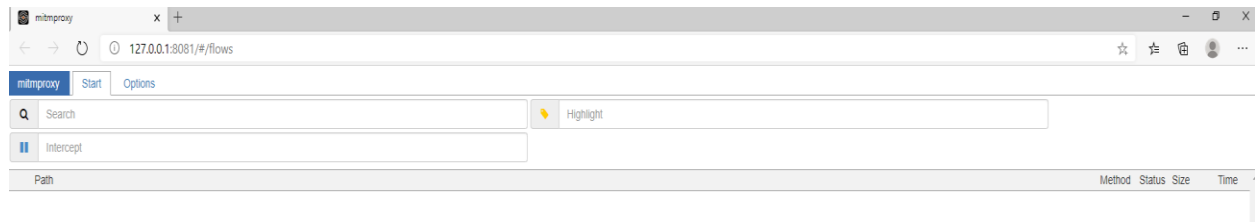
Nakon što je na Apple uređaju konfiguriran proxy prema računalu na kojem je spojen, potrebno je instalirati certifikat za taj proxy kako bi mu aplikacije vjerovale. Na Apple uređaju u **Safari** upisuje se: *mitm.it* te se instalirava certifikat za određeni sustav, konkretno u ovom primjeru preuzima se Apple certifikat (profil). Nakon što je certifikat preuzet potrebno ga je odobriti. Odobrenje preuzetog certifikata obavlja se tako da se na uređaju uđe u **Settings** te odabere **Profile Downloaded** tamo će biti prikazan mitmproxy certifikat koji je potrebno instalirati. Nakon što je certifikat instaliran, Apple uređaj počinje vjerovati tom certifikatu (djelomično) što je suprotno od Androida koji ne vjeruje korisničkim certifikatima. Kako bi Apple uređaj u potpunosti vjerovao certifikatu potrebno ga je dodati u provjerene certifikate. Odlaskom u **Settings** → **General** → **About** → **Certificate Trust Settings** prikazat će se sučelje u kojem je potrebno pridružiti "Potpuno povjerenje" mitmproxy certifikatu.



Slika 4.4 Prikazuje sučelje u kojem se dodjeljuje potpuno povjerenje korisničkim certifikatima

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

Kada je podešeno "Potpuno povjerenje" nad mitmproxy certifikatom, može se početi hvatati promet na računalu preko mitmproxy sučelja koje mora biti instalirano na računalu. Ako mitmproxy nije instaliran na računalu tada je potrebno posjetiti mitmproxy web stranicu te preuzeti aplikaciju tj. sučelje, ako je to obavljeno potrebno je potražiti **mitmproxy ui** koji će otvoriti sučelje u kojem ćemo pratiti promet:













Slika 4.5 Prikazuje mitmproxy sučelje u kojem se prikazuje uhvaćeni promet

Potrebno je naglasiti u ovom modu rada u kojem je trenutno Apple uređaj nije moguće pristupiti nekim aplikacijama kao što su npr. **Whatsapp, Snapchat** koji imaju sustav čim otkriju da se na uređaju nalazi korisnički certifikat s potpunim povjerenjem tada se nabrojane aplikacije neće povezati sa svojim poslužiteljima te nema komunikacije klijenta i poslužitelja, ono što nam je ostalo učitano, prije nego li smo se spojili na vezu koja glumi čovjeka u sredini, će nam se prikazati, ali nikakve promjene u aplikaciji neće biti moguće (osvježavanje aplikacije) sve dok se ne spojimo na drugu mrežu koja ne koristi proxy. Samim time te aplikacije su zaštićene od napada oblika čovjek u sredini jer ne postoji komunikacija između klijenta i servera pa samim time ne postoji paket kojeg se može preusmjeriti i pregledati njegov sadržaj.

Aplikacija **Stop COVID – 19** nema takav oblik zaštite kao gore navedene aplikacije, stoga je moguće preusmjeriti, tj. uhvatiti promet između servera i klijenta. Prilikom ulaska u samu aplikaciju potrebno je omogućiti komunikaciju API-a i Apple uređaja tako da se odobri spajanje. Prilikom tog odobrenja zabilježen je promet od 3 zahtjeva (1 GET zahtjev i 2 POST zahtjeva), podatci unutar tih zahtjeva su dostupni, ali su kriptirani. Svaki od zahtjeva koji je preuzet ima svoj: **Details, Request i Response**. Trenutno u **Detailsu** jedini korisni podatci su oni po kojima vidimo da aplikacija komunicira s APSI-ITem i Appleom.

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

Path	Method	Status	Size	Time
 http://mitm.it/	GET	200	16.7kb	70ms
 http://mitm.it/static/bootstrap.min.css	GET	200	156.5kb	22ms
 http://mitm.it/static/mitmproxy.css	GET	200	683b	72ms
 http://mitm.it/static/images/mitmproxy-long.png	GET	200	120.9kb	88ms
 http://mitm.it/static/images/favicon.ico	GET	200	5.3kb	15ms
 http://mitm.it/cert/pem	GET	200	1.3kb	42ms
 https://www.google.com/log?format=json&hasfast=true&authuser=0	POST	200	951b	276ms
 https://en.apis-it.hr/submission/diagnosis-key-file-urls?all=false	GET	200	150b	240ms
 https://gsp-ssl.ls.apple.com/ab.arpc	POST	200	372b	151ms
 https://gsp64-ssl.ls.apple.com/hvr/v3/use	POST	200	335b	416ms

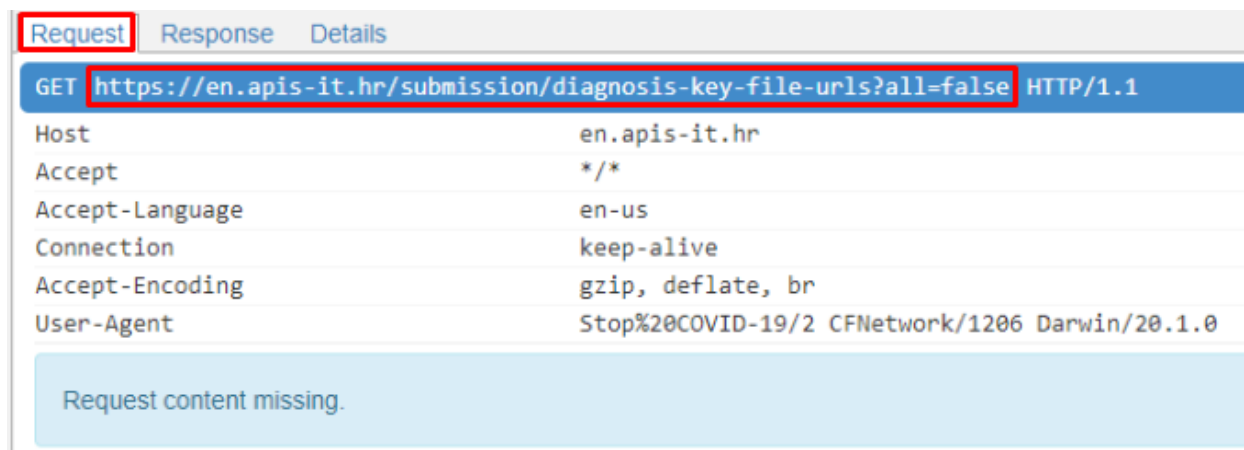
Slika 4.6 Prikazuje 3 zahtjeva koja su uhvaćena prilikom spajanja Apple uređaja i APIja

Request	Response	Details
Client Connection		
Address:	::ffff:192.168.137.224:60213:0:0	
<u>TLS SNI:</u>	en.apis-it.hr	
TLS version:	TLSv1.3	
cipher name:	TLS_AES_256_GCM_SHA384	
<u>ALPN:</u>	http/1.1	
Server Connection		
Address:	en.apis-it.hr:443	
<u>TLS SNI:</u>	en.apis-it.hr	
TLS version:	TLSv1.3	
<u>ALPN:</u>	http/1.1	
Timing		
Server conn. initiated:	2020-12-14 14:28:31.370(-131ms)	
Server conn. TCP handshake:	2020-12-14 14:28:31.401(-100ms)	
Client conn. established:	2020-12-14 14:28:31.354(-147ms)	
First request byte:	2020-12-14 14:28:31.501	
Request complete:	2020-12-14 14:28:31.501(0ms)	
First response byte:	2020-12-14 14:28:31.578(77ms)	
Response complete:	2020-12-14 14:28:31.741(240ms)	

Slika 4.6 Prikazuje Details od prvog zahtjeva (GET zahtjev)

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

Unutar **Request** taba od prvog GET zahtjeva postoji URL na kojem se traže određeni podatci koji se dobivaju u tabu **Response**, trenutno informacije koje su dobivene nisu previše korisne, ukoliko je potrebna neka autentifikacija u ovom tabu, taj bi se token za autentifikaciju ispisao te bi se s tim tokenom moglo dalje manipulirati, ali aplikacija ima zaštitu od toga jer ne koristi nikakve tokene niti zaštitu tog tipa.



Slika 4.7 Prikazuje Request od prvog zahtjeva (GET zahtjev)

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

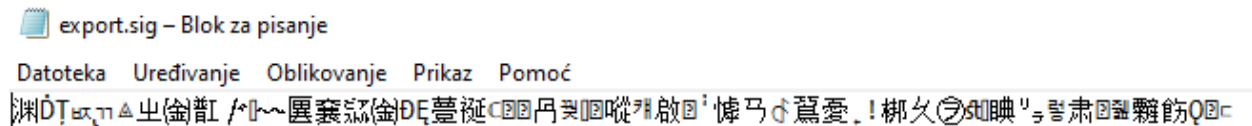
Unutar **Response** taba dobiven je rezultat GET zahtjeva te je uspješno zabilježen promet u JSON formatu koji prikazuje URL-ove zip datoteka koje se nalaze na web poslužiteljima tvrtke APIS-IT, moguće ih je preuzeti tako da se URL upiše u web preglednik te će se automatski skinuti određena zip datoteka.

Request	Response	Details
HTTP/1.1 200		
Date	Mon, 14 Dec 2020 13:28:30 GMT	
Server	Apache	
X-Frame-Options	SAMEORIGIN	
Strict-Transport-Security	max-age=63072000; includeSubdomains	
X-Content-Type-Options	nosniff	
X-XSS-Protection	1; mode=block	
Cache-Control	no-cache, no-store, max-age=0, must-revalidate	
Pragma	no-cache	
Expires	0	
X-Frame-Options	DENY	
Content-Type	application/json	
Vary	Accept-Encoding	
Content-Encoding	gzip	
Keep-Alive	timeout=3, max=30	
Connection	Keep-Alive	
Transfer-Encoding	chunked	
<pre>{ "urlList": ["https://en.apis-it.hr/Exposure/export-2020-11-30-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-01-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-02-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-03-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-04-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-05-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-06-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-07-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-08-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-09-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-10-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-11-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-12-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-13-HR-01.zip", "https://en.apis-it.hr/Exposure/export-2020-12-14-HR-01.zip"] }</pre>		

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

Slika 4.8 Prikazuje Response od prvog zahtjeva (GET zahtjeva)

Unutar zip datoteka nalazi datoteka **export.sig** kojoj je sadržaj kriptiran **SHA-256** algoritmom. Sadržaj te datoteke izgleda ovako:



Slika 4.9 Prikazuje sadržaj datoteke export.sig

Kad je prvi zahtjev obrađen prelazimo na drugi zahtjev koji je POST zahtjev, drugi zahtjev i treći zahtjev dijele isti **Details**.

Request	Response	Details
Client Connection		
Address:	::ffff:192.168.137.224:60214:0:0	
TLS_SNI:	gsp-ssl.ls.apple.com	
TLS version:	TLSv1.3	
cipher name:	TLS_AES_256_GCM_SHA384	
ALPN:	http/1.1	
Server Connection		
Address:	gsp-ssl.ls.apple.com:443	
TLS_SNI:	gsp-ssl.ls.apple.com	
TLS version:	TLSv1.3	
ALPN:	http/1.1	
Timing		
Server conn. initiated:	2020-12-14 14:28:44.638(-145ms)	
Server conn. TCP handshake:	2020-12-14 14:28:44.683(-101ms)	
Client conn. established:	2020-12-14 14:28:44.618(-165ms)	
First request byte:	2020-12-14 14:28:44.783	
Request complete:	2020-12-14 14:28:44.799(16ms)	
First response byte:	2020-12-14 14:28:44.919(135ms)	
Response complete:	2020-12-14 14:28:44.934(151ms)	

Slika 4.10 Prikazuje Details koji dijele 2. i 3. zahtjev (2 POST zahtjeva)

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

Mitmproxy također nudi jednu mogućnost a to je da se automatski skine cijeli Body koji se šalje u POST paketu te se pospremi u datoteku s predodređenim imenom, te nudi mogućnost skidanja cijelog Body-a od odgovora na POST zahtjev:

The screenshot shows the Mitmproxy interface with the 'Request' tab selected. The request is a POST to `https://gsp-ssl.ls.apple.com/ab.arpc` with HTTP/1.1. The headers are:

- Host: `gsp-ssl.ls.apple.com`
- Content-Type: `application/octet-stream`
- Connection: `keep-alive`
- Accept: `*/*`
- User-Agent: `geod/1 CFNetwork/1206 Darwin/20.1.0`
- Content-Length: `121`
- Accept-Language: `en-us`
- Accept-Encoding: `gzip, deflate, br`

The body is shown in hex and escaped characters:

```
\x00\x01\x00\x08en-HR_HR\x00\x0ecom.apple.geod\x00
14.2.18B92\x00\x00\x03\xf8\x00\x00\x00I
$CA671ED0-36F2-4100-ADAC-E82813754CCA\x1a!
\x02HR\x1a\x05en-HRJ\x00P\x01X\x0e` \x01\x80\x01\x03\x98\x01\x00\xb0\x01\x07\xba\x01\x02\x10\x01
```

At the bottom, the 'View' dropdown is set to 'auto' and the 'Raw' button is highlighted with a red box.

Slika 4.11 Prikazuje Request od 2. zahtjeva (POST zahtjeva)

The screenshot shows the Mitmproxy interface with the 'Response' tab selected. The response is an HTTP/1.1 200 OK. The headers are:

- content-length: `251`
- Date: `Mon, 14 Dec 2020 13:28:43 GMT`
- Age: `0`
- Connection: `keep-alive`
- Server: `ATS`
- CDNUUID: `70432113-0302-49dc-8470-c477342f2d61-5489266211`
- X-Cache: `skipped`

The body is shown in hex and escaped characters:

```
\x00\x01\x00\x00\x03\xf8\x00\x00\x00\xf1
$CA671ED0-36F2-4100-ADAC-E82813754CCA\x18\x00 \x00(\xc0\xd1\x022P
"
\x1aDirectionsMPTCPSERVICEType\x10\x01\x1a\x02\x08\x02
\x18SearchACMPTCPSERVICEType\x10\x01\x1a\x02\x08\x02\x12\x0855930.T1:\x05*\x03\x08\x9e\x1c8\x05*\x03\x08\x9e\x1cJW\x12P
"
\x1aDirectionsMPTCPSERVICEType\x10\x01\x1a\x02\x08\x02
\x18SearchACMPTCPSERVICEType\x10\x01\x1a\x02\x08\x02\x12\x0855930.T1*\x03\x08\x9e\x1cR\x05*\x03\x08\x9e\x1cX\x0d\x05
```

At the bottom, the 'View' dropdown is set to 'auto' and the 'Raw' button is highlighted with a red box.

Slika 4.12 Prikazuje Response od 2. zahtjeva (POST zahtjev)

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

Request Response Details

POST https://gsp64-ssl.ls.apple.com/hvr/v3/use HTTP/1.1

Host	gsp64-ssl.ls.apple.com
Content-Type	application/octet-stream
Connection	keep-alive
Accept	*/*
User-Agent	geod/1 CFNetwork/1206 Darwin/20.1.0
Accept-Language	en-us
Content-Length	325
Accept-Encoding	gzip, deflate, br

```

0000000000 00 02 00 08 65 6e 2d 48 52 5f 48 52 00 0e 63 6f ....en-HR_HR..co
0000000010 6d 2e 61 70 70 6c 65 2e 67 65 6f 64 00 0a 31 34 m.apple.geod..14
0000000020 2e 32 2e 31 38 42 39 32 00 04 4e 4f 4e 45 00 00 .2.18B92..NONE..
0000000030 03 f9 00 00 01 0f 0a 8c 02 b2 06 84 02 0a 23 98 .....#.
0000000040 06 c9 01 ca 0c 1c 0a 0a 31 34 2e 32 2e 31 38 42 .....14.2.18B
0000000050 39 32 12 0a 69 50 68 6f 6e 65 31 30 2c 34 18 00 92..iPhone10,4..
0000000060 20 00 0a 1f 98 06 ad 02 ea 12 18 0a 0e 63 6f 6d .....com
0000000070 2e 61 70 70 6c 65 2e 67 65 6f 64 12 03 31 2e 30 .apple.geod..1.0
0000000080 1a 01 31 0a 0e 98 06 92 03 92 19 07 0a 05 65 6e ..1.....en
0000000090 2d 48 52 0a 16 98 06 93 03 9a 19 0f 08 03 12 02 -HR.....
00000000a0 48 52 1a 05 48 54 20 48 52 20 03 0a 07 98 06 97 HR..HT HR .....
00000000b0 03 ba 19 00 0a 09 98 06 94 03 a2 19 02 08 00 0a .....
00000000c0 0b 98 06 da 04 d2 25 04 1a 02 08 00 0a 34 98 06 .....%.4..
00000000d0 d9 04 ca 25 2d 0a 15 08 a4 ce 87 f1 da f5 c4 a5 ...%-.....
00000000e0 6f 10 b1 a7 e0 93 e4 e7 8a f7 d3 01 19 00 00 00 o.....
00000000f0 f0 cf c3 c2 41 32 0b 08 d0 b2 9e ac 02 15 00 00 ....A2.....
0000000100 80 3f a0 06 06 d2 06 39 08 12 10 79 18 aa 02 80 .?.....9...y....
0000000110 01 88 03 88 01 c8 01 b2 01 04 70 72 6f 64 b8 01 .....prod..
0000000120 dd e7 7a c0 01 00 c8 01 00 92 03 12 31 39 32 2e .z.....192.
0000000130 31 36 38 2e 31 33 37 2e 31 3a 38 30 38 30 98 03 168.137.1:8080..
0000000140 00 c0 3e e0 5d ...>.]

```

View: auto Hex

Slika 4.13 Prikazuje Request od 3. zahtjeva (POST zahtjev)

Request Response Details

HTTP/1.1 200 OK

Server	dlb/1.0.2
Date	Mon, 14 Dec 2020 13:37:04 GMT
Content-Length	10
Connection	keep-alive
X-RID	fbd14466-a59e-4f5f-8ed4-481e54a694de
Strict-Transport-Security	max-age=31536000; includeSubDomains;
Via	17.57.12.11
X-DLB-Upstream	10.9.50.7:4001

```

0000000000 00 01 00 00 03 f9 00 00 00 00 .....

```

View: auto Hex

Slika 4.14 Prikazuje Response od 3. zahtjeva (POST zahtjev)

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

Prvi GET zahtjev ima sljedeći URL: <https://en.apis-it.hr/submission/diagnosis-key-file-urls?all=false> te ukoliko pokušamo izbrisati sve argumente tj. maknemo u URLu *?all=false* tada dobivamo isti rezultat kao i da postoji dani argument stoga nije implementirano dobro usmjerenje jer se za drugi URL dobiva ista stvar. Ne samo to, nego ukoliko dodamo još bilo kakav argument npr. *?all=false&first=true* također ćemo dobiti isti rezultat kao i da smo pozvali početni URL, tako da implementacijski gleda se samo jedan argument, postoji li taj argument (all=false) ili ih ima više uvijek se dobiva ista stvar, a to su exposure key-ovi za hrvatsku. Ukoliko je argument *?all=true* tada se dobiva zip datoteke koje predstavljaju exposure key-eve za cijelu Europu, no taj podataka nije trebao biti dostupan tako da smo uspjeli uhvatiti promet koji nismo smijeli. Tako smo manipulacijom GET Zahtjeva uspjeli dobiti resurse koji su nama trebali biti skriveni.

Kako bi smo lakše nalazili što se nalazi na URL-ovima od GET zahtjeva napisan jer jedan jednostavan JavaScript server koji šalje GET zahtjeve na određeni URL. Na slici 4.15 prikazan je izvorni kod servera te na kojim portovima se može naći rezultat GET zahtjeva. Konkretno u ovom slučaju to su **port 3000** i **port 3001**:

```
JS ProjektRServer.js > ...
1  const http = require("http");
2  const Axios = require("axios");
3
4  http.createServer(function (req, res) {
5
6      const url = "https://en.apis-it.hr/submission/diagnosis-key-file-urls?all=false";
7
8      Axios.get(url)
9          .then((result) => {
10              res.setHeader('Content-Type', 'application/json');
11              res.end(JSON.stringify(result.data))
12          })
13  }).listen(3000);
14
15  http.createServer(function (req, res) {
16
17      const url = "https://en.apis-it.hr/submission/diagnosis-key-file-urls?all=true";
18
19      Axios.get(url)
20          .then((result) => {
21              res.setHeader('Content-Type', 'application/json');
22              res.end(JSON.stringify(result.data))
23          })
24  }).listen(3001);
```

Slika 4.15 Prikazuje kod servera koji se koristi za slanje GET zahtjeva

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

5. Zaključci i preporuke

Reverzним інженерством pokušali smo saznati koje sve podatke aplikacija šalje na poslužitelje. Možemo zaključiti da aplikacija komunicira s APIS serverima koji su zaduženi za normalan rad aplikacije jer bi se na njih trebali slati ključevi koje aplikacija razmjenjuje s drugim mobilnim uređajima preko bluetootha. Sasvim neočekivano, otkrili smo da aplikacija komunicira i s Googleovim serverima, a komunikacija s dodatnim serverima nas dodatno zabrinjava zbog očuvanja naše privatnosti. Analizom paketa koje aplikacija šalje na poslužitelje nismo uspjeli saznati koji se točno podaci razmjenju zato što je sva komunikacija kriptirana. Iako u nijednom koraku analize aplikacije nismo uspjeli pronaći nešto što bi dalo slutiti da aplikacija šalje neželjene podatke na udaljene poslužitelje, upravo radi kriptirane komunikacije ne možemo sa stopostotnom sigurnošću reći da je aplikacija sigurna za korištenje i da čuva našu privatnost.

Preporuka za što bolju zaštitu aplikacije je da ne vjeruje korisničkim certifikatima kojima mi možemo dati potpuno povjerenje u postavkama, tj. da se radi na principu WhatsApp i Snapchat, ako je aktiviran nepoznati korisnički certifikat, spajanje na server nije moguće. Korištenje GET zahtjeva smanjiti na minimum jer je vrlo lako pogoditi argumente te doći do određenih informacija koje ne bi trebale biti dostupne, ako se već i koriste GET zahtjevi omogućiti pristup serveru samo određenim osobama, a ostale preusmjeriti na status 403 FORBIDDEN. Korištenje POST zahtjeva je poželjnije jer je potrebno u JSON-u koji se šalje postaviti ispravne parametre kako bismo izvukli informacije. Obrana od ovakvog tipa napada se izvršava provjerom tko šalje paket ako je ne očekivani pošiljalac POST zahtjeva tada bi se zahtjev trebao odbiti.

Covid-tracker	Verzija: 1.0
Tehnička dokumentacija	Datum: 11/1/2021

6. Literatura

- ¹ https://en.wikipedia.org/wiki/COVID-19_pandemic, 23.12.2020.
- ² <https://www.google.com/covid19/exposurenotifications/>, 23.12.2020.
- ³ <https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html>, 23.12.2020.
- ⁴ <https://github.com/DP-3T/documents>, 23.12.2020.
- ⁵ <https://ncase.me/contact-tracing/>, 23.12.2020.
- ⁶ <https://github.com/Stop-COVID-19-Croatia>, 23.12.2020.
- ⁷ <https://developer.android.com/studio>, 23.12.2020.
- ⁸ <https://play.google.com/store/apps/details?id=hr.miz.evidencijakontakata>, 23.12.2020.
- ⁹ <https://developers.google.com/android/exposure-notifications/exposure-notifications-api#glossary>, 23.12.2020.
- ¹⁰ <https://github.com/skylot/jadx>, 23.12.2020.
- ¹¹ [https://www.apis-it.hr/apisit/index.html#/,](https://www.apis-it.hr/apisit/index.html#/) 23.12.2020.
- ¹² <https://play.google.com/store/apps/details?id=app.greyshirts.sslcapture>, 23.12.2020.
- ¹³ <https://www.wireshark.org/>, 23.12.2020.
- ¹⁴ <https://developers.google.com/android/exposure-notifications/verification-system#codes-tokens-certs>
- ¹⁵ https://en.wikipedia.org/wiki/Man-in-the-middle_attack, 23.12.2020.
- ¹⁶ <https://www.telerik.com/fiddler>, 23.12.2020.
- ¹⁷ <https://mitmproxy.org/>, 23.12.2020.