CARNET

Telerik Fiddler

NCERT-PUBDOC-2018-6-362

CERT.hr

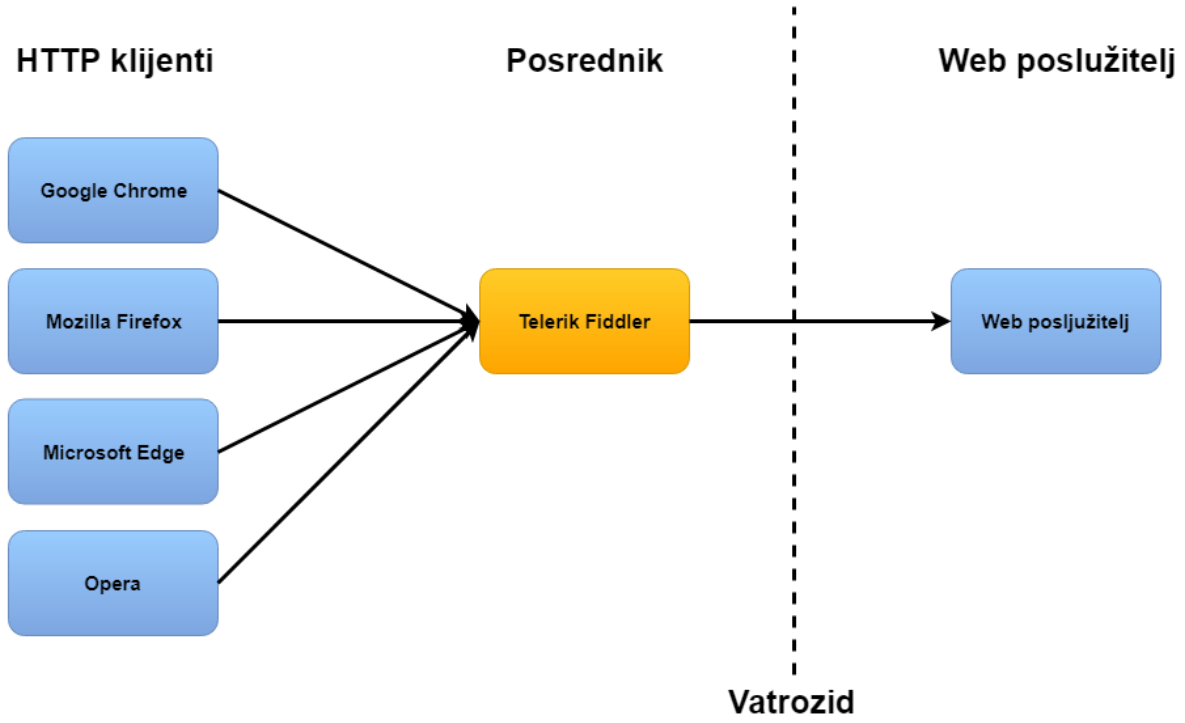
Sadržaj

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

Jedna od najbitnijih značajki računala mogućnost je pristupa internetu i njegovim sadržajima, pa je važno i korisno poznavati osnovna načela i mehanizme mrežne komunikacije. Mrežna komunikacija odvija se korištenjem različitih mrežnih protokola, pa je bitno razumjeti kako se oni mogu zloupotrijebiti te kako se zloupotreba može uočiti i spriječiti. U tu svrhu koriste se razni alati koji omogućavaju pregled i analizu mrežnog prometa.

Telerik Fiddler je HTTP posrednik (eng. *HTTP proxy*) pomoću kojeg se može promatrati mrežni promet između klijenata i poslužitelja kako bi se otkrile greške. Može se koristiti na svim često korištenim operacijskim sustavima, uz bilo koji Web preglednik te uz bilo koju razvojnu platformu. Kao i drugi HTTP posrednici, Telerik Fiddler se u mreži nalazi između HTTP klijenta, koji je najčešće Web preglednik, i Web poslužitelja. U normalnim sustavima klijent šalje poruke izravno poslužitelju. No, kad se koristi HTTP posrednik, HTTP klijent prvo šalje zahtjev posredniku koji ga zatim prosljeđuje poslužitelju kao što je prikazano na slici 1. Na isti način, odgovor poslužitelja šalje se posredniku koji će ga zatim proslijediti klijentu. Tijekom ovog procesa Fiddler snima sve dolazne i odlazne poruke koje prolaze preko njega.



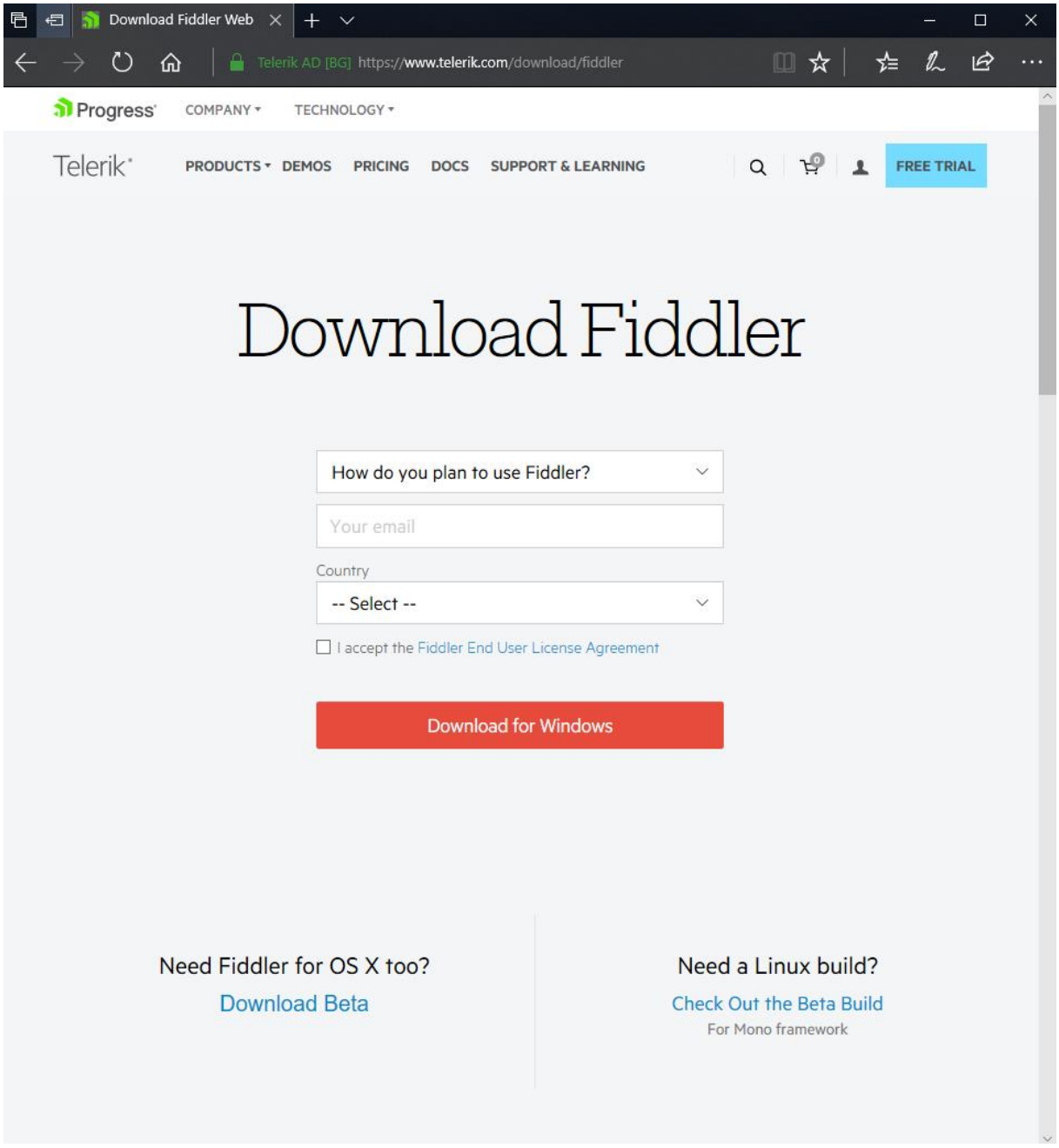
Slika 1: Slanje HTTP zahtjeva

Telerik Fiddler nudi niz funkcionalnosti od kojih su ključne snimanje mrežnog HTTP/HTTPS prometa, manipulacija Web sjednicama, testiranje performansi i sigurnosno testiranje. U sljedećim poglavljima opisan je postupak instalacije programa Telerik Fiddler te su opisani osnovni obrasci uporabe.

2 Instalacija alata Telerik Fiddler

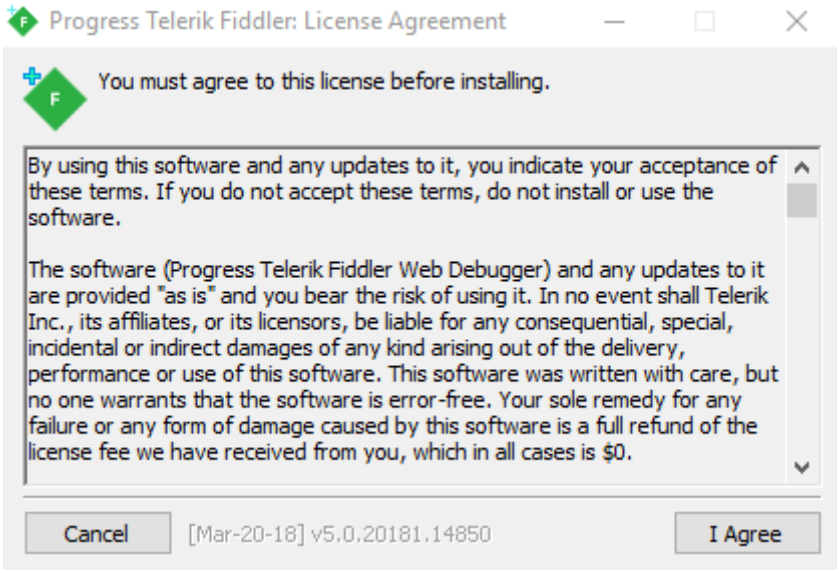
Telerik Fiddler dostupan je za operacijske sustave Windows, Linux i MacOS te za mobilne operacijske sustave iOS i Android. U sklopu ovog dokumenta instalacija i primjeri radit će se na operacijskom sustavu Windows 10, no postupak je analogan i za druge operacijske sustave. Neki operacijski sustavi zahtijevaju dodatne korake konfiguracije softvera o čemu je moguće više pročitati u službenoj dokumentaciji.

1. Za preuzimanje instalacijske datoteke Telerik Fiddler alata potrebno je otvoriti službene stranice alata, ispuniti tražene podatke te pritisnuti na crvenu ***Download for Windows*** tipku kao što je prikazano na slici 2.



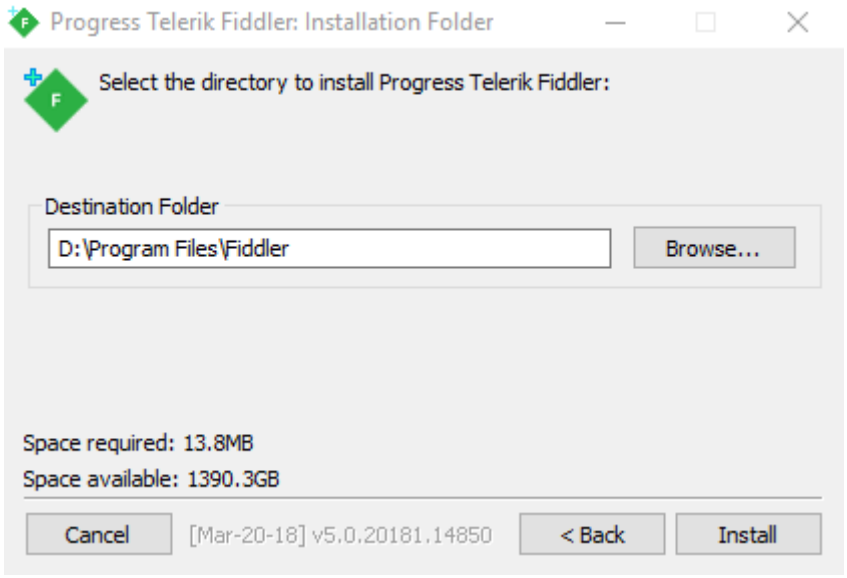
Slika 2: Preuzimanje alata Telerik Fiddler

2. Nakon preuzimanja instalacijske datoteke potrebno ju je pokrenuti. Ako se prilikom pokretanja pojavi prozor kojim aplikacija traži određena dopuštenja, nužno ih joj je dodijeliti. Prije instalacije potrebno je prihvatiti licencu za korištenje pritiskom na tipku ***I Agree*** kao što je prikazano na slici 3.



Slika 3: Prihvaćanje licence za korištenje softvera

3. Sljedeći je korak odabir instalacijskog direktorija alata što prikazuje slika 4. Pri završetku instalacije potrebno je zatvoriti instalacijski prozor.



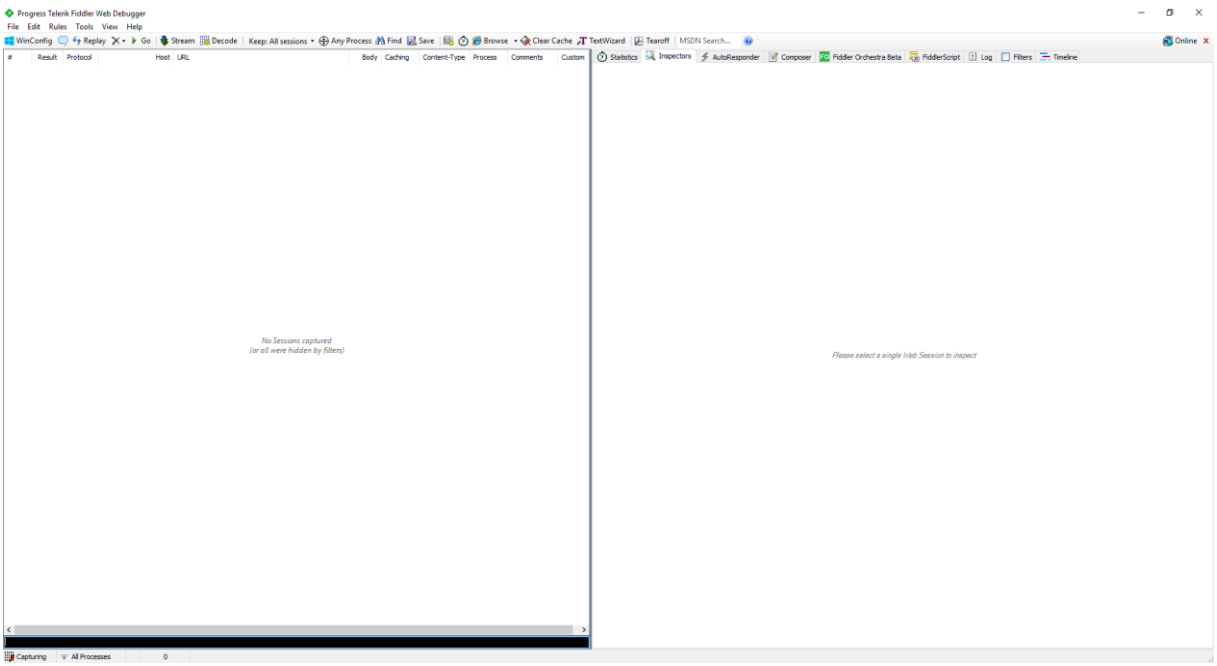
Slika 4: Odabir instalacijskog direktorija

3 Korištenje alata Telerik Fiddler

Iako će korištenje alata Telerik Fiddler biti objašnjeno na operacijskom sustavu Windows 10, postupci su analogni na ostalim operacijskim sustavima na kojima je alat dostupan.

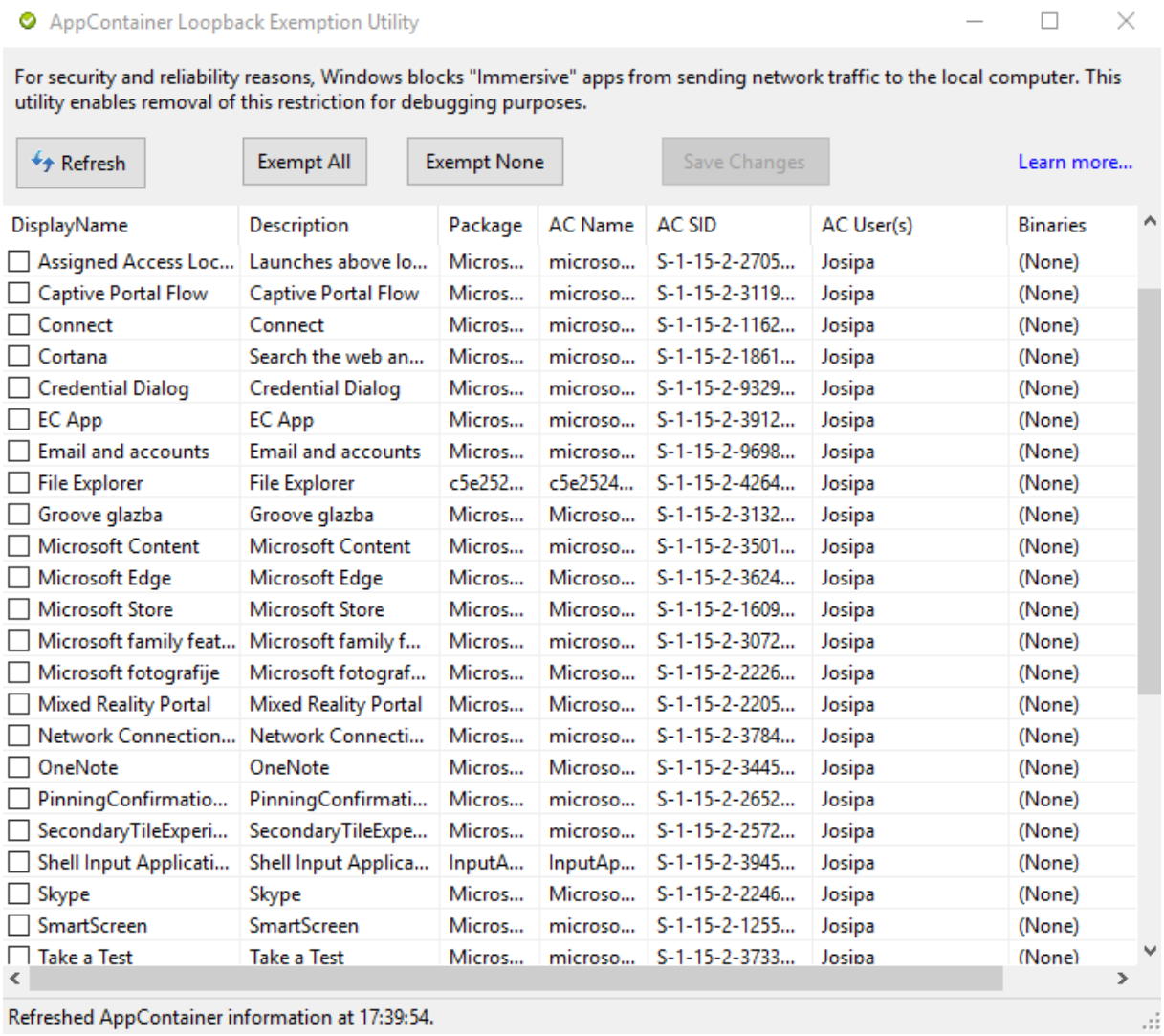
3.1 Osnovno korištenje

Pokretanjem se otvara glavi prozor alata Telerik Fiddler kao što je prikazano na slici 5 te započinje snimanje HTTP/HTTPS prometa. Fiddler može snimati promet od bilo kojeg programa koji ima mogućnosti korištenja HTTP posrednika.



Slika 5: Glavni prozor alata Telerik Fiddler

Zbog sigurnosnih razloga, Windows operacijski sustavi onemogućuju *Windows Runtime* aplikacijama korištenje lokalnog mrežnog sučelja (eng. *loopback interface*) za komunikaciju s drugim procesima, osim ako prilikom izrade aplikacije ta funkcionalnost nije izričito zatražena. Zato Fiddler ne može snimati mrežni promet takvih aplikacija bez dodatne konfiguracije. Jednostavno sučelje za konfiguriranje snimanja prometa takvih aplikacija dostupno je pritiskom na ***WinConfig*** tipku na alatnoj traci čime se otvara posebni alat prikazan na slici 6. U njemu je moguće za svaku aplikaciju pojedinačno odobriti korištenje lokalnog sučelja što omogućava Fiddleru da presreće njihov mrežni promet.



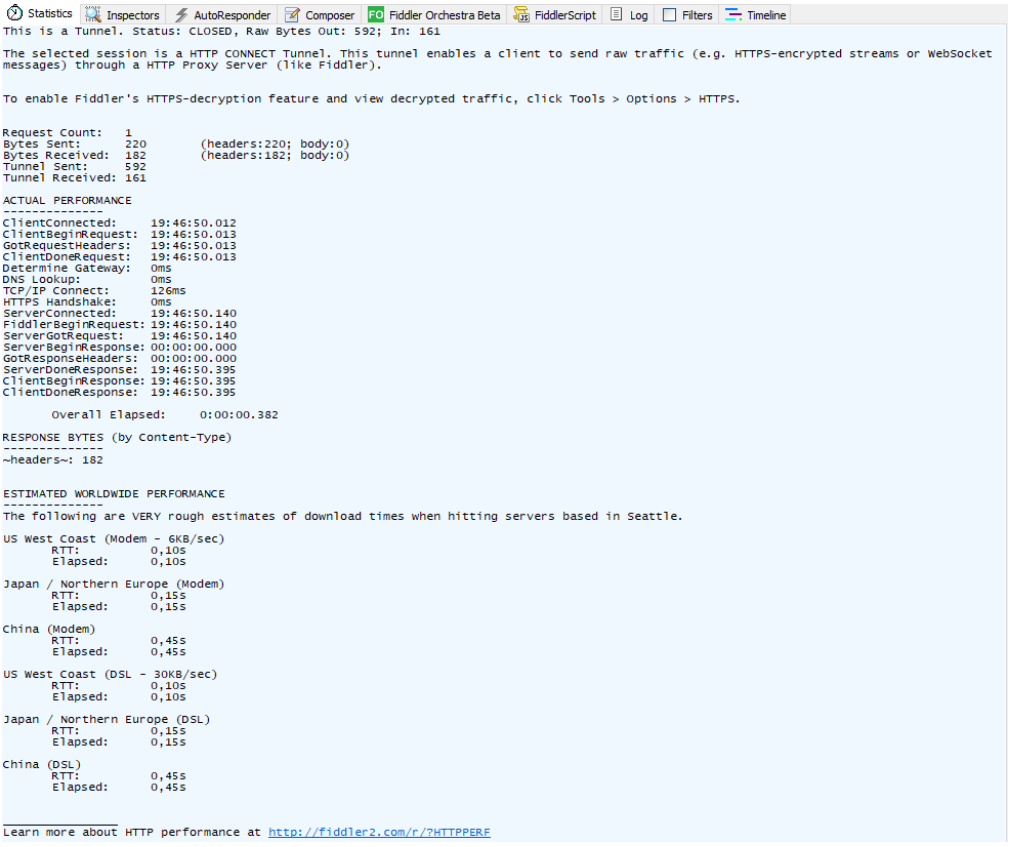
Slika 6: Omogućavanje preusmjeravanja mrežnog prometa na lokalno računalo

Unutar lijeve polovice glavnog ekrana Fiddlera nalazi se snimljeni mrežni promet koji se sastoji od svih HTTP/HTTPS zahtjeva poslanih s lokalnog računala. Za svaki od zahtjeva navedene su osnovne informacije poput statusa HTTP odgovora (eng. *HTTP response status code*), URL-a, veličine i vrste sadržaja (tijela = eng. *body*) odgovora te koji je proces poslao taj zahtjev. Na slici 7 moguće je vidjeti listu poslanih HTTP/HTTPS zahtjeva.

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process	Comments	Custom
1	200	HTTP	Tunnel to	dtzbdy9anri2p.cloudfront.net:443	0			chrome...		
2	200	HTTP	Tunnel to	d6vtbcy3ong79.cloudfront.net:443	0			chrome...		
3	200	HTTP	Tunnel to	d6vtbcy3ong79.cloudfront.net:443	0			chrome...		
4	200	HTTP	Tunnel to	scripts.demandbase.com:443	0			chrome...		
5	200	HTTP	Tunnel to	ajax.aspnetcdn.com:443	0			chrome...		
6	200	HTTP	Tunnel to	www.telerik.com:443	0			chrome...		
7	200	HTTP	Tunnel to	d2i2wahzwrm1n5.cloudfront.net:443	0			chrome...		
8	200	HTTP	Tunnel to	static.hotjar.com:443	0			chrome...		
9	200	HTTP	Tunnel to	www.telerik.com:443	0			chrome...		
10	200	HTTP	Tunnel to	d585tldpucybw.cloudfront.net:443	0			chrome...		
11	200	HTTP	Tunnel to	d585tldpucybw.cloudfront.net:443	0			chrome...		
12	200	HTTP	Tunnel to	d585tldpucybw.cloudfront.net:443	0			chrome...		
13	200	HTTP	Tunnel to	d585tldpucybw.cloudfront.net:443	0			chrome...		
14	200	HTTP	Tunnel to	d585tldpucybw.cloudfront.net:443	0			chrome...		
15	200	HTTP	Tunnel to	d585tldpucybw.cloudfront.net:443	0			chrome...		
16	200	HTTP	Tunnel to	sjs.bizographics.com:443	0			chrome...		
17	200	HTTP	Tunnel to	script.hotjar.com:443	0			chrome...		
18	200	HTTP	Tunnel to	d6vtbcy3ong79.cloudfront.net:443	0			chrome...		
19	200	HTTP	Tunnel to	d6vtbcy3ong79.cloudfront.net:443	0			chrome...		
20	200	HTTP	Tunnel to	d6vtbcy3ong79.cloudfront.net:443	0			chrome...		
21	200	HTTP	Tunnel to	fonts.gstatic.com:443	0			chrome...		
22	200	HTTP	Tunnel to	r11---sn-bvvbax-15be.googlevideo.com:443	0			chrome...		
23	200	HTTP	Tunnel to	r15---sn-bvvbax-15be.googlevideo.com:443	0			chrome...		
24	200	HTTP	Tunnel to	r9---sn-bvvbax-15be.googlevideo.com:443	0			chrome...		
25	200	HTTP	Tunnel to	r9---sn-bvvbax-15be.googlevideo.com:443	0			chrome...		
26	200	HTTP	Tunnel to	d6vtbcy3ong79.cloudfront.net:443	0			chrome...		
27	200	HTTP	Tunnel to	dtzbdy9anri2p.cloudfront.net:443	0			chrome...		
28	200	HTTP	Tunnel to	img.en25.com:443	0			chrome...		
29	200	HTTP	Tunnel to	connect.facebook.net:443	0			chrome...		
30	200	HTTP	Tunnel to	s3.amazonaws.com:443	0			chrome...		
31	200	HTTP	Tunnel to	vars.hotjar.com:443	0			chrome...		
32	200	HTTP	Tunnel to	vars.hotjar.com:443	0			chrome...		
33	200	HTTP	Tunnel to	www.facebook.com:443	0			chrome...		
34	200	HTTP	Tunnel to	www.telerik.com:443	0			chrome...		
35	200	HTTP	Tunnel to	rum-collector-2.pingdom.net:443	0			chrome...		
36	200	HTTP	Tunnel to	api.dec.sitefinity.com:443	0			chrome...		
37	200	HTTP	Tunnel to	r12---sn-bvvbax-15be.googlevideo.com:443	0			chrome...		
38	200	HTTP	Tunnel to	r12---sn-bvvbax-15be.googlevideo.com:443	0			chrome...		
39	200	HTTP	Tunnel to	pagead2.googlesyndication.com:443	0			chrome...		
40	200	HTTP	Tunnel to	r12---sn-bvvbax-15be.googlevideo.com:443	0			chrome...		
41	200	HTTP	Tunnel to	r12---sn-bvvbax-15be.googlevideo.com:443	0			chrome...		

Slika 7: Lista HTTP/HTTPS zahtjeva

Pritiskom na jedan ili više zahtjeva moguće je, u prozoru na desnom dijelu ekrana, saznati više informacija poput statistike i zaglavlja zahtjeva i odgovora. Na slici 8 prikazani su detaljni podaci o jednom od poslanih zahtjeva.



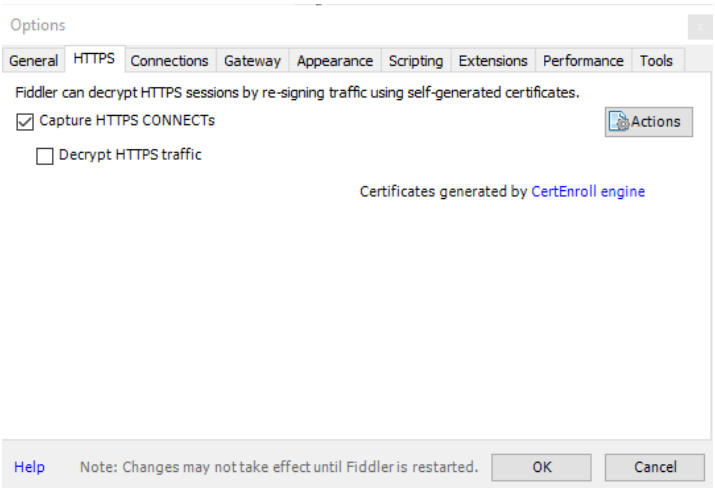
Slika 8: Detaljni podaci jednog od poslanih zahtjeva

3.2 Dešifriranje HTTPS prometa

Prema zadanim postavkama šifrirane HTTPS poruke se ne dešifriraju, ali, ako je potrebno, moguće je konfigurirati njihovo dešifriranje. Pritiskom na neki od zahtjeva koji sadrži šifrirane podatke pojavit će se upozorenje, prikazano na slici 9. Pritisak na upozorenje omogućava podešavanje postavki dešifriranja.

Slika 9: Upozorenje da je HTTPS dekripcija onemogućena

Iste se postavke mogu pronaći na alatnoj traci odabirom ***Tools*** > ***Options…*** > ***HTTPS*** nakon čega je potrebno označiti kvadratić ***Decrypt HTTPS traffic*** prikazanu na slici 10.



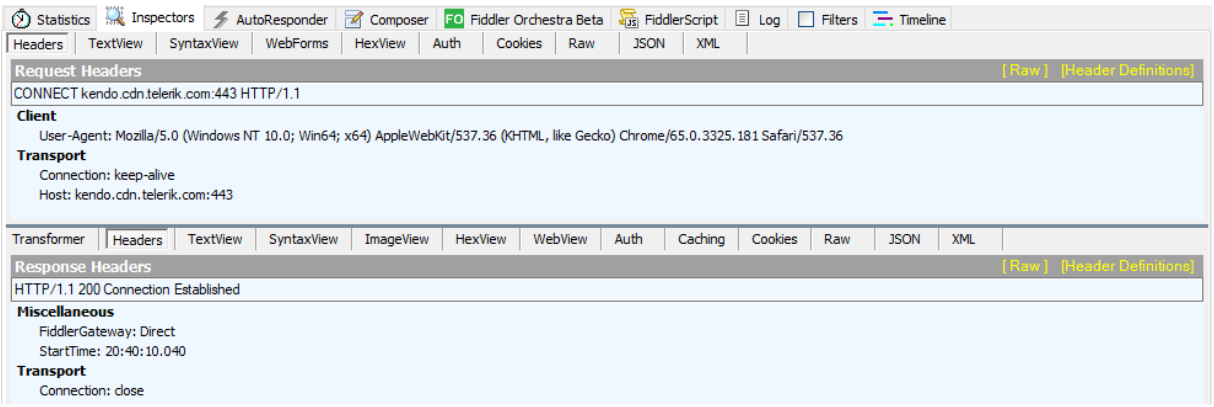
Slika 10: Omogućavanje HTTPS dekripcije

Nakon označavanja kvadratića pojavljuje se upozorenje prikazano na slici 11. Kako bi Fiddler mogao presretati HTTPS promet mora generirati jedinstveni vršni certifikat (eng. *Root certificate*). Moguće je konfigurirati da operacijski sustav vjeruje generiranom certifikatu kako bi se suzbila upozorenja vezana za neispravne certifikate. Ako se navedeno omogući, svi programi koji se oslanjaju na listu povjerljivih izdavača certifikata neće javljati upozorenja, dok će se u suprotnom upozorenja pojavljivati. Dešifriranje će biti omogućeno nakon ponovnog pokretanja alata neovisno o tome koja je opcija izabrana.

Slika 11: Upozorenje prilikom omogućavanja dešifriranja HTTPS prometa

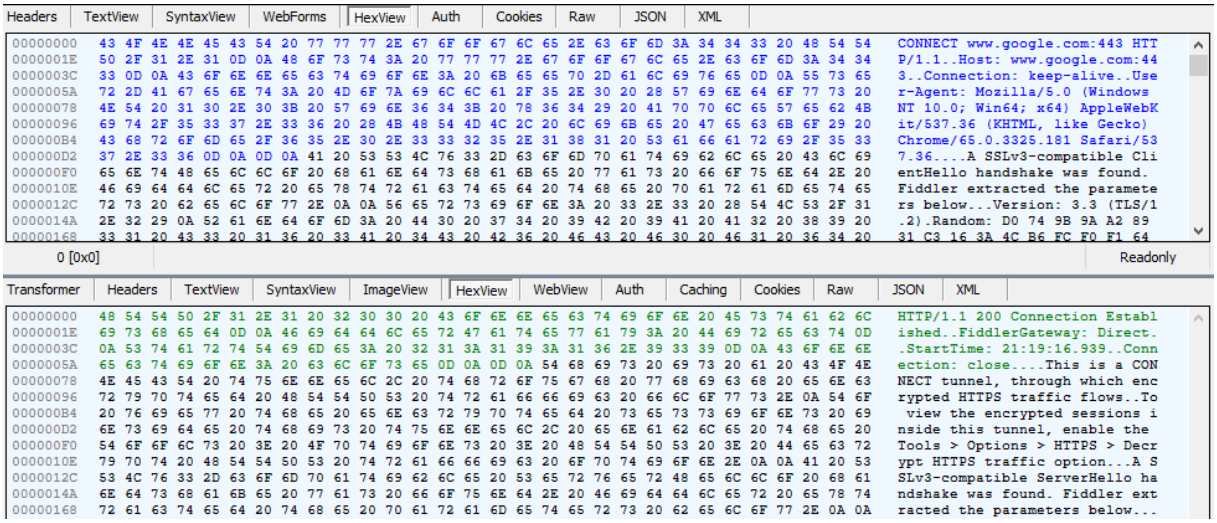
3.3 Pregled zahtjeva

Odabirom jednog od zahtjeva s liste snimljenog mrežnog prometa te odabirom kartice ***Inspector*** unutar desnog prozora alata moguće je vidjeti dodatne informacije o zahtjevu i odgovoru. U gornjoj polovici kartice nalaze se informacije vezane uz HTTP/HTTPS zahtjev dok su u donjoj informacije vezane uz odgovor na pripadajući zahtjev. Pritiskom na tipku ***Headers*** moguće je vidjeti zaglavlja zahtjeva i odgovora kao što prikazuje slika 12.



Slika 12: Zaglavlja zahtjeva i odgovora na zahtjev

Pritiskom na neku od sljedećih tipki moguće je vidjeti zahtjev i odgovor u odgovarajućem formatu ovisno o potrebama korisnika: ***TextView***, ***SyntaxView***, ***ImageView***, ***HexView***, ***WebView***, ***Raw***, ***JSON***, ***XML***. Slika 13 prikazuje pregled zahtjeva i odgovora u heksadekadskom obliku.



Slika 13: Heksadekadski prikaz zahtjeva i odgovora

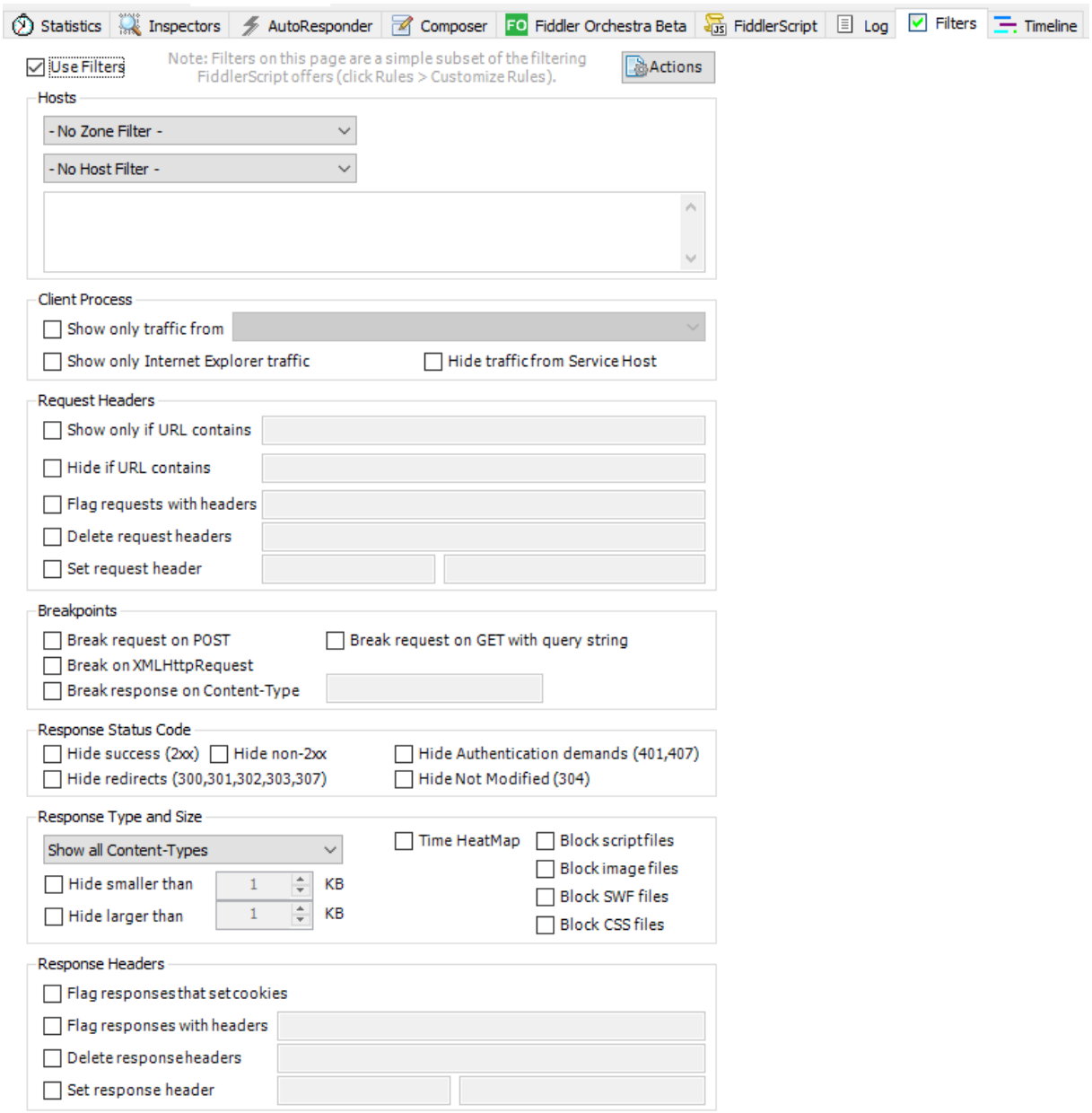
Tipka ***Cookies*** daje pregled svih dolaznih i odlaznih podataka o kolačićima (eng. *Cookies*).

Nadalje, tipka ***Auth*** sadrži podatke o poslanim i primljenim zaglavljima za autentifikaciju (eng. *Authentication headers*).

Caching tipka omogućava pregled podataka vezanih uz priručnu pohranu podataka (eng. *Caching*).

3.4 Filtriranje zahtjeva

Za lakše snalaženje u velikoj količini mrežnog prometa moguće je filtrirati HTTP/HTTPS zahtjeve. Na desnoj strani glavnog prozora moguće je izabrati karticu ***Filters*** te označiti kvadratić ***Use Filters*** kao što je prikazano na slici 14.



Slika 14: Omogućavanje filtera

Koristeći niz dostupnih opcija moguće je filtrirati mrežni promet na razne načine, između ostaloga: filtriranje po poslužitelju ili klijentu, URL-u, podacima iz zaglavlja, statusu odgovora te veličini i vrsti tijela odgovora. Više informacija o filtriranju mrežnog prometa dostupno je u službenoj dokumentaciji.

4 Zaključak

Ovaj dokument pruža kratki uvid u HTTP posrednike te, kroz opis instalacije i osnovnih obrasca korištenja, pruža potrebne informacije za stjecanje osnovnih vještina korištenja alata Telerik Fiddler. Navedene vještine imaju niz primjena poput otklanjanja grešaka koje se manifestiraju u mrežnom prometu, testiranja performansi, sigurnosnog testiranja te snimanja mrežnog HTTP/HTTPS prometa u razne druge svrhe. Sve navedeno čini alat Telerik Fiddler izuzetno korisnim i svestranim u kontekstu analize mrežnog prometa.

Za korištenje alata nisu potrebni posebna vještina ni znanje, već je naglasak na razumijevanju klijenata i poslužitelja koji se analiziraju.