







Sadržaj

1	UVO	D	
2	INST	ALACIJA ALATA TELERIK FIDDLER	4
3	KOR	IŠTENJE ALATA TELERIK FIDDLER	6
	3.1	Osnovno korištenie	6
	3.2	DEŠIFRIRANJE HTTPS PROMETA	
	3.3	PREGLED ZAHTJEVA	
	3.4	FILTRIRANJE ZAHTJEVA	
4	ZAK	LJUČAK	

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

Ovaj dokument vlasništvo je Nacionalnog CERT–a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega se pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.



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 <u>službenoj dokumentaciji</u>.

1. Za preuzimanje instalacijske datoteke Telerik Fiddler alata potrebno je otvoriti <u>službene stranice</u> 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.

Progress Telerik Fiddler: License Agreement —		\times
You must agree to this license before installing.		
By using this software and any updates to it, you indicate your ac these terms. If you do not accept these terms, do not install or us software.	ceptance of e the	
The software (Progress Telerik Fiddler Web Debugger) and any up are provided "as is" and you bear the risk of using it. In no event s Inc., its affiliates, or its licensors, be liable for any consequential, incidental or indirect damages of any kind arising out of the deliver performance or use of this software. This software was written wi no one warrants that the software is error-free. Your sole remedy failure or any form of damage caused by this software is a full refi- license fee we have received from you, which in all cases is \$0.	odates to it shall Telerik special, 'y, th care, bu for any und of the	t V
Cancel [Mar-20-18] v5.0.20181.14850	I Agre	e

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.

Progress Telerik Fiddler: Installation Folder	_		\times
Select the directory to install Progress Telerik Fi	ddler:		
Destination Folder			
D: \Program Files \Fiddler		Browse	
Space required: 13.8MB Space available: 1390.3GB			
Cancel [Mar-20-18] v5,0.20181,14850	< Back	Instal	I

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.



AppContainer Loopback Exemption Utility

For security and reliability reasons, Windows blocks "Immersive" apps from sending network traffic to the local computer. This utility enables removal of this restriction for debugging purposes.

∳ Refresh	Exempt All E	xempt Non	e	Save Changes		Learn more	e
DisplayName	Description	Package	AC Name	AC SID	AC User(s)	Binaries	^
Assigned Access Loc	Launches above lo	Micros	microso	S-1-15-2-2705	Josipa	(None)	
Captive Portal Flow	Captive Portal Flow	Micros	microso	S-1-15-2-3119	Josipa	(None)	
Connect	Connect	Micros	microso	S-1-15-2-1162	Josipa	(None)	
Cortana	Search the web an	Micros	microso	S-1-15-2-1861	Josipa	(None)	
Credential Dialog	Credential Dialog	Micros	microso	S-1-15-2-9329	Josipa	(None)	
EC App	EC App	Micros	microso	S-1-15-2-3912	Josipa	(None)	
Email and accounts	Email and accounts	Micros	microso	S-1-15-2-9698	Josipa	(None)	
File Explorer	File Explorer	c5e252	c5e2524	S-1-15-2-4264	Josipa	(None)	
Groove glazba	Groove glazba	Micros	Microso	S-1-15-2-3132	Josipa	(None)	
Microsoft Content	Microsoft Content	Micros	microso	S-1-15-2-3501	Josipa	(None)	
Microsoft Edge	Microsoft Edge	Micros	Microso	S-1-15-2-3624	Josipa	(None)	
Microsoft Store	Microsoft Store	Micros	Microso	S-1-15-2-1609	Josipa	(None)	
Microsoft family feat	Microsoft family f	Micros	microso	S-1-15-2-3072	Josipa	(None)	
Microsoft fotografije	Microsoft fotograf	Micros	Microso	S-1-15-2-2226	Josipa	(None)	
Mixed Reality Portal	Mixed Reality Portal	Micros	Microso	S-1-15-2-2205	Josipa	(None)	
Network Connection	Network Connecti	Micros	microso	S-1-15-2-3784	Josipa	(None)	
OneNote	OneNote	Micros	Microso	S-1-15-2-3445	Josipa	(None)	
PinningConfirmatio	PinningConfirmati	Micros	microso	S-1-15-2-2652	Josipa	(None)	
SecondaryTileExperi	SecondaryTileExpe	Micros	microso	S-1-15-2-2572	Josipa	(None)	
Shell Input Applicati	Shell Input Applica	InputA	InputAp	S-1-15-2-3945	Josipa	(None)	
Skype	Skype	Micros	Microso	S-1-15-2-2246	Josipa	(None)	
SmartScreen	SmartScreen	Micros	microso	S-1-15-2-1255	Josipa	(None)	
Take a Test	Take a Test	Micros	microso	S-1-15-2-3733	Josipa	(None)	~
<							>
Refreshed AppContainer in	formation at 17:39:54.						

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		
<u> </u>	200	HTTP	Tunnel to	d6vtbcy3ong79.cloudfront.net:443	0			chrome		
m 3	200	HTTP	Tunnel to	d6vtbcy3ong79.cloudfront.net:443	0			chrome		
👚 4	200	HTTP	Tunnel to	scripts.demandbase.com:443	0			chrome		
6	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.doudfront.net:443	0			chrome		
👚 8	200	HTTP	Tunnel to	static.hotjar.com:443	0			chrome		
<u> 9</u>	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		
節 19	200	HTTP	Tunnel to	d6vtbcy3ong79.cloudfront.net:443	0			chrome		
<u></u> 20	200	HTTP	Tunnel to	d6vtbcy3ong79.cloudfront.net:443	0			chrome		
🛱 21	200	HTTP	Tunnel to	fonts.gstatic.com:443	0			chrome		
<u></u> 22	200	HTTP	Tunnel to	r11sn-bvvbax-15be.googlevideo.com:443	0			chrome		
🛱 23	200	HTTP	Tunnel to	r15sn-bvvbax-15be.googlevideo.com:443	0			chrome		
🛱 24	200	HTTP	Tunnel to	r9sn-bvvbax-15be.googlevideo.com:443	0			chrome		
25	200	HTTP	Tunnel to	r9sn-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		
<u></u> 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	r12sn-bvvbax-15be.googlevideo.com:443	0			chrome		
🛱 38	200	HTTP	Tunnel to	r12sn-bvvbax-15be.googlevideo.com:443	0			chrome		
🛱 39	200	HTTP	Tunnel to	pagead2.googlesyndication.com:443	0			chrome		
🛱 40	200	HTTP	Tunnel to	r12sn-bvvbax-15be.googlevideo.com:443	0			chrome		
🛱 4 1	200	HTTP	Tunnel to	r12sn-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.

🖄 Statistics 💥 Inspectors 🗲 AutoResponder 📝 Composer 📧 Fiddler Orchestra Beta 🚟 Fiddler Script 🗄 Log 🗌 Filters 🚍 Timeline
This is a Tunnel. Status: CLOSED, Raw Bytes Out: 592; In: 161
The selected session is a HTTP CONNECT Tunnel. This tunnel enables a client to send raw traffic (e.g. HTTPS-encrypted streams or WebSocket messages) through a HTTP Proxy Server (like Fiddler).
To enable Fiddler's HTTPS-decryption feature and view decrypted traffic, click Tools > Options > HTTPS.
Request Count: 1 Bytes Sent: 220 (headers:220; body:0) Bytes Received: 182 (headers:182; body:0) Tunnel Sent: 592 Tunnel Sectived: 161
ACTUAL PERFORMANCE
clientconnected: 19:46:50.012 ClientconnetRequest: 19:46:50.013 GotRequestHeaders: 19:46:50.013 CollentDoinfequest: 19:46:50.013 Determine Gateway: Oms Determine Gateway: Oms CollentDoinfequest: 19:46:50.013 Determine Gateway: Oms ServerConfequest: 19:46:50.140 FiddlerBeginRequest: 19:46:50.140 FiddlerBeginRequest: 19:46:50.140 GotResponseHeaders: 00:00:000 ServerConfequest: 19:46:50.140 GotResponseHeaders: 00:00:0000 ServerConfequest: 19:46:50.395 ClientDoindecsponse: 19:46:50.395 ClientDoindecsponse: 19:46:50.395
Overall Elapsed: 0:00:00.382
RESPONSE BYTES (by Content-Type)
-headers-: 182
ESTIMATED WORLDWIDE PERFORMANCE
The following are VERY rough estimates of download times when hitting servers based in Seattle.
US West Coast (Modem - 6K8/sec) RTT: 0,10s Elapsed: 0,10s
Japan / Northern Europe (Modem) RTT: 0,155 Elapsed: 0,155
China (Modem) RTT: 0,455 Elapsed: 0,455
US West Coast (DSL - 30K8/sec) RTT: 0,105 Elapsed: 0,105
Japan / Northern Europe (DSL) RTT: 0,155 Elapsed: 0,155
China (DSL) TT: 0,455 Elapsed: 0,455
Learn more about HTTP performance at <u>http://fiddler2.com/r/7HTTPPERF</u>

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.

🖄 Statist	ics 🔍 Insp	ectors 🖌 Au	ItoResponder	Compose	FO FI	iddler Orches	stra Beta	🔓 Fiddler	Script	Log	Filters	🚍 Timeline		
					🛕 нт	TTPS decrypt	tion is dis	abled. Click	to config	gure				
Headers	TextView	SyntaxView	WebForms	HexView	Auth	Cookies	Raw	JSON	XML					

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.

Options								
General	HTTPS	Connections	Gateway	Appearance	Scripting	Extensions	Performance	Tools
Fiddler (can decry	pt HTTPS sessi	ions by re-si	igning traffic u	sing self-ge	nerated certi	ficates.	
🗸 Cap	ture HTT	PS CONNECTs						Actions
	ecrypt H	ITTPS traffic						
				Cer	tificates g	enerated by (CertEnroll engi	ne
Help	Note:	Changes may i	nottake eff	fect until Fiddl	eris restar	ted. (ОК	Cancel

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.

SCAR	Y TEXT AHEAD: Read Carefully!	x
	To intercept HTTPS traffic, Fiddler generates a unique root certificate.	
™ ₽	You may configure Windows to trust this root certificate to suppress security warnings. This is generally safe.	
	Click 'Yes' to reconfigure Windows' Trusted CA list. Click 'No' if this is all geek to you.	
	Trust the Fiddler Root certificate? Yes No	

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.

Headers	TextView	5	Synta	xVie	w	W	ebFo	orms		Hex	View		Auth		Co	okie	s	Ra	w]]	ISON		XML	_														
00000000	43 4F	4E	4E	45	43	54	20	77	77	77	2E	67	6F	6F	67	6C	65	2E	63	6F	6D	3A	34	34	33	20	48	54 5	54	CONN	CT ww	w. (goo	gle.	com:	443 HT	т	^
0000001E	50 2F	31	2E	31	OD	0A	48	6F	73	74	3A	20	77	77	77	2E	67	6F	6F	67	6C	65	2E	63	6F	6D	3A	34 3	34	P/1.3	Hos	st:	ww	. go	ogle	.com:4	4	
000003C	33 OD	0A	43	6F	6E	6E	65	63	74	69	6F	6E	3A	20	6B	65	65	70	2D	61	6C	69	76	65	0D	0A	55	73 (65	3C	nnect	ior	n: I	ceep	-ali	.veUs	e	
0000005A	72 2D	41	67	65	6E	74	3A	20	4D	6F	7A	69	6C	6C	61	2F	35	2E	30	20	28	57	69	6E	64	6F	77	73 2	20	r-Age	ent: M	lozi	i11	a/5.	D (1)	lindows		
00000078	4E 54	20	31	30	2E	30	3B	20	57	69	6E	36	34	3B	20	78	36	34	29	20	41	70	70	6C	65	57	65	62 4	4B	NT 1).0; W	line	64;	x64) Ap	pleWeb	K	
00000096	69 74	2F	35	33	37	2E	33	36	20	28	4B	48	54	4D	4C	2C	20	6C	69	6B	65	20	47	65	63	6B	6F	29 2	20	it/5	37.36	(KI	HTM	L, 1:	ike	Gecko)		
000000B4	43 68	72	6F	6D	65	2F	36	35	2E	30	2E	33	33	32	35	2E	31	38	31	20	53	61	66	61	72	69	2F	35 3	33	Chro	ne/65.	0.3	332	5.18	l Sa	fari/5	3	
00000D2	37 2E	33	36	0D	0A	0D	0A	41	20	53	53	4C	76	33	2D	63	6F	6D	70	61	74	69	62	6C	65	20	43	6C (69	7.36	Α	SSI	Lv3	-comj	pati	ble Cl	i	
000000F0	65 6E	74	48	65	6C	6C	6F	20	68	61	6E	64	73	68	61	6B	65	20	77	61	73	20	66	6F	75	6E	64	2E 2	20	entHe	ello h	and	dsh	ake 1	va s	found.		
0000010E	46 69	64	64	6C	65	72	20	65	78	74	72	61	63	74	65	64	20	74	68	65	20	70	61	72	61	6D	65	74 (65	Fidd:	er ex	tra	acte	ed tl	he p	aramet	e	
0000012C	72 73	20	62	65	6C	6F	77	2E	0A	0A	56	65	72	73	69	6F	6E	ЗA	20	33	2E	33	20	28	54	4C	53	2F 3	31	rs be	elow	.Ve	ers	ion:	3.3	(TLS/	1	
0000014A	2E 32	29	0A	52	61	6E	64	6 F	6D	3A	20	44	30	20	37	34	20	39	42	20	39	41	20	41	32	20	38	39 2	20	.2).1	landom	i: I	D0 '	74 91	B 97	A2 89		
00000168	33 31	20	43	33	20	31	36	20	33	41	20	34	43	20	42	36	20	46	43	20	46	30	20	46	31	20	36	34 2	20	31 C;	3 16 3	A 4	4C]	36 F(C FO) F1 64		~
0 [0)x0]																																			Read	lonly	
Transforme	r Heade	ers	Te	xtVie	ew	S	ynta	xVie	w	Im	ageV	iew	H	lex\	iew	1	Neb	View		Aut	h	Ca	achin	g	Co	okies	;	Raw		JSON	XML							
00000000	48 54	54	50	2F	31	2E	31	20	32	30	30	20	43	6F	6E	6E	65	63	74	69	6F	6E	20	45	73	74	61	62 (6C	HTTP,	1.1 2	200	Cor	nec	tior	Estab	1	~
0000001E	69 73	68	65	64	0D	0A	46	69	64	64	6C	65	72	47	61	74	65	77	61	79	3A	20	44	69	72	65	63	74 (0D	ished	IFid	ldle	erG	atew	ay:	Direct	-	
000003C	0A 53	74	61	72	74	54	69	6D	65	3A	20	32	31	3A	31	39	3A	31	36	2E	39	33	39	0D	0A	43	6F	6E (6E	.Sta:	tTime	20.2	21:	19:1	6.93	9Con	n	
0000005A	65 63	74	69	6F	6E	3A	20	63	6C	6 F	73	65	0D	0A	0D	0A	54	68	69	73	20	69	73	20	61	20	43	4F 4	4E	ectio	n: cl	ose	e	Th	is i	s a CO	N	
00000078	4E 45	43	54	20	74	75	6E	6E	65	6C	2C	20	74	68	72	6F	75	67	68	20	77	68	69	63	68	20	65	6E (63	NECT	tunne	1,	th:	cougl	h wh	ich en	c	
00000096	72 79	70	74	65	64	20	48	54	54	50	53	20	74	72	61	66	66	69	63	20	66	6C	6F	77	73	2E	0A	54 6	6F	rypte	d HTT	PS	tr	affi	e fl	.owsT	0	
000000B4	20 76	69	65	77	20	74	68	65	20	65	6E	63	72	79	70	74	65	64	20	73	65	73	73	69	6F	6E	73	20 (69	view	the the	end	ery	pted	ses	sions	i	
00000D2	6E 73	69	64	65	20	74	68	69	73	20	74	75	6E	6E	65	6C	2C	20	65	6E	61	62	6C	65	20	74	68	65 2	20	nside	this	s ti	unne	el, (enab	le the		
000000F0	54 6F	6F	6C	73	20	3E	20	4F	70	74	69	6F	6E	73	20	3E	20	48	54	54	50	53	20	3E	20	44	65	63 1	72	Tool	s > Op	tic	ons	> H	TTPS	> Dec	r	
0000010E	79 70	74	20	48	54	54	50	53	20	74	72	61	66	66	69	63	20	6F	70	74	69	6F	6E	2E	0A	0A	41	20 5	20 53 ypt HTTPS traffic optionA S									
0000012C	53 4C	76	33	2D	63	6F	6D	70	61	74	69	62	6C	65	20	53	65	72	76	65	72	48	65	6C	6C	6F	20	68 6	61	SLv3-	compa	ti	ble	Ser	verH	lello h	а	
0000014A	6E 64	73	68	61	6B	65	20	77	61	73	20	66	6F	75	6E	64	2E	20	46	69	64	64	6C	65	72	20	65	78 1	74	ndsh	ke wa	is f	Eou	nd. 1	Fidd	ler ex	t	
00000168	72 61	63	74	65	64	20	74	68	65	20	70	61	72	61	6D	65	74	65	72	73	20	62	65	6C	6F	77	2E	OA (AO	racte	d the	pa pa	ara	nete:	rs b	elow	-	

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.

🔊 Statistics 👯 Inspectors 🚿 AutoResponder 📝 Composer 🕫 Fiddler Orchestra Beta 🚟 Fiddler Script 🗉 Log 🗹 Filters 🚍 Timeline
Use Filters Note: Filters on this page are a simple subset of the filtering FiddlerScript offers (click Rules > Customize Rules).
Hosts
- No Zone Filter - V
- No Host Filter - 🗸 🗸
Show only traffic from
Show only Internet Explorer traffic Hide traffic from Service Host
Request Headers
Show only if URL contains
Hide if URL contains
Flag requests with headers
Delete request headers
Set request header
Breakpoints
Break request on POST Break request on GET with query string
Break on XMLHttpRequest
☐ Hide success (2∞) ☐ Hide non-2∞ ☐ Hide Authentication demands (401,407)
Hide redirects (300,301,302,303,307)
Response Type and Size
Show all Content-Types
Hide smaller than 1 KB Block SWF files
Hide larger than 1 👻 KB 🗌 Block CSS files
Response Headers
Flag responses that set cookies
Flag responses with headers
Delete response headers
Set response header

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 <u>službenoj dokumentaciji</u>.



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.