Several approaches to capture clear text of HTTPS packets

- Chrome DevTools
- Firefox Web Developer
- Fiddler Web Debugger

1. Chrome DevTools

If you are using Chrome browser, please **press 'F12'** to open DevTools. see below:

← → O ■ GitHub, Inc. [US] https://github.com											Ŷ
How peop	ble			Pic	sk a usernam	0		1			
build off				Ma	ur amall add			4			
	wa	re			ur email addi	ess					
Elements Console Sources Network Timeline Profiles Application Security	Audits										:
Olima No throatile		*									
	9										
S00 ms 1000 ms 1500 ms 2000 ms	wo manite	2500 ms	3000 ms	3500 ms	4000	1753	4500 ma	\$000 ms		5500 ms	600
		-									
	(1) I	Turn	Tellister		7-0		and the state of t				
vane	Status	type	unitiator	Size	time		meine - start (ime	2.001	3.00 s	4.001	5001
trameworks-c07e6f4b02b556d1d85052fb3853caf84c80e6b23dcdb1ae1b00f051da1115a2.css	200	stylesheet	(index):10		21.6 KB	404 ms					
github-4d14493830801ffc6d6d6363f3fcef8a6e41fd9e74776dce15fa2c18b2a9bb72.css	200	stylesheet	Endex:11		96.4 KB	758 ms					
ste-2999228080861987508205686965674005723859c0ec508972c70d246854fc.css	200	stylesneet	ondexc14		12.1 KB	571 ms					
nome-ii-ouid.pngrsn	200	png	DINDEXT236		6.6.8.8	236 ms					
in nome-u-workprogram	200	png	(indexc241		11.858	222 ms					
a nome-in-projects.prigram	200	phg	Enderh 251		20.7 6.0	240 ms					
	200	019	Index 285		05548	1184			_		
	200	section	Ender/347		85.5 KB	1.11.4			_		
010ub-4de68t49123132f5b0a89aer54469r246e4547998b891f18504dr5be11bbab51.is	200	script	(index):348		147 KB	981 ms					
roboto-regular.woff	200	font	(indext:347		13.6 KB	123 ms			-		
roboto-medium.woff	200	font	(index):347		13.6 KB	177 ms					
la home-hero.jpgTsn	200	lpeg	(index):347		114 KB	393 ms					
robote-light.woff	200	font	Endext:347		13.7 KB	92 ms					
collect	200	shr	frameworks-bb39ae7. jst6		293 8	195 ms			10		
page_view?dimensions[page]=https%3A%2P%2Fgithub.com%2F&dimensions[title]=How%20people%20build%	200	gif	Other		545.8	1.10 s					
stats	200	fetch	github-4de6854/s/2		770 B	1.50 s				-	-
18 requests 662 KB transferred Finish: 5.77 s DOMContentLoaded: 2.18 s Load: 4.27 s											
1 ALL 1											

click 'Network' label to open 'Network' panel. Here we can get insights into requests and response traffic of the web pages.

We can get the clear text information even if the packet is encrypted. For example, open the 'https://www.github.com' url, we can see all the packets interacted with the server.

🕞 🔂 🛛 Elements Console Sources Network Timeline Profiles Application Security	Audits									
🔸 🛇 📄 🕎 🛛 View: 📰 🛬 📄 Preserve log 💷 Disable cache 📄 Offline No throttlin	ig 🔻									
Filter Regex Hide data URLs A	WS Manifest Othe									
500 ms 1000 ms 1500 ms 2000 ms	2500	Ims	3000 ms 3500	ms	4000 ms	4500 ms		5000 ms	55	
Name	Status	Туре	Initiator	Size	Time	Timeline – Star	Time 20	0 s	3.00 s	4.00 s
github.com	200	document	Other	9.4 KB	994 m:					
frameworks-c07e6f4b02b556d1d85052fb3853caf84c80e6b23dcdb1ae1b00f051da1115a2.css	200	stylesheet	(index):10	21.6 KB	404 m:	:				
github-4d14493830801ffc6d6d6363f3fcef8a6e41fd9e74776dce15fa2c18b2a9bb72.css	200	stylesheet	(index):11	96.4 KB	758 m					
site-293f92180d0a619a750fa2b5eae9e36740f5723a59c0ec308972c70d24e834fc.css	200	stylesheet	(index):14	12-1 KB	571 m					
home-ill-build.png?sn	200	png	(index):236	6.6 KB	236 m			•		
home-ill-work.png?sn	200	png	(index):241	11.8 KB	395 m:			-		
a home-ill-projects.png?sn	200	png	(index):246	10.7 KB	240 m			•		
home-III-platform.png?sn	200	png	(index):251	8.6 KB	421 m			-		
org_example_nasa.png?sn	200	png	(index):285	95.5 KB	1.18					
frameworks-bb39ae7d848d40d6f01e67355e282964f54fa39137c0ecc9fc4ec37e7d469508.js	200	script	(index):347	86.6 KB	1.11					
github-4de68f49123132f5b0a89aec54469c246e4547998b891f18504dc5be11bbab51.js	200	script	(index):348	147 KB	981 m					
roboto-regular.woff	200	font	(index):347	13.6 KB	123 m					
roboto-medium.woff	200	font	(index):347	13.6 KB	177 m:					
m home-hero.jpg?sn	200	jpeg	(index):347	114 KB	393 m:					
roboto-light.woff	200	font	(index):347	13.7 KB	92 m	:				
Collect	200	xhr	frameworks-bb39ae7is:6	293 B	195 m	;				
page_view?dimensions[page]=https%3A%2F9%2Fgithub.com%2F8xdimensions[title]=How%20people%20build%	200	gif	Other	545 B	1.10					_

click one item in the panel. We can see the details in the right panel. See below, it's a GET request example.

Name	× Headers Preview Response Cookies Timing					
github.com	▼ General					
frameworks-c07e6f4b02b556d1d85052fb3853caf84c80e6b23dcdb1ae1b00f051da1115a2.css	Request URL: https://github.com/					
github-4d14493830801ffc6d6d6363f3fcef8a6e41fd9e74776dce15fa2c18b2a9bb72.css	Request Method: GET					
site-293f92180d0a619a750fa2b5eae9e36740f5723a59c0ec308972c70d24e834fc.css	Status Code: 200 0K Remote Address: 192.30.253.112:443					
nome-ill-build.png?sn	Response Headers (20)					
P home-ill-work.png?sn	Request Headers view parsed					
a home-ill-projects.png?sn	GET / HTTP/1.1					
home-ill-platform.png?sn	Host: github.com					
org_example_nasa.png?sn	Connection: keep-alive					
frameworks-bb39ae7d848d40d6f01e67355e282964f54fa39137c0ecc9fc4ec37e7d469508.js	Cache-Control: no-cache					
github-4de68f49123132f5b0a89aec54469c246e4547998b891f18504dc5be11bbab51.js	Upgrade-Insecure-Requests: 1					
roboto-regular.woff	User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like G					
roboto-medium.woff	Accept-Encoding: gzip, deflate, sdch, br					
🛥 home-hero.jpg?sn	Accept-Language: en-US,en;q=0.8					
roboto-light.woff	Cookie: logged_in=no; _gh_sess=eyJzZXNzaW9uX21kIjoiNTUyOTVjYjUwYmQzMWE1MjIyZjR1YmJ1NDY					
collect	nU0RzdYD0hvc0cwUIAvU089In0%3D61t/ad293d1t8//a/4b3acebtd29e5td//d45ce5; _ga=GA1.2.884 sia%2FShanghai					
page_view?dimensions[page]=https%3A%2F%2Fgithub.com%2F&dimensions[title]=How%20people%20build%20software						
18 requests 662 KB transferred Finish: 5.77 s DOMContentLoaded: 2.18 s Load: 4.27 s						

A POST request example:

× Headers Preview Response Cookies Timing			
▼ General			
Request URL: https://github.com/join			
Request Method: POST			
Status Code: 🖷 200 OK			
Remote Address: 192.30.253.112:443			
Response Headers (21)			
▼ Request Headers view parsed			
POST /join HTTP/1.1			
Host: github.com			
Connection: keep-alive			
Content-Length: 210			
Cache-Control: max-age=0			
Origin: https://github.com			
Upgrade-Insecure-Requests: 1			
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like	ecko) Chrome/54.0.2840.99	Safari/537.36	
Content-Type: application/x-www-form-urlencoded			
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8			
Referer: https://github.com/			
Accept-Encourng: grip, definite, br			
Cookie: logged in-no: octo-GH1 1 1228578324 1484276100; ga-GA1 2 884395312 1484276	5100, tz-Acia%2EShanghai, ga	+-1; ch cecc-ev]7774	NzaliQuV
zMWE1MiTv7iB1Vm11NDV00GVv7m0ilC1fV3Nv7190b2t1biT6Tm7iO2nwWXdKOT1ob18EeWdC7nErU0b502	ijuni lagzd Vhahvca cwi iTAvi i689 Tiw	icmVm7X1vVWxfV29k7STF	6Tmb0dH
LCJsYXN0X3dvaXB1TioxND#0Mic4MDM5NTU1f0%3D%3D1c543800662b3cdbf63ff99b8e94fc8d3d6d9	5f1	100000000000000000000000000000000000000	211110011
rorm Data view parsed			
utf8=%E2%9C%93&authenticity_token=TqNbj4WeTnlZJYKg0NPYBjmvsMVjIWFLsXQ4MeWxPoIEY97oFn	ilt0rkDmBJdGvnXFYp5bBcEBiSamB	rzZzJFFg%3D%3D&user%5	SBlogin
1%5D=test1234&user%5bpassword%5D=&source=form-home			

We can also get the post body 'Form Data' in the panel.

Please reproduce the issue, and check **the packet which triggered signature 030000138** and record the whole packet information.

2. Firefox Web Developer

If you are using Firefox browser, please **press 'F12'** to open Web Developer. see below:

C G GitHub, Inc. (US) https://github.com										
			Personal C	pen source Business Explore		Pricing Blog	Support			Sign ir
			0							
Ŗ	○ In	spector	≻ Console () Debugger {} Style Editor () Perf	ormance 🖙 Network						
Ē	All	HTML	CSS JS XHR Fonts Images Media Flash	Other						
Sta	itus	Method	File	Domain	Type	Transferred	Size	0 ms 640 ms	1.28 s	1.92
	301	GET	1	www.github.com	html	7.69 KB	UKB	→ 265 ms		
	200	GET	/	github.com	numi	21.03 KD	100 22 VP	- 249 ms		
	200	GET	ntarrieworks-coreor40020JJ00100J0121050J5cat036641fd0a74776dca	1562 A prosto-con github.com	cs:	05 72 KB	413.97 KB	→ 47 ms		
-	200	GET	cite_203f02180rd0a619a750fa2b5eae9e36740f5723a50c0ec3080	12:70 assets-cdn.github.com	C55	11.45 KB	58.52 KB	- 02 ms		
	200	GET	home-ill-huild.nng?sn	assets-cdn.github.com	png	5.99 KB	5.99 KB	■ → 78 ms		
•	200	GET	Mome-ill-work.png?sn	assets-cdn.github.com	png	11.23 KB	11.23 KB	→ 0 ms		
•	200	GET	a home-ill-projects.pnq?sn	assets-cdn.qithub.com	png	10.08 KB	10.08 KB	→ 0 ms		
•	200	GET	home-ill-platform.png?sn	assets-cdn.github.com	png	7.99 KB	7.99 KB	→ 0 ms		
•	200	GET	💼 org_example_nasa.png?sn	assets-cdn.github.com	png	94.92 KB	94.92 KB	→ 0 ms		
•	200	GET	frameworks-bb39ae7d848d40d6f01e67355e282964f54fa39137	:0ecc9 🔒 assets-cdn.github.com	js	85.97 KB	234.76 KB	II → 48 ms		
•	200	GET	github-4de68f49123132f5b0a89aec54469c246e4547998b891f1	3504d 🔒 assets-cdn.github.com	js	146.08 KB	489.11 KB	→ 32 ms		
•	200	GET	🙀 home-hero.jpg?sn	assets-cdn.github.com	jpeg	113.28 KB	113.28 KB		→ 16 m:	s
•	200	GET	roboto-regular.woff	assets-cdn.github.com	x-font-woff	13.00 KB	13.00 KB		→ 0 ms	
٠	200	GET	roboto-medium.woff	assets-cdn.github.com	x-font-woff	12.94 KB	12.94 KB		→ 16 m	5

click 'Network' label to open 'Network' panel. Here we can get insights into requests and response traffic of the web pages.

We can get the clear text information even if the packet is encrypted. For example, open the 'https://www.github.com' url, we can see all the packets interacted with the server.

R	🗘 In	spector	≻ Console 🔘 Debugger {} Style Editor 🙆 Performanc	e 🖙 Network							
Ê	All	HTML	CSS JS XHR Fonts Images Media Flash Other								
St	tatus	Method	File	Domain	Туре	Transferred	Size	0 ms	640 ms	1.28 s	1.92
	301	GET	/	a www.github.com	html	7.69 KB	0 KB	→ 265	ms		
•	200	GET	/	e github.com	html	7.69 KB	25.27 KB	-	249 ms		
٠	200	GET	frameworks-c07e6f4b02b556d1d85052fb3853caf84c80e6b23dcdb1a	assets-cdn.github.com	CSS	21.02 KB	109.32 KB		→ 47 ms		
•	200	GET	github-4d14493830801ffc6d6d6363f3fcef8a6e41fd9e74776dce15fa2	assets-cdn.github.com	CSS	95.72 KB	413.87 KB		■ → 62 ms		
٠	200	GET	site-293f92180d0a619a750fa2b5eae9e36740f5723a59c0ec308972c70	assets-cdn.github.com	CSS	11.45 KB	58.52 KB		→ 31 ms		
•	200	GET	home-ill-build.png?sn	assets-cdn.github.com	png	5.99 KB	5.99 KB		■ → 78 ms		
٠	200	GET	💽 home-ill-work.png?sn	assets-cdn.github.com	png	11.23 KB	11.23 KB		→ 0 ms		
•	200	GET	🛋 home-ill-projects.png?sn	assets-cdn.github.com	png	10.08 KB	10.08 KB		→ 0 ms		
٠	200	GET	home-ill-platform.png?sn	assets-cdn.github.com	png	7.99 KB	7.99 KB		→ 0 ms		
•	200	GET	org_example_nasa.png?sn	assets-cdn.github.com	png	94.92 KB	94.92 KB		→ 0 ms		
٠	200	GET	frameworks-bb39ae7d848d40d6f01e67355e282964f54fa39137c0ecc9	assets-cdn.github.com	js	85.97 KB	234.76 KB		II → 48 ms		
•	200	GET	github-4de68f49123132f5b0a89aec54469c246e4547998b891f18504d	assets-cdn.github.com	js	146.08 KB	489.11 KB		→ 32 ms		
٠	200	GET	🌆 home-hero.jpg?sn	assets-cdn.github.com	jpeg	113.28 KB	113.28 KB			→ 16 ms	
•	200	GET	roboto-regular.woff	assets-cdn.github.com	x-font-woff	13.00 KB	13.00 KB			→ 0 ms	
٠	200	GET	roboto-medium.woff	assets-cdn.github.com	x-font-woff	12.94 KB	12.94 KB			→ 16 ms	(
•	200	GET	roboto-light.woff	assets-cdn.github.com	x-font-woff	13.05 KB	13.05 KB			→ 0 ms	
٠	200	POST	collect	🔒 www.google-analytics.com	gif	0.03 KB	0.03 KB			1	

click one item in the panel. We can see the details in the right panel. See below, it's a GET request example.

Image Media Flash Other Status Method File Domal Cookies Params Respon 301 GET / ////////////////////////////////////	R	🗘 Ir	nspector	≿ Console 🛛 Debugger 👔 Style Editor 🖉 Performance	e 🖅 Network	
Status Method File Doma Headers Cookies Params Respon 301 GET / www.github.com/ genesit Genesit ////////////////////////////////////	Ô	All	HTML	CSS JS XHR Fonts Images Media Flash Other		
1 301 GET / 9. www.github.com Request WRL: https://github.com/ 2 200 GET / 9. github.edt Request WRL: https://github.com/ 2 200 GET fmomorks-c07e6f4b02b5561d85052fb3853cr84c80e6b23dc0ba 9. asset-cdn.github.com Request WRL: https://github.com/ 2 00 GET github-4d1449303001ffcd6dd3037frc8ha641d9c47fdc4c5fa2 9. asset-cdn.github.com 9. sitts: cdn.github.com 2 00 GET home-ill-pidicde1ga75frab2bae9e367d40572a58c0e309372cm 9. asset-cdn.github.com 9. Fitter headers 2 00 GET home-ill-pidicdenmyng3rn 9. asset-cdn.github.com 9. Fitter headers 2 00 GET home-ill-pidicde1g7355202964f34739137CleCc 9. asset-cdn.github.com Host: "gittybub.com" 2 00 GET informewirks-bb39ac7449404040f01c97355202964f347391837CleCc 9. asset-cdn.github.com Accept-texchinglappiCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/Atml.sml.gplCaton/A	St	atus	Method	File	Doma	i <mark>Headers</mark> Cookies Params Respo
200 GET / Gett / Request method: GET Request method: GET 200 GET fnameworks:-C07.66f.b0/2b556f.a05367364:60866b23de6b23de6b23de5b3 assetscdn.github.co Status code: 200 0K 200 GET github-4d14439300001ffc6d6d363673fcef8a6e41fd9e74776dc215fa2 assetscdn.github.co Assetscdn.github.co Filter headers 200 GET home-ill-build.png?sn assetscdn.github.co Request method: GET Filter headers 200 GET home-ill-build.png?sn assetscdn.github.co Request headers (1980 KB) 200 GET home-ill-poiets.png?sn assetscdn.github.co Host: "github.com" 200 GET nome-ill-patform.png?sn assetscdn.github.co Host: "github.com" 200 GET nome-ill-patform.png?sn assetscdn.github.co Host: "github.com" 200 GET github-dd6f042d0404d0f01e735520296454f330137c0ecos assetscdn.github.co Host: "github.com" 200 GET github-dd6f04260921332f50ba89aec54469224664547989891139504d assetscdn.github.co Accept-Lencoing: "github.com" 200 GET robotoregiusrwef assetscdn.github.co		301	GET	/	🔒 www.github.com	Request URL: https://github.com/
200 GET frameworks-c07ceff402b556d1d85052fb383ca84c80e6b23dcdbla a ssets-cdn.github.c0 Status code: 200 0 K 200 GET github-4d1443930001ffcdd8d537fbce8ba641fd9e747f5dc215fa2 a ssets-cdn.github.c0 GR. filter hadders 200 GET sithub-4d1443930001ffcdd8d537fbce8ba641fd9e747f5dc215fa2 a ssets-cdn.github.c0 GR. filter hadders 200 GET inheill-build.png?sn a ssets-cdn.github.c0 Response headers (0.281 KB) 200 GET home-ill-projects.png?sn a ssets-cdn.github.c0 Response headers (0.281 KB) 200 GET home-ill-platform.png?sn a ssets-cdn.github.c0 Response headers (0.281 KB) 200 GET frameworks-bb39ae7d84d4d0ff01e57352a29264f54f3313720ecc9 a ssets-cdn.github.c0 Response headers (0.281 KB) 200 GET frameworks-bb39ae7d84d4d0ff01e57352a29264f54f3313720ecc9 a ssets-cdn.github.c0 Response headers (0.281 KB) 200 GET frameworks-bb39ae7d84d4d0ff01e57352a29264f54f3313720ecc9 a ssets-cdn.github.c0 Commettion: "texp-slive" 200 GET roboto-regular.woff a ssets-cdn.github.c0 Commettion: "texp-slive"<	•	200	GET	1	🔒 github.com	Request method: GET Remote address: 192, 30, 253, 113:443
200 GET github-4d14493930001ffc6d6d6363f5rfcf8a6e41f49c747f6dc15f3	•	200	GET	frameworks-c07e6f4b02b556d1d85052fb3853caf84c80e6b23dcdb1a	🔒 assets-cdn.github.co	o Status code: 🌒 200 OK
200 GET site-2939218000a519a750fa2b5ae9e36740f5723a58c0ec308972c7.u.	•	200	GET	github-4d14493830801ffc6d6d6363f3fcef8a6e41fd9e74776dce15fa2	🔒 assets-cdn.github.co	Version: HTTP/1.1
200 GET home-ill-build.png?sn a ssets-cdn.github.co Response headers (0.281 kB) 200 GET home-ill-projects.png?sn a ssets-cdn.github.co Host: "github.com" 200 GET home-ill-projects.png?sn a ssets-cdn.github.co Host: "github.com" 200 GET org_example_nasa.png?sn a ssets-cdn.github.co Host: "github.com" 200 GET org_example_nasa.png?sn a ssets-cdn.github.co Host: "github.com" 200 GET farmeworks-bb39ac7d440d40df01e5735520296454f339137c0ecs a ssets-cdn.github.co Accept-TexcyImgaest: "motilary.Sn.gagest." 200 GET githubdde6f40123132f501a989ac5446942464547398989f118504d a ssets-cdn.github.co Accept-TexcoImg: "gip, deflate, br" 200 GET githubdde6f40123132f501a989ac544692246e4547998989f118504d a ssets-cdn.github.co Accept-TexcoImg: "gip, deflate, br" 200 GET roboto-regular.woff a ssets-cdn.github.co Accept-TexcoImg: "gip, deflate, br" 201 GET roboto-regular.woff a ssets-cdn.github.co Accept-TexcoImg: "gip, deflate, br" 2020 GET roboto-regular.woff a ssets-cdn.github.co Accept-TexcoImg: "gip, defl	٠	200	GET	site-293f92180d0a619a750fa2b5eae9e36740f5723a59c0ec308972c70	🔒 assets-cdn.github.co	o 9. Filter headers
200 GET mome-ill-work.png?sn a sistet-cdn.github.co Request hardsers (0.28118) 200 GET mome-ill-projects.png?sn a sistet-cdn.github.co Host: "github.com" 200 GET mome-ill-projects.png?sn a sistet-cdn.github.co Host: "github.com" 200 GET mome-ill-projects.png?sn a sistet-cdn.github.co Host: "github.com" 200 GET rameworks-bb33se7d84d4d06f01e573552829d6454f33137c0eces a sistet-cdn.github.co Accept :tex/hmil spglication/html.sml.gpglication/h	•	200	GET	home-ill-build.png?sn	🔒 assets-cdn.github.co	o 🕨 Response headers (1.988 KB)
200 GET is home-ill-projects.png?sn is assets-cdn.github.co 200 GET is home-ill-platform.png?sn is assets-cdn.github.co 200 GET is mew-ill-platform.png?sn is assets-cdn.github.co 200 GET is mew-ill-platform.png?sn is assets-cdn.github.co 200 GET is meworks-bb/39ac7484440d6f01e57355202964f54f33137c0ecc9 is assets-cdn.github.co 200 GET github-de68f49123132f5bb/89ac644692246645749898911984 is assets-cdn.github.co 200 GET github-de68f49123132f5b/89a9ac6446922466457499898911984 is assets-cdn.github.co 200 GET roboto-regular.woff assets-cdn.github.co 200 GET roboto-regular.woff assets-cdn.github.co 200 GET roboto-lightwwff assets-cdn.github.co 200 GET roboto-lightwwff assets-cdn.github.co 201 GET roboto-lightwwff assets-cdn.github.co 2020 GET roboto-lightwwff assets-cdn.github.co 203 GET roboto-lightwwff assets-cdn.github.co 204 OPTIONS stat apj.g	•	200	GET	💽 home-ill-work.png?sn	🔒 assets-cdn.github.co	o 🔻 Request headers (0.281 KB)
200 GET in home-ill-platform.png?in in assets-cdn.github.o 200 GET org_example_nasa.png?in in assets-cdn.github.o 200 GET frameworks-bb39ac1d848d4dbf1ef355c222964554f33137c1ecc9 in assets-cdn.github.o 200 GET github-4de68f49123132f5b0899ac544692246e4547398b9119b089119b04 in assets-cdn.github.o 200 GET github-4de68f49123132f5b0899ac544692246e4547998b99119b04 in assets-cdn.github.co 200 GET roboto-regular.woff in assets-cdn.github.co 200 GET roboto-regular.woff in assets-cdn.github.co 200 GET roboto-regular.woff in assets-cdn.github.co 200 GET roboto-lightwoff in assets-cdn.github.co 200 GET roboto-lightwoff in assets-cdn.github.co 201 GET roboto-lightwoff in assets-cdn.github.co 2020 GET roboto-lightwoff in assets-cdn.github.co 203 GET page_view?dimensions[page]=https://github.com/&dimension ic collector.github.com 204 OPTINNS stats in apj.github.com 205 POST	•	200	GET	a home-ill-projects.png?sn	assets-cdn.github.co	o Host: "github.com"
200 GET org_example_nasa.png?sn assets-cdn.github.co 200 GET framework-bb39ac7d848d40d6ff1e67355e282964f54f39137c0ecc9 assets-cdn.github.co 200 GET github-4de68f491231275b089acc54469c246e4547998b9118504d assets-cdn.github.co 200 GET github-4de68f491231275b089acc54469c246e4547998b9118504d assets-cdn.github.co 200 GET mone-hero.jpg?sn assets-cdn.github.co 200 GET roboto-regular.worff assets-cdn.github.co 200 GET roboto-regular.worff assets-cdn.github.co 200 GET roboto-regular.worff assets-cdn.github.co 200 GET roboto-regular.worff assets-cdn.github.co 200 GET roboto-lightwoff assets-cdn.github.co 200 GET roboto-lightwoff assets-cdn.github.co 200 GET page_view?dimensions/page]=https://github.com/&dimensio collector.github.com 201 OPTIONS stat apj.github.com	•	200	GET	home-ill-platform.png?sn	assets-cdn.github.co	User-Agent: "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0"
200 GET frameworks-bb39ae7d848d40d6f01e673552202964f54f339137c0ecc9	•	200	GET	org_example_nasa.png?sn	assets-cdn.github.co	Accept: text/numi.applicador/vxnmi.applicador/vxmi;q=0.5; / ;q=0.6
200 GET github-4de68/49123132f5b0a89aec546492246e4547998b99118504d A szstet-cdn.github.co Connection: "keep-alive" 200 GET Mone-hero.jpg?in A szstet-cdn.github.co 200 GET roboto-regular.woff A szstet-cdn.github.co 200 GET roboto-regular.woff A szstet-cdn.github.co 200 GET roboto-regular.woff A szstet-cdn.github.co 200 GET roboto-right.woff A szstet-cdn.github.co 200 GET collect A www.google-analytic 200 GET jage_view?dimensions/page]=https://github.com/&dimensio A collector.github.pom 201 OPTIONS stats A spi.github.com 202 POST stats A spi.github.com	•	200	GET	frameworks-bb39ae7d848d40d6f01e67355e282964f54fa39137c0ecc9	assets-cdn.github.co	Accept-Encoding: "gzip, deflate, br"
200 GET Manne-herojpg?an	•	200	GET	github-4de68f49123132f5b0a89aec54469c246e4547998b891f18504d	assets-cdn.github.co	o Connection: "keep-alive"
200 GET roboto-regular.woff	•	200	GET	🌃 home-hero.jpg?sn	assets-cdn.github.co	o
200 GET roboto-medium.woff assets-cdn.github.co 200 GET roboto-light.woff assets-cdn.github.co 200 POST collect www.google-analyti 200 GET page_view?dimensions[page]=https://github.com/&dimensio collector.githubaps. 201 OPTIONS stats apji.github.com	•	200	GET	roboto-regular.woff	assets-cdn.github.co	0
200 GET roboto-light.woff assets-cdr.github.co 200 POST collect www.google-analytic 200 GET page_view?dimensions[page]=https://github.com/&dimensio collector.githubapp.i 204 OPTIONS stats ap.igithub.com 200 POST stats ap.igithub.com	•	200	GET	roboto-medium.woff	assets-cdn.github.co	0
200 POST collect www.google-analyti 200 GET page_view?dimensions[page]=https://github.com/&dimension collector.githubapp.i 204 OPTIONS stats apj.github.com 200 POST stats apj.github.com	•	200	GET	roboto-light.woff	assets-cdn.github.co	0
200 GET page_view?dimensions[page]=https://github.com/&dimensio	•	200	POST	collect	🔒 www.google-analyti	ju li
204 OPTIONS stats ▲ api.github.com 200 POST stats ▲ api.github.com	•	200	GET	page_view?dimensions[page]=https://github.com/&dimensio	a collector.githubapp.	
● 200 POST stats	•	204	OPTIONS	stats	api.github.com	
	•	200	POST	stats	🔒 api.github.com	

A POST request example:

iai	Headers	Cookies	Params	Response	Timings	Security	1	^o review
	Request URL: https://g	ithub.com/join						
со	Request method: POST							
co.	Status code: 200 0V	.253.112:443				Editar	nd Resend	Raw headers
co	Version: HTTP/1.1							
co	Silter headers							
co	▶ Response headers (2.182	? KB)						
∕tic	🔻 Request headers (0.720 ł	KB)						
n.i	Host: "github.com"							
	User-Agent: "Mozilla/5	.8 (Windows NT 6.1; WOW	/64; rv:47.0) Gecko/20100101 F	Firefox/47.0"				
-ui	Accept: "text/html,appl	ication/xhtml+xml,applica	ation/xml;q=0.9,*/*;q=0.8"					
p.,	Accept-Language: "en-	US,en;q=0.5"						
	Accept-Encoding: "gzip	, deflate, br"						
	Referer: "https://githul	b.com/"						
	Cookie: "logged_in=no;	_gh_sess=eyJzZXNzaW9u	X2lkIjoiYTQxM2FiNWFmNDN	11NDgzYzA3ZGViYzE5OT4	279606; _octo=GH1.1.149998	86203.1484279606; tz=Amer	ica%2FLos_	Angeles; _gat=1"
	Connection: "keep-alive	e"						
	TRequest headers from u	pload stream (0.064 KB)						
	Content-Type: "applica	tion/x-www-form-urlence	oded"					
	Content-Length: "205"							

we can get the post body in 'Parms' label.

				0	1040030, 1,020.00	- THE ORES	
Headers	Cookies	Params	Response		Timings	Security	Preview
۹. Filter request paran	neters						
🔻 Form data							
utf8: "√"							
authenticity_token:	"11Fyb9n7/5I+j6CWbb2LRy	tBmWKQcAFpSyKFsrg1EOKHr4SFi	tfpt1tn402TRaJpHol	J+WTdrSdF	eCZKWOagDUYQ=	="	
user[login]: "a"							
user[email]: "a"							
user[password]: ""							
source: "form-home	e"						

Please reproduce the issue, and check **the packet which triggered signature 030000138** and record the whole packet information.

3. Fiddler Web Debugger

1) Download link: https://www.telerik.com/download/fiddler

Install the software and run it, see below



2) Config Fiddler to capture packet

click [Tools] -> [WinINET Options], 'Internet Properties' is opened:

Internet Prope	rties		?
eneral Securit	y Privacy Content	Connections	Programs Advanced
No set Setup.	up an Internet connec	ction, click	Setup
Dial-up and Virt	ual Private Network se	ttings ———	
			Add
			Add VPN
			Remove
Choose Setting server for a co	gs if you need to confiç nnection.	gure a proxy	Settings
Never dial	a connection		
🔵 Dial whene	ver a network connect	tion is not prese	ent
🔘 Always dia	l my default connectior	n	
Current	None		Set default
Local Area Net	vork (LAN) settings —		
LAN Settings of Choose Setting	to not apply to dial-up as above for dial-up se	connections. ettinas.	LAN settings
		-	
	0		Apply Apply

click 'LAN settings' and config as follows:

😪 Local Area Network (LAN) Settings 🛛 💌									
Automatic configuration Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.									
Use automatic configuration <u>s</u> cript Address									
Proxy server Use a proxy server for your LAN (These settings will not apply to dia -up or VPN connections).									
Address: Port: Advanced									
OK Cancel									



click 'OK'.

click [Tools] -> [Telerik Fiddler Options] -> [Connections], set the Fiddler listens on port 8888. It is according to the Internet LAN setting listening port.

Telerik Fiddler Options				L antonia -		X
General HTTPS Connections	Gateway	Appearance	Extensions	Performance	Tools	
Fiddler can debug traffic from a through Fiddler when "File > Ca	any applica apture Traf	tion that acce fic" is checked	pts a HTTP P	roxy. All WinIN	IET traffic	is routed
Fiddler listens on port: 888	38	🔲 Act	as system pi	roxy on startu	, ,	
Copy Browser Proxy Configu	ration URL	V Mo	nitor all conn	ections	Use PA	C Script
Capture FTP requests		🕅 De	faultLAN			
Allow remote computers t	VPI	N连接				
Reuse client connections						
Reuse server connections		Bypass	Fiddler for U	JRLs that start	with:	
		<-loop	oback>;			*
						~
Help Note: Changes may r	nottake eff	fect until Fiddl	er is restarte	d. ОК		Cancel

3) Config Fiddler to capture HTTPS traffic

click [Tools] -> [Telerik Fiddler Options] -> [HTTPS], configurations as follows:

Telerik Fiddler Options										
General	HTTPS	Connections	Gateway	Appearance	Extensions	Performance	Tools			
Fiddler can decrypt HTTPS sessions by re-signing traffic using self-generated certificates.										
Cap	Capture HTTPS CONNECTs									
Decrypt HTTPS traffic										
fr	from all processes Certificates generated by CertEnroll engine									
	☑ Ignore server certificate errors (unsafe)									
	Check for certificate revocation									
Protocols: <client>; ssl3;tls1.0</client>										
Skip decryption for the following hosts:										
Help	Note:	Changes may r	nottake eff	fect until Fiddl	eris restarte	d. OK		Cancel		

When you tick the "Decrypt HTTPS Traffic" checkbox, we will see a prompt:

SCARY	TEXT AHEAD: Read Carefully!	×					
C	To intercept HTTPS traffic, Fiddler generates a unique root certificate.						
20	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						

click 'Yes', the following prompt is:



click 'Yes' to install Fiddler certificate.

4) Open the Web site using Internet Explorer browser, now we can get all the traffic captured by

fiddler. Click the packet in the left panel, and the detail is in the right.

Tele	erik Fidd	ler Web Debi	ugger	and the second se					0 6 ×
Eile	Edit B	ules <u>T</u> ools	View Help 册 Fiddler	GeoEdge					
24	Replay	X · F Go	Stream 🔝 Decode	Keep: All sessions - Any Proce	ss 🕅 Fir	nd 🔝 Sav	re 🕫 🕲 i	🖉 Bro	wse 🔹 🛠 Clear Cache 🔏 TextWizard 🛛 🗁 Tearoff 🛛 MSDN Search. 😵 👘 🖏 🔂 Online 🤉
#	Re	Protocol	Host	URL	Body	Cac	Conten	Pre	🖄 Statistics 🖳 Inspectors 🎽 AutoResponder 📝 Composer 🗉 Log 🗔 Filters 🚍 Timeline 🌁 APITest
ē 1	200	HTTP	Tunnel to	github.com:443	0			ie	Headers TextView WebForms HexView Auth Cookies Raw JSON XML
尚 2	200	HTTP	Tunnel to	github.com:443	0			ie	GET https://github.com/ HTTP/1.1
3	200	HTTP	xml.tb.sogou.com	/xml.jsp?query=gi&h=F27A	928	max	text/x	SO	Host: github.com
64	200	HTTP	vinci.ie.sogou.com	/s?h=F27AF453303288C68	203		text/pla	50	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
m 5	200	HTTP	Tunnel to	github.com:443	0			50	Upgrade-Insecure-Requests: 1
1 6		HTTP	Tunnel to	dients1.google.com:443	-1			ch	DNT: 1
1 7	-	HTTP	Tunnel to	clients1.google.com:443	-1			ch	Accept-Encoding: gzip, deflate, sdch
18	-	HTTP	Tunnel to	clients1.google.com:443	-1			ch	Accept-Language: zh-CN,Zh;g=0.8
m 9	200	HTTP	Tunnel to	sp1.baidu.com:443	0			ie	conter
10	200	HTTPS	sp1.baidu.com	/5b1ZeDe5KgQFm2e88IuM	0		image/gif	ies	
₿11	200	HTTP	Tunnel to	github.com:443	0			50	
12		HTTP	Tunnel to	clients1.google.com:443	-1			ch	
013	502	HTTP	Tunnel to	www.google.com:443	582	по-с	text/ht	so	
14	200	HTTPS	aithub.com	1	60,164	по-с	text/ht	50	Find (press Ctri+Enter to highlight all) View in Notepad
m 15	200	HTTP	Tunnel to	assets-cdn.github.com:443	0			so	Cat Summer Gaus Transformer Handers Toutions Impactions Hadding Webling Auth Cathing
16	200	HTTP	Tunnel to	assets-cdn.github.com:443	0			SO	Get Syntaxview Transionner neaders rexiview Induciview nexview webview Addit Caching
m 17	200	HTTP	Tunnel to	avatars0.githubusercontent	0			so	HTTP/1 200 K
m 18	200	HTTP	Tunnel to	assets-cdn.github.com:443	0			so	Server: GitHub.com
m 19	200	HTTP	Tunnel to	assets-cdn.github.com:443	0			so	Date: Fri, 13 Jan 2017 07:05:16 GMT
1 20		HTTP	Tunnel to	clients1.google.com:443	-1			ch	Status 200 ok
121	-	HTTP	Tunnel to	clients1.google.com:443	-1			ch	Cache-Control: no-cache
1 22		HTTP	Tunnel to	clients1.google.com:443	-1			ch	Vary: X-PJAX
\$ 23		HTTP	Tunnel to	diants1 googla com:443				ch	Set-Cookie: user_sesion=bwfCDopyAURHEsi5mZmFE15030FkSpRgU_y7gy49sP_jw16-: path=/: e
									Set-Cookie:Host-user_sesion_same_site=bwfcDopAURHE3iszmeElS030FxSpRgL_y7qv49sF X-Require: 0.266601D5743eala284623054545e5 Content-security-Policy: default-src 'none'; base-uri 'self'; block-all-mixed-conten Strict-Transport-security: max-age=3184000; pin-sha256="woiwkyIovNa9ihaBciRSC7XHj1Ys9vwUGOIud X-prame-Orinos: down: onsniff
									X-XSS-Protection: 1; mode=block Vary: Accept-Encoding X-Served-By: f75e9d284bba49dfdb3929780833971c
									X-GitHub-Réquest-Id: 3D958FE2:6F44:12EE8645:58787C2B Content-Length: 60164
									<pre><locrype html=""> <html class="is-u2f-enabled" lang="en"> <html class="is-u2f-enabled" lang="en"> <html class="is-u2f-enabled"> <html class=" is-u2f-e</td></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></locrype></pre>
_									
C	_		m		-	_	_	•	End. (mean Original Tester to Mehleter all) Manual Methods

Take 'https://github.com/' as an example, the HTTPS packet is decrypted.

Please reproduce the issue, and check **the packet which triggered signature 030000138** and record the whole packet information.