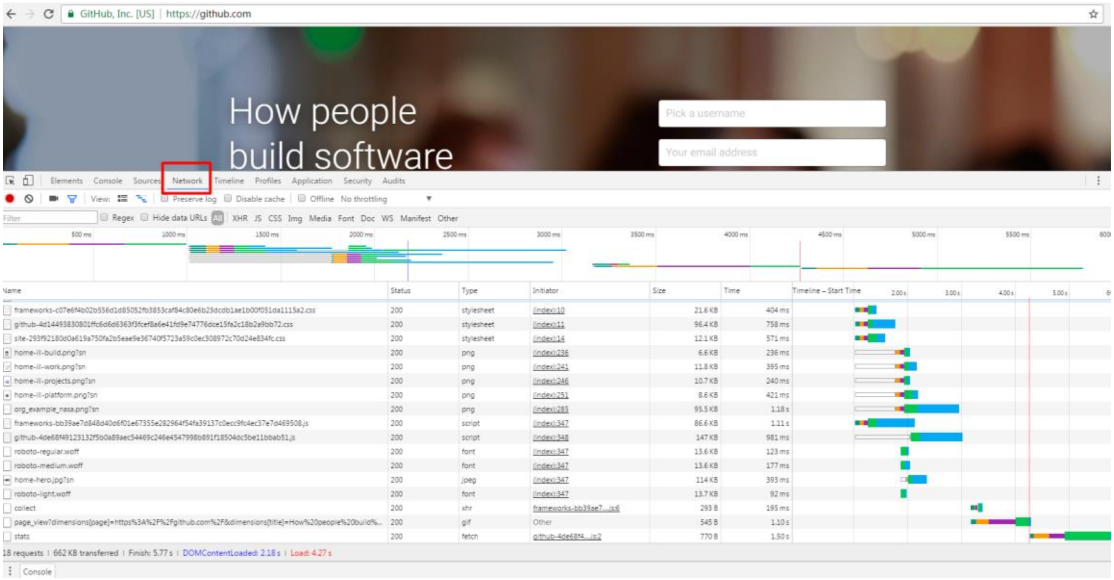
Several approaches to capture clear text of HTTPS packets

- 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:

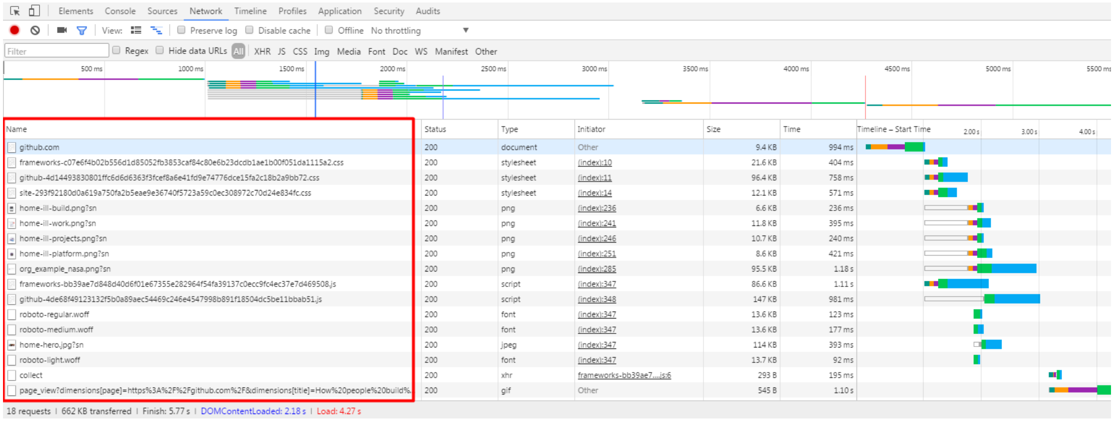


Name	Status	Type	Initiator	Size	Time
frameworks-c07e6f4b02b556d1d85052fb3853caf84c80e6b23dcdb1ae1b00f051da1115a2.css	200	stylesheet	(index):10	21.6 KB	404 ms
github-4d14493830801ffc6d6d6363f3fcef8a6e41fd9e74776dce15fa2c18b2a9bb72.css	200	stylesheet	(index):11	96.4 KB	758 ms
site-293f92180d0a619a750fa2b5eae9e36740f5723a59c0ec308972c70d24e834fc.css	200	stylesheet	(index):14	12.1 KB	571 ms
home-ill-build.png?sn	200	png	(index):236	6.6 KB	236 ms
home-ill-work.png?sn	200	png	(index):241	11.8 KB	395 ms
home-ill-projects.png?sn	200	png	(index):246	10.7 KB	240 ms
home-ill-platform.png?sn	200	png	(index):251	8.6 KB	421 ms
org_example_nasa.png?sn	200	png	(index):285	95.5 KB	1.18 s
frameworks-bb39ae7d848d40d6f01e67355e282964f54fa39137c0ecc9fc4ec37e7d469508.js	200	script	(index):347	86.6 KB	1.11 s
github-4de68f49123132f5b0a89aec54469c246e4547998b891f18504dc5be11bbab51.js	200	script	(index):348	147 KB	981 ms
roboto-regular.woff	200	font	(index):347	13.6 KB	123 ms
roboto-medium.woff	200	font	(index):347	13.6 KB	177 ms
home-hero.jpg?sn	200	jpeg	(index):347	114 KB	393 ms
roboto-light.woff	200	font	(index):347	13.7 KB	92 ms
collect	200	xhr	frameworks-bb39ae7....js:6	293 B	195 ms
page_view?dimensions[page]=https%3A%2F%2Fgithub.com%2F&dimensions[title]=How%20people%20build%...	200	gif	Other	545 B	1.10 s
stats	200	fetch	github-4de68f4....js:2	770 B	1.50 s

18 requests | 662 KB transferred | Finish: 5.77 s | DOMContentLoaded: 2.18 s | Load: 4.27 s

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

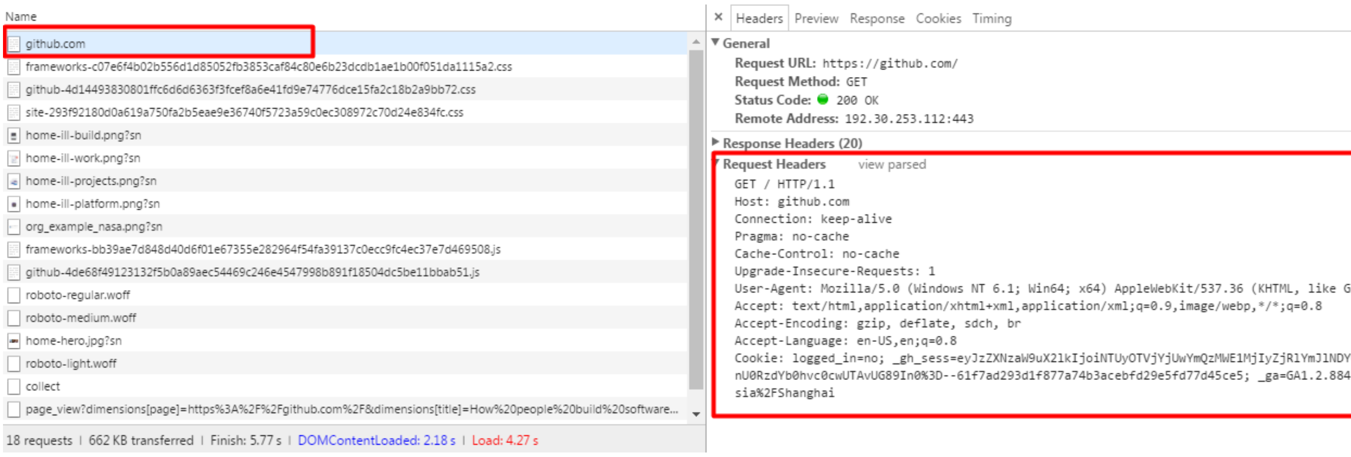
We can get the clear text information even if the packet is encrypted. For example, open the 'https://www.github.com' url, we can see all the packets interacted with the server.



Name	Status	Type	Initiator	Size	Time
github.com	200	document	Other	9.4 KB	994 ms
frameworks-c07e6f4b02b556d1d85052fb3853caf84c80e6b23dcdb1ae1b00f051da1115a2.css	200	stylesheet	(index):10	21.6 KB	404 ms
github-4d14493830801ffc6d6d6363f3fcef8a6e41fd9e74776dce15fa2c18b2a9bb72.css	200	stylesheet	(index):11	96.4 KB	758 ms
site-293f92180d0a619a750fa2b5eae9e36740f5723a59c0ec308972c70d24e834fc.css	200	stylesheet	(index):14	12.1 KB	571 ms
home-ill-build.png?sn	200	png	(index):236	6.6 KB	236 ms
home-ill-work.png?sn	200	png	(index):241	11.8 KB	395 ms
home-ill-projects.png?sn	200	png	(index):246	10.7 KB	240 ms
home-ill-platform.png?sn	200	png	(index):251	8.6 KB	421 ms
org_example_nasa.png?sn	200	png	(index):285	95.5 KB	1.18 s
frameworks-bb39ae7d848d40d6f01e67355e282964f54fa39137c0ecc9fc4ec37e7d469508.js	200	script	(index):347	86.6 KB	1.11 s
github-4de68f49123132f5b0a89aec54469c246e4547998b891f18504dc5be11bbab51.js	200	script	(index):348	147 KB	981 ms
roboto-regular.woff	200	font	(index):347	13.6 KB	123 ms
roboto-medium.woff	200	font	(index):347	13.6 KB	177 ms
home-hero.jpg?sn	200	jpeg	(index):347	114 KB	393 ms
roboto-light.woff	200	font	(index):347	13.7 KB	92 ms
collect	200	xhr	frameworks-bb39ae7....js:6	293 B	195 ms
page_view?dimensions[page]=https%3A%2F%2Fgithub.com%2F&dimensions[title]=How%20people%20build%...	200	gif	Other	545 B	1.10 s

18 requests | 662 KB transferred | Finish: 5.77 s | DOMContentLoaded: 2.18 s | Load: 4.27 s

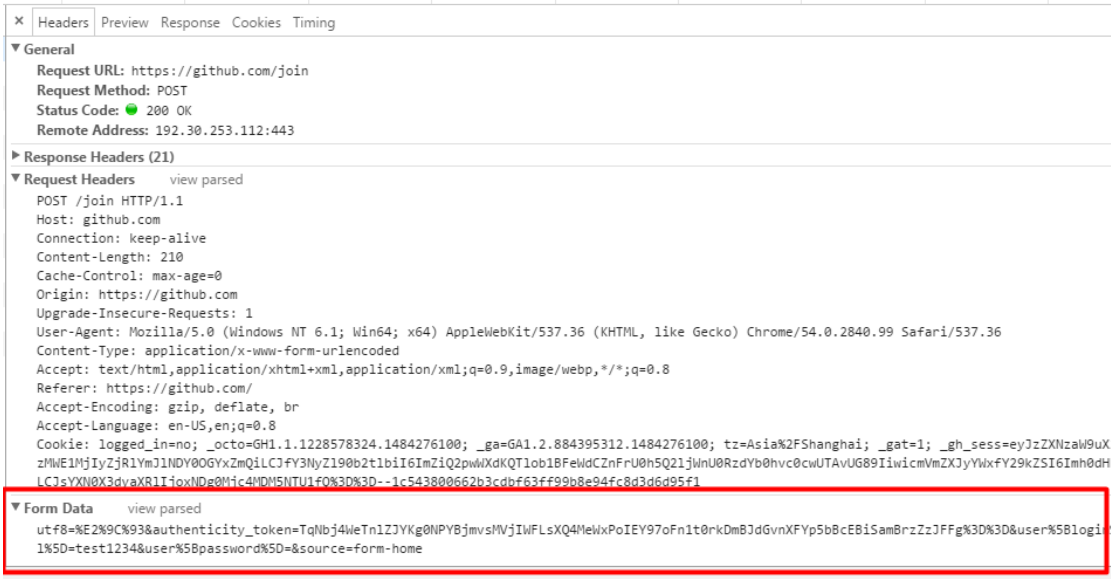
click one item in the panel. We can see the details in the right panel. See below, it's a GET request example.



```
github.com
frameworks-c07e6f4b02b556d1d85052fb3853caf84c80e6b23dcdb1ae1b00f051da1115a2.css
github-4d14493830801ffc6d6d6363f3fcef8a6e41fd9e74776dce15fa2c18b2a9bb72.css
site-293f92180d0a619a750fa2b5eae9e36740f5723a59c0ec308972c70d24e834fc.css
home-ill-build.png?sn
home-ill-work.png?sn
home-ill-projects.png?sn
home-ill-platform.png?sn
org_example_nasa.png?sn
frameworks-bb39ae7d848d40d6f01e67355e282964f54fa39137c0ecc9fc4ec37e7d469508.js
github-4de68f49123132f5b0a89aec54469c246e4547998b891f18504dc5be11bbab51.js
roboto-regular.woff
roboto-medium.woff
home-hero.jpg?sn
roboto-light.woff
collect
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
```

```
▼ General
   Request URL: https://github.com/
   Request Method: GET
   Status Code: ● 200 OK
   Remote Address: 192.30.253.112:443
▶ Response Headers (20)
▼ Request Headers     view parsed
   GET / HTTP/1.1
   Host: github.com
   Connection: keep-alive
   Pragma: no-cache
   Cache-Control: no-cache
   Upgrade-Insecure-Requests: 1
   User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like G
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
   Accept-Encoding: gzip, deflate, sdch, br
   Accept-Language: en-US,en;q=0.8
   Cookie: logged_in=no; _gh_sess=eyJzZXNzaW9uX2lkIjoiNTUyOTVjYjUwYmQzMWE1MjIyZjR1YmJ1NDY
   nU0RzdYb0hvc0cwUTAvUG89In0%3D--61f7ad293d1f877a74b3acebfd29e5fd77d45ce5; _ga=GA1.2.884
   sia%2FShanghai
```

A POST request example:



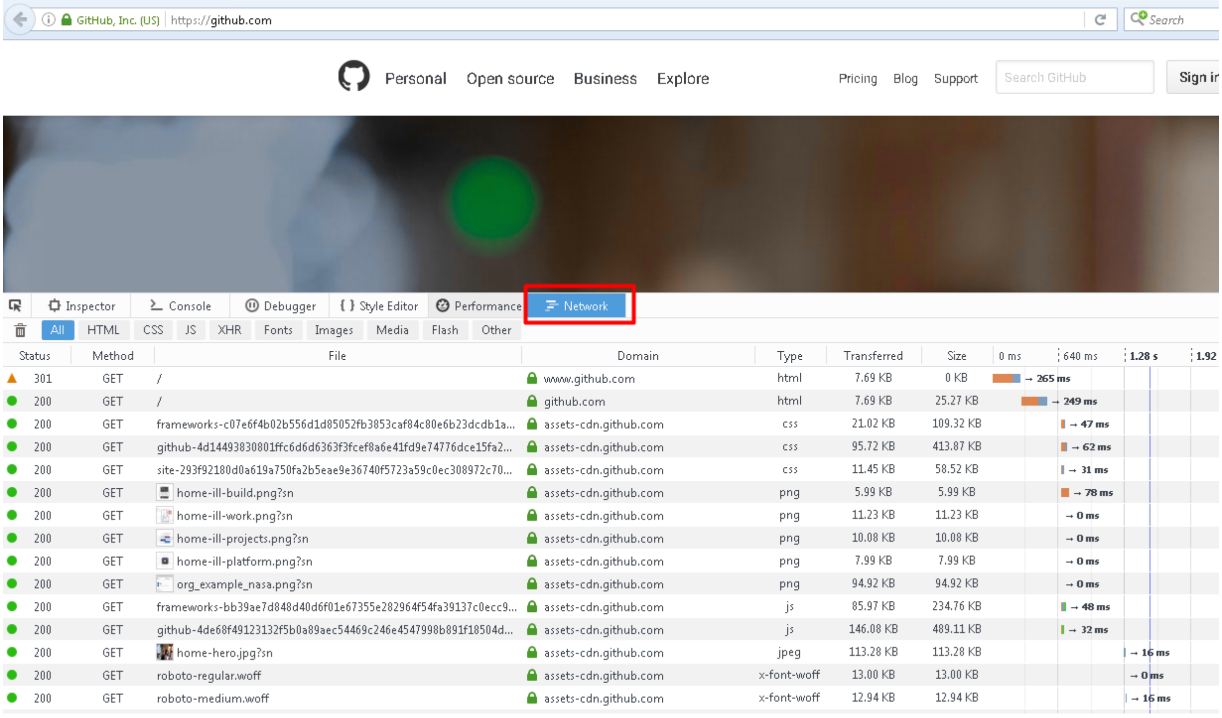
```
▼ General
   Request URL: https://github.com/join
   Request Method: POST
   Status Code: ● 200 OK
   Remote Address: 192.30.253.112:443
▶ Response Headers (21)
▼ Request Headers     view parsed
   POST /join HTTP/1.1
   Host: github.com
   Connection: keep-alive
   Content-Length: 210
   Cache-Control: 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 Gecko) 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-Encoding: gzip, deflate, br
   Accept-Language: en-US,en;q=0.8
   Cookie: logged_in=no; _octo=GH1.1.1228578324.1484276100; _ga=GA1.2.884395312.1484276100; tz=Asia%2FShanghai; _gat=1; _gh_sess=eyJzZXNzaW9uX
   zMWE1MjIyZjR1YmJ1NDY0OGYxZmQiLCJfY3NyZl90b2tlbiI6ImZiQ2pwWXdKQTlob1BFeWdCZnFrU0h5Q2ljWnU0RzdYb0hvc0cwUTAvUG89IiwicmVmZXJyYWxfY29kZSI6Imh0dH
   LCJsYXN0X3dyaXRlIjoxNDg0Mjc4MDM5NTU1fQ%3D%3D--1c543800662b3cdbf63ff99b8e94fc8d3d6d95f1
▼ Form Data     view parsed
   utf8=%E2%9C%93&authenticity_token=TqNbj4WeTnlZJYKg0NPYBjmvsMVjIWFLsXQ4MeWxPoIEY97oFn1t0rkDmBJdGvnXFYp5bBcEBiSamBrzZzJFFg%3D%3D&user%5Blogi
   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

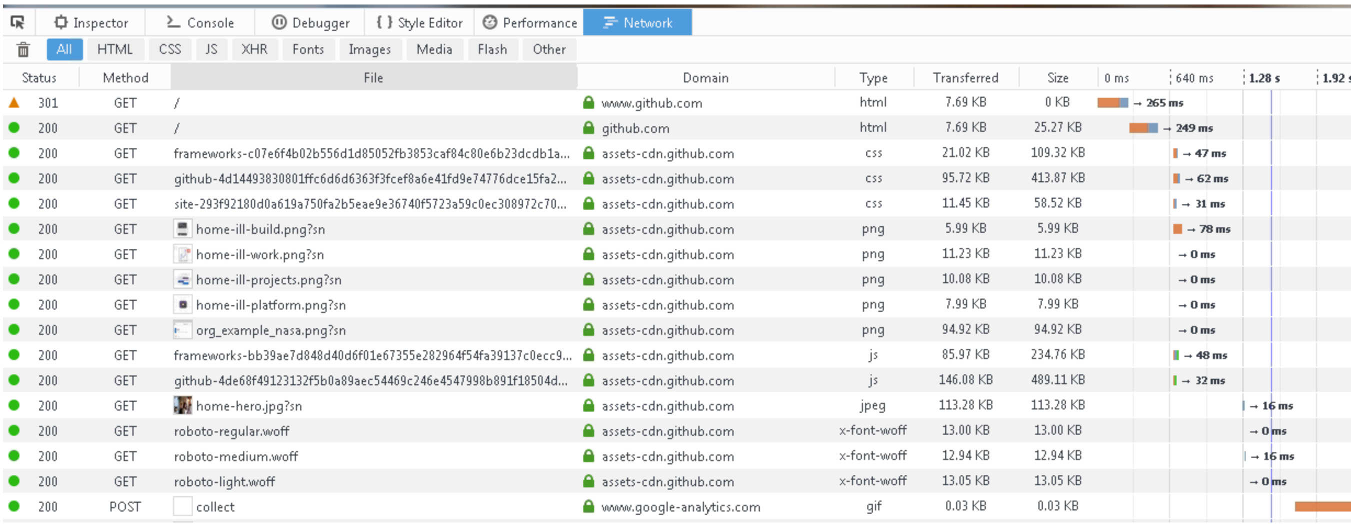
If you are using Firefox browser, please **press 'F12'** to open Web Developer. see below:



Status	Method	File	Domain	Type	Transferred	Size	0 ms 640 ms 1.28 s 1.92
▲ 301	GET	/	www.github.com	html	7.69 KB	0 KB	→ 265 ms
● 200	GET	/	github.com	html	7.69 KB	25.27 KB	→ 249 ms
● 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
● 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
● 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
● 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-bb39ae7d848d40d6f01e67355e282964f54fa39137c0ecc9...	assets-cdn.github.com	js	85.97 KB	234.76 KB	→ 48 ms
● 200	GET	github-4de68f49123132f5b0a89aec54469c246e4547998b891f18504d...	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 ms
● 200	GET	roboto-regular.woff	assets-cdn.github.com	x-font-woff	13.00 KB	13.00 KB	→ 0 ms
● 200	GET	roboto-medium.woff	assets-cdn.github.com	x-font-woff	12.94 KB	12.94 KB	→ 16 ms

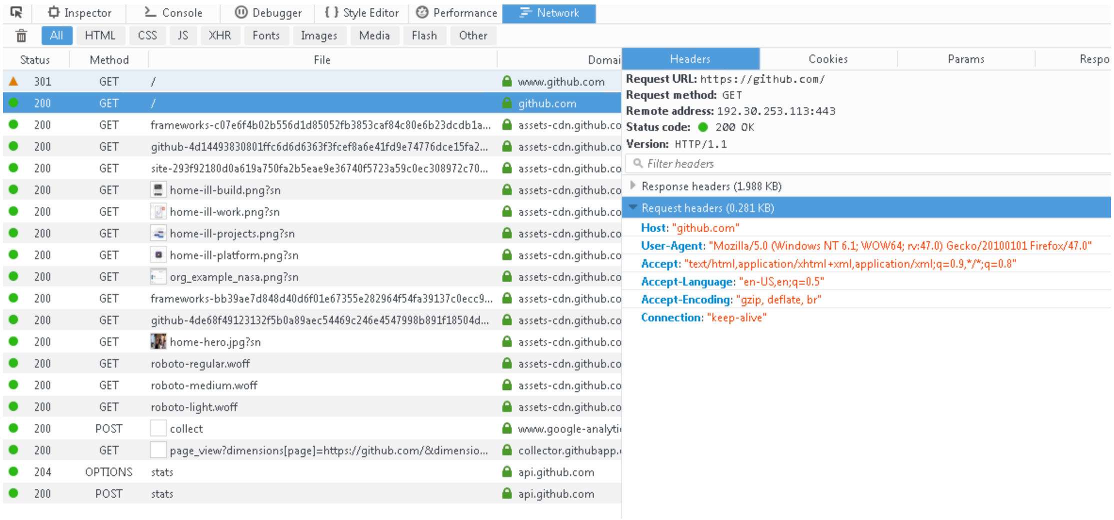
click 'Network' label to open 'Network' panel. Here we can get insights into requests and response traffic of the web pages.

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.



Status	Method	File	Domain	Type	Transferred	Size	0 ms 640 ms 1.28 s 1.92 s
▲ 301	GET	/	www.github.com	html	7.69 KB	0 KB	→ 265 ms
● 200	GET	/	github.com	html	7.69 KB	25.27 KB	→ 249 ms
● 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
● 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
● 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
● 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-bb39ae7d848d40d6f01e67355e282964f54fa39137c0ecc9...	assets-cdn.github.com	js	85.97 KB	234.76 KB	→ 48 ms
● 200	GET	github-4de68f49123132f5b0a89aec54469c246e4547998b891f18504d...	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 ms
● 200	GET	roboto-regular.woff	assets-cdn.github.com	x-font-woff	13.00 KB	13.00 KB	→ 0 ms
● 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
● 200	POST	collect	www.google-analytics.com	gif	0.03 KB	0.03 KB	

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



Status	Method	File	Domai
301	GET	/	www.github.com
200	GET	/	github.com
200	GET	frameworks-c07e6f4b02b556d1d85052fb3853caf84c80e6b23dcdb1a...	assets-cdn.github.co
200	GET	github-4d14493830801ffc6d6d6363f3fcef8a6e41fd9e74776dce15fa2...	assets-cdn.github.co
200	GET	site-293f92180d0a619a750fa2b5eae9e36740f5723a59c0ec308972c70...	assets-cdn.github.co
200	GET	home-ill-build.png?sn	assets-cdn.github.co
200	GET	home-ill-work.png?sn	assets-cdn.github.co
200	GET	home-ill-projects.png?sn	assets-cdn.github.co
200	GET	home-ill-platform.png?sn	assets-cdn.github.co
200	GET	org_example_nasa.png?sn	assets-cdn.github.co
200	GET	frameworks-bb39ae7d848d40d6f01e67355e282964f54fa39137c0ecc9...	assets-cdn.github.co
200	GET	github-4de68f49123132f5b0a89aec54469c246e4547998b891f18504d...	assets-cdn.github.co
200	GET	home-hero.jpg?sn	assets-cdn.github.co
200	GET	roboto-regular.woff	assets-cdn.github.co
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.githubapp.
204	OPTIONS	stats	api.github.com
200	POST	stats	api.github.com

Request URL: `https://github.com/`
Request method: GET
Remote address: 192.30.253.113:443
Status code: ● 200 OK
Version: HTTP/1.1

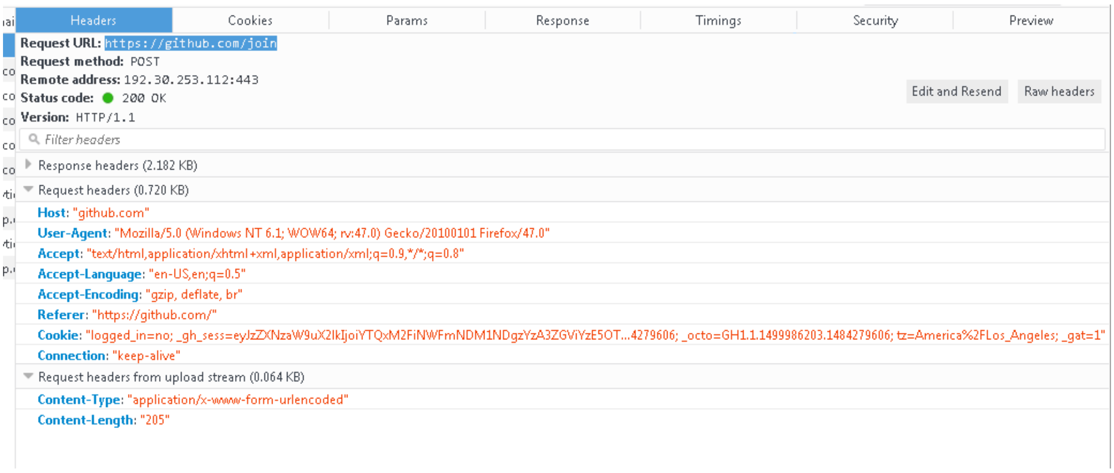
Filter headers

Response headers (1.988 KB)

Request headers (0.281 KB)

```
Host: "github.com"
User-Agent: "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0"
Accept: "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
Accept-Language: "en-US,en;q=0.5"
Accept-Encoding: "gzip, deflate, br"
Connection: "keep-alive"
```

A POST request example:



Request URL: `https://github.com/join`
Request method: POST
Remote address: 192.30.253.112:443
Status code: ● 200 OK
Version: HTTP/1.1

Filter headers

Response headers (2.182 KB)

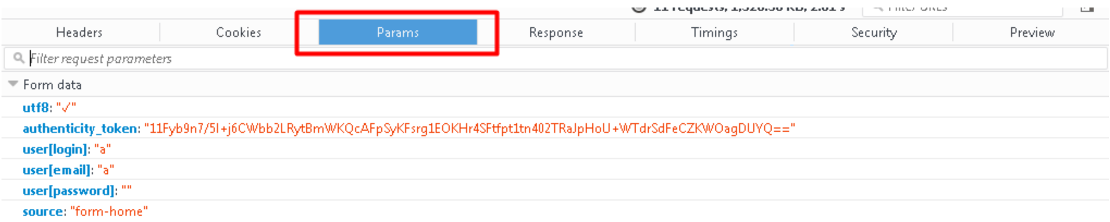
Request headers (0.720 KB)

```
Host: "github.com"
User-Agent: "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0"
Accept: "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
Accept-Language: "en-US,en;q=0.5"
Accept-Encoding: "gzip, deflate, br"
Referer: "https://github.com/"
Cookie: "logged_in=no; _gh_sess=eyJzZXNzaW9uX2lkIjoiYTQxM2FiNWFmNDM1NDgzYzA3ZGViYzE5OT...4279606; _octo=GH1.1.1499986203.1484279606; tz=America%2FLos_Angeles; _gat=1"
Connection: "keep-alive"
```

Request headers from upload stream (0.064 KB)

```
Content-Type: "application/x-www-form-urlencoded"
Content-Length: "205"
```

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



Filter request parameters

Form data

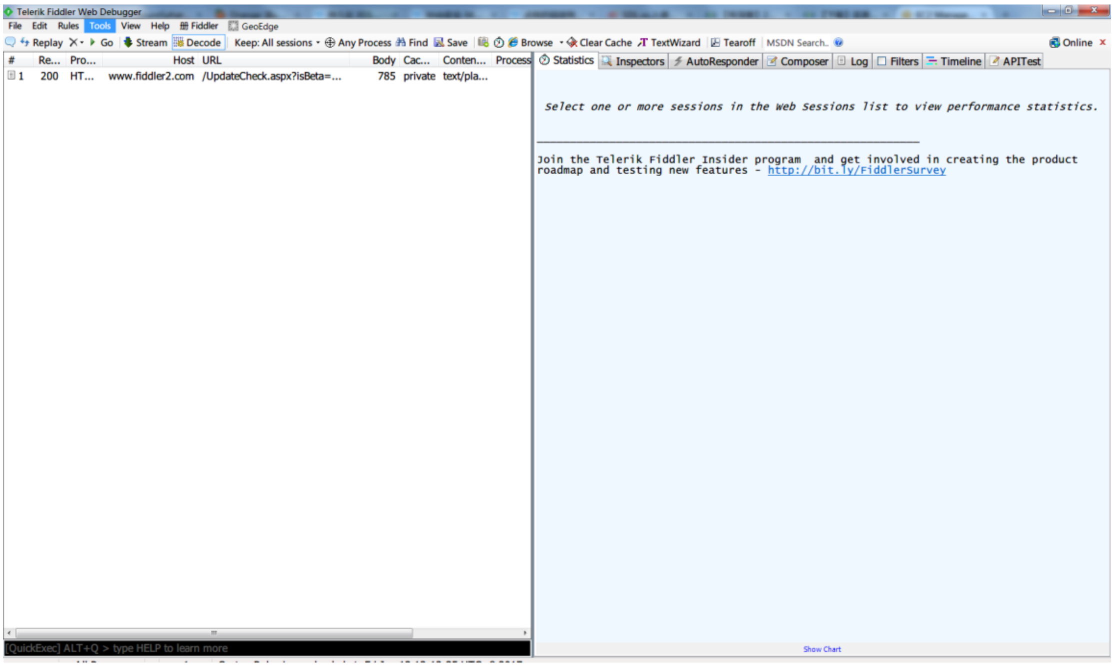
```
utf8: "✓"
authenticity_token: "11Fyb9n7/5I+j6CWbb2LRytBmWKQcAFpSyKFsrg1EOKHr4SFtfpt1tn402TRaJpHoU+WTdrSdFeCZKWOagDUYQ=="
user[login]: "a"
user[email]: "a"
user[password]: ""
source: "form-home"
```

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



Telerik Fiddler Web Debugger
File Edit Rules Tools View Help Fiddler GeoEdge
Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search... Online
Statistics Inspectors AutoResponder Composer Log Filters Timeline APITest
[QuickExec] ALT+Q > type HELP to learn more
Show Chart

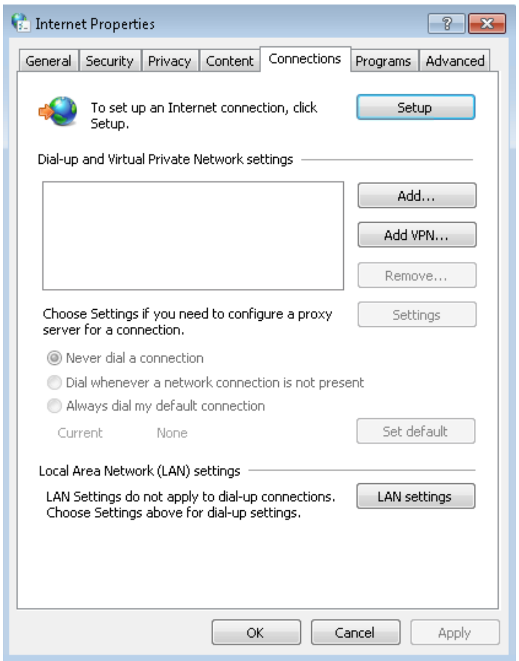
#	Re...	Pro...	Host	URL	Body	Cac...	Conten...	Process
1	200	HT...	www.fiddler2.com	/UpdateCheck.aspx?isBeta=...	785	private	text/pla...	

Select one or more sessions in the Web Sessions list to view performance statistics.

Join the Telerik Fiddler Insider program and get involved in creating the product roadmap and testing new features - http://bit.ly/FiddlerSurvey

2) Config Fiddler to capture packet

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



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

○ Dial whenever a network connection is not present

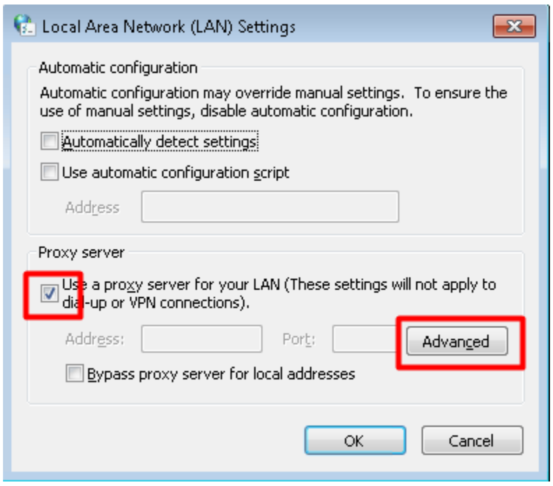
○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

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.

□ Automatically detect settings

□ Use automatic configuration script

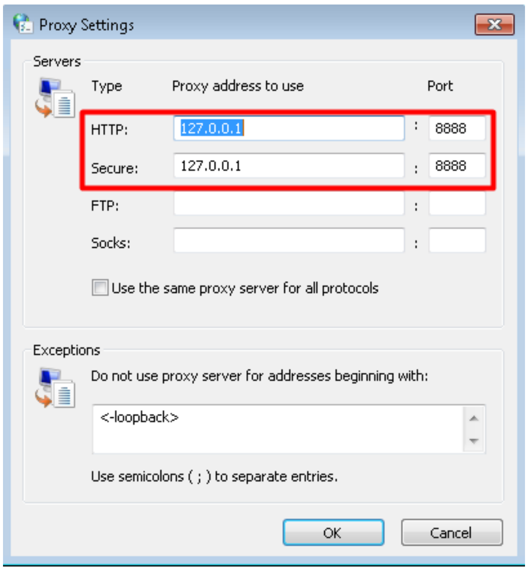
Address:

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

□ Bypass proxy server for local addresses



Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:	127.0.0.1	8888
Secure:	127.0.0.1	8888
FTP:		
Socks:		

□ Use the same proxy server for all protocols

Exceptions

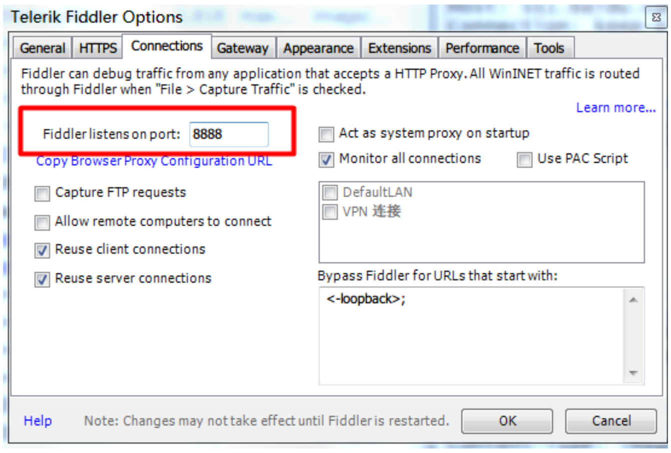
Do not use proxy server for addresses beginning with:

<-loopback>

Use semicolons (;) to separate entries.

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

Fiddler can debug traffic from any application that accepts a HTTP Proxy. All WinINET traffic is routed through Fiddler when "File > Capture Traffic" is checked.

Learn more...

Fiddler listens on port: 8888

Copy Browser Proxy Configuration URL

□ Capture FTP requests

□ Allow remote computers to connect

☑ Reuse client connections

☑ Reuse server connections

□ Act as system proxy on startup

☑ Monitor all connections □ Use PAC Script

□ DefaultLAN

□ VPN 连接

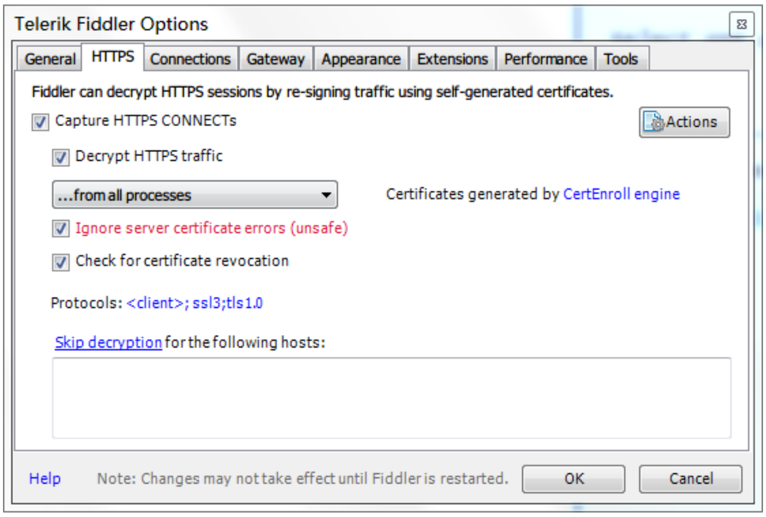
Bypass Fiddler for URLs that start with:

<-loopback>;

Help Note: Changes may not take effect until Fiddler is restarted.

3) Config Fiddler to capture HTTPS traffic

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



Fiddler can decrypt HTTPS sessions by re-signing traffic using self-generated certificates.

☑ Capture HTTPS CONNECTs

☑ Decrypt HTTPS traffic

...from all processes

Certificates generated by CertEnroll engine

☑ Ignore server certificate errors (unsafe)

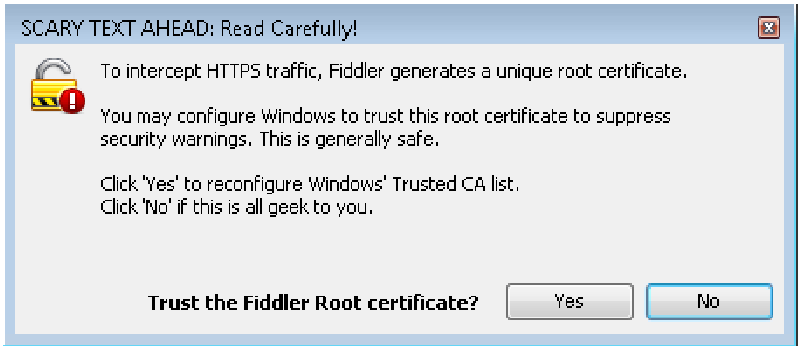
☑ Check for certificate revocation

Protocols: <client>; ssl3;tls1.0

Skip decryption for the following hosts:

Note: Changes may not take effect until Fiddler is restarted.

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



SCARY TEXT AHEAD: Read Carefully!

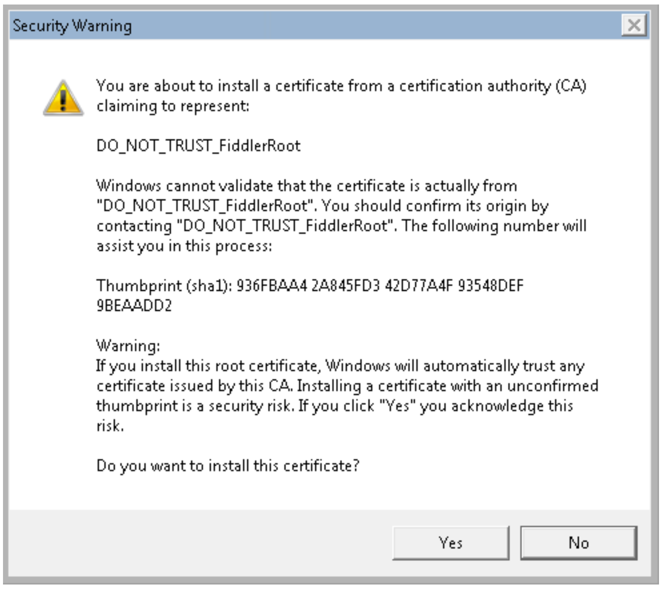
To intercept HTTPS traffic, Fiddler generates a unique root certificate.

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?

click 'Yes', the following prompt is:



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

DO_NOT_TRUST_FiddlerRoot

Windows cannot validate that the certificate is actually from "DO_NOT_TRUST_FiddlerRoot". You should confirm its origin by contacting "DO_NOT_TRUST_FiddlerRoot". The following number will assist you in this process:

Thumbprint (sha1): 936FBAA4 2A845FD3 42D77A4F 93548DEF 9BEAADD2

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

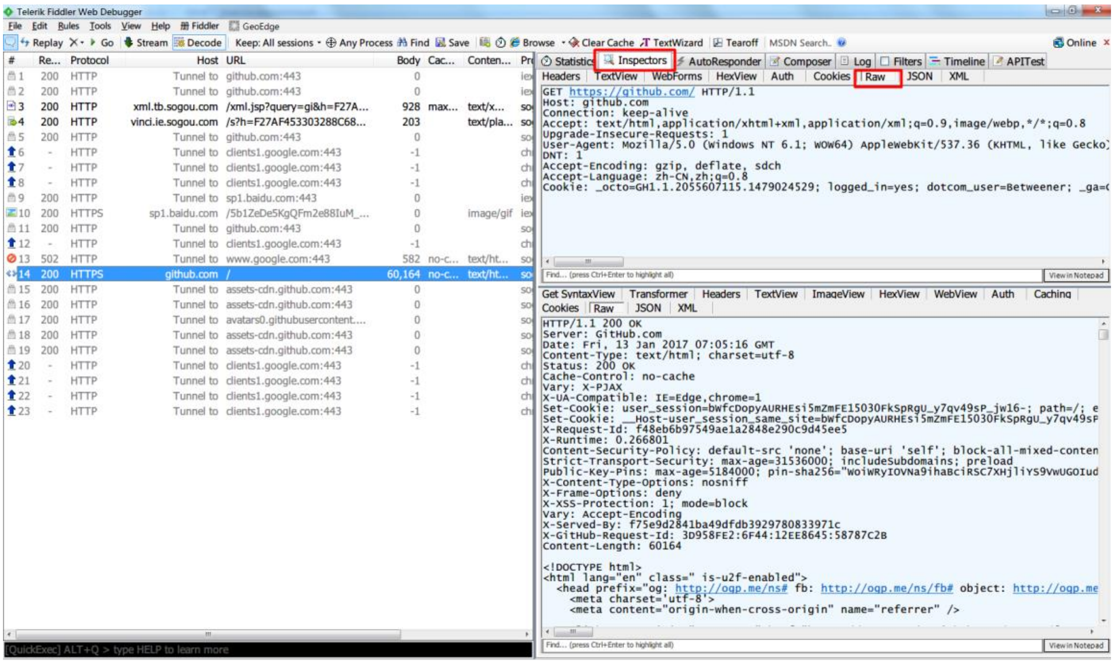
Do you want to install this certificate?

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.

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



Telerik Fiddler Web Debugger
File Edit Rules Tools View Help Fiddler GeoEdge
Replay X▾ Go Stream Decode Keep: All sessions ▾ Any Process Find Save Browse ▾ Clear Cache TextWizard Tearoff MSDN Search... Online
Statistics Inspectors AutoResponder Composer Log Filters Timeline APITest
Headers TextView WebForms HexView Auth Cookies Raw JSON XML
Find... (press Ctrl+Enter to highlight all)
View in Notepad
Get SyntaxView Transformer Headers TextView ImageView HexView WebView Auth Caching
Cookies Raw JSON XML
[QuickExec] ALT+Q > type HELP to learn more

#	Re...	Protocol	Host	URL	Body	Cac...	Conten...	Pr
1	200	HTTP	Tunnel to	github.com:443	0			ie
2	200	HTTP	Tunnel to	github.com:443	0			ie
3	200	HTTP	xml.tb.sogou.com	/xml.jsp?query=gi&h=F27A...	928	max...	text/x...	so
4	200	HTTP	vinci.ie.sogou.com	/s?h=F27AF453303288C68...	203		text/pla...	so
5	200	HTTP	Tunnel to	github.com:443	0			so
6	-	HTTP	Tunnel to	clients1.google.com:443	-1			ch
7	-	HTTP	Tunnel to	clients1.google.com:443	-1			ch
8	-	HTTP	Tunnel to	clients1.google.com:443	-1			ch
9	200	HTTP	Tunnel to	sp1.baidu.com:443	0			ie
10	200	HTTPS	sp1.baidu.com	/5b1ZeDe5KgQFm2e88IuM_...	0		image/gif	ie
11	200	HTTP	Tunnel to	github.com:443	0			so
12	-	HTTP	Tunnel to	clients1.google.com:443	-1			ch
13	502	HTTP	Tunnel to	www.google.com:443	582	no-c...	text/ht...	so
14	200	HTTPS	github.com	/	60,164	no-c...	text/ht...	so
15	200	HTTP	Tunnel to	assets-cdn.github.com:443	0			so
16	200	HTTP	Tunnel to	assets-cdn.github.com:443	0			so
17	200	HTTP	Tunnel to	avatars0.githubusercontent....	0			so
18	200	HTTP	Tunnel to	assets-cdn.github.com:443	0			so
19	200	HTTP	Tunnel to	assets-cdn.github.com:443	0			so
20	-	HTTP	Tunnel to	clients1.google.com:443	-1			ch
21	-	HTTP	Tunnel to	clients1.google.com:443	-1			ch
22	-	HTTP	Tunnel to	clients1.google.com:443	-1			ch
23	-	HTTP	Tunnel to	clients1.google.com:443	-1			ch

```
GET https://github.com/ HTTP/1.1
Host: github.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
DNT: 1
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: _octo=GH1.1.2055607115.1479024529; logged_in=yes; dotcom_user=Betweener; _ga=(
```

```
HTTP/1.1 200 OK
Server: GitHub.com
Date: Fri, 13 Jan 2017 07:05:16 GMT
Content-Type: text/html; charset=utf-8
Status: 200 OK
Cache-Control: no-cache
Vary: X-PJAX
X-UA-Compatible: IE=Edge,chrome=1
Set-Cookie: user_session=bWfcDopyAURHEsi5mZmFE15030FkSpRgU_y7qv49sP_jw16-; path=/; e
Set-Cookie: __Host-user_session_same_site=bWfcDopyAURHEsi5mZmFE15030FkSpRgU_y7qv49sP
X-Request-Id: f48eb6b97549ae1a2848e290c9d45ee5
X-Runtime: 0.266801
Content-Security-Policy: default-src 'none'; base-uri 'self'; block-all-mixed-conten
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Public-Key-Pins: max-age=5184000; pin-sha256="WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-XSS-Protection: 1; mode=block
Vary: Accept-Encoding
X-Served-By: f75e9d2841ba49dfdb3929780833971c
X-GitHub-Request-Id: 3D958FE2:6F44:12EE8645:58787C2B
Content-Length: 60164

<!DOCTYPE html>
<html lang="en" class=" is-u2f-enabled">
  <head prefix="og: http://ogp.me/ns# fb: http://ogp.me/ns/fb# object: http://ogp.me
    <meta charset='utf-8'>
    <meta content="origin-when-cross-origin" name="referrer" />
```

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