

Инструменты прокси-трафика

Урок 3





План курса





План урока

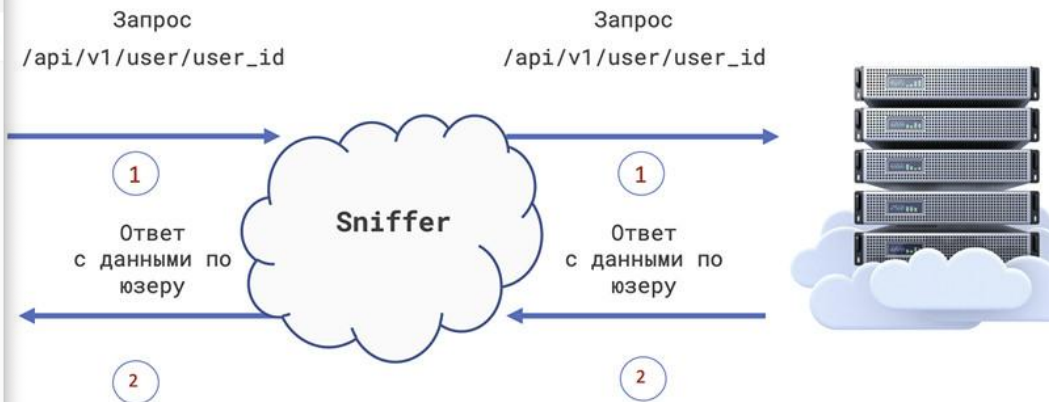
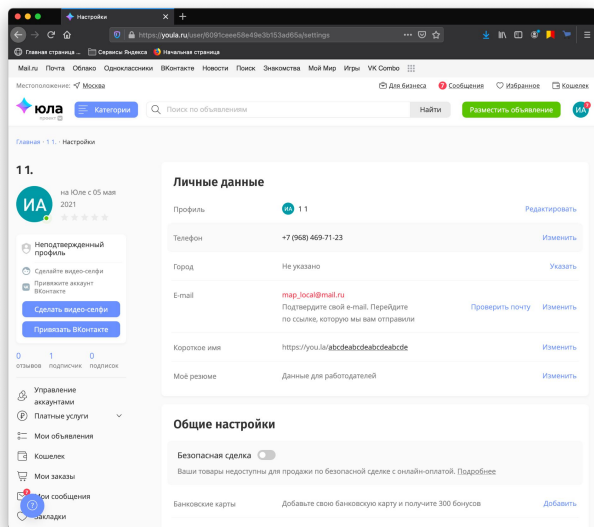
1. Что такое sniffing трафика.
2. Как осуществляется проксирование трафика.
3. Какие существуют инструменты прокси-трафика.
4. Charles Proxy.



Что такое сниффинг трафика и как он осуществляется

Сниффинг

Сниффинг — процесс мониторинга и перехвата всех пакетов, проходящих через сеть, с помощью инструментов сниффинга.





Какие существуют инструменты прокси-трафика

Progress Telerik Fiddler Web Debugger

File Edit Rules Tools View Help

WinConfig Play X Go Stream Decode Keep All sessions + Any Process Find Save Clear Cache Text Wizard Teatoff MSDN Search... Online X

#	Result	Host	URL	Body	Caching	Content-Type	Process	Comments	Cust
183	304	HTTPS	api.youla.io /files/com-on-cat-reality...	0	max-age=...		Firefox...		
184	200	HTTPS	r.yandex.ru /AS/CD/BA8A4A/breast...	50 167	max-ag...	application/...	Firefox...		
165	200	HTTP	Tunnel to cdn0.youla.io:443	716	0		Firefox...		
166	200	HTTP	Tunnel to gum.criteo.com:443	0	max-ag...		Firefox...		
167	200	HTTPS	cdn0.youla.io /files/images/360_360/SF...	27 167	max-ag...	image/jpeg	Firefox...		
168	200	HTTP	Tunnel to dnach.net:443	0	max-ag...		Firefox...		
169	200	HTTP	Tunnel to g-gbc.criteo.com:443	0	max-ag...		Firefox...		
170	200	HTTP	Tunnel to gum.gbc.criteo.com:443	0	max-ag...		Firefox...		
171	200	HTTP	Tunnel to vk.com:443	0	max-ag...		Firefox...		
172	200	HTTP	Tunnel to www.google-analytics.co...	0	max-ag...		Firefox...		
173	200	HTTP	Tunnel to rs.mal.ru:443	0	max-ag...		Firefox...		
174	200	HTTP	Tunnel to mc.yandex.ru:443	806	0		Firefox...		
175	200	HTTP	Tunnel to an.yandex.ru:443	0	max-ag...		Firefox...		
176	200	HTTP	Tunnel to gum.criteo.com:443	0	max-ag...		Firefox...		
177	200	HTTP	Tunnel to rs.mal.ru:443	0	max-ag...		Firefox...		
178	200	HTTP	Tunnel to sdwidget.criteo.com:443	0	max-ag...		Firefox...		
179	204	HTTPS	api.youla.io /api/v1/products/app_id=...	0	no cache	application/...	Firefox...		
180	200	HTTPS	mc.yandex.ru /metrika/tag.js	93 251	max-ag...	application/...	Firefox...		
181	200	HTTPS	mc.yandex.ru /metrika/tag.js	96 039	max-ag...	application/...	Firefox...		
182	200	HTTPS	rs.mal.ru /pxel/AACR7WfErSbz7qTU...	43	private	image/gif	Firefox...		
183	200	HTTPS	vk.com /t/rtp=W-KRTG-103341...	65	no-store	image/gif	Firefox...		
184	200	HTTPS	rs.mal.ru /pxel/AACR7WfErSbz7qTU...	43	private	image/gif	Firefox...		
185	200	HTTPS	an.yandex.ru /system/context.js	41 494	public	text/javascript	Firefox...		
186	302	HTTPS	mc.yandex.ru /watch/50439127?mode=...	0	private		Firefox...		
187	200	HTTP	Tunnel to an.yandex.ru:443	0	max-ag...		Firefox...		
188	200	HTTPS	mc.yandex.ru /watch/50439127/?mode=...	221	private	application/...	Firefox...		
189	200	HTTPS	gum.criteo.com /jsync?=405&r=2&v=tus...	163	private	text/javascript	Firefox...		
190	200	HTTPS	dnach.net /dna	2	no-cac...	application/...	Firefox...		
191	302	HTTPS	an.yandex.ru /meta/248298?ig=adC...	0	private		Firefox...		
192	304	HTTPS	youla.youla /build/pwa/hotfixes-to-	0	max-ag...		Firefox...		
193	200	HTTPS	an.yandex.ru /meta/248298?hot-fix-setun...	147	private	application/...	Firefox...		
194	200	HTTPS	an.yandex.ru /newid	19	no-cac...	application/...	Firefox...		
195	200	HTTPS	gem-gbc.criteo.com /newid	19	no-cac...	application/...	Firefox...		
196	200	HTTPS	an.yandex.ru /system/context.js	41 552	public	text/javascript	Firefox...		
197	200	HTTPS	www.google-analytics.js	18 817	public	text/javascript	Firefox...		
198	200	HTTPS	cdn0.youla.io /files/images/360_360/SF...	20 128	max-ag...	image/jpeg	Firefox...		
199	200	HTTPS	mc.yandex.ru /dmap/50439127?page=ur...	43	private	image/gif	Firefox...		
200	200	HTTPS	cdn0.youla.io /files/images/360_360/SF...	26 601	max-ag...	image/jpeg	Firefox...		
201	200	HTTPS	cache3.youla.io /files/images/360_360/SF...	16 532	max-ag...	image/jpeg	Firefox...		
202	200	HTTPS	cdn0.youla.io /files/images/360_360/SF...	25 487	max-ag...	image/jpeg	Firefox...		
203	200	HTTPS	cache3.youla.io /files/images/360_360/SF...	17 041	max-ag...	image/jpeg	Firefox...		
204	200	HTTPS	cdn0.youla.io /files/images/360_360/SF...	22 962	max-ag...	image/jpeg	Firefox...		
205	200	HTTPS	cdn0.youla.io /files/images/360_360/SF...	2					



Fiddler Everywhere

The screenshot displays the Fiddler Everywhere application window. The interface is divided into several sections:

- Top Bar:** Includes the application name "Fiddler Everywhere", a "FREE" badge, an "Upgrade Now" button, and a user profile "Tammy Munoz".
- Left Sidebar:** Contains a "Sessions" list with "Live Traffic (Paused)", "Login (Recorded)", and "Forgot Password (Recorded)". Below this is a "Requests" list with "Request 1" (GET), "Request 2" (POST), "Request 3" (PUT), and "Request 4" (POST).
- Main Panel:** Displays a table of recorded requests. The table has columns for #, Result, Protocol, Host, URL, and Body. The data shows 10 requests, all with a status of 200 and protocol of HTTP, originating from "Tunnel 2" to "www.fiddler2.com".
- Right Panel:** Shows the "Inspectors" tab with "Request" and "Response" sections. The "Request" section displays headers for a CONNECT request to "telemetry.dropbox.com:443". The "Response" section displays headers for an HTTP/1.1 200 Connection Established response.

#	Result	Protocol	Host	URL	Body
01	200	HTTP	Tunnel 2	www.fiddler2.com	-1
02	200	HTTP	Tunnel 2	www.fiddler2.com	0
03	200	HTTP	Tunnel 2	www.fiddler2.com	0
04	200	HTTP	Tunnel 2	www.fiddler2.com	0
05	200	HTTP	Tunnel 2	www.fiddler2.com	0
06	200	HTTP	Tunnel 2	www.fiddler2.com	-1
07	200	HTTP	Tunnel 2	www.fiddler2.com	0
08	200	HTTP	Tunnel 2	www.fiddler2.com	-1
09	200	HTTP	Tunnel 2	www.fiddler2.com	0
10	200	HTTP	Tunnel 2	www.fiddler2.com	-1

Request Headers:

```
CONNECT telemetry.dropbox.com:443 HTTP/1.1
Connection: keep-alive
connection: keep-alive
host: telemetry.dropbox.com:443
```

Response Headers:

```
HTTP/1.1 200 Connection Established
FiddlerGateway: Direct
StartTime: 11:05:17.212
Connection: close
EndTime: 11:06:32.887
ClientToServerBytes: 1509
ServerToClientBytes: 657
```




Charles Proxy

Charles Proxy interface showing a list of intercepted requests and the selected response details.

Structure **Sequence**

Code	Method	Host	Path	Start	Duration	Size	Status
200	GET	api.youla.io	/api/v1/user/5e6222bbbedcc5975d2375f8?adv_id=E01A2BD7-9AE2-4347-934E-4AC9...	19:00:53	118 ms	19.50 KB	Complete
200	POST	api.youla.io	/api/v1/user/5e6222bbbedcc5975d2375f8/push?adv_id=E01A2BD7-9AE2-4347-934E-4...	19:00:53	62 ms	1.17 KB	Complete
200	POST	api.youla.io	/api/v1/user/5e6222bbbedcc5975d2375f8/push?adv_id=E01A2BD7-9AE2-4347-934E-4...	19:00:53	52 ms	1.17 KB	Complete
200	POST	api.youla.io	/api/v1/user/5e6222bbbedcc5975d2375f8/push?adv_id=E01A2BD7-9AE2-4347-934E-4...	19:00:53	52 ms	1.17 KB	Complete
200	GET	api.youla.io	/api/v1/user/5e6222bbbedcc5975d2375f8?adv_id=E01A2BD7-9AE2-4347-934E-4AC9...	19:00:54	112 ms	2.32 KB	Complete
200	POST	api.youla.io	/api/v1/user/5e6222bbbedcc5975d2375f8/push?adv_id=E01A2BD7-9AE2-4347-934E-4...	19:00:55	49 ms	1.17 KB	Complete
200	CONNECT	sun1-94.userapi.com		19:00:56	2 m 0 s	155.91 KB	Complete
200	GET	api.youla.io	/api/v1/user/5e6222bbbedcc5975d2375f8?adv_id=E01A2BD7-9AE2-4347-934E-4AC9...	19:00:57	89 ms	2.32 KB	Complete
200	GET	api.youla.io	/api/v1/users/coupons?adv_id=E01A2BD7-9AE2-4347-934E-4AC96D9B447C&app_id=...	19:00:57	53 ms	891 bytes	Complete
200	GET	api.youla.io	/api/v1/user/5e6222bbbedcc5975d2375f8/profile/products?adv_id=E01A2BD7-9AE2-43...	19:00:57	158 ms	4.24 KB	Complete
200	POST	api.youla.io	/api/v1/user/5e6222bbbedcc5975d2375f8/push?adv_id=E01A2BD7-9AE2-4347-934E-4...	19:00:57	81 ms	1.17 KB	Complete
200	CONNECT	sun1-30.userapi.com		19:00:57	3 m 0 s	12.69 KB	Complete
200	CONNECT	sun9-45.userapi.com		19:00:57	31.80 s	271.20 KB	Complete
200	CONNECT	sun1-97.userapi.com		19:00:59	3 m 0 s	17.38 KB	Complete
404	GET	api.youla.io	/api/v1/stories/user/5e6222bbbedcc5975d2375f8/preview?adv_id=E01A2BD7-9AE2-43...	19:01:10	57 ms	952 bytes	Complete

Filter: user

Overview **Request** **Response** **Summary** **Chart** **Notes**

```

{
  "last_name": "\u041f\u0435\u0442\u0440\u0438\u0442\u0430\u0442\u0430",
  "display_phone_num": "79250762995",
  "is_phone_verified": true,
  "email": null,
  "date_email_confirm": null,
  "account": {
    "is_bonus_card_bind_applied": false,
    "bonus_code": "xUgcNG",
    "bonus_cnt": 15,
    "bonus_per_share": 15,
    "is_bonus_verify_email_applied": false
  },
  "wallet": {
    "payment_enabled": true,

```



Mitmproxy

```

~/mitmproxy/mitmproxy
Flows
>> POST https://events.reddit.com/v2 HTTP/2.0
    ← 200 [no content] 1.47s
GET https://z.moatads.com/redditadzerk107343723525/m
    oatad.js
    ← 200 application/x-javascript 74.99k 853ms
GET https://adservice.google.co.nz/adsid/integrator.js?domain=www.reddit.com HTTP/2.0
    ← 200 application/javascript 107b 1.44s
GET https://adservice.google.com/adsid/integrator.js?domain=www.reddit.com HTTP/2.0
    ← 200 application/javascript 107b 1.20s
GET https://securepubads.g.doubleclick.net/gpt/pubad_s_impl_181.js HTTP/2.0
    ← 200 text/javascript 61.73k 1.37s
GET https://github.com/
    ← 200 text/html 13.49k 989ms
GET https://px.moatads.com/pixel.gif?e=17&i=REDDITADZERK1&hp=1&cm=1&kq=2&hq=0&hs=0&hu=0&hr=0&ht=1&bq=0&f=1&nh=1&tw...
    ← 200 image/gif 43b 184ms
GET https://assets-cdn.github.com/assets/frameworks-7a12427f1445.css
    ← 200 text/css 22.66k 340ms
GET https://assets-cdn.github.com/assets/github-fca0cb55603c.css
    ← 200 text/css 92.73k 548ms
GET https://assets-cdn.github.com/assets/site-e1e1bc98a53e.css
    ← 200 text/css 9.68k 295ms
GET https://assets-cdn.github.com/assets/frameworks-

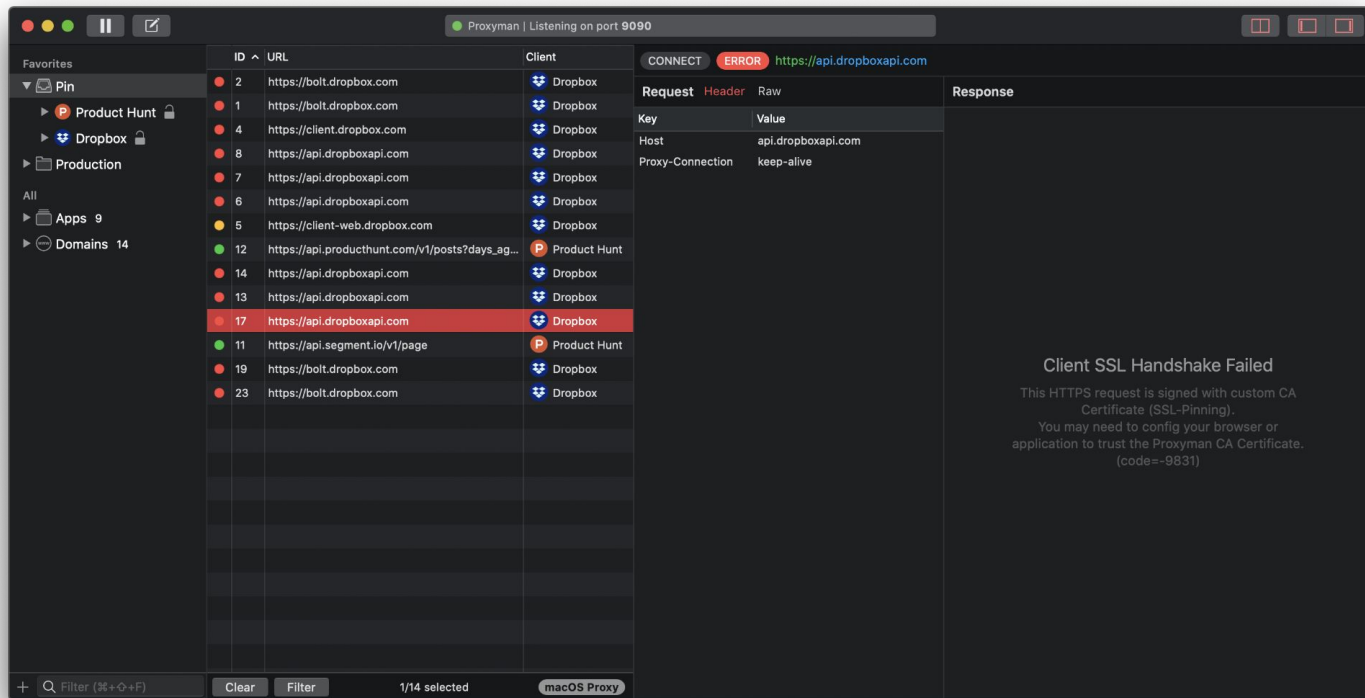
Command Reference
browser.start
console.bodyview flow choice
console.bodyview.options -> [str]
console.choose str [str] cmd *arg
console.choose.cmd str cmd cmd *arg
console.command *str
console.command.set str
console.edit.focus choice
console.edit.focus.options -> [str]
console.exit
>> console.flowview.mode -> str
console.flowview.mode.options -> [str]
console.flowview.mode.set choice
console.grideditor.add
console.grideditor.delete
console.grideditor.editor
console.grideditor.insert
console.grideditor.load path
console.grideditor.load_escaped path
console.grideditor.save path
console.intercept.toggle
console.key.bind [str] str cmd *arg
console.key.contexts -> [str]
console.key.edit.focus
console.key.execute.focus

Command Help
Get the display mode for the current flow view.

[1/56] [*:8080]
```



Proxyman





Демо Charles Proxy



Спасибо
за внимание

