MISC01 – Fiddler , questo sconosciuto

Carmine Punella
carmine.punella@gmail.com - @cpunella
Development engineer @ modomodo
Microsoft MVP

Grazie a

Sponsor

Agenda

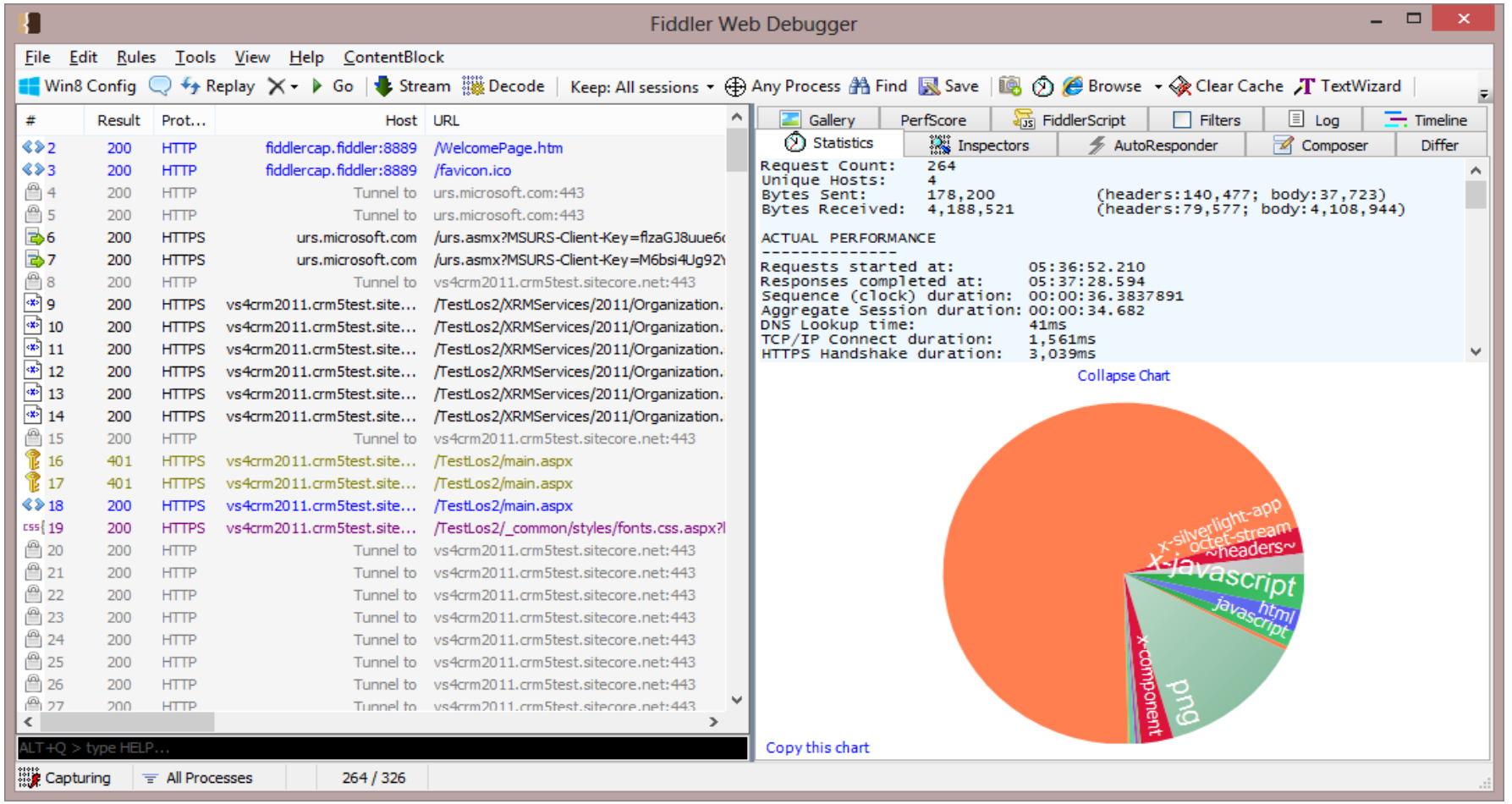
- Da dove iniziare
- Il traffico nelle nostre mani
  - Monitoring
  - Analysis
  - Manipulation
- HTTPS
- Varie ed eventuali

Da dove iniziare

Installiamolo

- E' Free: scaricabile da qui: http://www.telerik.com/fiddler
- Ci sono due versioni .NET 2 / 4
- Disponibile anche per Mac e Linux (Mono)
- Richiede almeno 512MB di Ram (2GB consigliati)

Primo sguardo

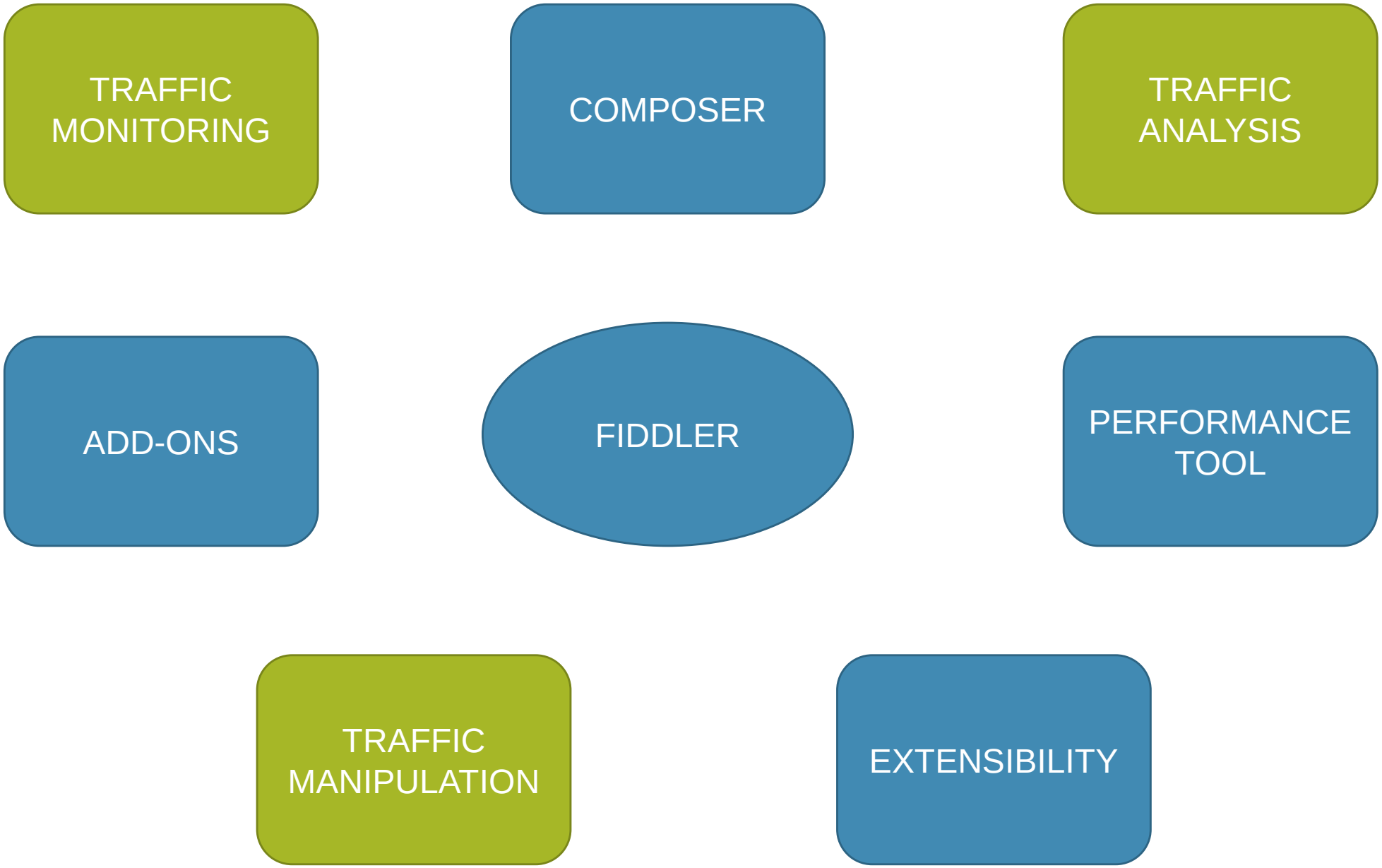


Quando usare Fiddler

- Ho bisogno di vedere il traffico web di un browser, un servizio o anche di un device
- Devo modificare una request/respone
- Devo decriptare una richiesta in HTTPs
- Ho bisogno di lavorare offline
- Devo gestire in automatico delle risposte, filtrarle, sostituire l'host per puntare su un altro server
- Voglio sviluppare software più robusto

Quando no

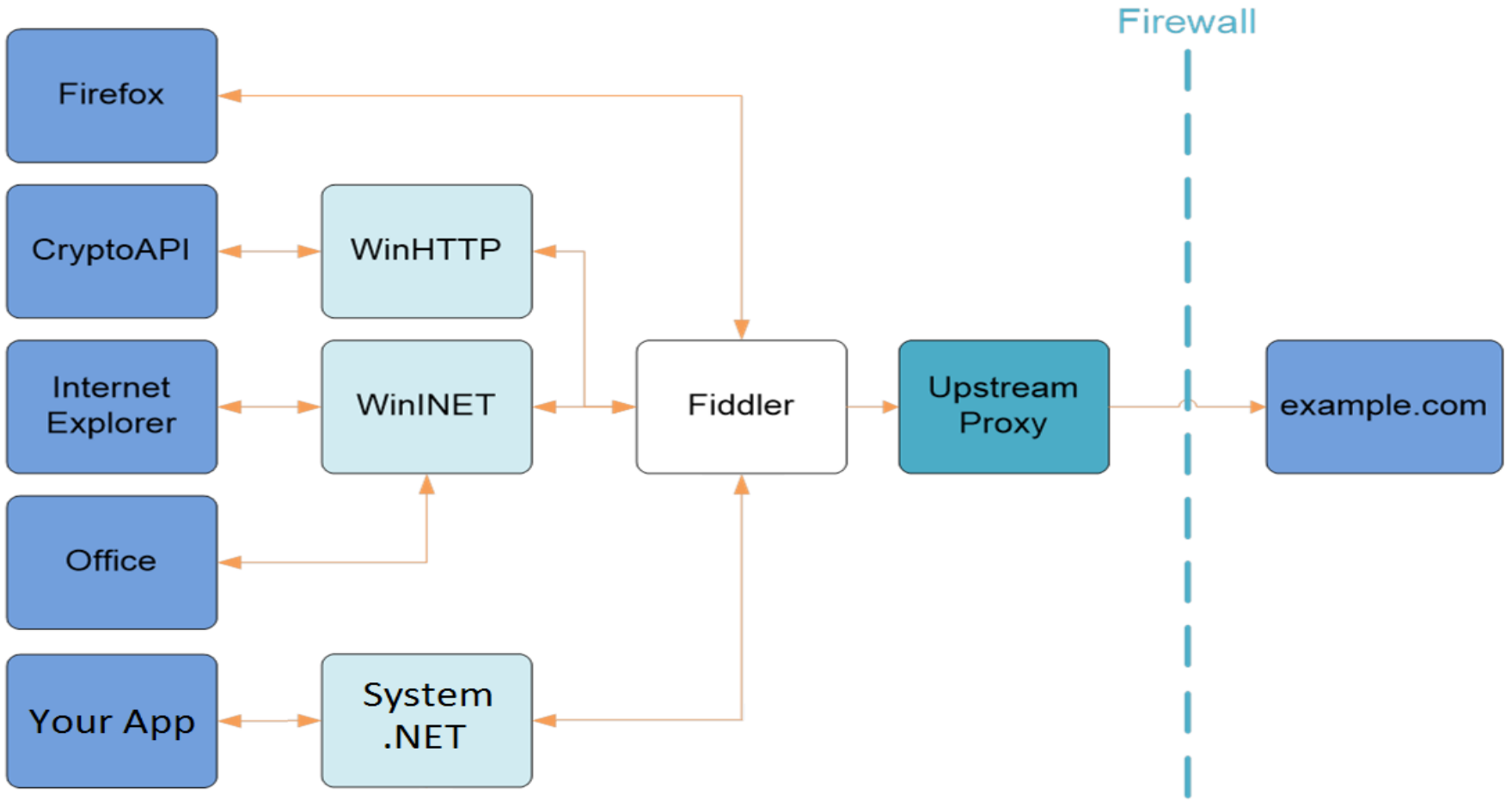
- Debuggare richieste con un protocollo diverso da HTTP/FTP
- Controllare richieste molto grandi, perché lavora in memoria (max 2GB)
- Rimuovere magicamente i bug per te ☺


TRAFFIC MONITORING
COMPOSER
TRAFFIC ANALYSIS
ADD-ONS
FIDDLER
PERFORMANCE TOOL
TRAFFIC MANIPULATION
EXTENSIBILITY

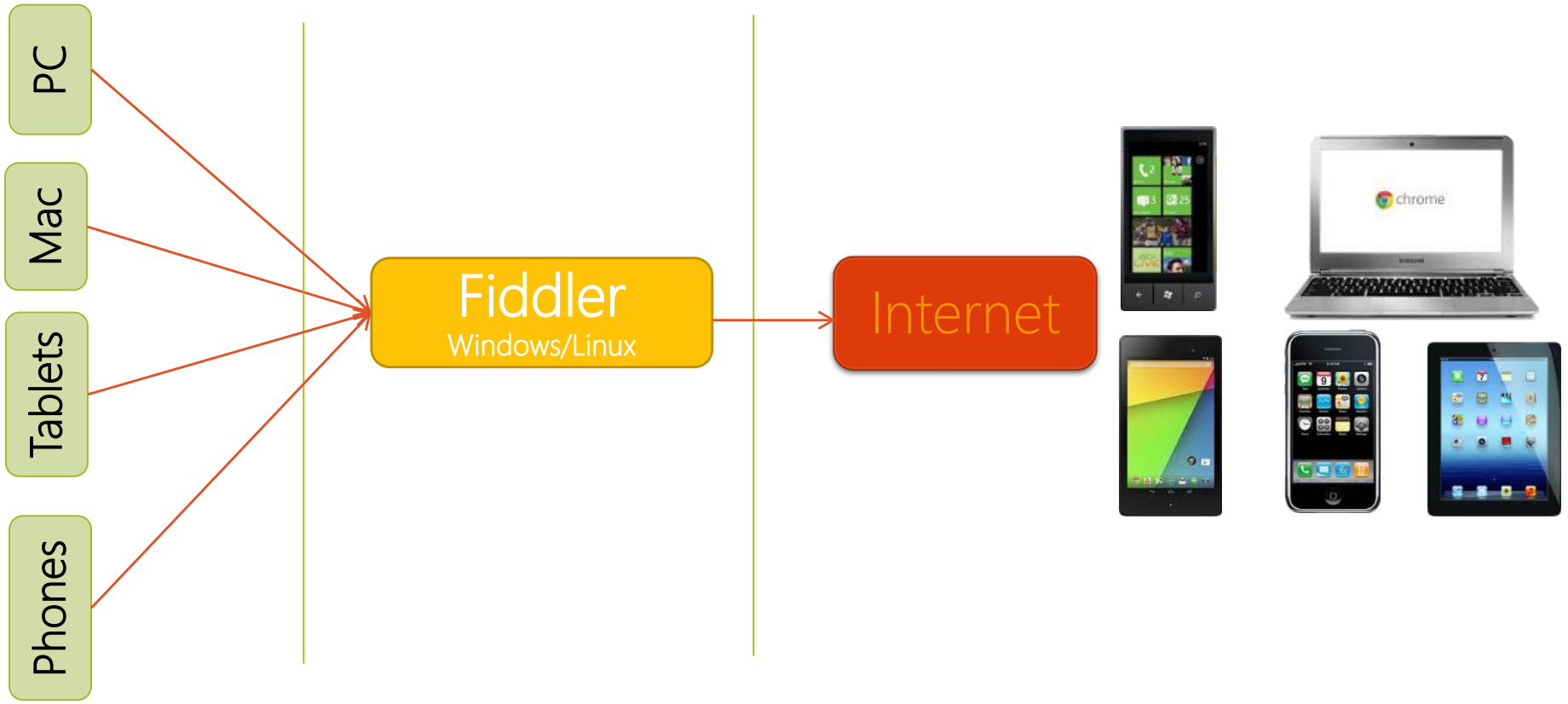
Il traffico nelle nostre mani

Traffic Monitoring

Architettura



Usando i device



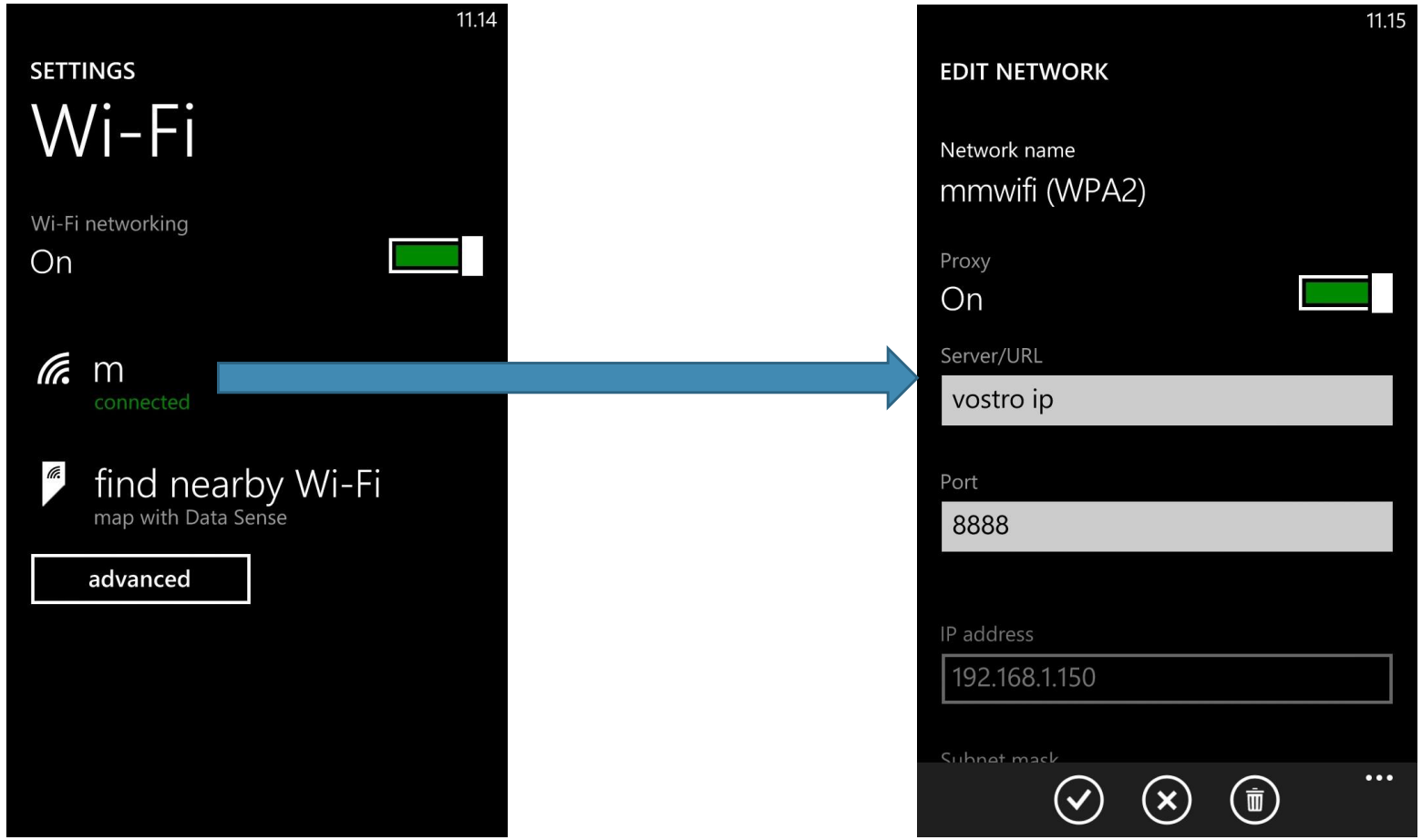
Windows Phone Emulator

- Abilitare la possibilità di connessione da pc remote (Tools→ Connections)
- Lanciare il comando
  - **prefs set fiddler.network.proxy.registrationhostname *HostName***

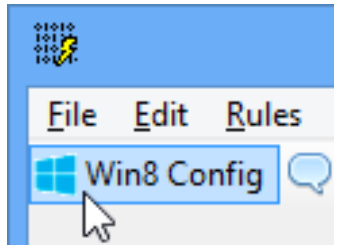
Post

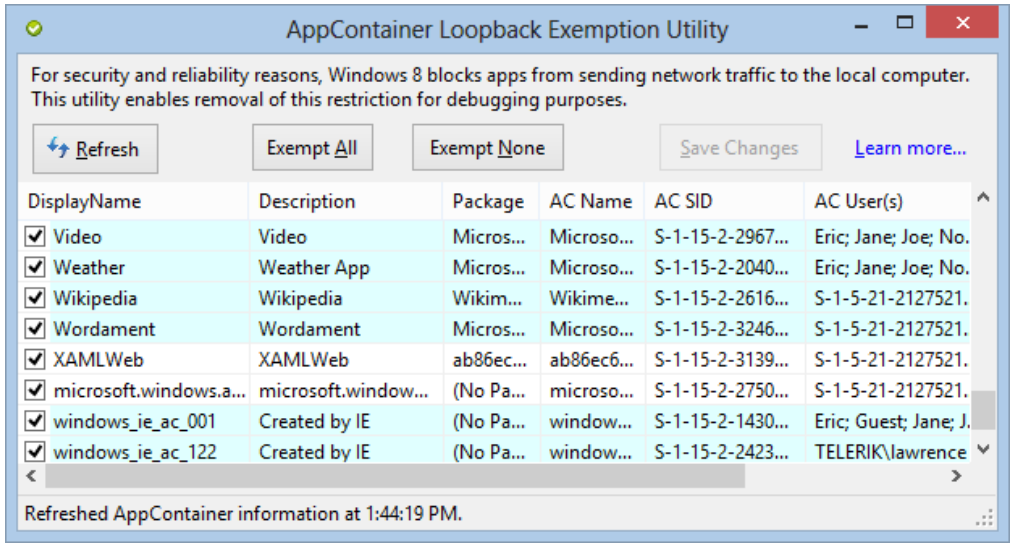
http://dotnetlombardia.org/b/remixx/archive/2011/11/12/fiddler-e-l-emulatore-di-windows-phone-7.aspx

Windows Phone



Windows Store APP



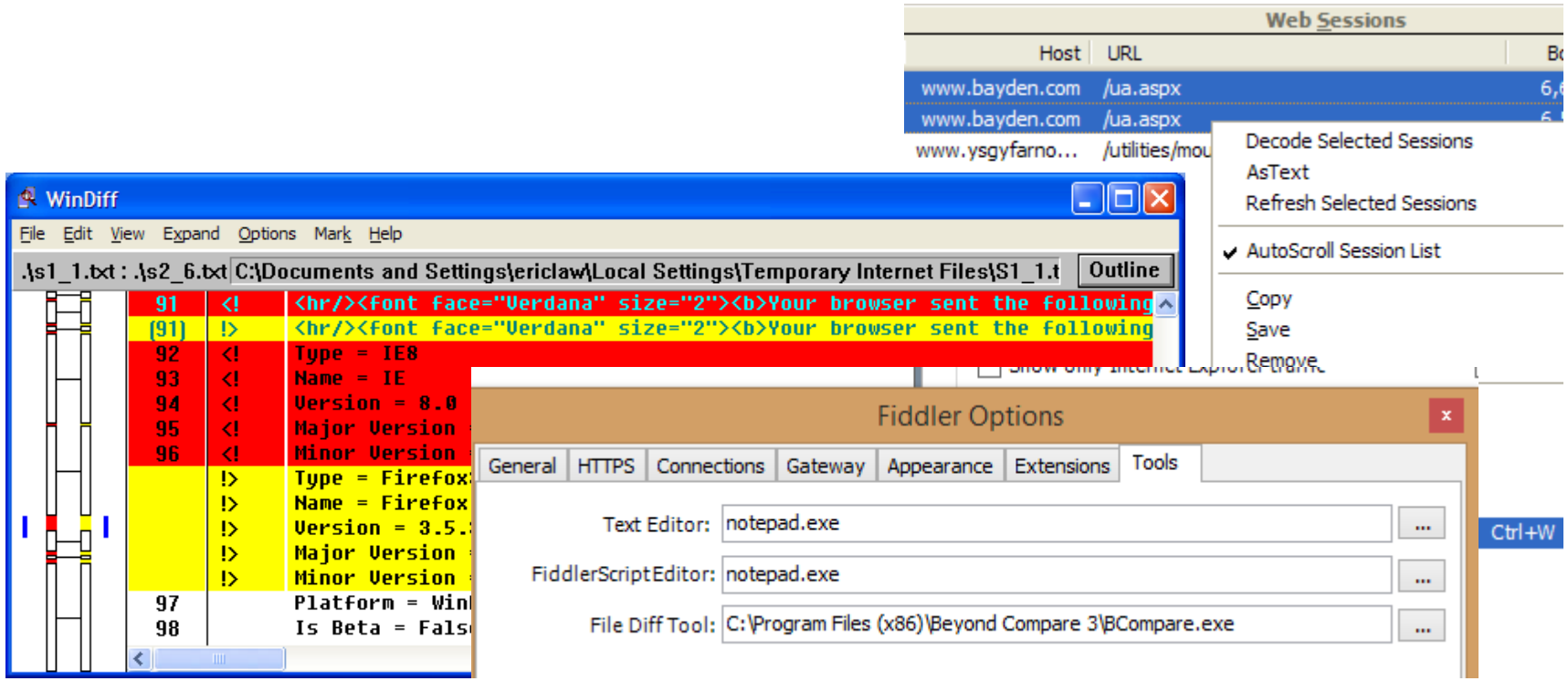


.NET Applications

```
<configuration>
  <system.net>
    <defaultProxy>
      <proxy bypassonlocal="false"
             usesystemdefault=“false"
             proxyaddress=
               "http://127.0.0.1:8888" />
    </defaultProxy>
  </system.net>
</configuration>
```

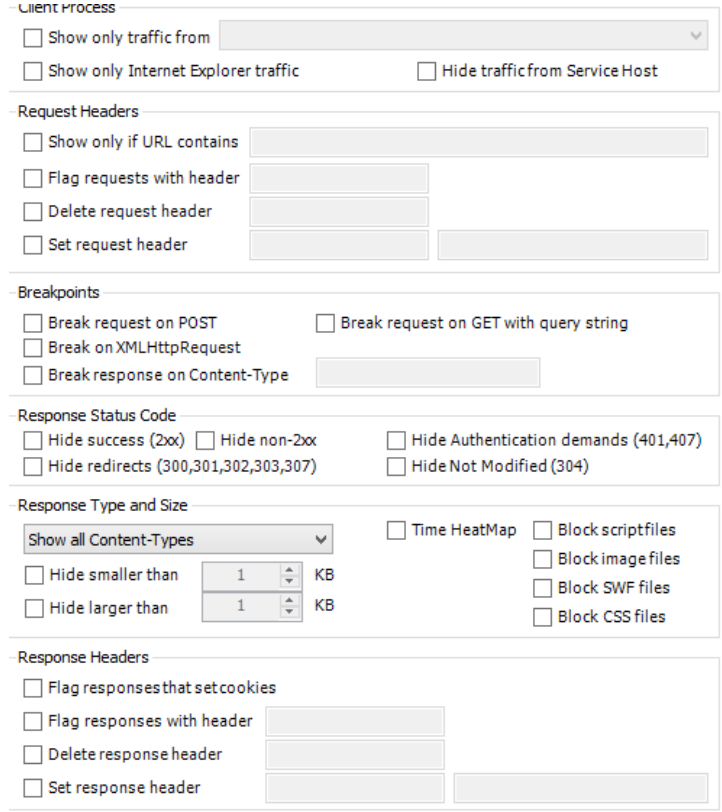
Traffic Analysis

Confrontare due sessioni



Filtrare il traffico

- Ignorare immagini e connessioni protette
- In base all' Application Type
- In base all'host
- In base al processo
- Tramite le n..mila regole che si possono specificare nel tab Filter ☺



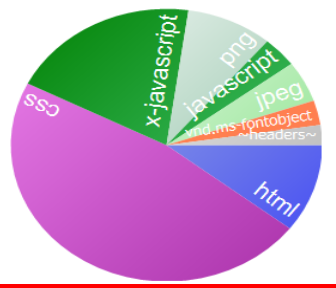
Analizzarlo

#	Result	Host	URL	Body	Caching	C
1	200	codeplanet.io	/principles-good-restful-api-design/	66.647		ti
2	200	codeplanet.io	/wp-content/themes/codeplanet/bootstrap.css	102.897		ti
3	200	codeplanet.io	/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1	7.200		a
4	200	codeplanet.io	/wp-content/themes/codeplanet/style.css?ver=3.8.1	8.757		ti
5	200	codeplanet.io	/wp-content/plugins/crayon-syntax-highlighter/fonts/monaco.css?ver=2.4.3	529		ti
6	200	codeplanet.io	/wp-includes/js/comment-reply.min.js?ver=3.8.1	757		a
7	200	codeplanet.io	/wp-content/plugins/crayon-syntax-highlighter/css/min/crayon.min.css?ver=2.4.3	19.613		ti
8	200	codeplanet.io	/wp-content/plugins/wp-about-author/wp-about-author.css?ver=3.8.1	1.104		ti
9	200	codeplanet.io	/wp-content/plugins/crayon-syntax-highlighter/themes/tomorrow-night/tomorrow-night.css...	5.041		ti
10	200	codeplanet.io	/wp-includes/js/jquery/jquery.js?ver=1.10.2	93.085		a
11	200	codeplanet.io	/wp-content/themes/codeplanet/images/CodePlanetLogo.png	7.353		in
12	200	use.typekit.net	/vcz0ypr.js	23.022	public, ...	ti
13	200	codeplanet.io	/wp-content/plugins/crayon-syntax-highlighter/js/min/crayon.min.js?ver=2.4.3	24.168		a
14	200	codeplanet.io	/wp-content/themes/codeplanet/js/skip-link-focus-fix.js?ver=20130115	733		a
15	200	Tunnel to	urs.microsoft.com:443	0		
16	200	1.gravatar.com	/avatar/9171705459b4dfd18c8badc3cf50acf9?s=100&d=http%3A%2F%2F1.gravatar.co...	4.924	max-ag...	in
17	200	1.gravatar.com	/avatar/9171705459b4dfd18c8badc3cf50acf9?s=125&d=http%3A%2F%2F1.gravatar.co...	6.594	max-ag...	in
18	200	1.gravatar.com	/avatar/ff760f3896b0449eca7d5fe57d10c243?s=125&d=http%3A%2F%2F1.gravatar.co...	5.417	max-ag...	in
19	200	codeplanet.io	/wp-content/plugins/wp-about-author/images/twitter.png	1.196		in
20	302	1.gravatar.com	/avatar/1a8bef1cd88bf70217e8b16aff3b307a?s=125&d=http%3A%2F%2F1.gravatar.co...	0	max-ag...	ti
21	302	1.gravatar.com	/avatar/58b801e06786585078d3f0b1bb3424a4?s=125&d=http%3A%2F%2F1.gravatar.c...	0	max-ag...	ti
22	200	1.gravatar.com	/avatar/9171705459b4dfd18c8badc3cf50acf9?s=64&d=http%3A%2F%2F1.gravatar.com...	2.588	max-ag...	in
23	200	0.gravatar.com	/avatar/c41774bd27fb7e396faa7400f0646298?s=125&d=http%3A%2F%2F0.gravatar.co...	13.553	max-ag...	in
24	200	0.gravatar.com	/avatar/08ff8754a9145694da7f956d41a606de?s=125&d=http%3A%2F%2F0.gravatar.co...	5.439	max-ag...	in
25	200	codeplanet.io	/wp-includes/images/smilies/icon_smile.gif	174		in
26	200	1.gravatar.com	/avatar/1fb67ccd10b0e263fdada0184f292bf9?s=125&d=http%3A%2F%2F1.gravatar.co...	5.928	max-ag...	in
27	302	1.gravatar.com	/avatar/dff8263515d80592f7b4de7948848197?s=125&d=http%3A%2F%2F1.gravatar.co...	0	max-ag...	ti
28	302	0.gravatar.com	/avatar/6c3107aadf495846f3557688a40185?s=125&d=http%3A%2F%2F0.gravatar.co...	0	max-ag...	ti
29	200	codeplanet.io	/wp-content/themes/codeplanet/images/twitter.png	1.478		in
30	200	codeplanet.io	/wp-content/themes/codeplanet/images/facebook.png	1.254		in
31	200	codeplanet.io	/wp-content/themes/codeplanet/images/youtube.png	1.382		in
32	200	codeplanet.io	/wp-content/themes/codeplanet/images/google+.png	1.705		in
33	200	1.gravatar.com	/avatar/ad516503a11cd5ca435acc9bb6523536?s=125	5.909	max-ag...	in
34	200	1.gravatar.com	/avatar/ad516503a11cd5ca435acc9bb6523536?s=125	5.909	max-ag...	in
35	200	1.gravatar.com	/avatar/ad516503a11cd5ca435acc9bb6523536?s=125	5.909	max-ag...	in
36	200	0.gravatar.com	/avatar/ad516503a11cd5ca435acc9bb6523536?s=125	5.909	max-ag...	in
37	200	use.typekit.net	/c/2395d5/museo-slab:n5,myriad-pro:i4:i7:n4:n7.WH7:N:2,Xc8:N:2,Xc3:N:2,XcH:N:2,Xc0:N...	161.573	public, ...	ti
38	200	codeplanet.io	/wp-content/plugins/crayon-syntax-highlighter/fonts/monaco/monaco-webfont.eot?	18.525		a
39	200	codeplanet.io	/wp-content/plugins/crayon-syntax-highlighter/css/images/toolbar/buttons.png	2.236		in
40	200	p.typekit.net	/p.gif?s=1&k=vcz0ypr&ht=tk&h=codeplanet.io&f=6846.6851.6848.6847.2030&a=635009...	35	max-ag...	in
41	200	www.google-analytics.com	/collect?v=1&_v=j16&a=781936179&t=pageview&_s=1&dl=http%3A%2F%2Fcodeplanet...	35	private...	in
42	200	codeplanet.io	/wp-content/plugins/crayon-syntax-highlighter/css/images/toolbar/buttons@2x.png	3.245		in
44	200	Tunnel to	urs.microsoft.com:443	0		

Statistics | Inspectors | AutoResponder | Composer | FiddlerScript | Filters | Log | Timeline

```
Request Count:   43
Unique Hosts:    7
Bytes Sent:      20.019          (headers:20.019; body:0)
Bytes Received:  637.012         (headers:15.189; body:621.823)

ACTUAL PERFORMANCE
--------------
Requests started at:        15:45:48.118
Responses completed at:     15:45:53.861
Sequence (clock) duration:  00:00:05.742
Aggregate Session duration: 00:00:21.943
DNS Lookup time:            663ms
TCP/IP Connect duration:    3.181ms

RESPONSE CODES
--------------
HTTP/200:     39
HTTP/302:     4

RESPONSE BYTES (by Content-Type)
--------------
                      text/css: 299.514
     application/x-javascript: 125.943
                     text/html: 66.647
                     image/png: 57.038
                    image/jpeg: 30.890
                text/javascript: 23.022
application/vnd.ms-fontobject: 18.525
                   ~headers~: 15.189
                     image/gif: 244

REQUESTS PER HOST
--------------
           codeplanet.io: 22
            1.gravatar.com: 11
            0.gravatar.com: 4
         urs.microsoft.com: 2
           use.typekit.net: 2
www.google-analytics.com: 1
             p.typekit.net: 1

ESTIMATED WORLDWIDE PERFORMANCE
--------------
The following are VERY rough estimates of download times when hitting servers based in Seattle.

US West Coast (Modem - 6KB/sec)
       RTT:          4,30s
       Elapsed:      113,30s

Japan / Northern Europe (Modem)
       RTT:          6,45s
       Elapsed:      115,45s

China (Modem)
       RTT:          19,35s
       Elapsed:      128,35s
```

Collapse Chart



Traffic Manipulation

- Auto Responder
- HOSTS
- Breakpoint
- User-Agent / Performance Simulator
- Composer

Demo

HTTPS

HTTPS

- Per ragioni di sicurezza , di default, Fiddler non può «aprire» in pacchetti inviati in HTTPS

#	Result	Host	URL	Body
2	200	Tunnel to	www.bing.com:443	0
3	200	Tunnel to	www.bing.com:443	0

- Per funzionare usa una tecnica chiamata «man-in-the-middle»
- Per attivarla Tools → Fiddler Options →HTTPS → Decrypt HTTPS Traffic e installare il certificato generato

#	Result	Host	URL	Body	Caching	Content-Type	Process	Comments	Custom
1	200	Tunnel to	www.bing.com:443	0			iexplor…		
2	200	www.bing.com	/	44.809	private…	text/html; c…	iexplor…		
3	200	www.bing.com	/rewardsapp/reportActivity	0	no-cac…	application/…	iexplor…		

Varie ed eventuali

Salvare le sessioni

- Salvare intere sessioni
- Salvare solo la request/response
- Salvare solo parte della request/response (header / body)
- Salvare più sessioni in un unico pacchetto .saz
- Salvare le regole dell' AutoResponder
- Salvare i Filtri

- Timeline
- TextWizard
- Supporto per le REGEX ovunque
- Fiddler Add-ons (http://www.telerik.com/fiddler/add-ons)
- Fiddler Script (Jscript.NET)
- Image\PDF\Metadata & Geolocation View
- Syntax View Formatting (JSON/XML)

E…

…dulcis in fundo…

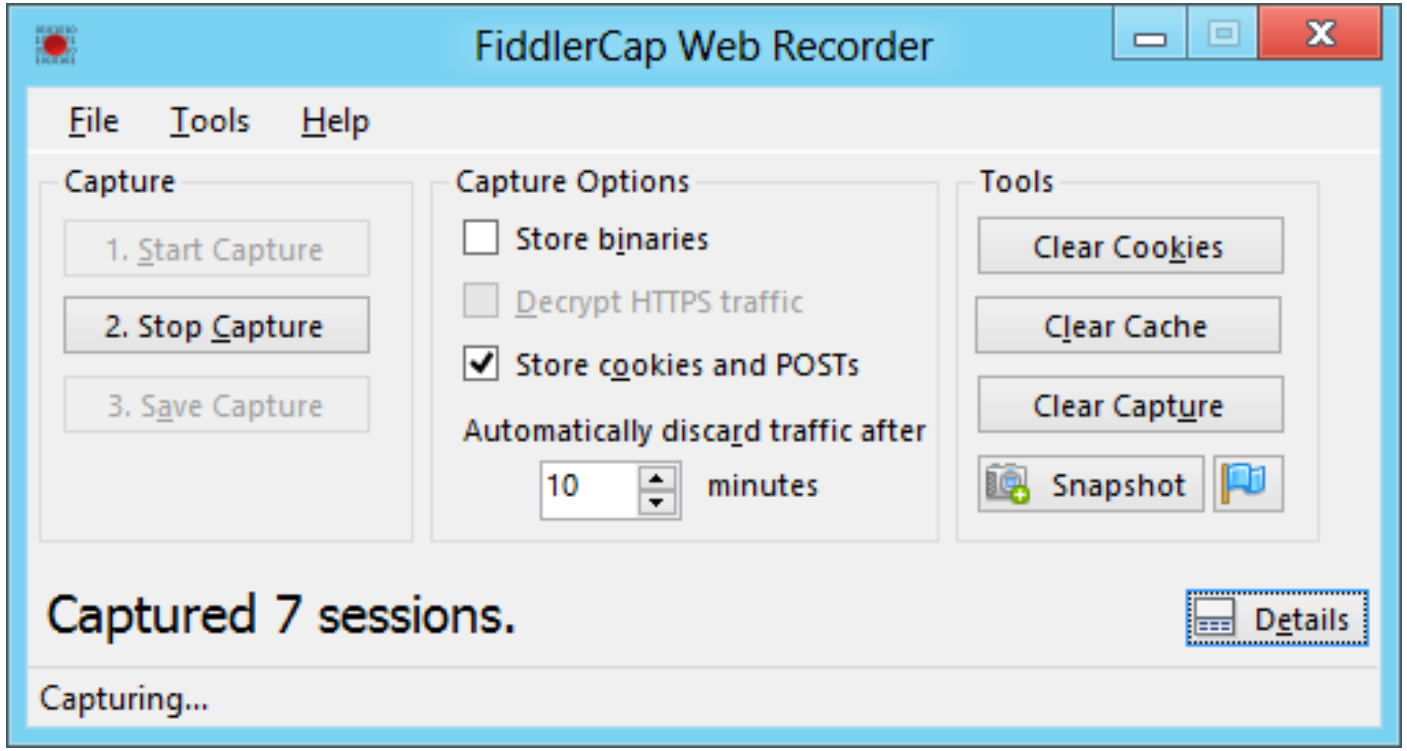
…ciliegina sulla torta…

…la créme de la crème…

…LINQ per noi sviluppatori…

FiddlerCap

- Scaricabile da qui http://www.fiddlercap.com



Q&A

Tutto il materiale di questa sessione su

http://www.communitydays.it/

Lascia il feedback su questa sessione,

potrai essere estratto per i nostri premi!

Seguici su

Twitter @CommunityDaysIT

Facebook http://facebook.com/cdaysit

#CDays14