Introduction Charles Proxy

CHECK24

Agenda

1. Charles Overview
2. SSL
3. Practical Tips

Charles Overview

CHECK24

What is Charles?

Charles is an HTTP proxy written in Java (https://www.charlesproxy.com)

- Works under Windows, macOS, Linux
- Can be used as system proxy on the Mac
- Supports HTTP and HTTP/2, not other protocols
- Displays XML, json etc. very readable
- User can intervene in network traffic

Alternatives

- For Windows: Fiddler (https://www.telerik.com/fiddler)
- For all platforms: Burp Suite (https://portswigger.net/burp)
- For low level and other protocols: Wireshark (https://www.wireshark.org)

Short overview HTTP

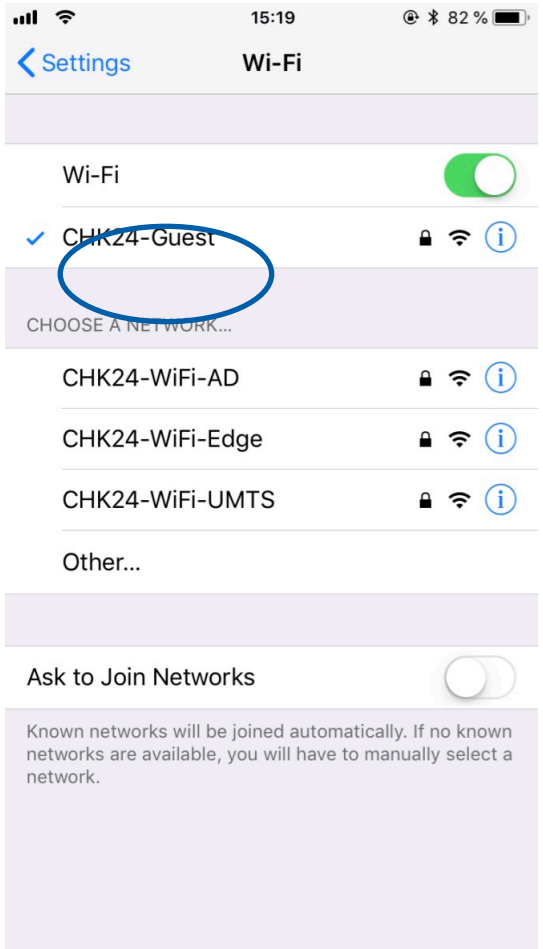
HTTP is a stateless protocoll for the application layer, ususally based on TCP/IP

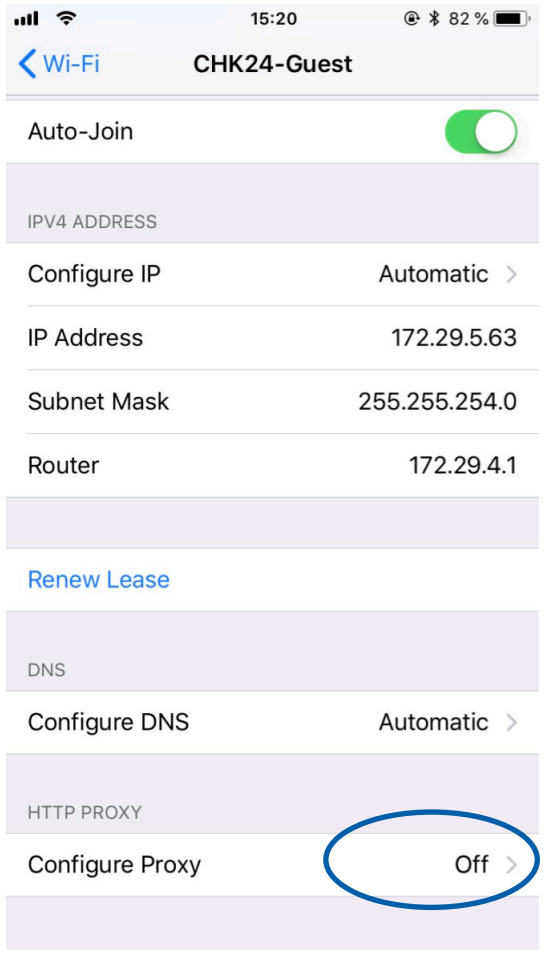
- Charles can‘t deal with other protocols, for instance ftp or Apple Push Notifications
- HTTP responses are divided into body and header
- The body matches the file content
- The header contains meta information like status code or timestamps
- Example for status codes:
  - Sucess (2xx, for example 200)
  - Redirection (3xx, for example 304 Not Modified)
  - Client errors (4xx, for example 404 Not Found)
  - Server errors (5xx, for example 500)

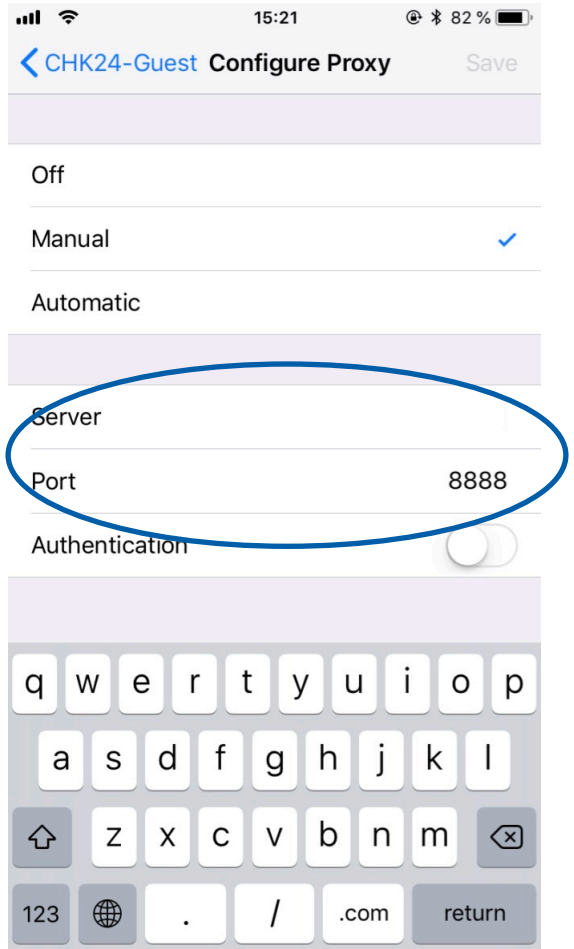
Mac as Proxy for iOS devices

- Both the Mac as the smartphone need to be in the same network (for example CHK24-Guest)
- In Charles go to „Proxy“ -> „Proxy Settings“ -> „Proxies“, enter „8888“ as port and enable „transparent HTTP Proxying“
- Chose the proper wifi network in the smartphone and enter the proxy manually. Port is by default “8888“, server is the IP address of your Mac
  - iOS: „Settings“ -> „Wi-Fi“ -> $networkName -> „Configure Proxy“ -> „Manual“
  - Android: “Menu“ -> „Settings“ -> „Wi-Fi“ -> long press on $networkName
- For testing purposes open a page in Mobile Safari and accept the incoming connection in Charles

Mac as Proxy for iOS Devices







CHECK24

HTTPS / SSL
Hacking!

HTTPS / SSL
Own Root Certificate Authority

You need your own RCA so that Charles can create new SSL certificates and the devices accepts them as being legit.

Charles creates a dedicated RCA per installation, this should be sufficienctly secure. Nevertheless I would install the certificat on the iOS simulator and test devices only. On my personal phone I would deinstall the certificate after testing, on my Mac I would never install it.

If you are paranoid, create your the RCA yourself: http://0x74696d.com/posts/CharlesSSL

HTTPS / SSL
Install Certificate on the iPhone and the Simulator

iPhone Simulator

- In Charles: „Help“ -> „SSL Proxying“ -> „Install Charles Root Certificate in iOS Simulators“
- Reboot Simulator just to be sure
- Then the Simulator has installed the root certificate, but not your Mac

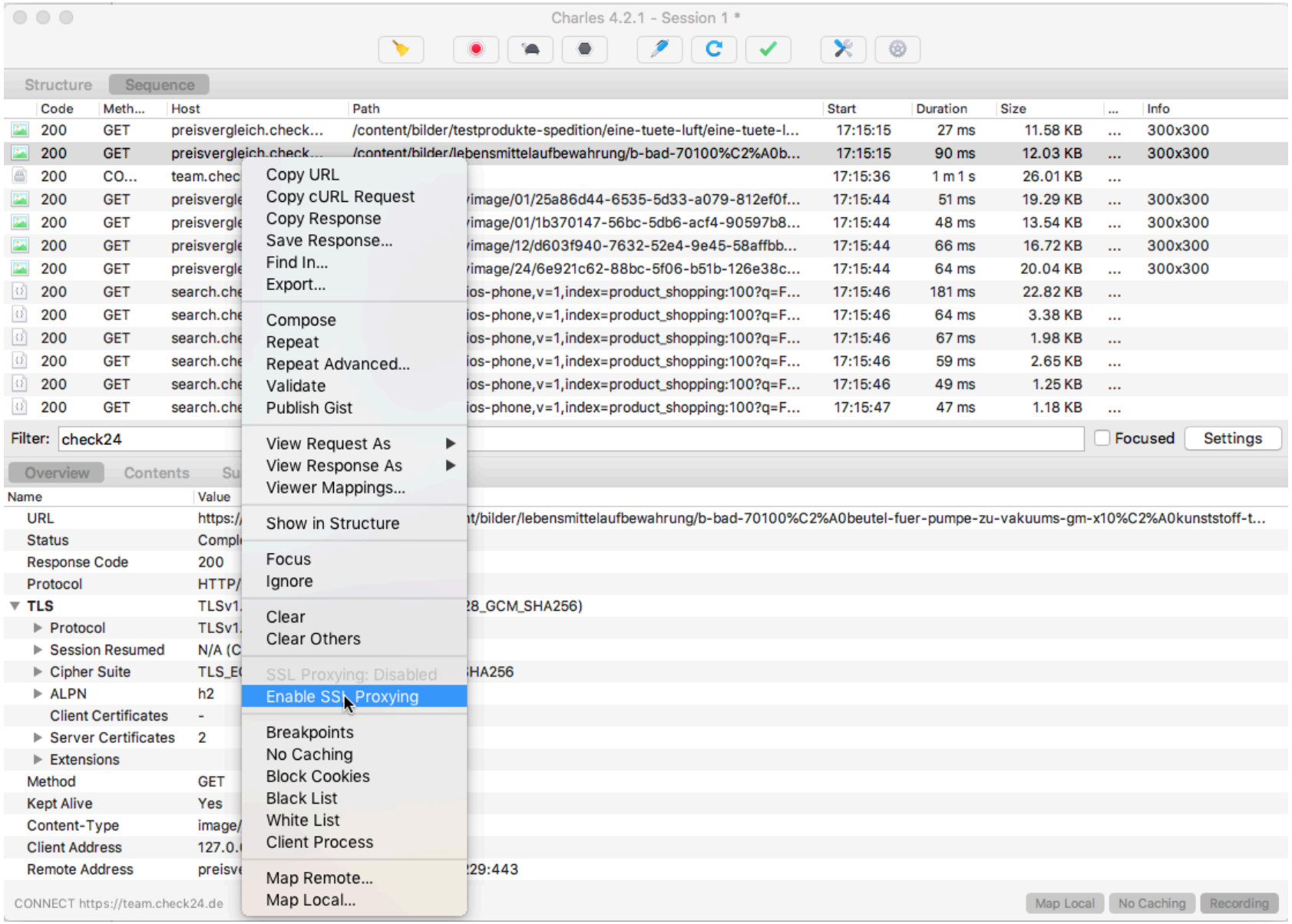
Smartphone

- Prerequisites: The smartphone needs to be in the same network as the computer running Charles. Additionaly the proper proxy settings must be used (see earlier in this presentation)
- In Charles: „Help“ -> „SSL Proxying‘ -> „Install Charles Root Certificate on a Mobile Device or Remote Browser“
- Load the page Charles tells you and install the certificate
- This certificate can be deinstalled after debugging

HTTPS / SSL
Usage in Charles

- For every host you need to activate SSL separately (In the sequence diagram right click onto the URL and check SSL, see next page). The list of all Hosts is later retrievable via „Proxy“ -.> “Proxy Settings“ -> “SSL“. There “Enable SSL Proxying“ must be checked.

HTTPS / SSL


Charles 4.2.1 - Session 1 *
Structure
Sequence
Code
Meth...
Host
Path
Start
Duration
Size
...
Info
200 GET preisvergleich.check... /content/bilder/testprodukte-spedition/eine-tuete-luft/eine-tuete-l... 17:15:15 27 ms 11.58 KB ... 300x300
200 GET preisvergleich.check... /content/bilder/lebensmittelaufbewahrung/b-bad-70100%C2%A0b... 17:15:15 90 ms 12.03 KB ... 300x300
200 CO... team.chec 17:15:36 1 m 1 s 26.01 KB ...
200 GET preisvergle /image/01/25a86d44-6535-5d33-a079-812ef0f... 17:15:44 51 ms 19.29 KB ... 300x300
200 GET preisvergle /image/01/1b370147-56bc-5db6-acf4-90597b8... 17:15:44 48 ms 13.54 KB ... 300x300
200 GET preisvergle /image/12/d603f940-7632-52e4-9e45-58affbb... 17:15:44 66 ms 16.72 KB ... 300x300
200 GET preisvergle /image/24/6e921c62-88bc-5f06-b51b-126e38c... 17:15:44 64 ms 20.04 KB ... 300x300
200 GET search.che ios-phone,v=1,index=product_shopping:100?q=F... 17:15:46 181 ms 22.82 KB ...
200 GET search.che ios-phone,v=1,index=product_shopping:100?q=F... 17:15:46 64 ms 3.38 KB ...
200 GET search.che ios-phone,v=1,index=product_shopping:100?q=F... 17:15:46 67 ms 1.98 KB ...
200 GET search.che ios-phone,v=1,index=product_shopping:100?q=F... 17:15:46 59 ms 2.65 KB ...
200 GET search.che ios-phone,v=1,index=product_shopping:100?q=F... 17:15:46 49 ms 1.25 KB ...
200 GET search.che ios-phone,v=1,index=product_shopping:100?q=F... 17:15:47 47 ms 1.18 KB ...
Filter: check24
Focused
Settings
Overview
Contents
Name
Value
URL
Status
Response Code 200
Protocol
TLS
Protocol
Session Resumed
Cipher Suite
ALPN h2
Client Certificates
Server Certificates 2
Extensions
Method GET
Kept Alive Yes
Content-Type
Client Address
Remote Address
t/bilder/lebensmittelaufbewahrung/b-bad-70100%C2%A0beutel-fuer-pumpe-zu-vakuums-gm-x10%C2%A0kunststoff-t...
28_GCM_SHA256)
HA256
29:443
Copy URL
Copy cURL Request
Copy Response
Save Response...
Find In...
Export...
Compose
Repeat
Repeat Advanced...
Validate
Publish Gist
View Request As
View Response As
Viewer Mappings...
Show in Structure
Focus
Ignore
Clear
Clear Others
SSL Proxying: Disabled
Enable SSL Proxying
Breakpoints
No Caching
Block Cookies
Black List
White List
Client Process
Map Remote...
Map Local...
CONNECT https://team.check24.de
Map Local
No Caching
Recording

Practical Tips

Practical Tips: Overview

Network traffic from the Mac

- Don‘t use the system proxy with Firefox and then use Firefox for everything that shouldn‘t appear in Charles
- Deactivate the proxy for certain hosts under „Proxy“ -> „Proxy Settings“ -> „Options“

Network traffic from the iPhone

- Deactivate the Mac OS Proxy („Proxy“ -> „Mac OS Proxy“)
- Check from which device the traffic is coming

Everywhere

- Activate „Tools“ -> „No Caching“ to avoid 304-responses with empty body

Breakpoints

- Adjustable under „Proxy“ -> „Breakpoints“ or via right click on request in sequence diagram
- Breakpoints for whole hosts or specific URLs
- Breakpoint for request and/or response
- You can change both request and response manually
- Tip: Use asterisks * for parts of the URL, then breakpoints are triggered for slightly different URLs

- Example for usage: Is the view big enough if text is 4 lines long?

Mapping

- Under „Tools“ or via right click on request you find „Map Local“, “Map Remote“ and „Rewrite“
- „Map Remote“ loads another URL than the requested one
- „Map Local“ loads fixed content from your hard drive
- „Rewrite“ modifies requests or responses according to given rules (works even with regular expressions)
- Tip: Use asterisks * for parts of the URL, then mapping is triggered for slightly different URLs

- Example for Map Local: If some bug only happens with specific content, save this content in a file. This file can even be added to Jira for later testing
- Example for Map Remote: Use a staging backend server for certain requests

Mapping

With Local Mapping with .txt-files Charles will always use text/plain as content type.

Some json parsers can‘t deal with that.

So better use .json as file extension or use a Rewrite rule for a correct header:

Simulating slow networks

- You can slow down the traffic under „Proxy“ -> „Start Throttling“ and „Throttle Settings“
- In breakpoints you can cancel certain requests or force a timeout through long waiting. Take care: The behavior is not exactly the same as in reality!

Charles iOS app

Use Charles on your iPhone (new in 2018)

- Advantage: No difficult configuration, always with you
- Advantage: Not only Wifi, works with cellular
- Disadvantage: less features, less overview

Questions?

Contact

Carsten Wenderdel

Team Lead Native Apps
carsten.wenderdel@check24.de

CHECK24 Vergleichsportal GmbH
Erika-Mann-Str. 66
80636 München