

## NLS web interceptor

The fourth generation web recorder for SPECTO®

## NLS **web interceptor**

### Basics

The NLS **interceptor** for SPECTO®

- is an add-on for common web browsers and
- relies on the new WebExtensions framework
- which had initially been developed by Google and in the meantime is supported by most browsers
- Features recording of web sessions executed manually in a browser
- Supports HTTPS connections
- Records direct and indirect accesses
- Records authentication requests

## Installation:

### Installation Firefox

1. Select in URL Line: `about:debugging`
2. Button ‚Add-on temporär laden‘
3. Navigate to the directory with the interceptor extension files, and select file `manifest.json`.

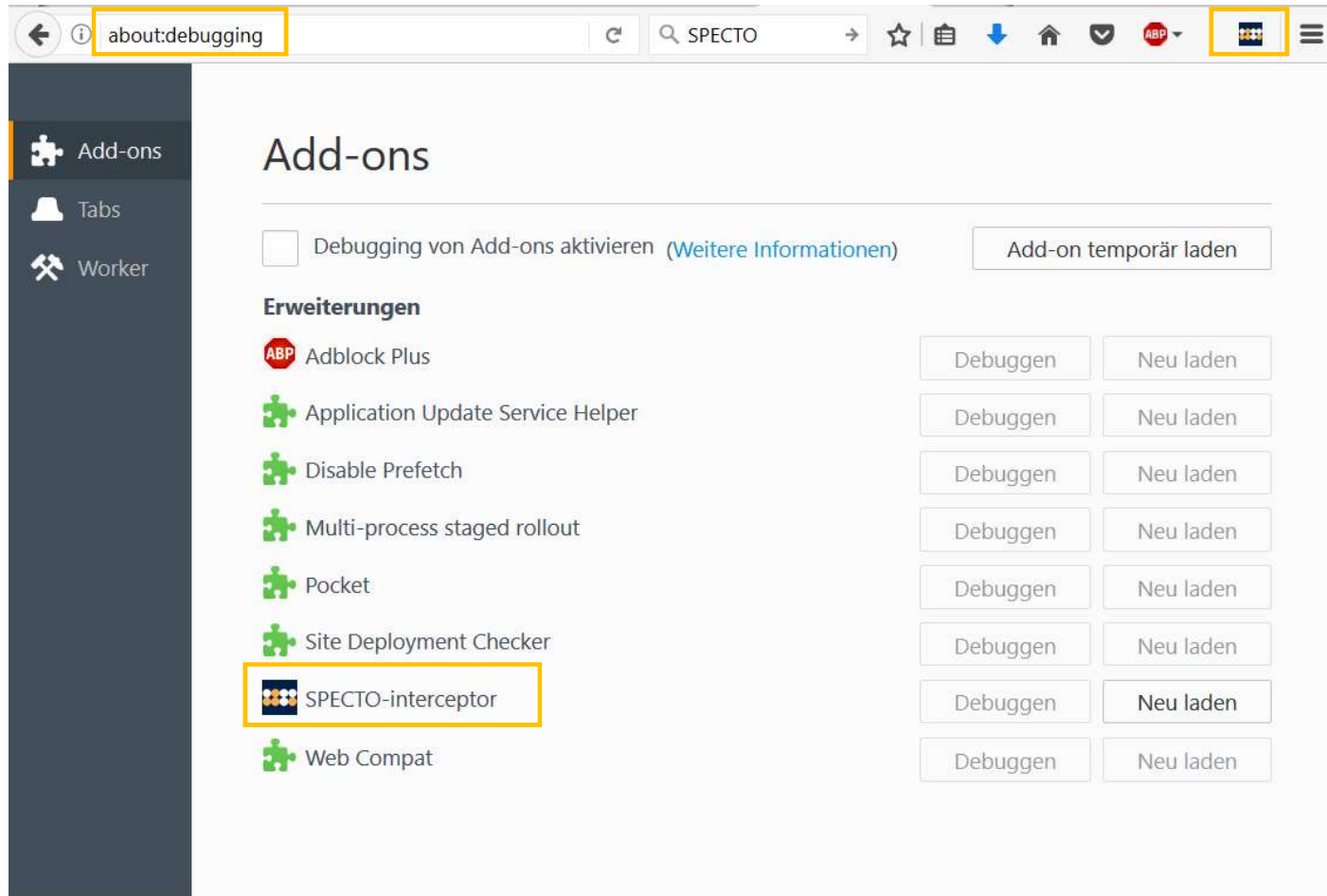
### Installation Chrome

1. Select in URL Line: `chrome://extensions` (or open up the Chrome menu by clicking the icon with the three horizontal bars and select Extensions under the Tools menu).
2. Ensure that the Developer mode checkbox in the top right-hand corner is checked.
3. Click Load unpacked extension... to pop up a file-selection dialog.
4. Navigate to the directory with the interceptor extension files, and select it.

### Installation Edge

1. Select in URL Line: `about:flags`
2. Select the **Enable extension developer features** checkbox.
3. Go to menu ‚More‘ (...)
4. Load extension

Final appearance of a successful sample installation in Mozilla Firefox:



## NLS **interceptor**

### Sample Session

- In the browser, by clicking on the **interceptor** icon, open the **interceptor** main menu.
- The status should display as 'off'
- Select the 'SPECTO interceptor on' menu item
- The status should change to 'on' with 0 recorded items.



In the browser, enter URL 'https://nolp.dhl.de/nextt-online-public/de/'

The german post order tracking web site should open .

Open the 'SPECTO interceptor' menu and verify that the status shows a number of recorded requests

The screenshot shows a browser window with the URL `https://nolp.dhl.de/nextt-online-public/de/` in the address bar. The page header features the DHL logo and the text "DHL Sendungsverfolgung". The main content area contains the heading "Mit der DHL Sendungsverfolgung haben Sie jederzeit den Status Blick." and a sub-heading "Hier können Sie jederzeit den Status Ihrer Sendungen abfragen. Tragen Sie hierzu einfach Ihre Sendungs-, Abholauftragsnummer in das vorgesehene Eingabefeld ein." Below this is a search form with the label "Nach Sendungsnummer suchen", a checkbox for "Eingabe mehrerer Sendungsnummern", an input field with the placeholder "Sendungsnummer eingeben", and a red "Suchen" button. A link for "Hilfe & Kontakt" is also visible. On the right side, the SPECTO interceptor menu is open, showing the "Mode" section with "SPECTO interceptor on" selected. The status section shows "Status: on" and "17 requests recorded; 17 requests selected." The "Options" section includes a filter for file requests with the list "data:, .png, .gif, .jpg, .jpeg".

On the german post order tracking web site enter any number and click on the 'Suche' button.  
 Open the 'SPECTO interceptor' menu and verify that the status shows an increased number of recorded requests.  
 The switch the Interceptor off

https://nolp.dhl.de/nextt-online-public/de/search?piececode=4711

**DHL** DHL Sendungsverfolgung

Zur Sendung "4711" liegen uns derzeit keine Informationen vor.

Wir erwarten Ihre Sendungsdaten in Kürze. Bitte beachten Sie jedoch, dass wir Sendungen erst beauskunften können wenn der Versender die Sendung oder die Sendungsdaten an uns übermittelt hat.

Sie benötigen [Hilfe](#) zur Sendungsverfolgung?

< Zurück Suche wiederholen >

**SPECTO interceptor**

Mode

SPECTO interceptor on

**SPECTO interceptor off**

SPECTO interceptor new

Status: off  
 33 requests recorded;  
 33 requests selected.

Copy chain to clipboard

**Options**

Filter for file requests:  
 data:, .png, .gif, .jpg, .jpeg

(Re-)Apply filters

Define as content check:

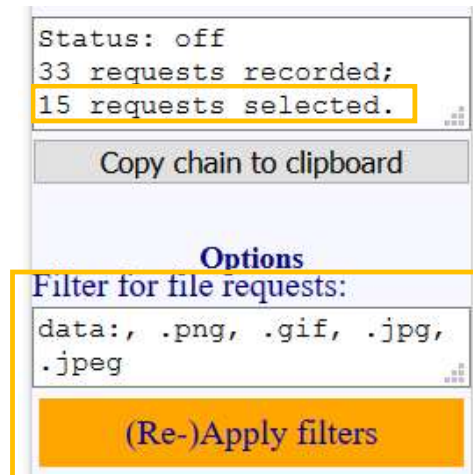
Set content check

Prepare as variables:

(Re-)Apply preparation

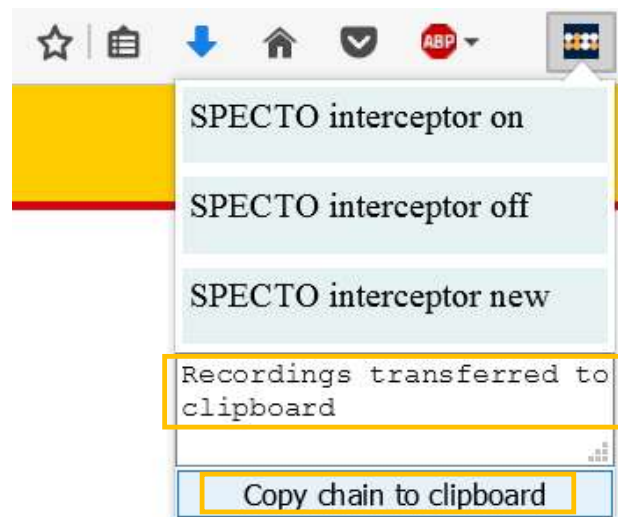
You may filter out certain URL types.

Note that filtering is non-destructive. You may reapply r remove any previous filters and reapply.





Open the 'SPECTO interceptor' menu and select the 'Copy chain to clipboard' item.  
Verify that the transfer to the clipboard is acknowledged



It is recommended to turn the SPECTO interceptor off using the associated menu entry now in order to prevent recording of superfluous entries.  
Or, using 'SPECTO interceptor new', a new recording can be started immediately.

Open any text editor or XML viewer and paste the clipboard content:

As an option you may remove non-essential URL requests here.

```
1 <?xml version="1.0" standalone="yes" ?>
2 <SPECTO:CHAIN xmlns:SPECTO="http://www.mathesis.de/specto/">
3   <Chain Id="2" Name="new">
4     <ch_documentation>
5       <ch_docu_line>Created by Specto Interceptor 0.92</ch_docu_line>
6     </ch_documentation>
7     <ch_type>1</ch_type>
8     <ch_sequence>2</ch_sequence>
9     <ch_flags>0</ch_flags>
10    <ch_period>300</ch_period>
11    <NumURLs>59</NumURLs>
12    <URL Id=0 method=GET>
13      <url_id>0</url_id>
14      <url_symbolic_name></url_symbolic_name>
15      <url_flags>1</url_flags>
16      <url_sequence>0</url_sequence>
17      <url_wait_between>5000</url_wait_between>
18      <url_type>0</url_type>
19      <url_url>http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000</url_url>
20      <url_sessionid></url_sessionid>
21      <url_timeout>3500</url_timeout>
22      <url_toolong>2000</url_toolong>
23      <numPars>1</numPars>
24      <Parameter>
25        <par_name>param.name</par_name>
26        <par_value>param.value</par_value>
27        <par_type>d</par_type>
28      </Parameter>
29    </URL>
30    <URL Id=1 method=GET>
31      <url_id>0</url_id>
32      <url_symbolic_name></url_symbolic_name>
33      <url_flags>1</url_flags>
34      <url_sequence>1</url_sequence>
35      <url_wait_between>5000</url_wait_between>
36      <url_type>0</url_type>
37      <url_url>http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000</url_url>
38      <url_sessionid></url_sessionid>
39      <url_timeout>3500</url_timeout>
40      <url_toolong>2000</url_toolong>
41      <numPars>1</numPars>
42      <Parameter>
43        <par_name>param.name</par_name>
44        <par_value>param.value</par_value>
45        <par_type>d</par_type>
46      </Parameter>
47    </URL>
48    <URL Id=2 method=GET>
49      <url_id>0</url_id>
```

Import the recorded chain via menu entry 'import recorded':

- Without specifying a filename,
- In mode '2'
- And the recorded content pasted from the clipboard into the 'content' field.

( The equivalent 'xcr' command may be used instead of the menu driven approach ).

The screenshot shows the SPECTO business service monitoring interface. On the left is a navigation tree with the following structure:

- Explore
  - Contract
  - Standard
- maintenance
  - users
  - clients
  - database
  - time / NTP
  - logging
  - application
    - modify chains...
  - export database
  - imp./exp. (XML)
    - up- and downloads
    - application
      - base data...
        - export base data...
        - import base data...
      - current threads
      - chain configurations
        - export complete client...
        - export all clients...
        - export single chain...
        - import complete client...
        - import single chain...
        - upload recorded...
        - import recorded...
  - results
  - engine upgrade
  - file handling
  - customizing
    - online help
    - log out

The main 'Input form' area contains the following fields:

- filename: (empty text box)
- chain id: 27
- chain name: DHL Tracking (Demo Interceptor)
- mode: 2
- content: XML code pasted from clipboard:
 

```
<?xml version="1.0" standalone="yes" ?>
<SPECTO:CHAIN
xmlns:SPECTO="http://www.mathesis.de/specto/">
  <Chain Id="2" Name="new">
    <ch_documentation>

<ch_docu_line>Created by Specto
Interceptor 0.92</ch_docu_line>
    </ch_documentation>
    <ch_type>1</ch_type>

<ch_sequence>2</ch_sequence>
    <ch_flags>0</ch_flags>
    <ch_period>300</ch_period>
    <NumURLs>59</NumURLs>
    <URL Id=0 method=GET>
```

Buttons for 'Execute' and 'from clipboard' are visible. The footer shows 'Command:' with an empty field, 'Execute', 'ref.', 'SPECTO® release 1.97 sup doc', and '© MATHESIS GmbH'.

# Log of an Successful import:

**SPECTO® business service monitoring**

Explode Contract Standard

Command output Back / History / Home noERR primary : alpha : Demo

- network
  - startup\_procs
  - variables
  - attribute cache
  - reporting cache
  - delayed write
  - lock status
  - user exits
  - web server
    - list
    - commands
    - reset statistics
  - operator messages
    - display list
    - delete messages
    - manual message
    - dynamic...
  - alive messages
    - status
    - sync to now
- consoles
- mail / net
- maintenance
  - users
  - clients
  - database
  - time / NTP
  - logging
  - application
    - modify chains...
  - export database
  - imp/exp. (XML)
    - up- and downloads
    - application
      - base data...
        - export base data...
        - import base data...
      - current threads
    - chain configurations
      - export complete client...
      - export all clients...
      - export single chain...
      - import complete client...
      - import single chain...
      - upload recorded...
      - import recorded...
  - results
  - engine upgrade
  - file handling
  - customizing
  - online help
  - log out

```

Importing from recorded XML file ' Created by Specto Interceptor 0.92 1 2 0 300 59 0 1 0 5000 0 http://de.reuters.com/assets
/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 1 5000 0 http://de.reuters.com/assets
/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 2 5000 0 http://de.reuters.com/assets
/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 3 5000 0 http://de.reuters.com/assets
/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 4 5000 0 http://de.reuters.com/assets
/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 5 5000 0 http://de.reuters.com/assets
/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 6 5000 0 http://de.reuters.com/assets
/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 7 5000 0 http://de.reuters.com/assets
/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 8 5000 0 http://de.reuters.com/assets
/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 9 5000 0 http://de.reuters.com/assets
/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 10 5000 0 https://nolp.dhl.de/nextt-online-
public/de/ 3500 2000 0 0 1 11 5000 0 https://nolp.dhl.de/nextt-online-public/de/static/assets/css/index.unccss.min.css 3500 2000
0 0 1 12 5000 0 https://nolp.dhl.de/nextt-online-public/de/static/libs/cdnload.js 3500 2000 0 0 1 13 5000 0
https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js 3500 2000 0 0 1 14 5000 0 https://nolp.dhl.de/nextt-online-
public/de/static/bundle.min.js 3500 2000 0 0 1 15 5000 0 http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500
2000 1 param.name param.value d 0 1 16 5000 0 http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1
param.name param.value d 0 1 17 5000 0 http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name
param.value d 0 1 18 5000 0 http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 19
5000 0 http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 20
5000 0 http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 21 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 22 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 23 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 24 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 25 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 26 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 27 5000 0
https://nolp.dhl.de/nextt-online-public/de/search?piececode=4711 3500 2000 1 param.name param.value d 0 1 28 5000 0
https://nolp.dhl.de/nextt-online-public/de/static/assets/css/index.unccss.min.css 3500 2000 0 0 1 29 5000 0 https://nolp.dhl.de
/nextt-online-public/de/static/assets/img/parcel_not_found_new.jpg 3500 2000 0 0 1 30 5000 0 https://nolp.dhl.de/nextt-online-
public/de/static/libs/cdnload.js 3500 2000 0 0 1 31 5000 0 https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js 3500
2000 0 0 1 32 5000 0 https://nolp.dhl.de/nextt-online-public/de/static/bundle.min.js 3500 2000 0 0 1 33 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 34 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 35 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 36 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 37 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 38 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 39 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 40 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 41 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 42 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 43 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 44 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 45 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 46 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 47 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 48 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 49 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 50 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 51 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 52 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 53 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 54 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 55 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 56 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 57 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d 0 1 58 5000 0
http://de.reuters.com/assets/jsonWireNews?startTime=1491902389000 3500 2000 1 param.name param.value d ' for chain '93/DHL
Tracking (Demo Interceptor)'.
Bytes read from file : 32320.

XML parse: 'Reading chain 'DHL Tracking (Demo Interceptor)', ID=93(94)' at line 3.

Checking data consistency...
Importing of chain 'DHL Tracking (Demo Interceptor)' into client 'Demo', (ID=0)...
Finished.

```

## NLS interceptor

### Advanced 1 : chains

The NLS interceptor for SPECTO® allows for filtering of unimportant accesses to be discarded.

- Filters may be specified on basis of wildcards (\*.css) or regular expressions
- Filters may be saved in named local files on project and global levels

The NLS interceptor for SPECTO® supports detection of session identifiers.

- Auto-detection based on parameter postings during the chain
- Detection via multiple recordings (auto playback as a further option)

## NLS interceptor

### Advanced 2 : URLs

- Content Checks can be added to the actual URL
- HTTP/S headers are recognized and may be included noted in the URL documentation
- HTTP/S redirects are recognized and resolved (recorded as individual non-redirected request)
- HTTP/S authentication requests are recognized and (currently) are noted in the URL documentation

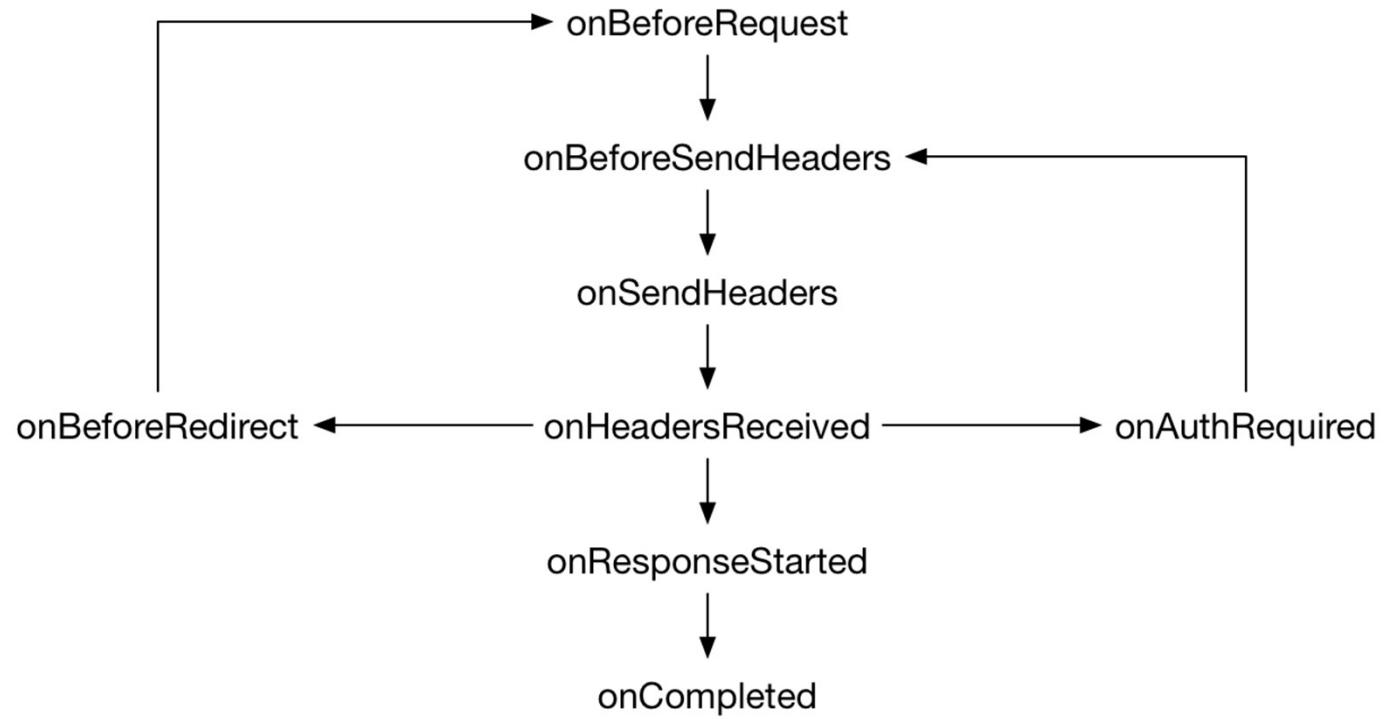
NLS interceptor

Forecast for next release

- Re-runs of a session with highlighting of changes (to detect session-identifiers)

### NLS interceptor

#### Internal event model





## NLS **interceptor**

### Non-Disclosure

Due to :

1. the current state of the several browser suppliers support of signing of add-ons based on the WebExtension framework
2. the possibility to recompile signed add-ons
3. the ongoing development of interceptor for SPECTO

this application has to be delivered in source code.

In order to protect the efforts MATHESIS has put into the development of Interceptor for SPECTO; participants of the current beta program have to sign a non-disclosure agreement committing them to:

1. Not use **interceptor** outside of the SPECTO environment
2. Actively prevent distribution of **interceptor** outside the agreed upon users
3. Not share technical knowledge of **interceptor** with third parties

The NLS **web interceptor**

Thank you !