

# Übungsprotokoll

## ITSI – Informationstechnologie Sicherheit

 htlkrems Bautechnik & IT	<b>Übungsdatum:</b> 28.04.2021	<b>Klasse:</b> 2AHIT	<b>Name:</b> Felix Schneider
	<b>Abgabedatum:</b> 28.04.2021	<b>Gruppe:</b> ITSI2	<b>Note:</b>
<b>Leitung:</b> Jürgen HAUPTMANN	<b>Mitübende:</b> -		

### Übungsbezeichnung:

Browserschutz

## **Inhaltsverzeichnis:**

1	Aufgabenstellung.....	2
2	Abstract (English).....	2
3	Theoretische Grundlagen.....	3
4	Übungsdurchführung .....	3
4.1	ohne Security-Plugin.....	3
4.2	mit NoScript.....	9
4.3	mit requestblock.....	15
4.4	Adblock Plus .....	21
4.5	Testen der einzelnen Erweiterungen auf der bekannten Website YouTube .....	27
5	Ergebnisse.....	28
6	Kommentar.....	28

## **1 Aufgabenstellung**

Mozilla Firefox ist ein Webbrowser, der die Möglichkeit bietet, verschiedenste Erweiterungen (Add-ons) zu installieren. Diese Erweiterungen können auch als Browserschutz dienen. Verwenden Sie eine virtuelle Maschine und installieren Sie den Browser Mozilla Firefox. Installieren Sie die genannten Erweiterungen. Beschreiben und vergleichen Sie die angegebenen Plugins und testen und dokumentieren Sie die Auswirkungen auf den Browserfingerprint (<https://panopticlick.eff.org/>). Beschreiben Sie die Unterschiede bei den Erweiterungen. Besuchen Sie einzelne bekannte Webseiten und beschreiben Sie das Browserverhalten.

- 1 Mozilla Firefox ohne Security-Plugin
- 2 Mozilla Firefox mit NoScript (<https://addons.mozilla.org/de/firefox/addon/noscript/>)
- 3 Mozilla Firefox mit requestblock (<https://addons.mozilla.org/de/firefox/addon/requestblock/>)
- 4 Mozilla Firefox mit Adblock Plus (<https://addons.mozilla.org/de/firefox/addon/adblock-plus/>)

## **2 Abstract (English)**

Mozilla Firefox is a web browser that offers the possibility of installing various extensions (add-ons). These extensions can also serve as browser protection. Use a virtual machine and install the Mozilla Firefox browser. Install the extensions mentioned. Describe and compare the specified plugins and test and document the effects on the browser fingerprint (<https://panopticclick.eff.org/>). Describe the differences in the extensions. Visit individual known websites and describe your browser behavior.

- 1 Mozilla Firefox without security plug-in
- 2 Mozilla Firefox with NoScript (<https://addons.mozilla.org/de/firefox/addon/noscript/>)
- 3 Mozilla Firefox with request block (<https://addons.mozilla.org/de/firefox/addon/requestblock/>)
- 4 Mozilla Firefox with Adblock Plus (<https://addons.mozilla.org/de/firefox/addon/adblock-plus/>)

### 3 Theoretische Grundlagen

<https://panopticlick.eff.org/>

<https://addons.mozilla.org/de/firefox/addon/requestblock/>

<https://addons.mozilla.org/de/firefox/addon/noscript/>

<https://addons.mozilla.org/de/firefox/addon/adblock-plus/>

### 4 Übungsdurchführung

#### 4.1 ohne Security-Plugin

Mit keinem Add-on aktiviert ist der Browser nur wenig geschützt. Man ist etwas gegen Werbung geschützt und der Fingerprint ist fast einzigartig.

## HOW TO READ YOUR REPORT

You will see a summary of your overall tracking protection. The first section gives you a general idea of what your browser configuration is blocking (or not blocking). Below that is a list of specific browser characteristics in the format that a tracker would view them. We also provide descriptions of how they are incorporated into your fingerprint.

## HOW CAN TRACKERS TRACK YOU?

Trackers use a variety of methods to identify and track users. Most often, this includes tracking cookies, but it can also include browser fingerprinting. Fingerprinting is a sneaky way to track users and makes it harder for users to regain control of their browsers. This report measures how easily trackers might be able to fingerprint your browser.

## HOW CAN I USE MY RESULTS TO BE MORE ANONYMOUS?

Knowing how easily identifiable you are, or whether you are currently blocking trackers, can help you know what to do next to protect your privacy. While most trackers can be derailed by browser add-ons or built-in protection mechanisms, the sneakiest trackers have ways around even the strongest security. We recommend you use a tracker blocker like [Privacy Badger](#) or use a browser that has fingerprinting protection built in.

## WHAT IS A BIT OF INFORMATION?

A "bit" is a basic unit of information for computers. The bit represents a logical state with one of two possible values, often represented as "1" or "0", for example. In your results from Cover Your Tracks, some metrics may be listed as "1" or "0", or "true" or "false", indicating whether a setting is enabled or disabled. While each individual metric's details may seem like a small amount of information, when combined with your browser's other metrics, they can uniquely identify your browser. Your results are measured in "bits of identifying information," which is a combined summary of all these metrics.

Here are your Cover Your Tracks results. They include an overview of how visible you are to trackers, with an index (and glossary) of all the metrics we measure below.

**Our tests indicate that you have **some protection** against Web tracking, but it has **some gaps**.**

### IS YOUR BROWSER:

Blocking tracking ads?	<u>Partial protection</u>
Blocking invisible trackers?	<u>Partial protection</u>
Protecting you from fingerprinting?	Your browser has a nearly-unique fingerprint

Still wondering how fingerprinting works?

[LEARN MORE](#)

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

## Your Results

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 136183.5 browsers have the same fingerprint as yours**.

Currently, we estimate that your browser has a fingerprint that conveys **17.06 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can [read more about our methodology, statistical results, and some defenses against fingerprinting here](#).

## Detailed Results

Here's some more granular information we gathered about your browser. Your report includes examples of several different kinds of metrics:

### WEB HEADERS

Whenever you connect to a website (in our case, "<https://coveryourtracks.eff.org>"), your device sends a request that includes HTTP headers. These headers contain information like your device's timezone, language, privacy settings, and cookies. Web headers are transmitted by your browser with every site visit.

### JAVASCRIPT-DERIVED CHARACTERISTICS

## Detailed Results

Here's some more granular information we gathered about your browser. Your report includes examples of several different kinds of metrics:

### WEB HEADERS

Whenever you connect to a website (in our case, "<https://coveryourtracks.eff.org>"), your device sends a request that includes HTTP headers. These headers contain information like your device's timezone, language, privacy settings, and cookies. Web headers are transmitted by your browser with every site visit.

### JAVASCRIPT-DERIVED CHARACTERISTICS

Some details about your browser can be discovered by using JavaScript code. This includes fonts, certain details about your hardware configuration, and your canvas fingerprint.

Select a characteristic

User Agent



DEFAULT VIEW

DETAILED VIEW

### USER AGENT

Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

Bits of identifying information: 7.0

One in x browsers have this value: 128.23

---

### HTTP\_ACCEPT HEADERS

text/html, \*/\*; q=0.01 gzip, deflate, br de,en-US;q=0.7,en;q=0.3

Bits of identifying information: 6.06

One in x browsers have this value: 66.76

---

## BROWSER PLUGIN DETAILS

undefined

**Bits of identifying information: 0.86**  
**One in x browsers have this value: 1.81**

---

## TIME ZONE OFFSET

-120

**Bits of identifying information: 2.64**  
**One in x browsers have this value: 6.23**

---

## TIME ZONE

Europe/Vienna

**Bits of identifying information: 7.7**  
**One in x browsers have this value: 208.39**

---

## SCREEN SIZE AND COLOR DEPTH

1600x1200x24

**Bits of identifying information: 10.57**  
**One in x browsers have this value: 1521.6**

---

## SYSTEM FONTS

Arial, Bitstream Vera Sans Mono, Courier New, Times New Roman (via javascript)

**Bits of identifying information: 9.33**  
**One in x browsers have this value: 645.42**

---

## ARE COOKIES ENABLED?

Yes

**Bits of identifying information: 0.13**  
**One in x browsers have this value: 1.1**

---

## LIMITED SUPERCOOKIE TEST

DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No, openDatabase: false, indexed db: true

**Bits of identifying information: 1.08**  
**One in x browsers have this value: 2.11**

---

## HASH OF CANVAS FINGERPRINT

3ecd43b98d1b5487b92cfdfb1e3e7e9e

**Bits of identifying information: 7.77**  
**One in x browsers have this value: 218.07**

---

## HASH OF WEBGL FINGERPRINT

37200c952122f5d6e42baa5b5f167426

**Bits of identifying information: 12.56**  
**One in x browsers have this value: 6052.6**

---

## WEBGL VENDOR & RENDERER

VMware, Inc.-llvmpipe (LLVM 7.0, 256 bits)

**Bits of identifying information: 10.78**  
**One in x browsers have this value: 1757.21**

---

## DNT HEADER ENABLED?

False

**Bits of identifying information: 0.95**  
**One in x browsers have this value: 1.94**

---

## LANGUAGE

de

**Bits of identifying information: 5.69**  
**One in x browsers have this value: 51.58**

---

## PLATFORM

Linux x86\_64

**Bits of identifying information: 2.95**  
**One in x browsers have this value: 7.72**

---

## TOUCH SUPPORT

Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false

**Bits of identifying information: 0.72**  
**One in x browsers have this value: 1.65**

---

## AD BLOCKER USED

False

**Bits of identifying information: 0.27**  
**One in x browsers have this value: 1.2**

---

## AUDIOCONTEXT FINGERPRINT

35.73833402246237

**Bits of identifying information: 4.14**  
**One in x browsers have this value: 17.59**

---

## CPU CLASS

N/A

**Bits of identifying information: 0.14**  
**One in x browsers have this value: 1.1**

---

## HARDWARE CONCURRENCY

1

**Bits of identifying information: 8.18**  
**One in x browsers have this value: 289.75**

---

## DEVICE MEMORY (GB)

N/A

**Bits of identifying information: 1.03**  
**One in x browsers have this value: 2.05**

---

[Back to Top ↑](#)

[RE-TEST YOUR BROWSER](#)

## 4.2 mit NoScript

Mit der NoScript-Erweiterung ist man stark gegen Werbung aller Art geschützt. Gegen Fingerprinting ist man allerdings nicht geschützt. Außerdem hat NoScript den Nachteil, dass Javascript (logischerweise) nicht verfügbar ist, weshalb zum Beispiel auf die Zeitzone nicht zugegriffen werden kann. Wenn man dies allerdings so haben will, ist das ein Vorteil.



 Empfohlen

## NoScript

von Giorgio Maone

Die bestmögliche Sicherheit für Ihren Browser!  
Erlauben Sie das Ausführen von aktiven Inhalten nur Seiten, denen Sie vertrauen – damit schützen Sie sich gegen XSS- und Clickjacking-Angriffe, "Spectre", "Meltdown" und andere JavaScript Schwachstellen.

 Entfernen

**Our tests indicate that you have strong protection against Web tracking, though your software isn't checking for Do Not Track policies.**

IS YOUR BROWSER:

Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
Protecting you from fingerprinting?	No

Still wondering how fingerprinting works?

[LEARN MORE](#)

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

## Your Results

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 27239.4 browsers have the same fingerprint as yours.**

Currently, we estimate that your browser has a fingerprint that conveys **14.73 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can [read more about our methodology, statistical results, and some defenses against fingerprinting here.](#)

## Detailed Results

Here's some more granular information we gathered about your browser. Your report includes examples of several different kinds of metrics:

### WEB HEADERS

Whenever you connect to a website (in our case, "<https://coveryourtracks.eff.org>"), your device sends a request that includes HTTP headers. These headers contain information like your device's timezone, language, privacy settings, and cookies. Web headers are transmitted by your browser with every site visit.

### JAVASCRIPT-DERIVED CHARACTERISTICS

Some details about your browser can be discovered by using JavaScript code. This includes fonts, certain details about your hardware configuration, and your canvas fingerprint.

### USER AGENT

Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

**Bits of identifying information: 7.0**

**One in x browsers have this value: 128.13**

---

### HTTP\_ACCEPT HEADERS

text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8 gzip, deflate, br de,en-US;q=0.7,en;q=0.3

**Bits of identifying information: 8.84**

**One in x browsers have this value: 459.35**

---

### BROWSER PLUGIN DETAILS

no javascript

**Bits of identifying information: 3.49**

**One in x browsers have this value: 11.22**

---

## TIME ZONE OFFSET

no javascript

**Bits of identifying information: 3.49**  
**One in x browsers have this value: 11.21**

---

## TIME ZONE

no javascript

**Bits of identifying information: 3.47**  
**One in x browsers have this value: 11.12**

---

## SCREEN SIZE AND COLOR DEPTH

no javascript

**Bits of identifying information: 3.49**  
**One in x browsers have this value: 11.22**

---

## SYSTEM FONTS

no javascript

**Bits of identifying information: 3.49**  
**One in x browsers have this value: 11.22**

---

## ARE COOKIES ENABLED?

Yes

**Bits of identifying information: 0.13**  
**One in x browsers have this value: 1.1**

---

## LIMITED SUPERCOOKIE TEST

no javascript

Bits of identifying information: **3.49**

One in x browsers have this value: **11.22**

---

## HASH OF CANVAS FINGERPRINT

no javascript

Bits of identifying information: **3.49**

One in x browsers have this value: **11.22**

---

## HASH OF WEBGL FINGERPRINT

no javascript

Bits of identifying information: **3.49**

One in x browsers have this value: **11.22**

---

## WEBGL VENDOR & RENDERER

no javascript

Bits of identifying information: **2.37**

One in x browsers have this value: **5.16**

---

## DNT HEADER ENABLED?

False

Bits of identifying information: **0.95**

One in x browsers have this value: **1.94**

---

## LANGUAGE

no javascript

**Bits of identifying information: 3.49**  
**One in x browsers have this value: 11.21**

---

## PLATFORM

no javascript

**Bits of identifying information: 3.49**  
**One in x browsers have this value: 11.2**

---

## TOUCH SUPPORT

no javascript

**Bits of identifying information: 3.49**  
**One in x browsers have this value: 11.22**

---

## AD BLOCKER USED

no javascript

**Bits of identifying information: 3.49**  
**One in x browsers have this value: 11.22**

---

## AUDIOCONTEXT FINGERPRINT

no javascript

**Bits of identifying information: 3.49**  
**One in x browsers have this value: 11.22**

---

### CPU CLASS

no javascript

**Bits of identifying information: 3.49**  
**One in x browsers have this value: 11.22**

---

### HARDWARE CONCURRENCY

no javascript

**Bits of identifying information: 3.49**  
**One in x browsers have this value: 11.22**

---

### DEVICE MEMORY (GB)

no javascript

**Bits of identifying information: 3.49**  
**One in x browsers have this value: 11.22**

**RE-TEST YOUR BROWSER**

## 4.3 mit requestblock

Mit dem Add-on requestblock (der von der Mozilla-Erweiterungs-Website nicht empfohlen ist) ist man ebenfalls sehr stark gegen Werbung aller Art geschützt und der Fingerprint ist fast einzigartig. Die Website Panopticlick erkennt allerdings nicht, dass man einen Add-on aktiviert hat, wie man auf einem dieser Bilder sehen kann:



## requestblock

von [Firefox-Benutzer 13242001](#)

block cross origin request. subset of RequestPolicy (only temporary allow for origin).

 Entfernen

⚠ Dieses Add-on wird von Mozilla nicht aktiv auf seine Sicherheit überwacht. Stellen Sie sicher, dass Sie ihm vertrauen, bevor Sie es installieren.

[Weitere Informationen](#)

**Our tests indicate that you have **strong protection against Web tracking**, though your software isn't checking for Do Not Track policies.**

### IS YOUR BROWSER:

Blocking tracking ads?	<u>Yes</u>
Blocking invisible trackers?	<u>Yes</u>
Protecting you from fingerprinting?	Your browser has a nearly-unique fingerprint

Still wondering how fingerprinting works?

[LEARN MORE](#)

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

## Your Results

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 136211.5 browsers have the same fingerprint as yours.**

Currently, we estimate that your browser has a fingerprint that conveys **17.06 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can [read more about our methodology, statistical results, and some defenses against fingerprinting here.](#)

## Detailed Results

Here's some more granular information we gathered about your browser. Your report includes examples of several different kinds of metrics:

### WEB HEADERS

Whenever you connect to a website (in our case, "<https://coveryourtracks.eff.org>"), your device sends a request that includes HTTP headers. These headers contain information like your device's timezone, language, privacy settings, and cookies. Web headers are transmitted by your browser with every site visit.

### JAVASCRIPT-DERIVED CHARACTERISTICS

Some details about your browser can be discovered by using JavaScript code. This includes fonts, certain details about your hardware configuration, and your canvas fingerprint.

Select a characteristic

User Agent ▾

DEFAULT VIEW

DETAILED VIEW

### USER AGENT

Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

Bits of identifying information: 7.0

One in x browsers have this value: 128.14

---

### HTTP\_ACCEPT HEADERS

text/html, \*/\*; q=0.01 gzip, deflate, br de,en-US;q=0.7,en;q=0.3

Bits of identifying information: 6.06

One in x browsers have this value: 66.75

---

### BROWSER PLUGIN DETAILS

undefined

Bits of identifying information: 0.86

One in x browsers have this value: 1.81

## TIME ZONE OFFSET

-120

**Bits of identifying information: 2.64**  
**One in x browsers have this value: 6.22**

---

## TIME ZONE

Europe/Vienna

**Bits of identifying information: 7.7**  
**One in x browsers have this value: 207.64**

---

## SCREEN SIZE AND COLOR DEPTH

1600x1200x24

**Bits of identifying information: 10.57**  
**One in x browsers have this value: 1521.92**

---

## SYSTEM FONTS

Arial, Bitstream Vera Sans Mono, Courier New, Times New Roman (via javascript)

**Bits of identifying information: 9.33**  
**One in x browsers have this value: 644.03**

---

## ARE COOKIES ENABLED?

Yes

**Bits of identifying information: 0.13**  
**One in x browsers have this value: 1.1**

---

## LIMITED SUPERCOOKIE TEST

DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No, openDatabase: false, indexed db: true

Bits of identifying information: 1.08

One in x browsers have this value: 2.11

---

## HASH OF CANVAS FINGERPRINT

3ecd43b98d1b5487b92cfdfb1e3e7e9e

Bits of identifying information: 7.77

One in x browsers have this value: 217.76

---

## HASH OF WEBGL FINGERPRINT

37200c952122f5d6e42baa5b5f167426

Bits of identifying information: 12.56

One in x browsers have this value: 6053.84

---

## WEBGL VENDOR & RENDERER

VMware, Inc.~llvmpipe (LLVM 7.0, 256 bits)

Bits of identifying information: 10.78

One in x browsers have this value: 1757.57

---

## DNT HEADER ENABLED?

False

Bits of identifying information: 0.95

One in x browsers have this value: 1.94

---

## LANGUAGE

de

**Bits of identifying information: 5.69**  
**One in X browsers have this value: 51.58**

---

## PLATFORM

Linux x86\_64

**Bits of identifying information: 2.95**  
**One in X browsers have this value: 7.72**

---

## TOUCH SUPPORT

Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false

**Bits of identifying information: 0.72**  
**One in X browsers have this value: 1.65**

---

## AD BLOCKER USED

False

**Bits of identifying information: 0.27**  
**One in X browsers have this value: 1.2**

---

## AUDIOCONTEXT FINGERPRINT

35.73833402246237

**Bits of identifying information: 4.14**  
**One in X browsers have this value: 17.59**

---

## CPU CLASS

N/A

Bits of identifying information: **0.14**  
One in x browsers have this value: **1.1**

## HARDWARE CONCURRENCY

1

Bits of identifying information: **8.18**  
One in x browsers have this value: **289.5**

## DEVICE MEMORY (GB)

N/A

Bits of identifying information: **1.03**  
One in x browsers have this value: **2.05**

[Back to Top ↑](#)

[RE-TEST YOUR BROWSER](#)

## 4.4 Adblock Plus

Adblock Plus schützt den Browser halbwegs gegen Werbungen und ist somit nicht so stark wie NoScript oder requestblock. Der Fingerabdruck ist fast einzigartig. Adblock Plus wird, wie requestblock, ebenfalls von der Mozilla-Erweiterungs-Website nicht empfohlen.



## Adblock Plus von Adblock Plus

Blockiere Werbeanzeigen auf Sites wie Facebook, YouTube und anderen Sites mit diesem kostenlosen Adblocker für Firefox. Adblock Plus blockiert störende Anzeigen und unterstützt Sites, indem unaufdringliche Werbung nicht blockiert wird (einstellbar).

 Entfernen

⚠ Dieses Add-on wird von Mozilla nicht aktiv auf seine Sicherheit überwacht. Stellen Sie sicher, dass Sie ihm vertrauen, bevor Sie es installieren.

Weitere Informationen

**Our tests indicate that you have some protection against Web tracking, but it has some gaps.**

### IS YOUR BROWSER:

Blocking tracking ads?	<u>Partial protection</u>
Blocking invisible trackers?	<u>Partial protection</u>
Protecting you from <u>fingerprinting</u> ?	Your browser has a nearly-unique fingerprint

Still wondering how fingerprinting works?

[LEARN MORE](#)

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

## Your Results

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 136219.0 browsers have the same fingerprint as yours.**

Currently, we estimate that your browser has a fingerprint that conveys **17.06 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can [read more about our methodology, statistical results, and some defenses against fingerprinting here](#).

## Detailed Results

Here's some more granular information we gathered about your browser. Your report includes examples of several different kinds of metrics:

### WEB HEADERS

Whenever you connect to a website (in our case, "<https://coveryourtracks.eff.org>"), your device sends a request that includes HTTP headers. These headers contain information like your device's timezone, language, privacy settings, and cookies. Web headers are transmitted by your browser with every site visit.

### JAVASCRIPT-DERIVED CHARACTERISTICS

Some details about your browser can be discovered by using JavaScript code. This includes fonts, certain details about your hardware configuration, and your canvas fingerprint.

Select a characteristic

User Agent

DEFAULT VIEW

DETAILED VIEW

### USER AGENT

Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

Bits of identifying information: 7.0

One in x browsers have this value: 128.15

---

### HTTP\_ACCEPT HEADERS

text/html, \*/\*; q=0.01 gzip, deflate, br de,en-US;q=0.7,en;q=0.3

Bits of identifying information: 6.06

One in x browsers have this value: 66.74

---

### BROWSER PLUGIN DETAILS

undefined

Bits of identifying information: 0.86

One in x browsers have this value: 1.81

## TIME ZONE OFFSET

-120

**Bits of identifying information: 2.64**  
**One in x browsers have this value: 6.22**

---

## TIME ZONE

Europe/Vienna

**Bits of identifying information: 7.7**  
**One in x browsers have this value: 207.33**

---

## SCREEN SIZE AND COLOR DEPTH

1600x1200x24

**Bits of identifying information: 10.57**  
**One in x browsers have this value: 1522.0**

---

## SYSTEM FONTS

Arial, Bitstream Vera Sans Mono, Courier New, Times New Roman (via javascript)

**Bits of identifying information: 9.33**  
**One in x browsers have this value: 644.06**

---

## ARE COOKIES ENABLED?

Yes

**Bits of identifying information: 0.13**  
**One in x browsers have this value: 1.1**

---

### LIMITED SUPERCOOKIE TEST

DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No, openDatabase: false, indexed db: true

**Bits of identifying information: 1.08**  
**One in x browsers have this value: 2.11**

---

### HASH OF CANVAS FINGERPRINT

3ecd43b98d1b5487b92cfdfb1e3e7e9e

**Bits of identifying information: 7.77**  
**One in x browsers have this value: 217.78**

---

### HASH OF WEBGL FINGERPRINT

37200c952122f5d6e42baa5b5f167426

**Bits of identifying information: 12.56**  
**One in x browsers have this value: 6054.18**

---

### WEBGL VENDOR & RENDERER

VMware, Inc.~llvmpipe (LLVM 7.0, 256 bits)

**Bits of identifying information: 10.78**  
**One in x browsers have this value: 1757.66**

---

### DNT HEADER ENABLED?

False

**Bits of identifying information: 0.95**  
**One in x browsers have this value: 1.94**

---

## LANGUAGE

de

**Bits of identifying information: 5.69**  
**One in x browsers have this value: 51.57**

---

## PLATFORM

Linux x86\_64

**Bits of identifying information: 2.95**  
**One in x browsers have this value: 7.72**

---

## TOUCH SUPPORT

Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false

**Bits of identifying information: 0.72**  
**One in x browsers have this value: 1.65**

---

## AD BLOCKER USED

False

**Bits of identifying information: 0.27**  
**One in x browsers have this value: 1.2**

---

## AUDIOCONTEXT FINGERPRINT

35.73833402246237

**Bits of identifying information: 4.14**  
**One in x browsers have this value: 17.59**

---

#### CPU CLASS

N/A

Bits of identifying information: **0.14**  
One in x browsers have this value: **1.1**

---

#### HARDWARE CONCURRENCY

1

Bits of identifying information: **8.18**  
One in x browsers have this value: **289.52**

---

#### DEVICE MEMORY (GB)

N/A

Bits of identifying information: **1.03**  
One in x browsers have this value: **2.05**

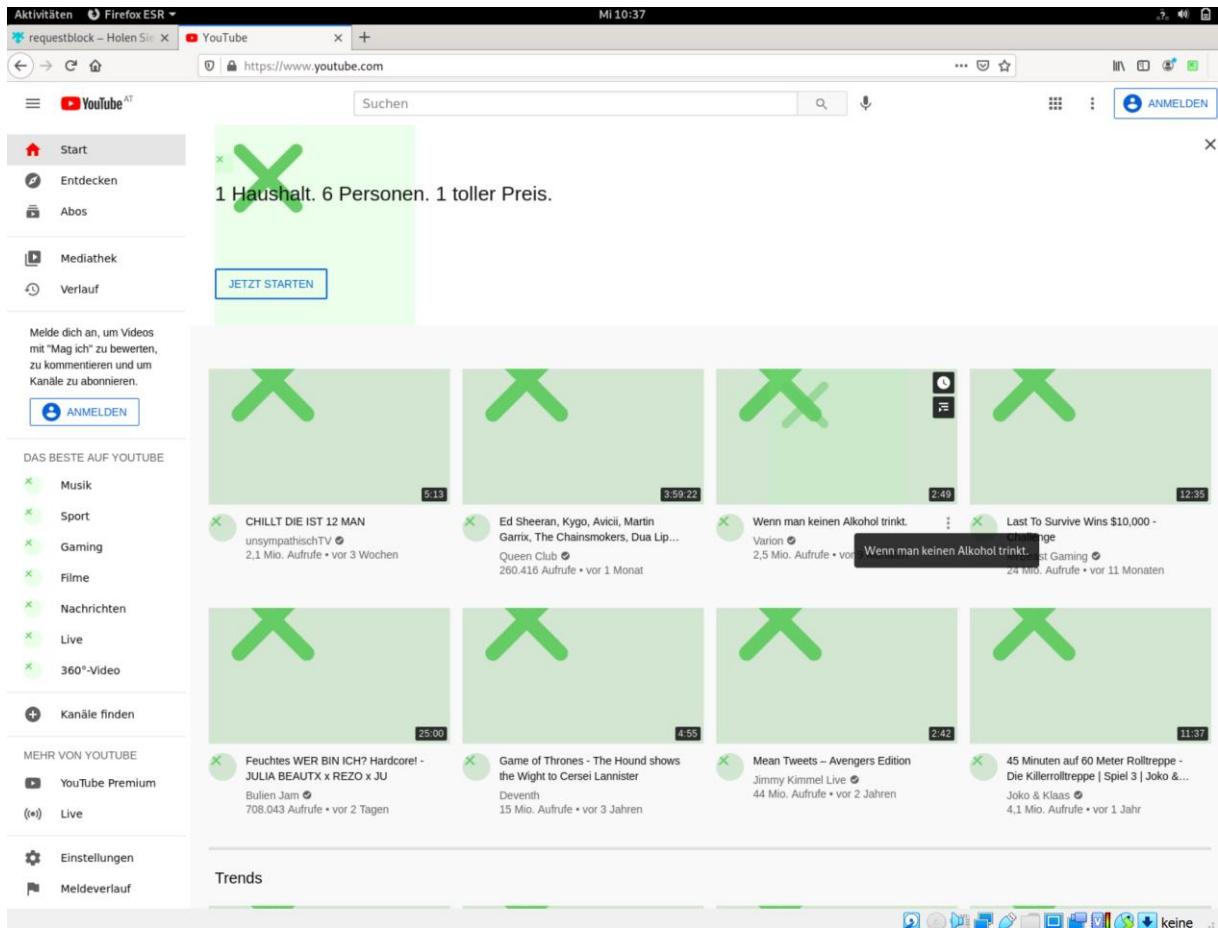
---

[Back to Top ↑](#)

[RE-TEST YOUR BROWSER](#)

## 4.5 Testen der einzelnen Erweiterungen auf der bekannten Website YouTube

NoScript macht einen Blackscreen über die Werbung bei YouTube, während requesteblock auf der Website alles blockiert, sodass nichts mehr funktioniert. Hier ein Beispiel anhand eines Bildes:



AdBlock hat keine Auswirkungen auf die YouTueb-Website.

## 5 Ergebnisse

NoScript ist ein sehr guter Add-on weil er nicht zu übertrieben und aggressive arbeitet, wie z.B.: requestblock. AdBlock würde ich in meinem Browser auch aktiviert lasse.

## 6 Kommentar

Nun habe ich einen Überblick über drei verschiedene Add-ons und kann gut einschätzen, welchen Add-on ich verwenden will.

## Über diese Erweiterung

### WICHTIG

[Eine Anleitung in die Grundlagen von NoScript 10](#)

Ist die neue Oberfläche von NoScript 10 immer noch ungewohnt?  
Sehen Sie sich diese [von Nutzern erstellte NoScript 10 Einführung](#) und diesen [Vergleich zwischen NoScript 10 "Quantum" und NoScript 5 "Classic"](#) an.

Als Gewinner des "PC World World Class Award" und ausgeliefert als Teil des Tor Browsers bietet Ihnen NoScript den besten verfügbaren Schutz im Internet.

Mit NoScript können Sie JavaScript, Flash, Java und andere ausführbare Inhalte bloß auf vertrauenswürdigen Domains Ihrer Wahl zulassen, z.B. beim Online-Banking. Somit verhindern Sie aus der Ferne ausnutzbare Schwachstellen inklusive Spectre und Meltdown.

Ihre vertrauenswürdigen Bereiche werden dank der einmaligen ClearClick Technologie gegen seitenübergreifende Scripting-Attacken (XSS), Cross-Zone DNS Rebinding / CSRF Attacken (Router Hacking), und Clickjacking-Versuche geschützt.

Dieser präventive Ansatz verhindert das Ausnutzen von (bekannten und unbekannten!) Sicherheitslücken ohne Verlust an Funktionalität, wo Sie diese benötigen.

Experten sind sich einig: Firefox wird wirklich noch sicherer mithilfe von NoScript ;)

FAQ: <https://noscript.net/faq>

Forum: <https://noscript.net/forum>