

GUERILLAPÄDAGOGIK IN DER INFORMATIONSTECHNIK: WIE PRIMARSCHÜLERINNEN DEIN PASSWORT CRACKEN

Winterkongress der Digitalen Gesellschaft 2019-02-23

Harald von Waldow <blackbelly@computerdetektive.ch>

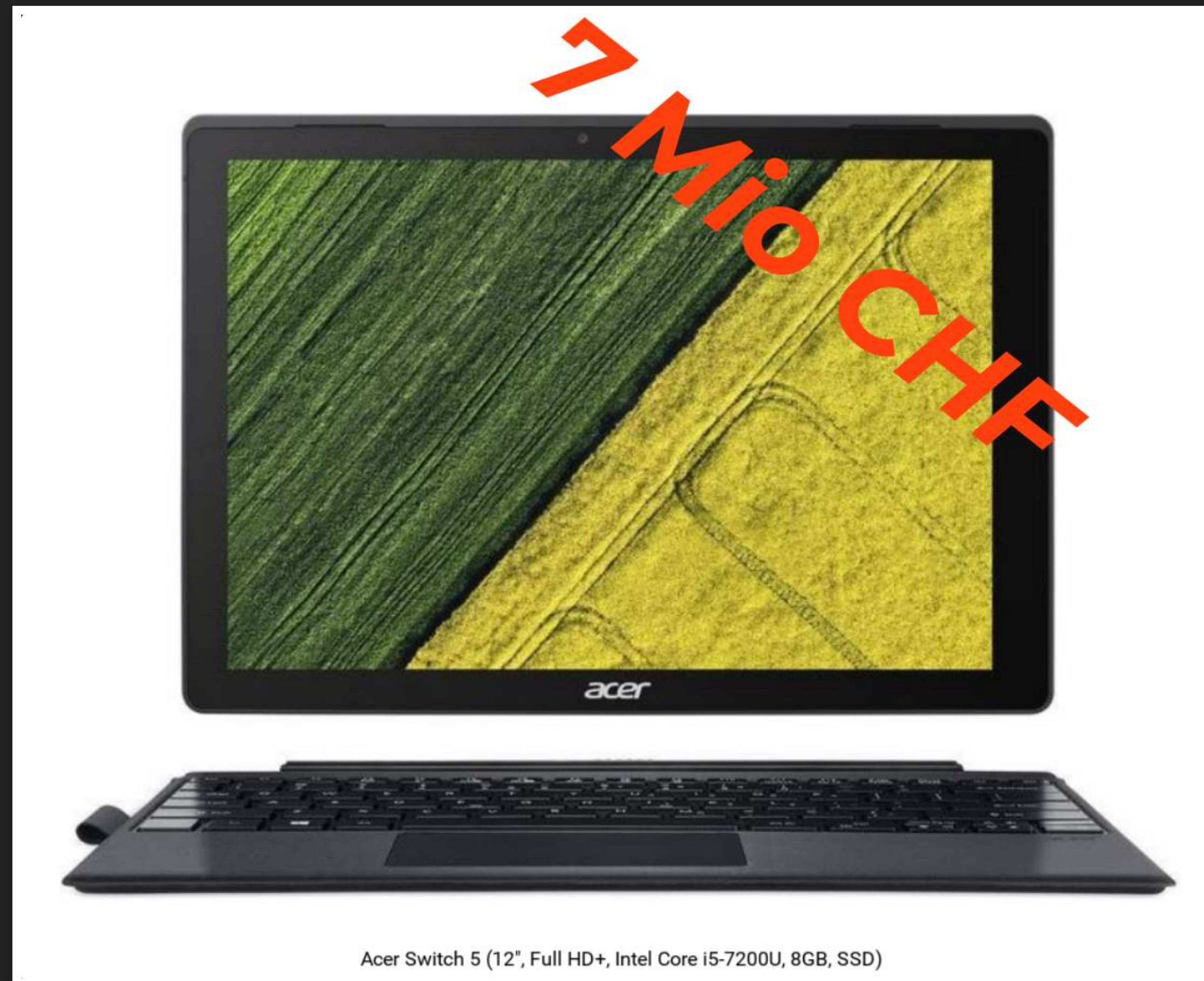
Ranjan Benz



WORUM GEHT ES?

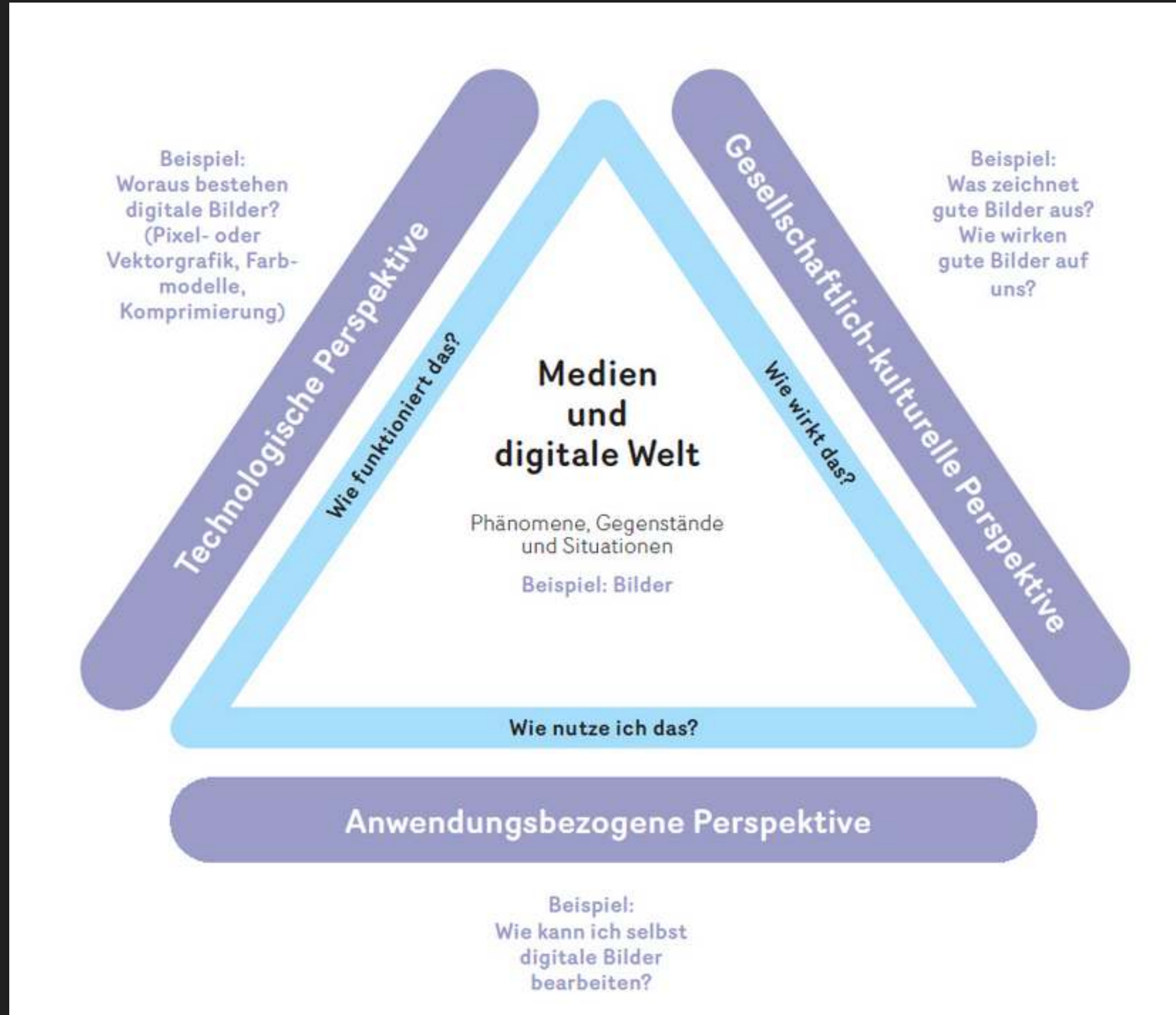
COMPUTERDETEKTIVE

- Ein IT Kurs für Primaschülerinnen
- Klassenstufen 4 - 6 (9 - 12 Jahre)
- 12 Termine à 1h 45m im GZ
Zürich-Seebach
- September - Dezember 2018



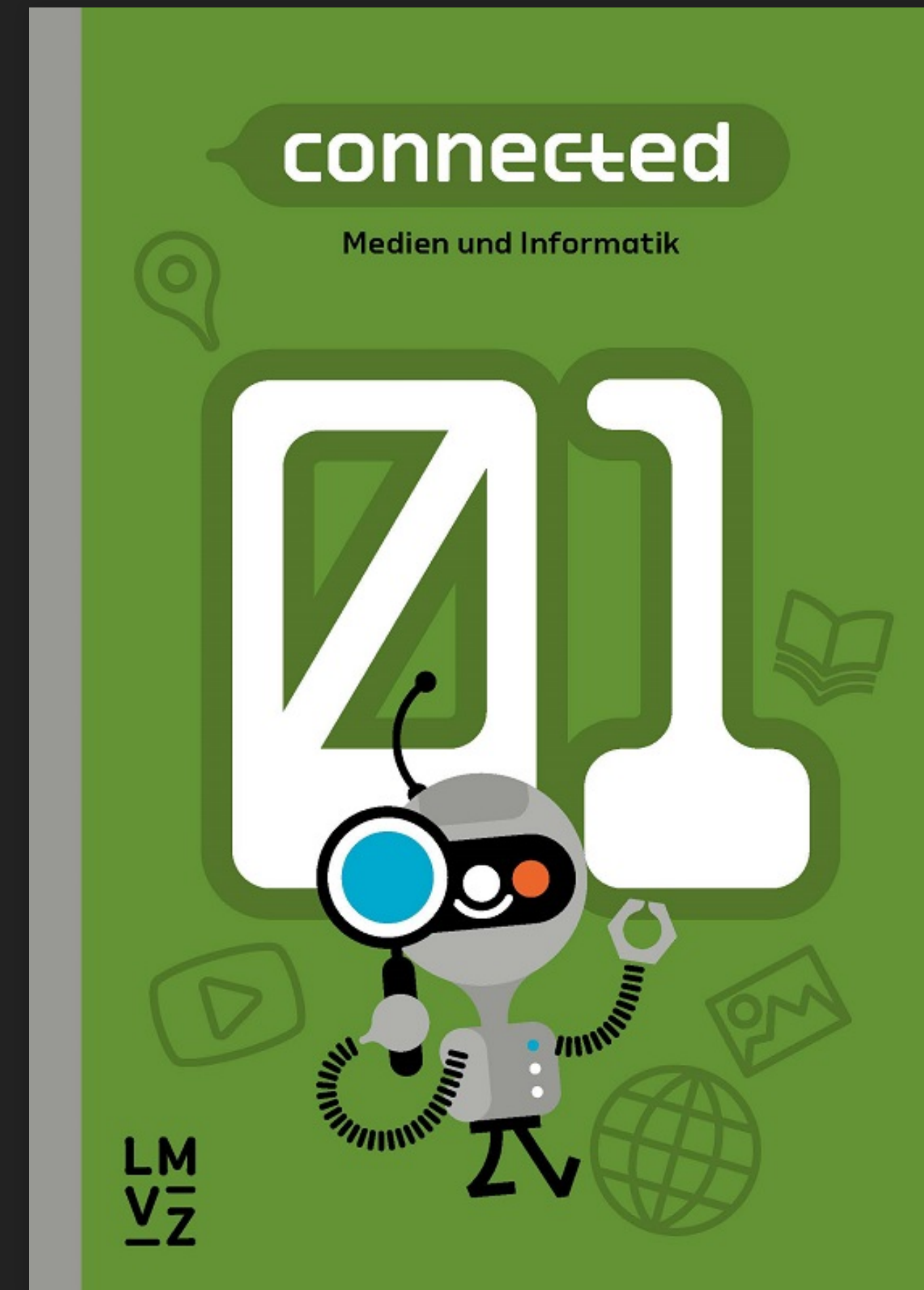
- "Digitale Bildung" ist in aller Munde
- **Lehrplan 21**: "Medien und Informatik"
- Ab diesem Schuljahr, ab Klasse 5

MOTIVATION



Quelle: [Lehrmittelverlag Zürich](#)

- Beispiel *Bilder*
- Wichtige Grundlage?



Quelle: [Lehrmittelverlag Zürich](#)

- Kunst & Zeichenunterricht?
- Macht 20% des Lehrbuchs aus!

ELTERNPERSPEKTIVE

- Tragfähige technische Grundlagen
- Souveräner Umgang mit dem Computer
 - "Ich passe die Maschine meinen Bedürfnissen an, nicht umgekehrt."
- ⇒ Grundlage für Kreativität
- Sicherheit, Datenschutz, Privatsphäre
- Schutz vor Angriffen, "bösen Männern", Betrug, Datenklau

GESELLSCHAFTLICHE PERSPEKTIVE

- Digitalisierung durchdringt alle gesellschaftlichen Bereiche.
 - Wir sind überfordert.
 - Beispiele aus der Tagespolitik:
 - Überwachungs- und Manipulationsskandale (FB, Google, Microsoft, ...)
 - "Netzsperrern" (Geldspielgesetz)
 - E-Voting Debatte
 - Debatten und Reaktionen sind durch technische Ignoranz geprägt.
- => Es besteht massiver Bildungsbedarf

~~*"Machs doch besser, wenn dich so viel stört!"*~~

*"Versuche etwas anderes, das hoffentlich
Sinn macht"*

VORHABEN

- Technische Grundlagen mit langer Halbwertszeit vermitteln.
 - Direkt anwendbares technisches Know-How vermitteln; Spass und Nutzen.
 - Ein paar essentielle digitale Überlebensregeln vermitteln.
- Begeisterung und Selbstvertrauen wecken!
 - Ich kann die Maschine beherrschen und verstehen; sie gehorcht mir.
 - Meiner Kreativität sind praktisch keine Grenzen gesetzt.
 - Ein Computer ist viel mehr, als ein Gerät mit vielen Knöpfen.

SETUP



- Laptops: 10 (geliehen von [Labdoo.org](https://labdoo.org)) + 3
- 5 Schul-Tablets
- 16 Memory-Sticks (booten angepasstes Ubuntu 18.04 / Gnome 3)
- Mäuse, Adapter, lose Komponenten
- 2 Desktop PCs

SETUP

- 12 Teilnehmer/innen:
5 Maidli, 7 Buebe, 9 x 5. Klasse, 1 x 3. Klasse 1 x 6.Klasse
- Computerraum im GZ-Seebach

SO IT BEGINS

- Detektivstory => kaputter Computer
- Gehäuse, Mainboard, CPU, Lüfter, RAM, Festplatte
 - Was ist das?
 - Wozu dient das?
- Anfassen, einbauen

SCHNITZELJAGT

- Ein 2. Rechner muss gefunden werden!
- Koordinaten?
=> openstreetmap.org, maps.google.com, [swisstopo](https://www.swisstopo.ch)
- Oh, kein WLAN - Passwort!

Was tun Erwachsene oft mit Passwörter?

- SSID / Hotspot / Signalstärke

Achtung: Nur in Betrieb nehmen, wenn du Hardware von Software unterscheiden kannst!

NOTFALLPROZEDUR FUER G.A.S.P

FILESYSTEM

Wenn du diesen Text liest, ist etwas schief gelaufen und unser Projekt ist in Gefahr. Wahrscheinlich wurden wir von unseren Gegnern ueberrascht und mussten fliehen. Es liegt an dir, unseren Plan jetzt auszufuehren!

Wir brauchen deine Hilfe, aber nur, wenn du dich mit Computern auskennst, sonst hast du keine Chance. Der Notfallplan ist deshalb auf diesem Rechner gut geschuetzt und verschlueselt versteckt. Finde als erstes die Datei mit dem Namen

- Finde eine Datei mit einem bestimmtem Namen.
- Finde Datei mit bestimmtem Inhalt!
- Und zwar in einem Verzeichnisbaum mit
 - 64 directories,
 - 168 files,
 - mit insgesamt 144 MB interessantem Inhalt

```
##### End of Transmission #####
darlene@riddle-1:~$
darlene@riddle-1:~$
```


GUI:

- Kennenlernen von Filetypen und ihren Endungen
- Typische File-Größen
- Welche Anwendungen starten, wenn man draufklickt?
- Struktur eines Verzeichnisbaums

CLI:

- Filetransfer

```
rsync -rv darlene@192.168.1.9:secret_sauce .
```

- Finde Datei mit bestimmtem Namen

```
find . -name "L1D1ueber.ods"
```

- Finde Datei mit bestimmtem Inhalt!

```
grep -Hr "G.A.S.P." .
```


NOTFALLPROZEDUR FUER G.A.S.P

CLIFFHANGER

#####

Wenn du diesen Text liest, ist etwas schief gelaufen und unser Projekt ist in Gefahr. Wahrscheinlich wurden wir von unseren Gegnern ueberrascht und mussten fliehen. Es liegt an dir, unseren Plan jetzt auszufuehren!

Wir brauchen deine Hilfe, aber nur, wenn du dich mit Computern auskennst, sonst
Der Notfallplan ist deshalb auf diesem Rechner

Code: ROT13

Qh unfg nyfb nhpu qvr mjrvgr Anpuevpug trshaqra haq ragfpuyüffryg. Thg trznpug!

Qra aäpufgra jvpugvtra Nhsgent reuäyfg qh nhs qvrfre Jrofrvgr:

fpvraprqngn.pu/tnfc_abgsnyycebgbxbyy.ugzy

-----> end of transmission -- G.A.S.P./4711-12 <-----

#####

darlene@riddle-1:~\$

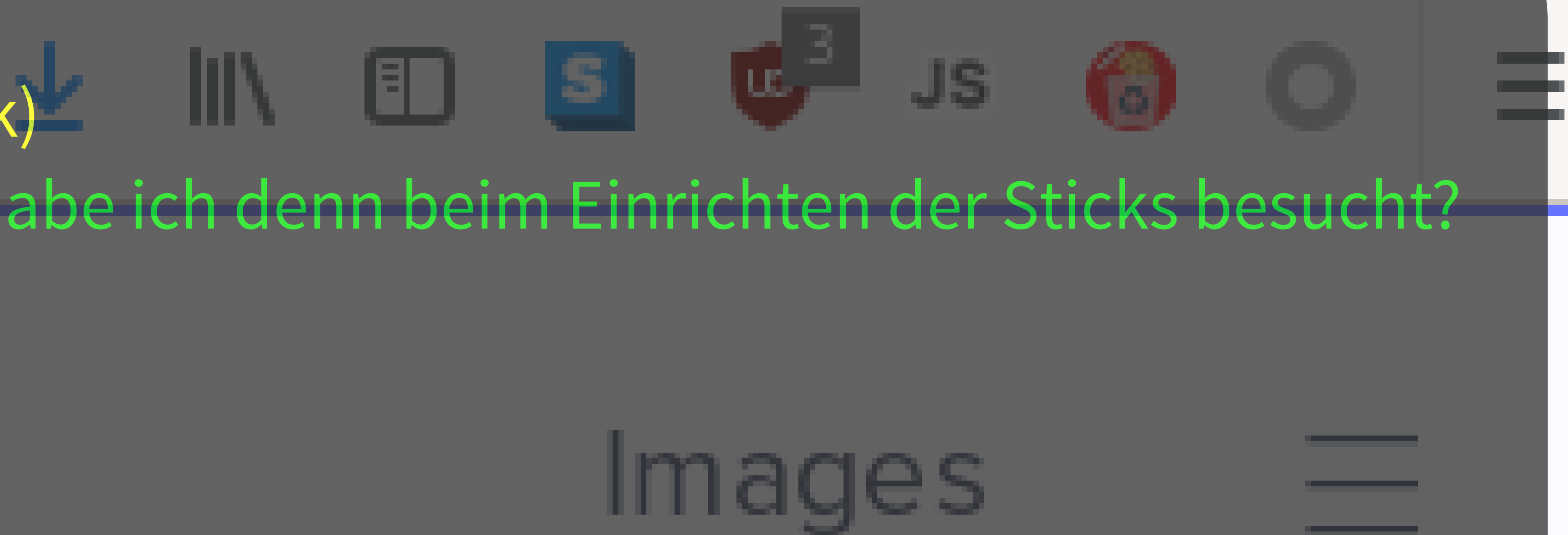
darlene@riddle-1:~\$ █

BROWSER BASICS

- Bookmarks (Lesezeichen)
- Tabs
- History (Chronik)

Welche Seiten habe ich denn beim Einrichten der Sticks besucht?

- History löschen
- Private mode
- Plugins
 - uBlock origin
 - Toggle-JS
 - HTTPS Everywhere
 - Cookiemanager



BROWSER BASICS

D E M O

- uBlock origin
- JS-Toggle
- [tagi.ch](#) und [SPON](#)

WEBSEITEN

The screenshot shows a web browser with developer tools open. The browser's address bar shows a URL from 'stadt-zuerich.ch'. The developer tools are open to the 'Elements' panel, showing the HTML structure of the page. The page content is a list of school staff members, including 'Klassenlehrpersonen', 'Kindergartenlehrpersonen', 'Fachlehrpersonen', 'Betreuungspersonen', and 'Schulsozialarbeit'. A contact form is also visible, with the name 'Matze Zimtstern' highlighted in red. The developer tools show the HTML structure of the page, including the 'div#content.layout_column' and the 'div#content.layout_column'.

Columns: div#content.layout_column

activitymap.
page=schulen/de/buhn/ueberuns/kontakt
link=Fachlehrpersonen
region=BODY
pageIDType=1
.activitymap
.a
.c
pid=schulen/de/buhn/ueberuns/kontakt
pidt=1
oid=https://www.stadt-zuerich.ch/schulen/de/buhn/ueberuns/kontakt/fachlehrpersonen.html
qt=A
s=1920x1200

- Wir können das Web ändern!
- Nicht ganz wirklich, aber ...

SUCHMASCHINEN

Es gibt gute Gründe, Google zu vermeiden. Benutze

- startpage.com
- duckduckgo.com

SUCH-OPERATOREN

Startpage-Metasuche:

```
url:"supported-by-startpage" site:startpage.com
```

Musik-Suche:

```
https://www.google.com/search?q=title:"index of"+mp3+eminem
```

Kann laut werden!

Code: ROT13

 Qh unfg nyfb nhpu qvr mjrvgr Anpuevpug trshaqra haq ragfpuyüffryg. Thg
 trznpug!

Qra aäpufgra jvpugvtra Nhsgent reuäyfg qh nhs qvrfre Jrofrvgr:

fpvraprqngn.pu/tnfc_abgsnyycebgbxbyy.ugzy

-----> end of transmision -- G.A.S.P./4711-12 <-----

- Suche im Netz: Was ist das?
- Wie kann ich das entschlüsseln?

Du hast also auch die zweite Nachricht gefunden und entschlüsselt. Gut gemacht!

Den nächsten wichtigen Auftrag erhältst du auf dieser Webseite:

https://sciencedata.ch/gasp_notfallprotokoll.html

WHOIS

```
harald@w1:~/private/digiges2019$ whois sciencedata.ch
This information is subject to an Acceptable Use Policy.
See https://www.nic.ch/terms/aup/
```

```
Domain name:
sciencedata.ch
```

```
Holder of domain name:
Harald Von Waldow
[redacted]
[redacted]
Switzerland
```


JUNIOR CAPTURE THE FLAG

- Eigentlich ein Trainingsformat für Computersicherheitsfachleute
- Abgewandelt, um Kinder spannend und "realistisch" mit UNIX und bash vertraut zu machen.
- Merci beaucoup à Axelle Apvrille ( @cryptax) , die das erfunden und viele Challenges geschrieben hat!
- **CTFd**: CTF - Framework, das Teams, Aufgaben, Punkte, etc. verwaltet.
- **juniorctf**: Aufgaben (und Stories) und ein Docker-Container pro Challenge.
- Aufgaben werden auf via Terminal auf einem entfernten Computer (= Docker-Container) gelöst.

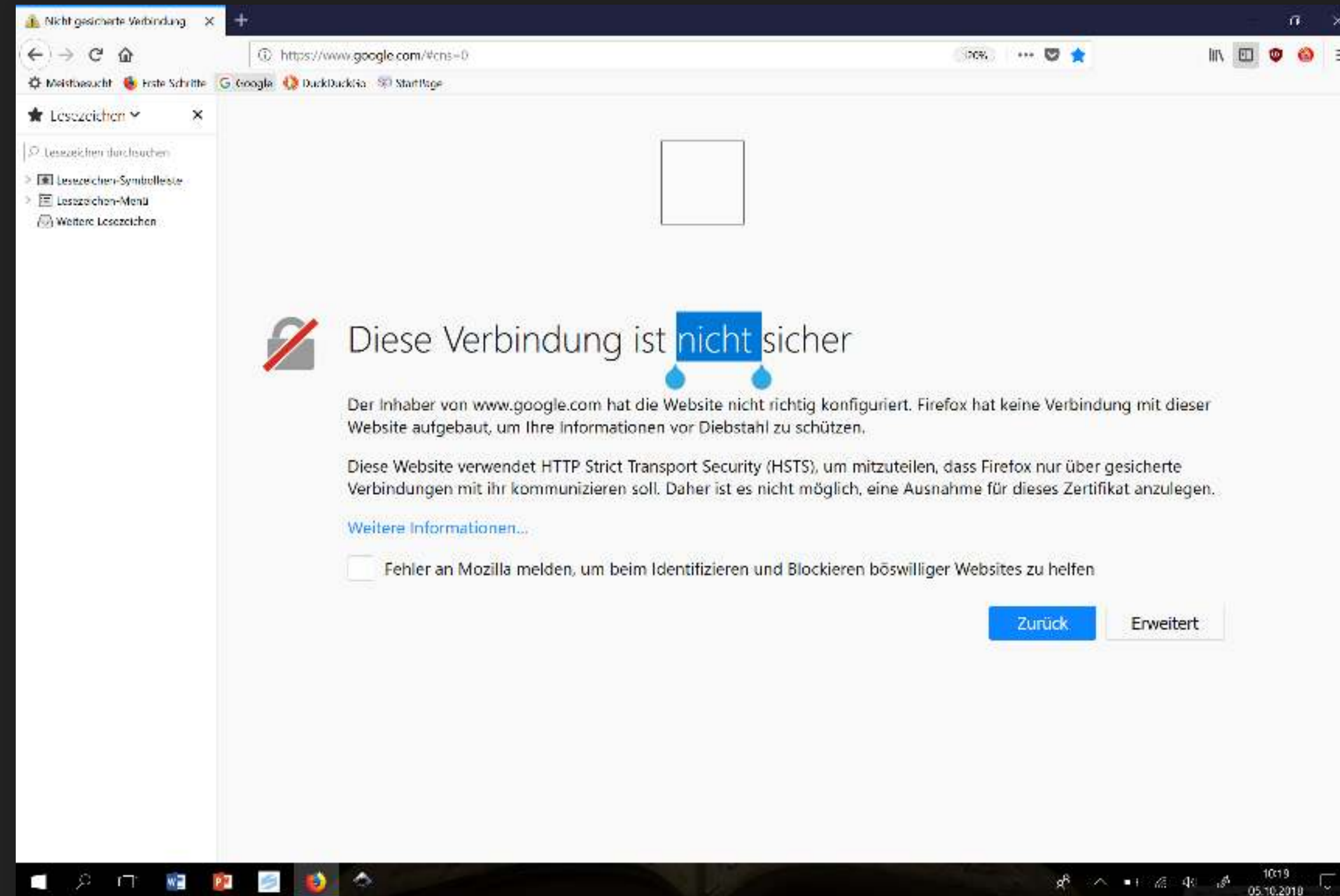
ANONY SURFEN



Alexander Lehmann

- Eigene IP-Adresse & Geoinfo via browserleaks.com/ip
- Vergleich mit scheinbarer Ursprungs-IP mit Tor-Browser.
- => Die ganze Welt und die Schweiz mitten drin.
- Was passiert mit euren Suchergebnissen?

DAS SCHULNETZ BESCHÜTZT DICH



- IE auf Schul-Tablet akzeptiert gefälschte SSL-Zertifikate.
- Firefox bringt eigene root-CAs mit. => Bemerkt MITM-Angriff.
- Warum? Was kann ich tun, um mich selbst vor unerwünschten Inhalten zu schützen?

EINE MAIL AUS DEM HAUPTQUARTIER

```
From: G.A.S.P. Hauptquartier <gasp-hq@computerdetektive.ch>  
To: blackbelly@computerdetektive.ch  
Subject: ODK-Einsatz 2018  
Date: Thu, 6 Dec 2018 13:59:27 +0100  
  
Von: G.A.S.P. Hauptquartier  
  
An: Alle Instruktoren  
  
Betrifft: Trainingseinheiten für Computerdetektive / Klasse 2018  
  
---- msg start -----  
  
Alle Detektive, die die CTF-Unix Lektionen und die Lektion  
"Tor-Netzwerk" absolviert haben, bekommen weitere Anweisungen auf  
dieser  
Webseite:  
  
http://sciencedata.ch/geoblocked/  
  
----- msg end -----
```

sciencedata.ch/geoblocked

EINIGE TAKE-AWAYS

- Scratch wird möglicherweise überschätzt - nächstes Mal versuchen wir Turte als Programmiersprache.
- Es gib Primarschülerinnen, die können und wollen die Kommandozeile benutzen!
- Online(Web)-Spiele sind die Pest. Nächstes mal vielleicht einen Pi-Hole vorschalten?
- juniorCTF ist eine absolute Geheimwaffe, die für nächstes Mal massiv ausgebaut wird.

DANKE

 Labdoo.org für die Laptops

 für die Räumlichkeiten

Den Computerdetektiven Seebach fürs mitmachen!

