

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

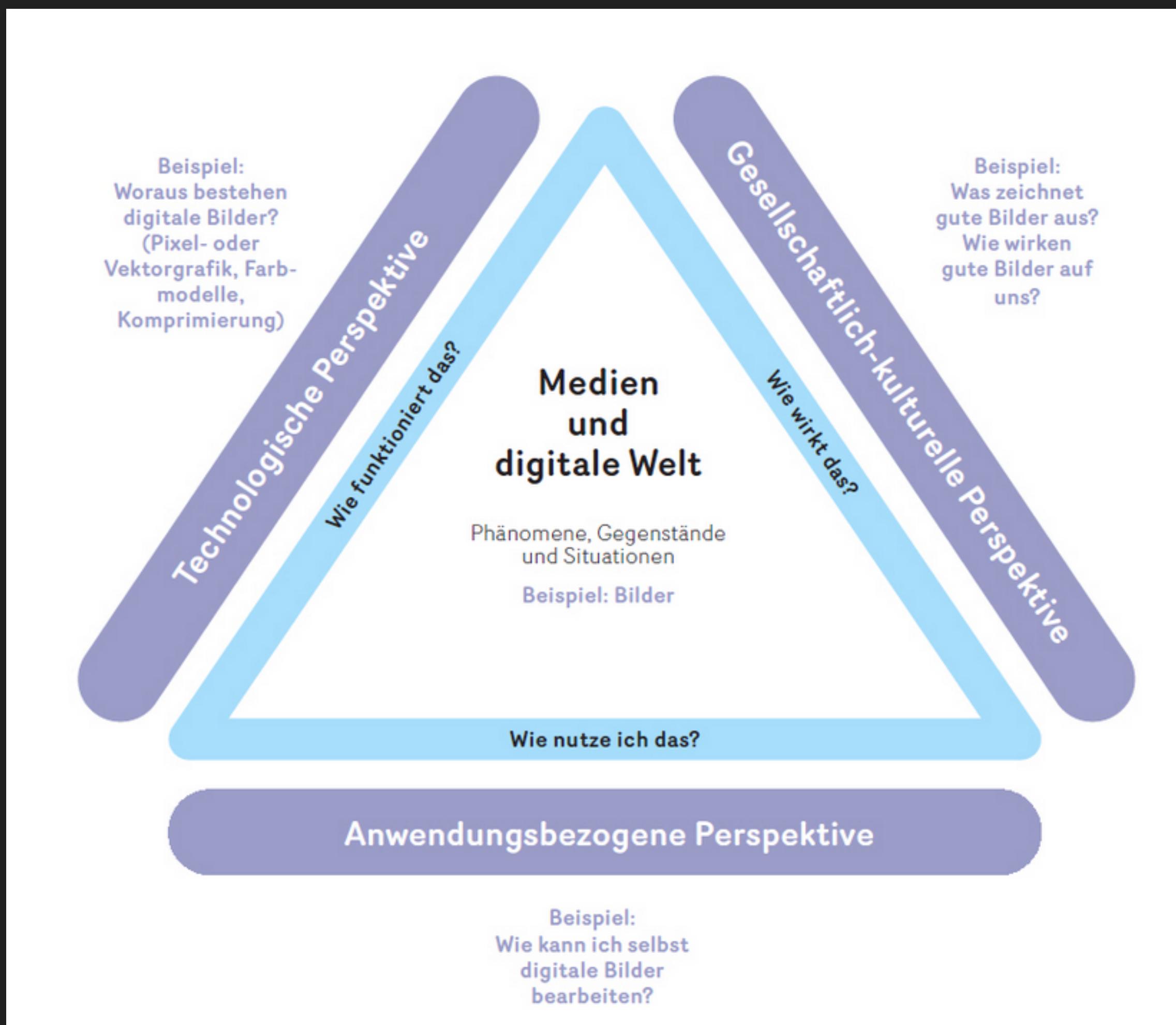
MOTIVATION



Acer Switch 5 (12", Full HD+, Intel Core i5-7200U, 8GB, SSD)

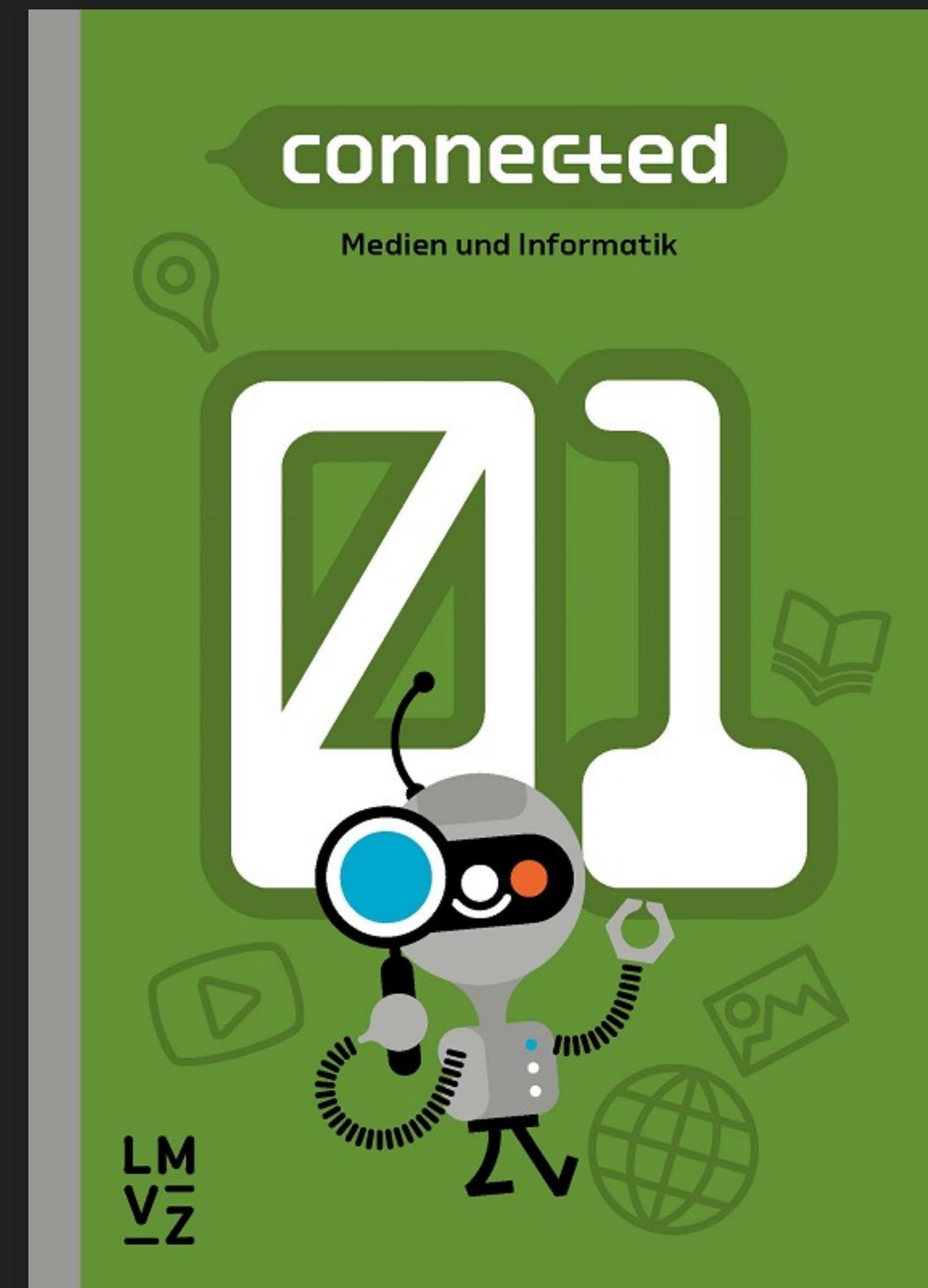
- "Digitale Bildung" ist in aller Munde
- **Lehrplan 21:** "Medien und Informatik"
- Ab diesem Schuljahr, ab Klasse 5

MOTIVATION



Quelle: Lehrmittelverlag Zürich

- Beispiel *Bilder*
- Wichtige Grundlage?



Quelle: Lehrmittelverlag Zürich

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

MOTIVATION

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

MOTIVATION

GESELLSCHAFTLICHE PERSPEKTIVE

- Digitalisierung durchdringt alle gesellschaftlichen Bereiche.
- Wir sind überfordert.
- Beispiele aus der Tagespolitik:
 - Überwachungs- und Manipulationsskandale (FB, Google, Microsoft, ...)
 - "Netzsperren" (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"*

MOTIVATION

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) + 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



- 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](http://swisstopo.ch)
- Oh, kein WLAN - Passwort!
Was tun Erwachsene oft mit Passwörter?
- SSID / Hotspot / Signalstärke
(47.42463, 8.54406)

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 Na

- 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

```
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 überrascht und mussten fliehen. Es liegt an dir, unseren Plan jetzt auszuführen!

Wir brauchen deine Hilfe, aber nur, wenn du dich mit Computern auskennst, sonst
wirfst du uns sicher wieder ein. Der Notfallplan ist deshalb auf diesem Rechner
gespeichert. Bitte lade die Datei mit dem Namen

Code: ROT13

Qh unfg nyfb nhpu qvr mjrvgr Anpuevug trshaqra haq ragfpuyüffryg. Thg trznug!

Qra aäpufgra jvpugvtra Nhsgent reuäyfg qh nhs qvrfre Jrofrvgr:

fpvraprqngn.pu/tnfc_abgsnyycebgbxbyy.ugzy

-----> end of transmision -- 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

Images

BROWSER BASICS

D E M O

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

pdfIcon wikipedia

Console Inspector Debugger Style Editor Performance Memory Network Storage Accessibility HTTP

Search HTML

WEBSEITEN

Filter Styles

inline

green and (min-width: 1025px) label, .mod_contactcard

rem+ ↴

label, margin ↴ { 75; ↴

var_small, main.css:15702 label, margin ↴ { ↴

W01_71488914, "Helvetica, Arial, sans-serif"; ↴

green and (min-width: 1025px) guidePanelNode .guidePanelNode

guidePanelNode ion, h4 ↴ { rem+ ↴

guidePanelNode main.css:953 guidePanelNode

guidePanelDescription, h4 ↴

columns > div#content.layout_column

wichtige Links unserer Schule +

Klassenlehrpersonen

Kindergartenlehrpersonen

Fachlehrpersonen

Betreuungspersonen

Schulsozialarbeit

Ruth Bannwart

Deutsch als Zweitsprache

Kontaktformular

Mattia Gimino Matze Zimtstern

Fachunterricht

Kontaktformular

Denisa Delic

Integrative Förderung, Deutsch als Zweitsprache Kindergarten

- 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
trznug!

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 erhälst du auf dieser Webseite:

https://sciencedata.ch/gasp_notfallprotokoll.html

EXKURS

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.

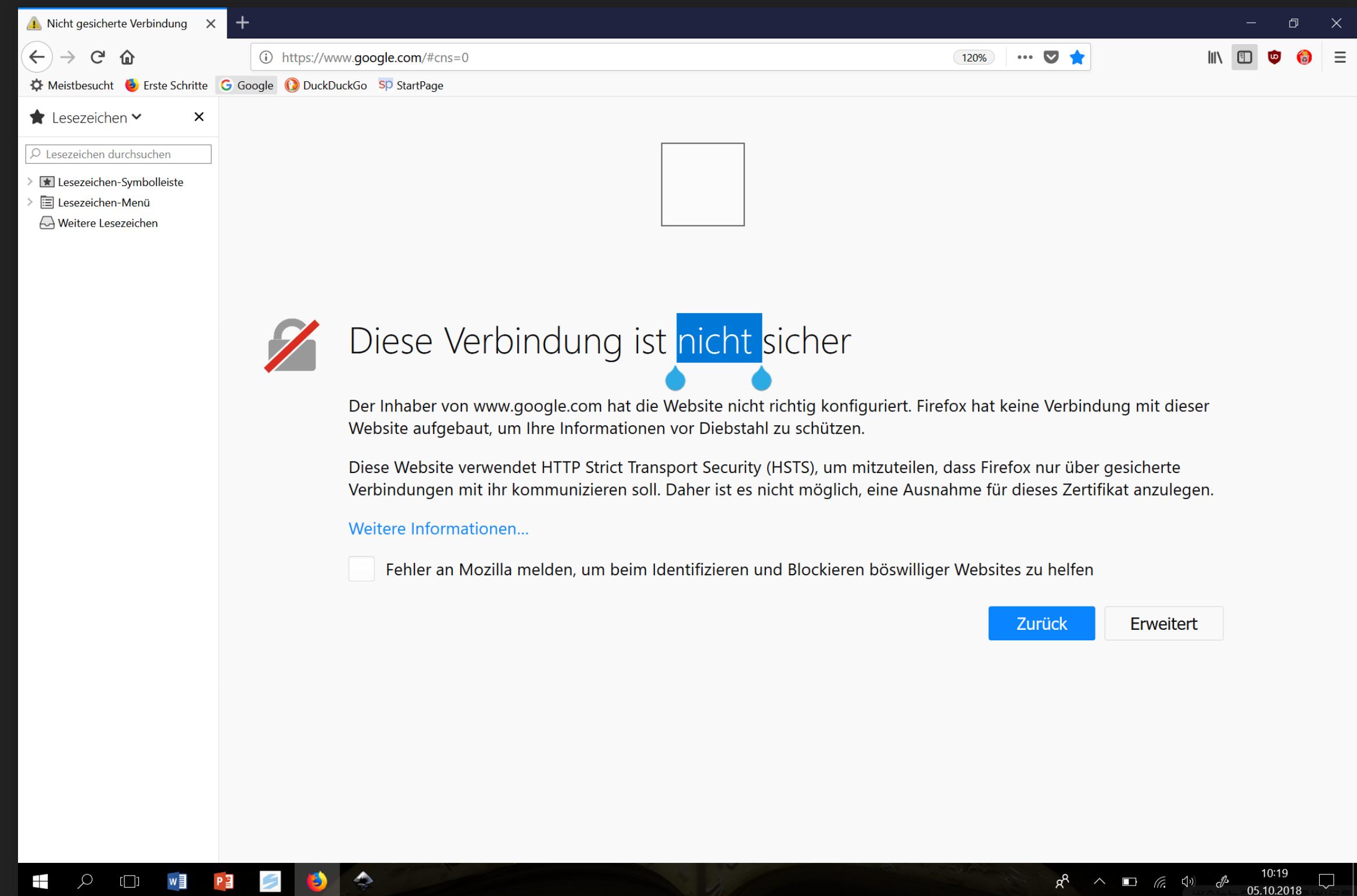
ANONY SURFEN



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 Lktionen und die Lktion "Tor-Netzwerk" absolviert haben, bekommen weitere Anweisungen auf dieser
Webseite:

<http://sciedata.ch/geoblocked/>

----- msg end -----

sciedata.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

gzseebach

für die Räumlichkeiten

Den Computerdetektiven Seebach fürs mitmachen!

