

# Social Engineering for Fun, Profit and Science

## Definition Verfassungsschutz

---

Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung, meist unter Verschleierung der eigenen Identität (Verwenden einer Legende). Social Engineering hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.

Gut Lügen und Betrügen um an kostenlose Dienstleistungen oder Informationen zu kommen

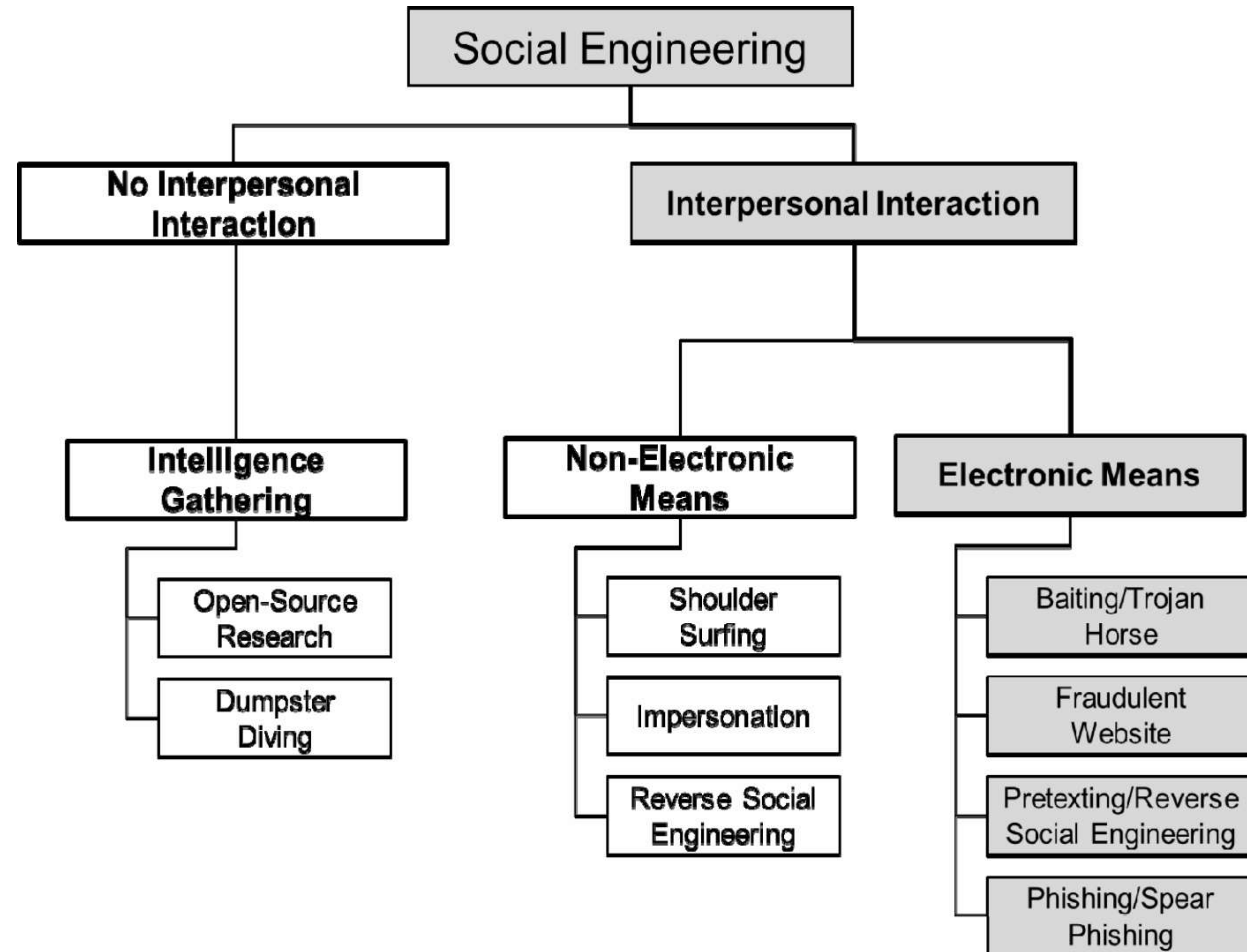
# Social Engineering, more art than science?

Wenig Methodik, im wissenschaftlichen Diskurs oft als „Hokus-Pokus“ abgetan

Einer der meist genutzten Initial Infection Vectors

Nutzer müssen aufwendig geschult werden, keine Patches.

Nutzer ohne technisches Hintergrundwissen zu schulen ist ein Problem



PERSONENBEZOGENER  
KONTAKT

EINE FREMDE  
WEBSITE SOLL  
BESUCHT WERDEN

DATEI/EN SOLLEN  
HERUNTERGELADEN/  
GEÖFFNET WERDEN

BESTIMMTE  
HANDLUNG SOLL  
AUSGEFÜHRT WERDEN



## Prince of Nigeria (419 Scam)

„An Old Swindle Revived“ – New York Times,  
1898

The method now in use follows that adopted when the swindle was begun so closely as to indicate that it is and has been successful. A man in this country receives a letter from a foreign city. Havana used to be a favorite place, but it is not used now, probably because communication with it is so frequent and easy. The letter is written on thin, blue, cross-lined paper, such as is used for foreign letters, and is written as fairly well-educated foreigners write English, with a word misspelled here and there, and an occasional foreign idiom. The writer is always in jail because of some political offense. He always has some large sum of money hid, and is invariably anxious that it should be recovered and used to take care of his young and helpless daughter by some honest man. He knows of the prudence and good character of the recipient of the letter through a mutual friend, whom he does not

## Prince of Nigeria (419 Scam)

„An Old Swindle Revived“ – New York Times,  
1898

Nigeria wird politischer und wirtschaftlicher  
Unruhen zum florierenden Scamming-Ort,  
~1980

The method now in use follows that adopted when the swindle was begun so closely as to indicate that it is and has been successful. A man in this country receives a letter from a foreign city. Havana used to be a favorite place, but it is not used now, probably because communication with it is so frequent and easy. The letter is written on thin, blue, cross-lined paper, such as is used for foreign letters, and is written as fairly well-educated foreigners write English, with a word misspelled here and there, and an occasional foreign idiom. The writer is always in jail because of some political offense. He always has some large sum of money hid, and is invariably anxious that it should be recovered and used to take care of his young and helpless daughter by some honest man. He knows of the prudence and good character of the recipient of the letter through a mutual friend, whom he does not

## Prince of Nigeria (419 Scam)

„An Old Swindle Revived“ – New York Times, 1898

Nigeria wird politischer und wirtschaftlicher Unruhen zum florierenden Scamming-Ort, ~1980

Unzählige Variationen des Scams im Umlauf

The method now in use follows that adopted when the swindle was begun so closely as to indicate that it is and has been successful. A man in this country receives a letter from a foreign city. Havana used to be a favorite place, but it is not used now, probably because communication with it is so frequent and easy. The letter is written on thin, blue, cross-lined paper, such as is used for foreign letters, and is written as fairly well-educated foreigners write English, with a word misspelled here and there, and an occasional foreign idiom. The writer is always in jail because of some political offense. He always has some large sum of money hid, and is invariably anxious that it should be recovered and used to take care of his young and helpless daughter by some honest man. He knows of the prudence and good character of the recipient of the letter through a mutual friend, whom he does not



Ladies and Gentlemen,  
I'm a rich prince from Nigeria and I am with you in an urgent matter! I have total of 1,040,000 US dollars, which i gladly donate to you ...please reply very quickly with your personal information so we can contact to this e-mail. Thank you and God bless you.

## Facebook, ein Alltime Classic



# Recon

Einstellung

Vorlieben

Interessen

Aktivitäten

Orte

Kontakte

Gruppe

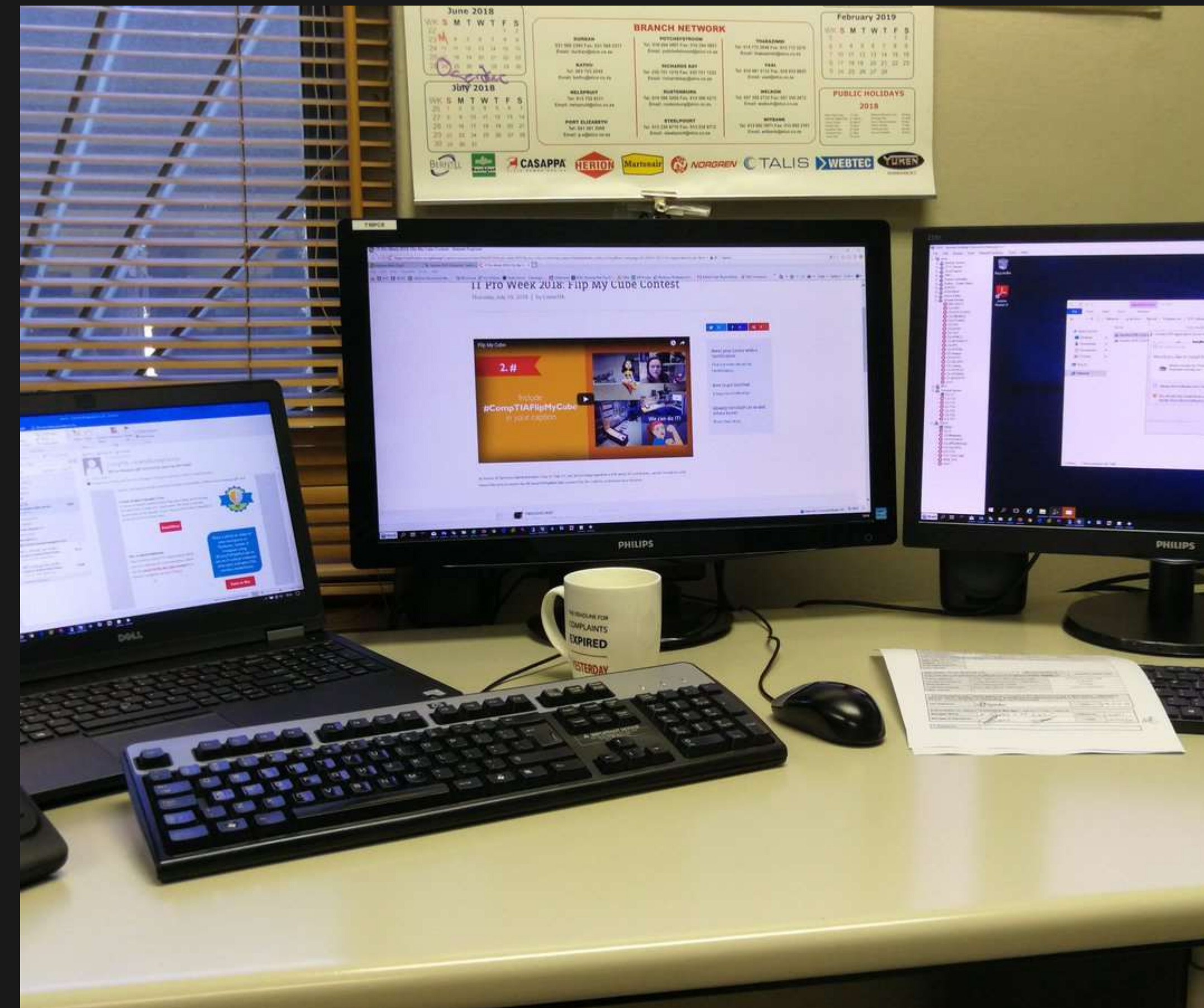
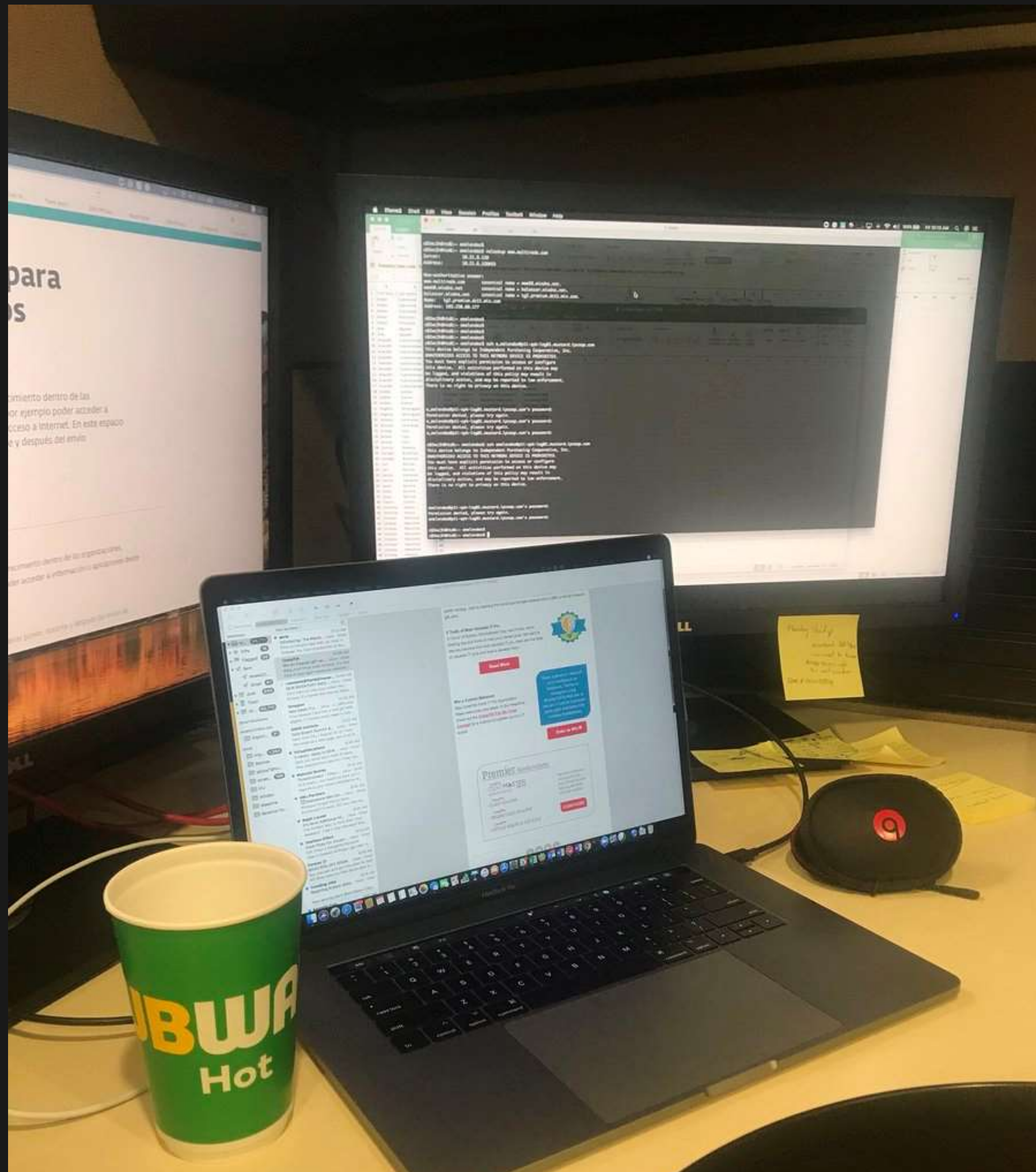
Orientierung

Anknüpfungspunkte



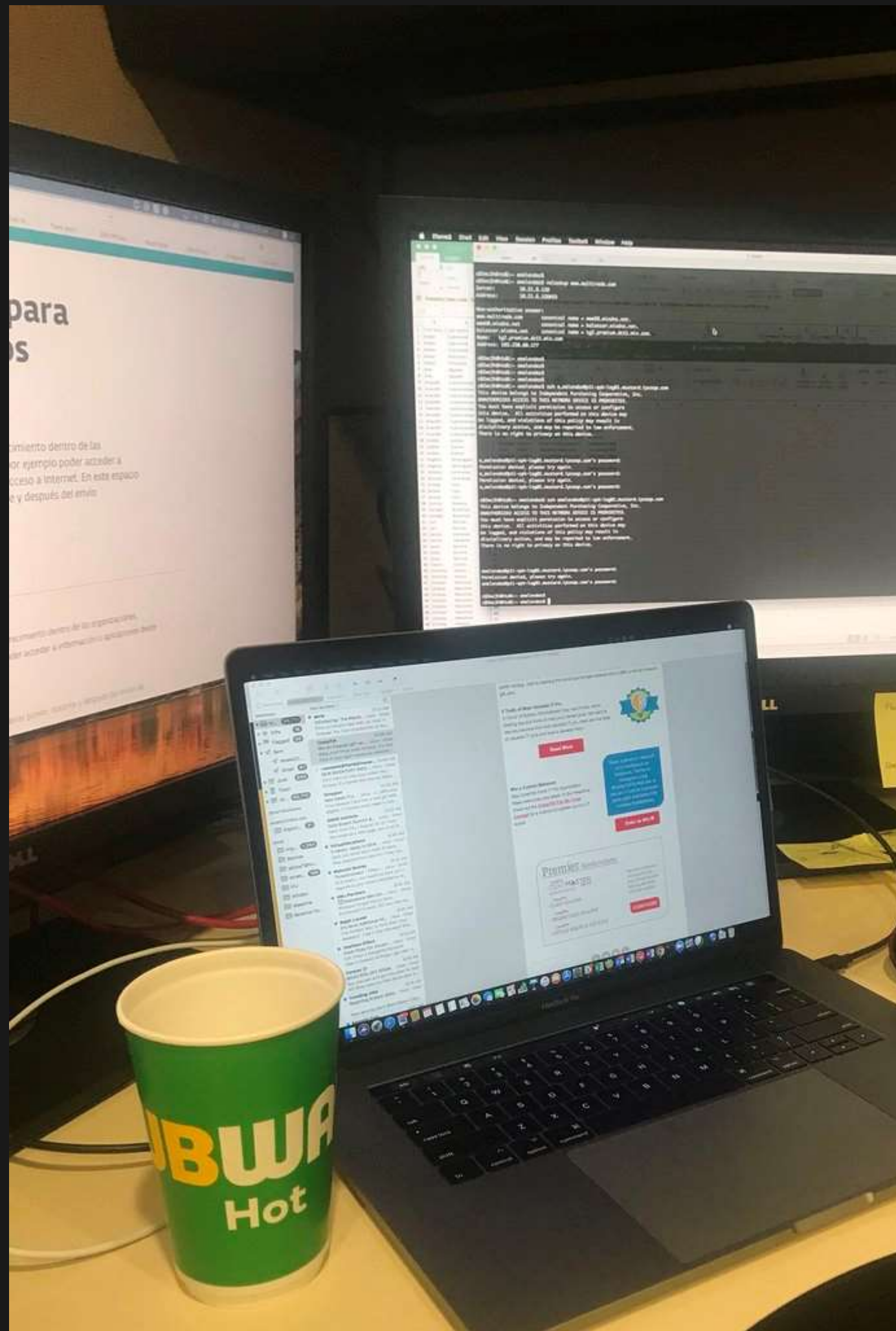
# Twitter Hashtags

## #comptiaflipmycube Competition



# Twitter Hashtags

#comptiaflipmycube competition



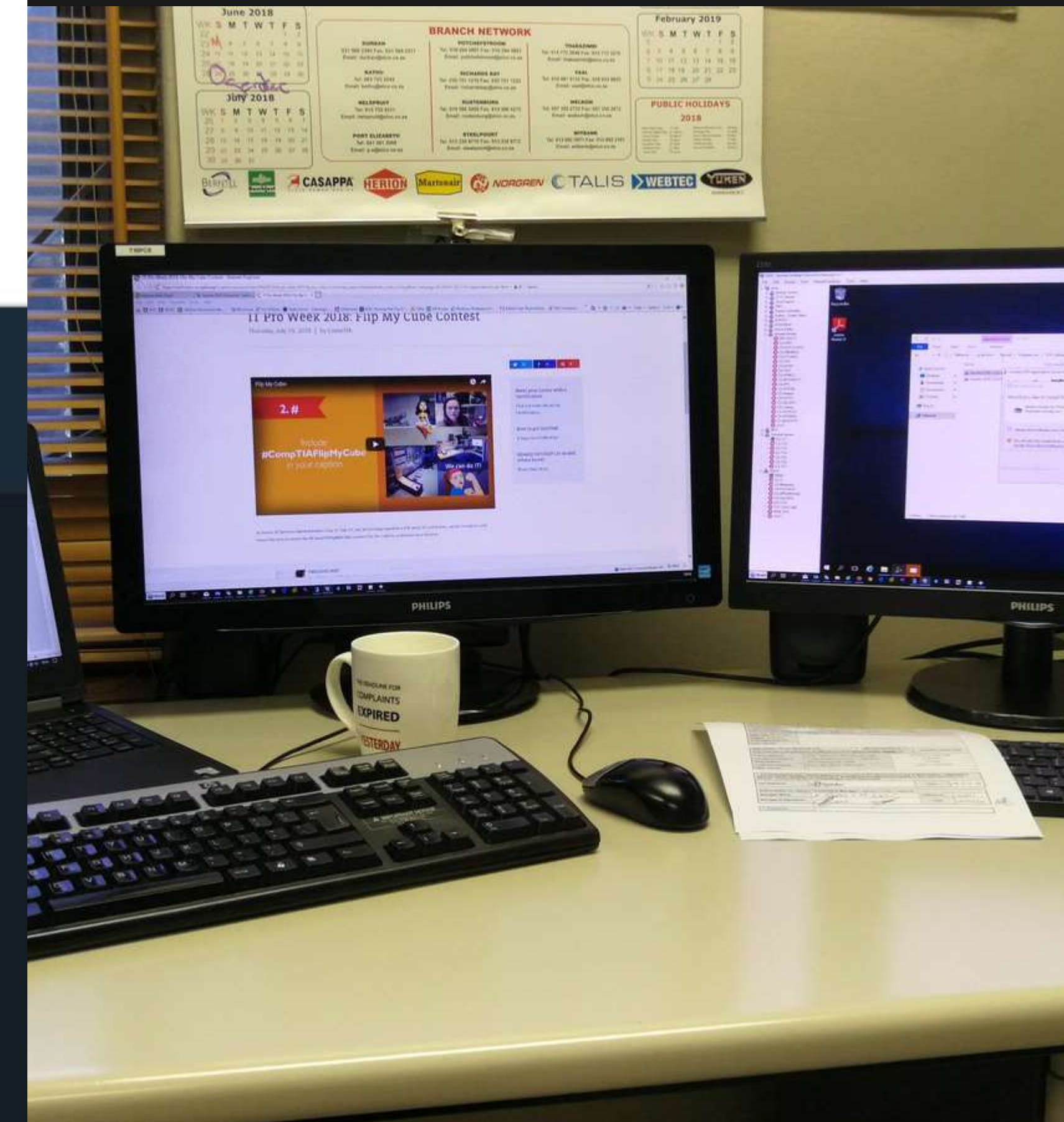
preciation  
-27, 1



**CompTIA** ✓  
@CompTIA

The world's leading technology association, CompTIA is Advancing the global tech industry.

📍 Illinois, USA  
[comptia.org](https://www.comptia.org)





# Wir können International gehen



site:glowing.com/community/topic/



Alle

Bilder

News

Shopping

Maps

Mehr

Einstellungen

Tools

Ungefähr 2.670.000 Ergebnisse (0,25 Sekunden)

Google-Anzeige

## [In Google Search Console überprüfen](#)

[www.google.com/webmasters/](http://www.google.com/webmasters/)

Gehört dir **glowing.com/community/topic**? Rufe Indexierungs- und Rankingdaten von Google ab.

## [Ovulation tests- positive / negative - Glow Community](#)

<https://glowing.com> › [Community](#) › [General TTC](#) ▾ [Diese Seite übersetzen](#)

14.10.2015 - Ovulation tests- positive / negative It looks positive but the digital ones are saying no?!?!

## [Difference between pregnancy belly and bloated stomach? - Glow ...](#)

<https://glowing.com> › [Community](#) › [First Time Moms](#) ▾ [Diese Seite übersetzen](#)

The sucking in factor I would go off of. Also if I woke up and stomach was gone, because you go 8 hours w/o eating. When I started waking up with a belly I knew I popped. 2 Upvotes. Ka. Posted at Fri, Mar 13 2015. here's my bloat (this is a long time ago): here's my bump when I first popped: 1 Upvote. Ka. Kaylee  
• Mar 12 ...

# Benutzernamen analysieren

Bereits die Verwendung von gleichen Benutzernamen ist ein Sicherheitsrisiko.

**Namech\_k**

Download Results

Username

Facebook	YouTube	Twitter	Instagram	Blogger	GooglePlus	Twitch	Reddit	Ebay	Wordpress	Pinterest	Yelp
Slack	Github	Basecamp	Tumblr	Flickr	Pandora	ProductHunt	Steam	MySpace	Foursquare	OkCupid	Vimeo
UStream	Etsy	SoundCloud	BitBucket	Meetup	CashMe	Dailymotion	About.me	Disqus	Medium	Behance	Photobucket
Bit.ly	Cafe Mom	Coderwall	Fanpop	deviantART	Good Reads	Instagram	Keybase	Kongregate	LiveJournal	StumbleUpon	Angellist





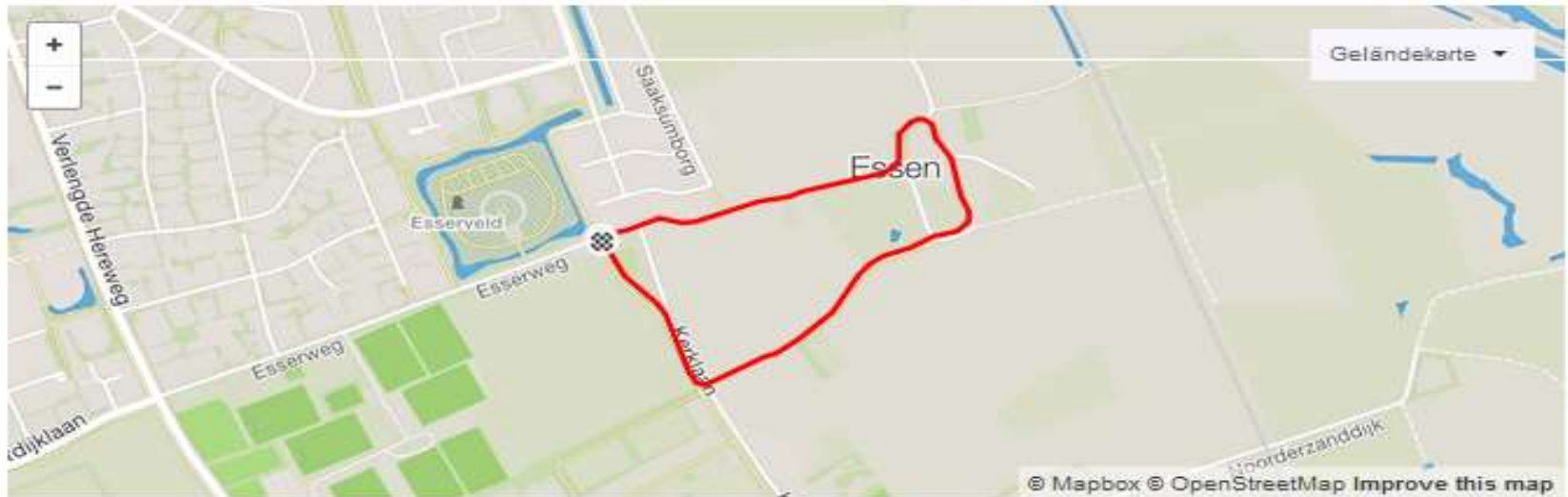
Interessante Punkte auf der Heatmap suchen





## Segmente suchen



## Bestenlisten ansehen



Schnellste Zeiten

- 
**Michel van Kruchten**  
 CR 5:50 07.08.2016
- 
**Linda Bras**  
 CR 7:23 18.05.2017

[Leistungen vergleichen](#)

Ein Ziel für dieses Segment festlegen [Alle ansehen](#)


[Ziel setzen](#)

[Im Blog einbetten](#) [Aktionen](#)

### Bestenlisten

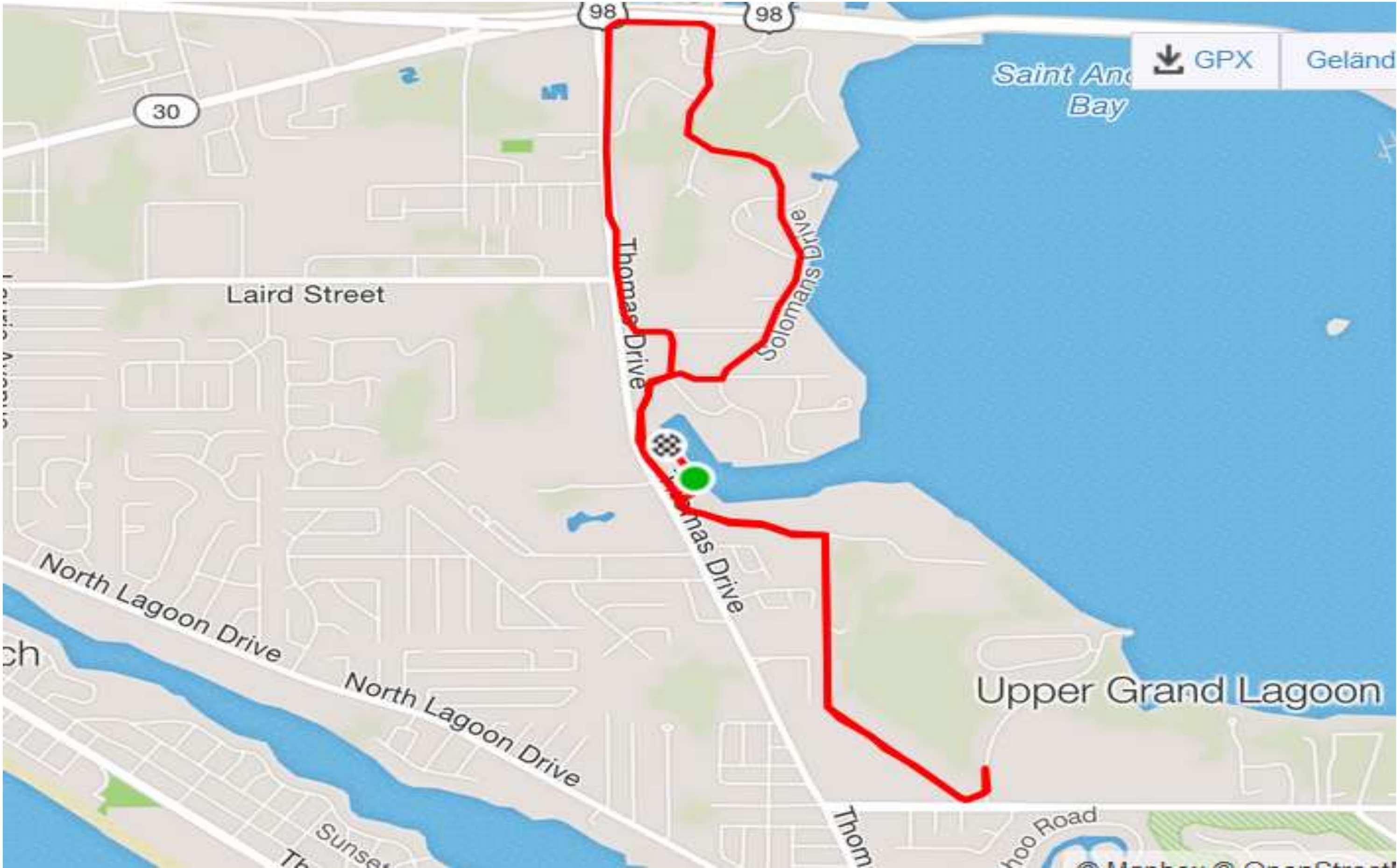
- Gesamt**
- Dieses Jahr
- Meine Ergebnisse
- Leute, denen ich folge
- Meine Clubs
- Strava Essen
- ASICS FrontRunner
- running-podcast.de
- Laufen in NRW
- Polar - Running
- STRAVA PREMIUM**
- Nach Altersklasse

### Gesamt

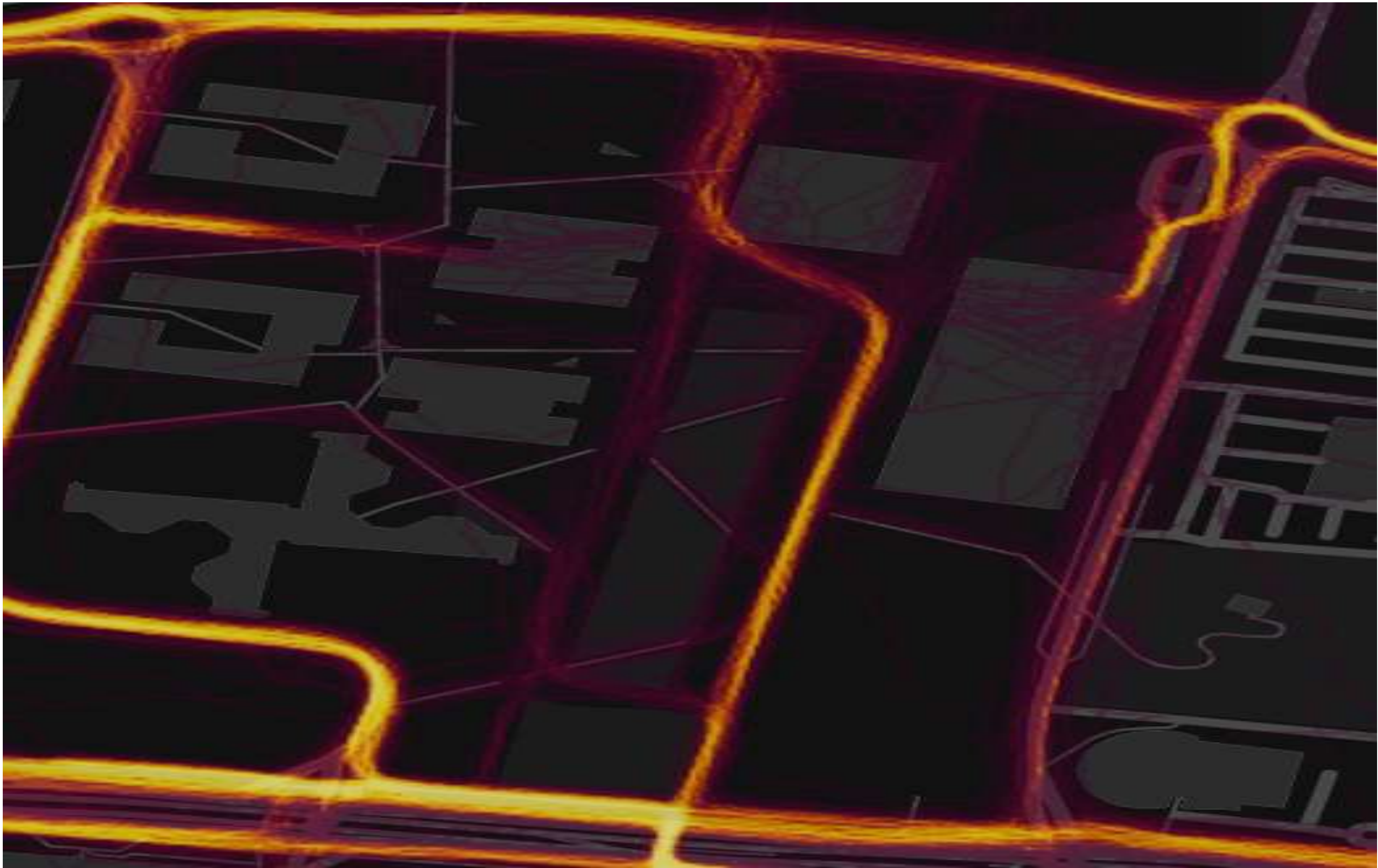
Rang	Name	Datum	Tempo	HF	VAM	Zeit
1	 <b>Michel van Kruchten</b>	7. Aug. 2016	3:46/km	183bpm	-	5:50
2	Ping-Fai Teng	8. Aug. 2016	3:55/km	-	-	6:03
3	Raymund Prins	14. Mai 2017	4:18/km	141bpm	-	6:40
4	Frank Simons	13. Juni 2017	4:24/km	166bpm	-	6:49

# Strava Case-Study

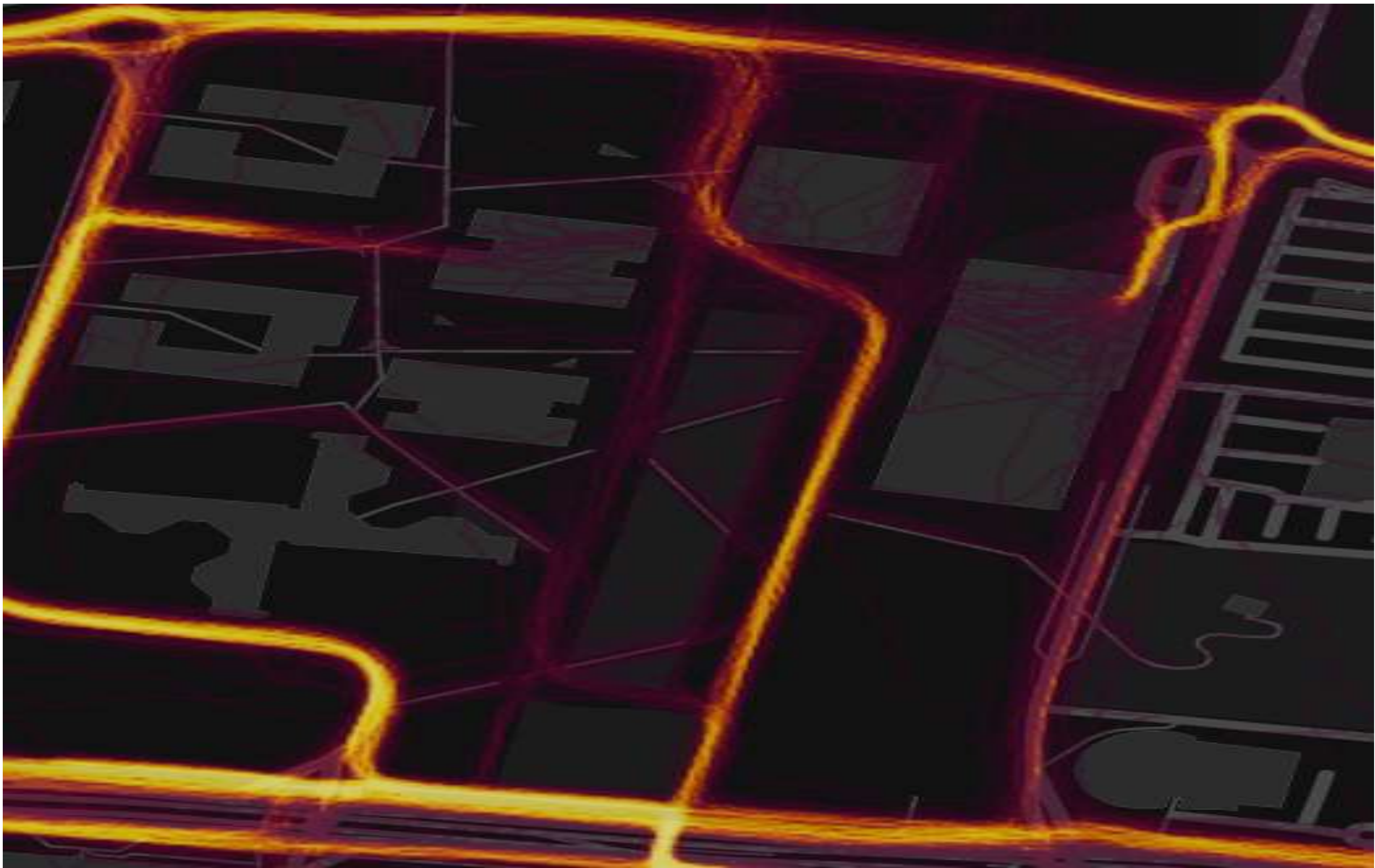
Einzelpersonen zu unterschiedlichen Einsatzorten folgen



Startpunkte für „Fahrradpendler“ erkennbar



„Malicious“-Segment für einzelne Firmen erstellen



```
<trkpt lat="51.#####" lon="-6.#####"/> <time>2018-02-28T09:32:21Z</time>
```

Bonus Points



**BUGS**

**BUGS EVERYWHERE**



Let's get physical



# USB – Universal Serial Error?



# USB – Universal Serial Error?



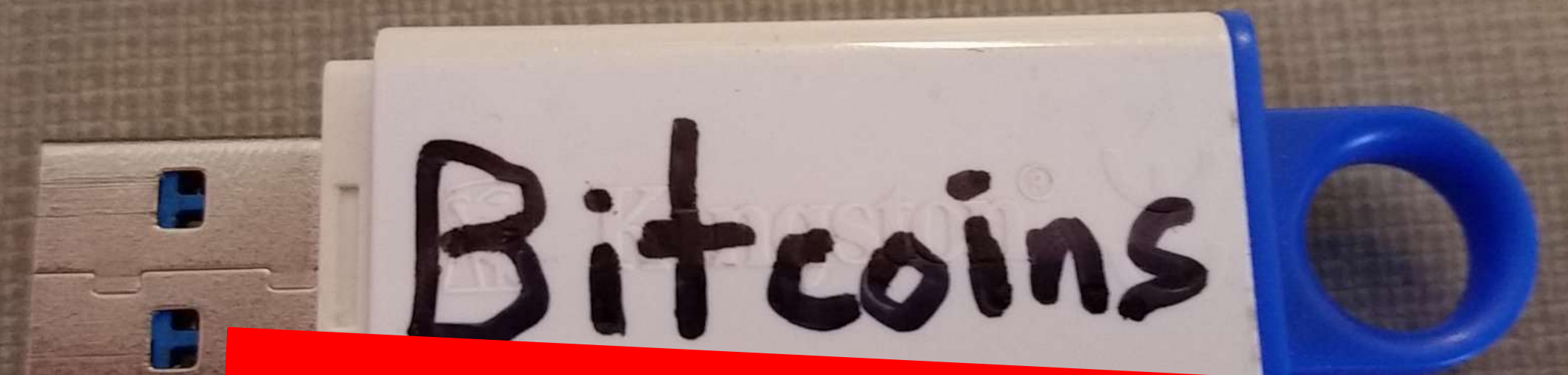
# USB – Universal Serial Error?

Malware



Tastatureingaben

Keylogger



Eavesdropping

Einfache und Effektive aber räumlich sehr beschränkte Möglichkeit an Informationen zu kommen

Einfache und Effektive aber räumlich sehr beschränkte Möglichkeit an Informationen zu kommen



Einfache und Effektive aber räumlich sehr beschränkte Möglichkeit an Informationen zu kommen



Einfache und Effektive aber räumlich sehr beschränkte Möglichkeit an Informationen zu kommen





Einfache und Effektive aber räumlich sehr beschränkte Möglichkeit an Informationen zu kommen



# Shoulder Surfing

Einfache und Effektive aber räumlich sehr beschränkte Möglichkeit an Informationen zu kommen



# Shoulder Surfing

Einfache und Effektive aber räumlich sehr beschränkte Möglichkeit an Informationen zu kommen



**Educate**



Empower



