Geek speak !

Your favourite tool

Moderator : Ana Lutzky, Data Editor at AEF info
@anouchka

Olaya Argüeso Pérez, Editor-in-chief at Correctiv

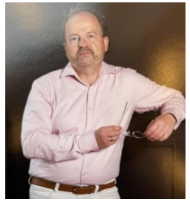
Keybase, a tool for team communication. Like Slack, but encrypted !

@oargueso

Alex Pyrgiotis, software developer

Dangerzone, an open-source tool for sanitizing untrusted documents

@apyrgio



Marcus Lindemann, investigative journalist

Tracking stuff with Bluetooth !

@marcuslindemann

Stefanie Helbig, investigative journalist

Tracking stuff with Bluetooth !

@stefaniehelbig


CORRECTIV
Recherchen für die
Gesellschaft

My favourite digital tool: Keybase

What is Keybase?

- Keybase is a an encrypted Slack: it allows you send messages and share files in a secure way.

- It provides end-to-end encryption, so that (theoretically) only the intended recipients can access and read your messages or files.

- It is open-source, which should allow for more transparency and help improve any vulnerability

My favourite digital tool: Keybase

What you can do with Keybase:

- Send private messages with other individuals on the platform
- Create teams of people and channels within those teams to specific topics
- Share (large) files securely with individuals or with a team

My favourite digital tool: Keybase

Cons:

- Limited Adoption
- Can be daunting for some users

Warning!

- ⚠ Install ALWAYS in more than just one device ⚠

Thanks!

Olaya Argüeso Pérez
CORRECTIV - Recherchen für die Gesellschaft

olaya.argueso@correctiv.org
correctiv.org

Dangerzone

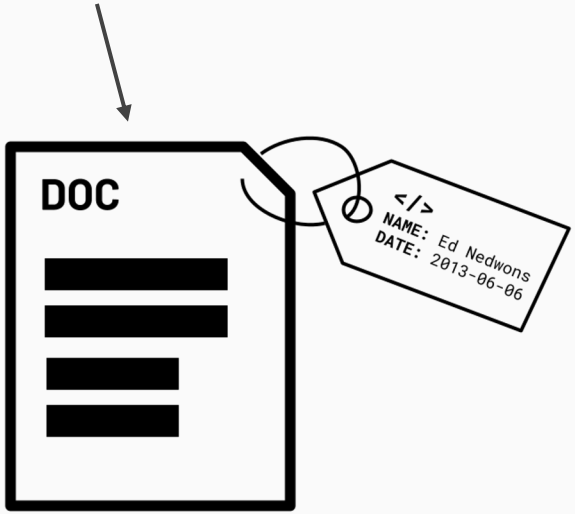
Handling Docs Safely

June 2023

Alex Pyrgiotis (@apyrgio)

Typical security advice: “Don’t open attachments!”

⚠ Malicious documents may contain malware



Is it still relevant?

UNIT 42

Spear Phishing Attacks Target Organizations in Ukraine, Payloads Include the Document Stealer OutSteel and the Downloader SaintBot

eset
Progress. Protected.

Lazarus targets aerospace company in the Netherlands and political journalist in Belgium to steal data

threatpost

Nation-state Hackers Target Journalists with Goldbackdoor Malware

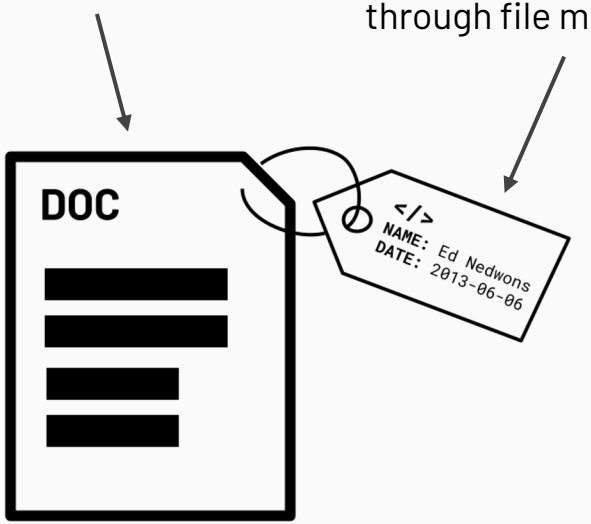
Headlines from 2022 articles on malware attacks

Yeap.

.... and of course:
“Don’t out your sources!”

⚠ Malicious documents may contain malware

⚠ Source info may accidentally be exposed through file metadata



But how could I?...

The Register

Metadata ruins Google's anonymous eBay Australia protest

WIRED

Oops! Did Vice Just Give Away John McAfee's Location With Photo Metadata?

Headlines on leaks from file metadata

Leaks happen.

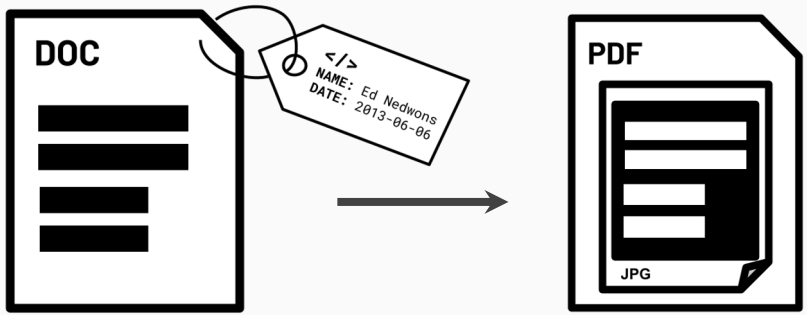
Enter Dangerzone

What is Dangerzone?

- **Open-source** tool written in 2020 by **Micah Lee**, Director of Information Security at "The Intercept"
- Inspired by the **TrustedPDF** Qubes OS feature
- Maintained since 2022 by **Freedom of the Press Foundation**, who also maintains **SecureDrop**
- **Desktop application** that can take a **suspicious document**, sanitize it, and produce a **safe PDF**
- Intended for **technical and non-technical** folks alike!
- Check out https://dangerzone.rocks

Dangerzone

Dangerzone Features



Malware / Tracker removal
Sanitizes files in a process similar to photocopying their pages into a PDF

Source protection
Strips all file metadata

Privacy
Sanitization takes place in a local, offline sandbox, that runs within your computer.

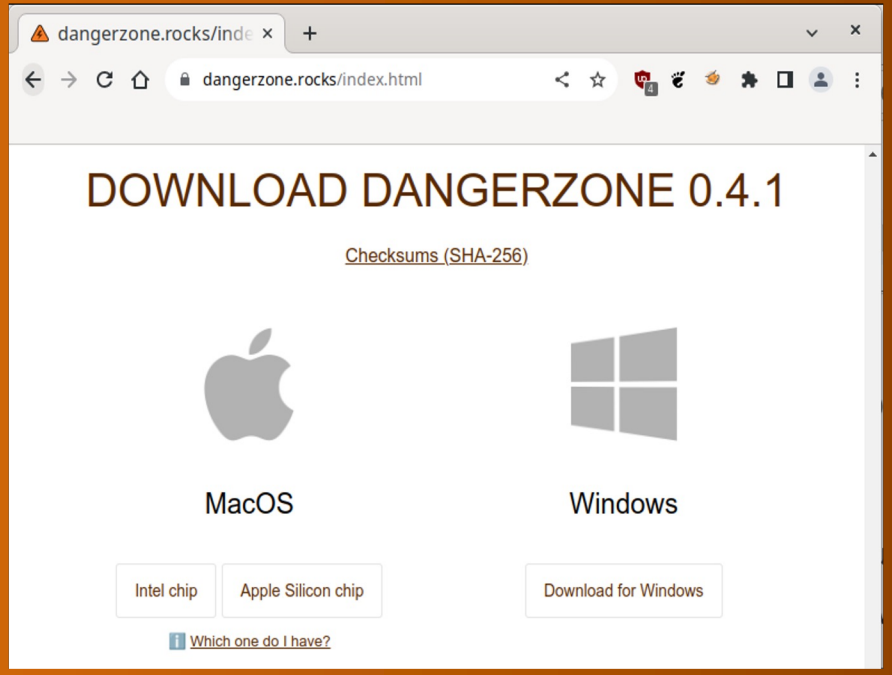
Many supported files
PDFs, Office documents & Images

Supports major operating systems
Windows, Mac & Linux

Dangerzone

How it works?

- Install Dangerzone in your computer



Dangerzone

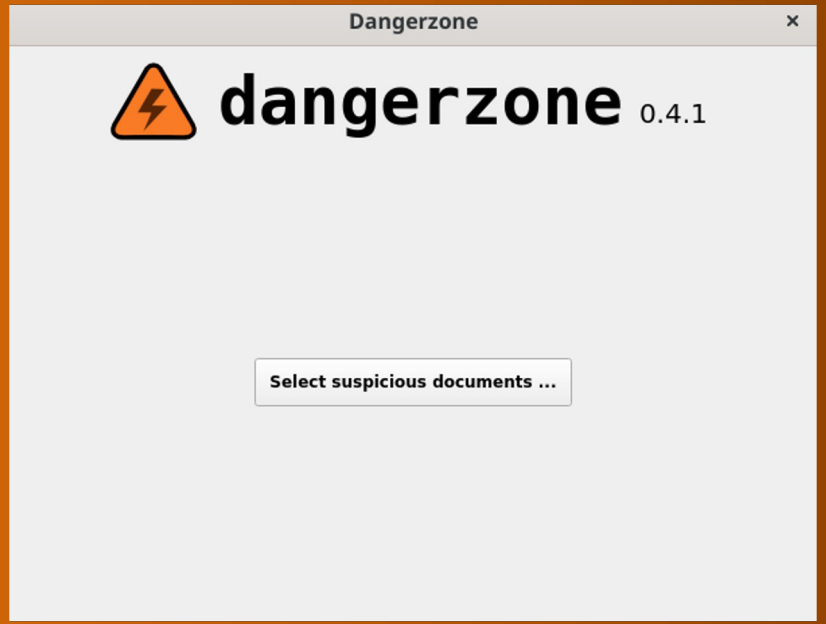
How it works?

- Install Dangerzone in your computer
- Install Docker Desktop (MacOS/Win)

Dangerzone

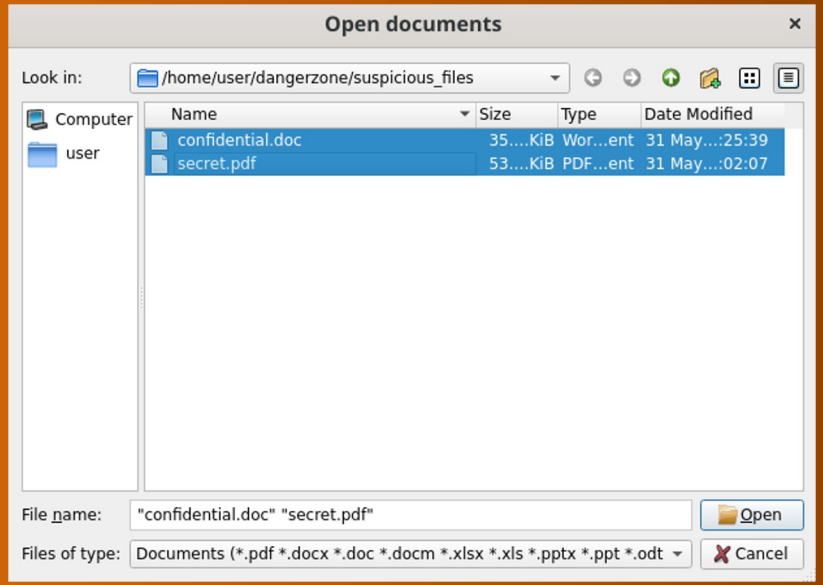
How it works?

- Install Dangerzone in your computer
- Install Docker Desktop (MacOS/Win)
- Open the Dangerzone application



How it works?

- Install Dangerzone in your computer
- Install Docker Desktop (MacOS/Win)
- Open the Dangerzone application
- Choose the suspicious document



Dangerzone

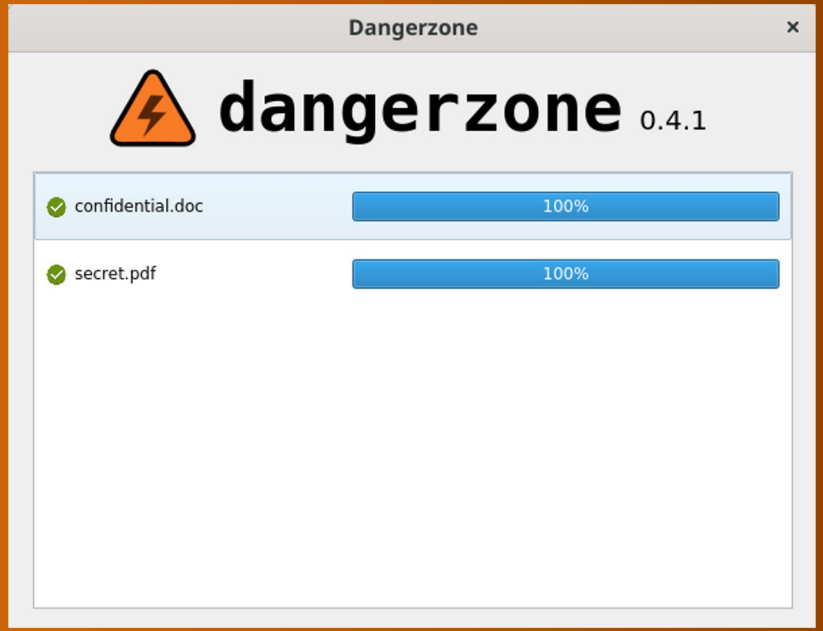
How it works?

- Install Dangerzone in your computer
- Install Docker Desktop (MacOS/Win)
- Open the Dangerzone application
- Choose the suspicious document
- Choose the location for the safe PDF

How it works?

- Install Dangerzone in your computer
- Install Docker Desktop (MacOS/Win)
- Open the Dangerzone application
- Choose the suspicious document
- Choose the location for the safe PDF
- Start the conversion

You can now open your safe document 🎉



Security Limitations

1. **Very targeted attackers** (state-sponsored)
   Targeting you, your computer or Dangerzone specifically
2. Protecting against **non-file metadata** (printer dots, canary traps, etc.)
   - Remember Reality Winner's case

Usability Limitations

1. **Mobile phones** are not supported
2. No **file preview** support before conversion
3. **Password-protected files** aren't currently supported

tl;dw

- Document challenges: malware attacks and metadata leaks
- Dangerzone sanitizes docs by “photocopying” them
- Good security against most known types of attacks
- Visit https://dangerzone.rocks

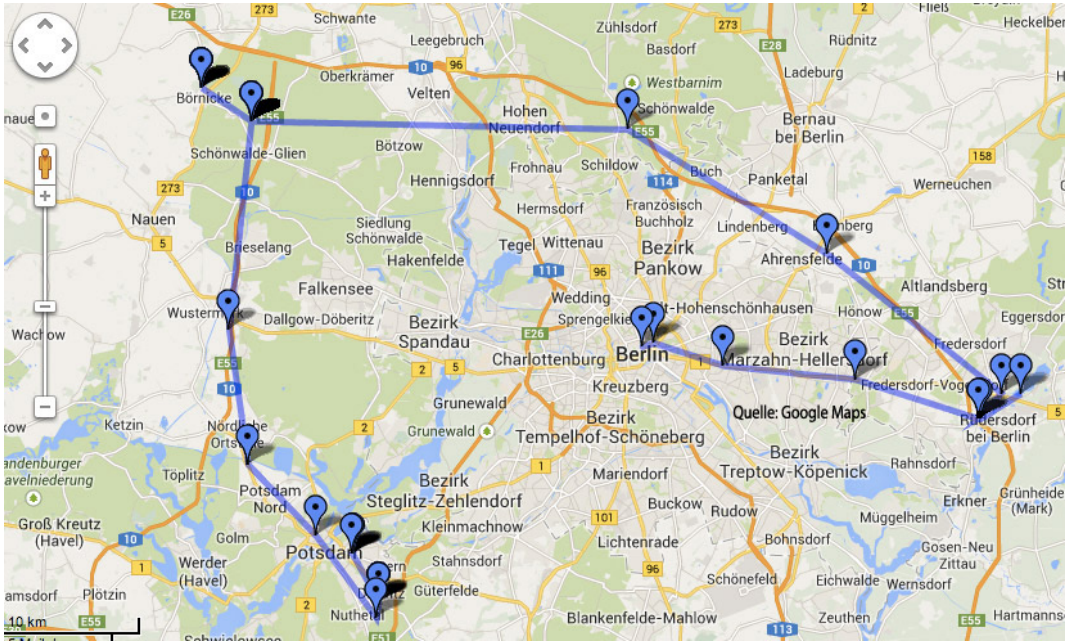
Questions?

Dangerzone

Bluetooth tracking – first learnings

Steffi Helbig, Claus Hesseling, Adrian Kaul,
Sebastian Mondial and Marcus Lindemann, Mechelen, 2023

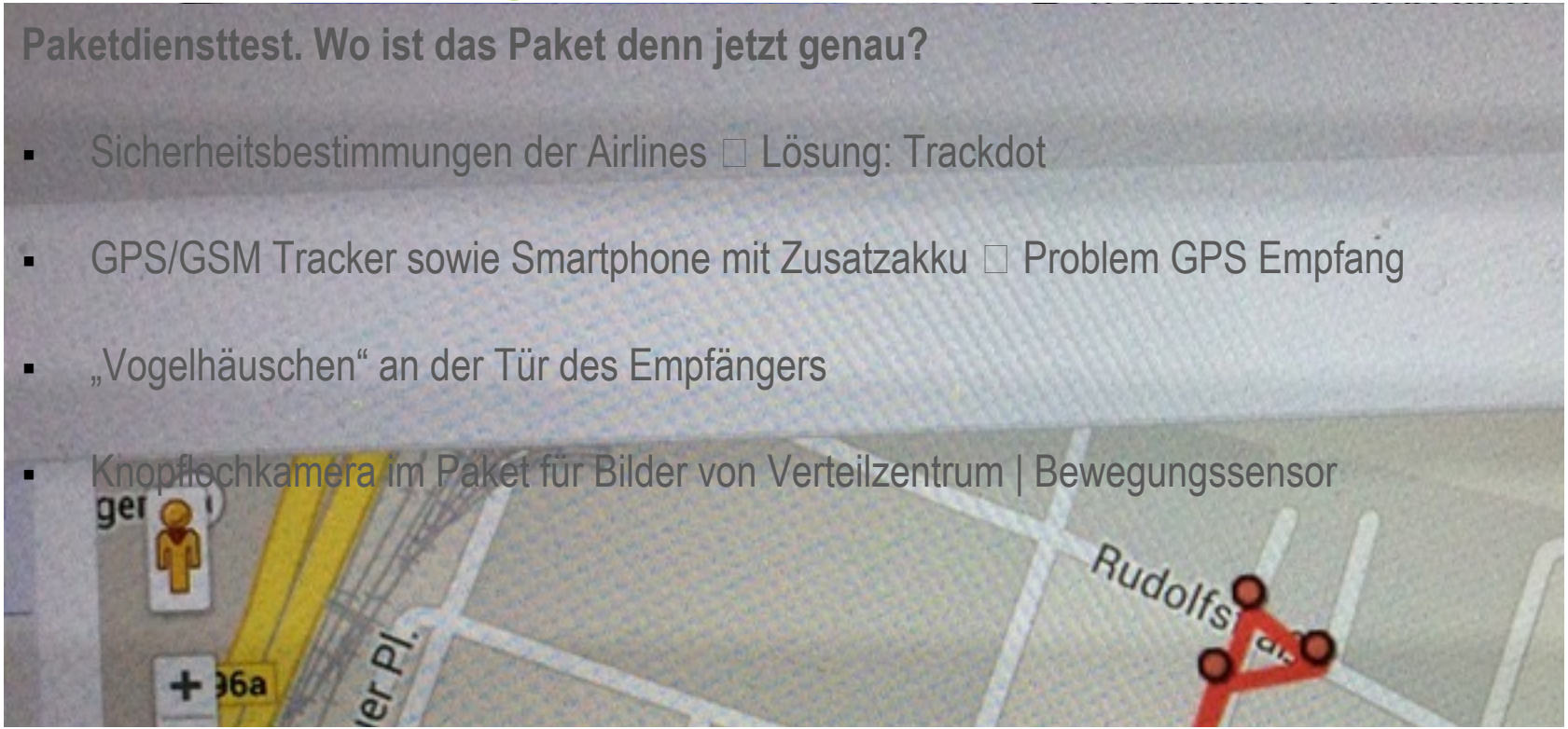
Video und Tracking 2



Video und Tracking 2

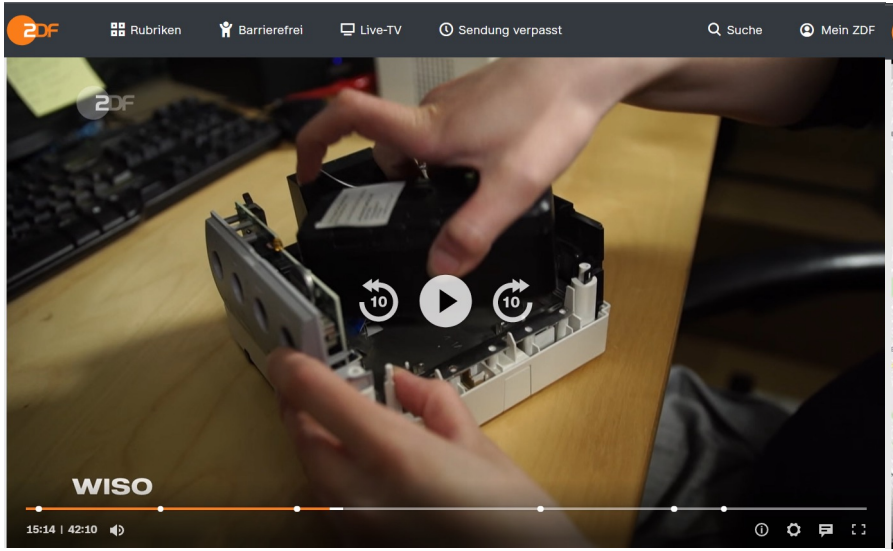
Paketdiensttest. Wo ist das Paket denn jetzt genau?

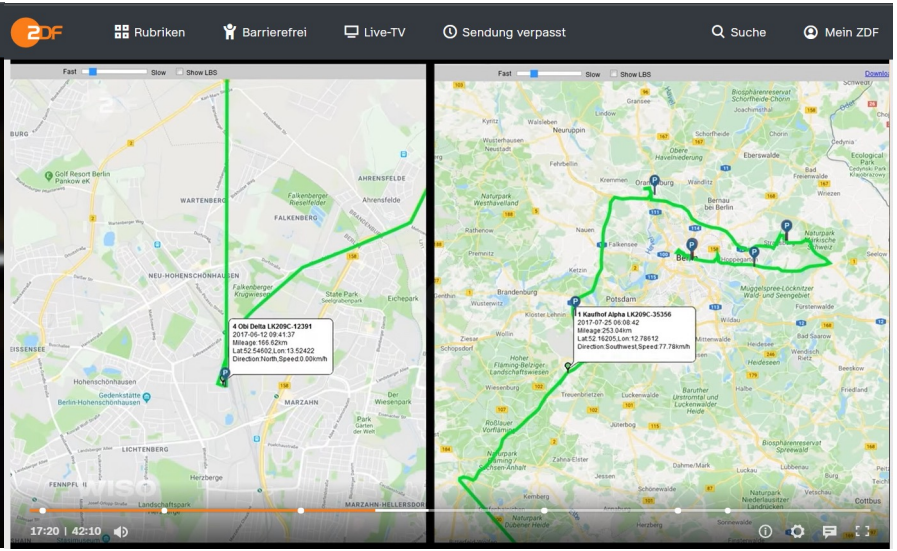
- Sicherheitsbestimmungen der Airlines Lösung: Trackdot
- GPS/GSM Tracker sowie Smartphone mit Zusatzakku Problem GPS Empfang
- „Vogelhäuschen“ an der Tür des Empfängers
- Knopflochkamera im Paket für Bilder von Verteilzentrum | Bewegungssensor



knopfloch tv

2018 – 2020: tracking electronic waste

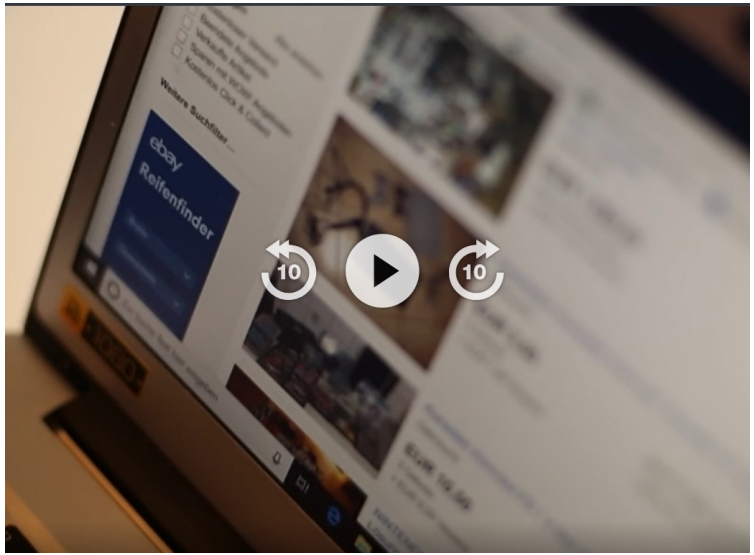


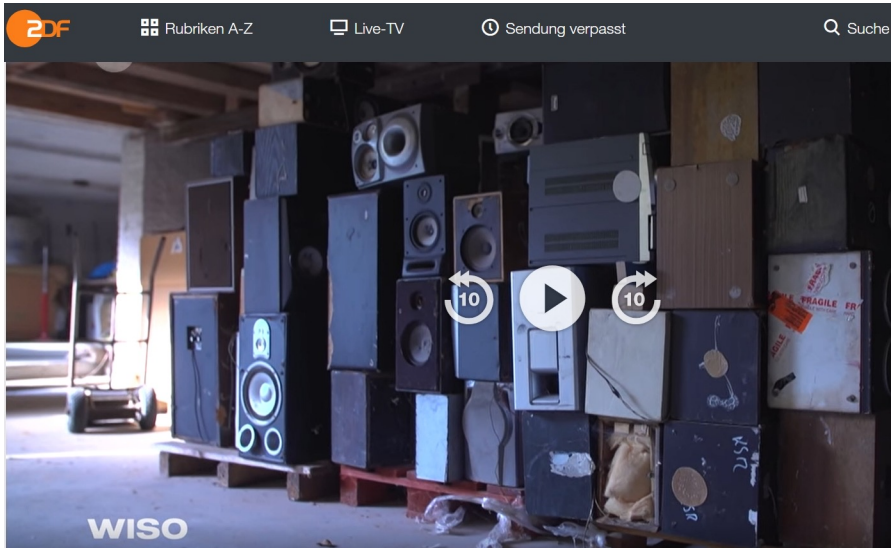


knopfloch tv

2018 – 2020: tracking electronic waste

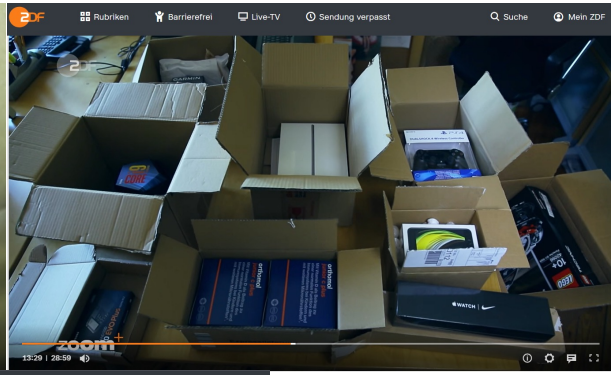
2018 – 2020: tracking electronic waste

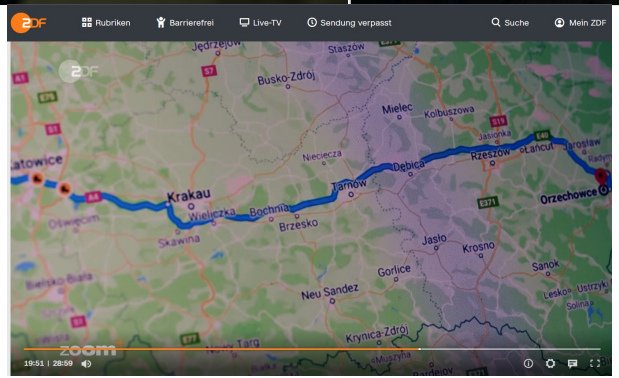




knopfloch tv

2020: investigating online fraud





Gadget curently used for tracking

LKGPS – tracker from China, approx 100 € - currently we run 10 of these
Monitoring online lkgps.net, App also available
http://www.lkgpstrakcer.com/sale-8616423-lkgps-car-tracking-system-platform-gps-software-lk209b.html

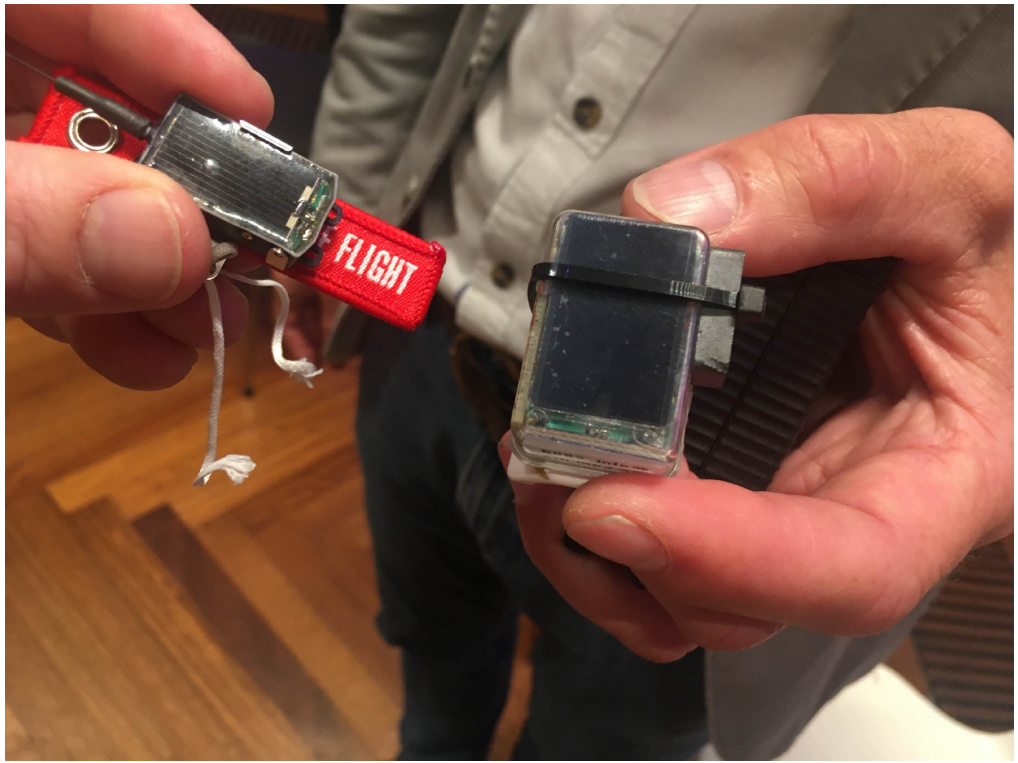
Finnish Yepzon 2.0, 99 €

Probably best, but at 300€: http://www.sherlog.com/ (if recovery of the tracker is secured...)

To find a SIM that roams globally, google [„machine to machine" OR m2m SIM] – from 0,95 €/month

currently testing: Samsung smarttags and Apple airtags

Gadgets of the future – small trackers used on animals



Kostenlose Gravur

AirTag kaufen

Personalisiere dein AirTag mit einer kostenlosen Gravur.
Nur bei Apple.

Wie viele möchtest du haben?

1er-Pack	39,00 €
4er-Pack	129,00 €

nlos liefern lassen
vorrätige Artikel im
le Store abholen

Kostenlose persönliche Gravur

Kostenlose, einfache Rückgabe

(2)

Samsung Galaxy Sm

€79.90

IN STOCK, IMMEDIATELY READY FOR DELIVERY

1

Fixed delivery €4.95 Up

05.07.14

Using Bluetooth instead of GPS

How it works

- Bluetooth connection to devices around (Apple or Samsung)
- GPS-data comes from the mobile phones around

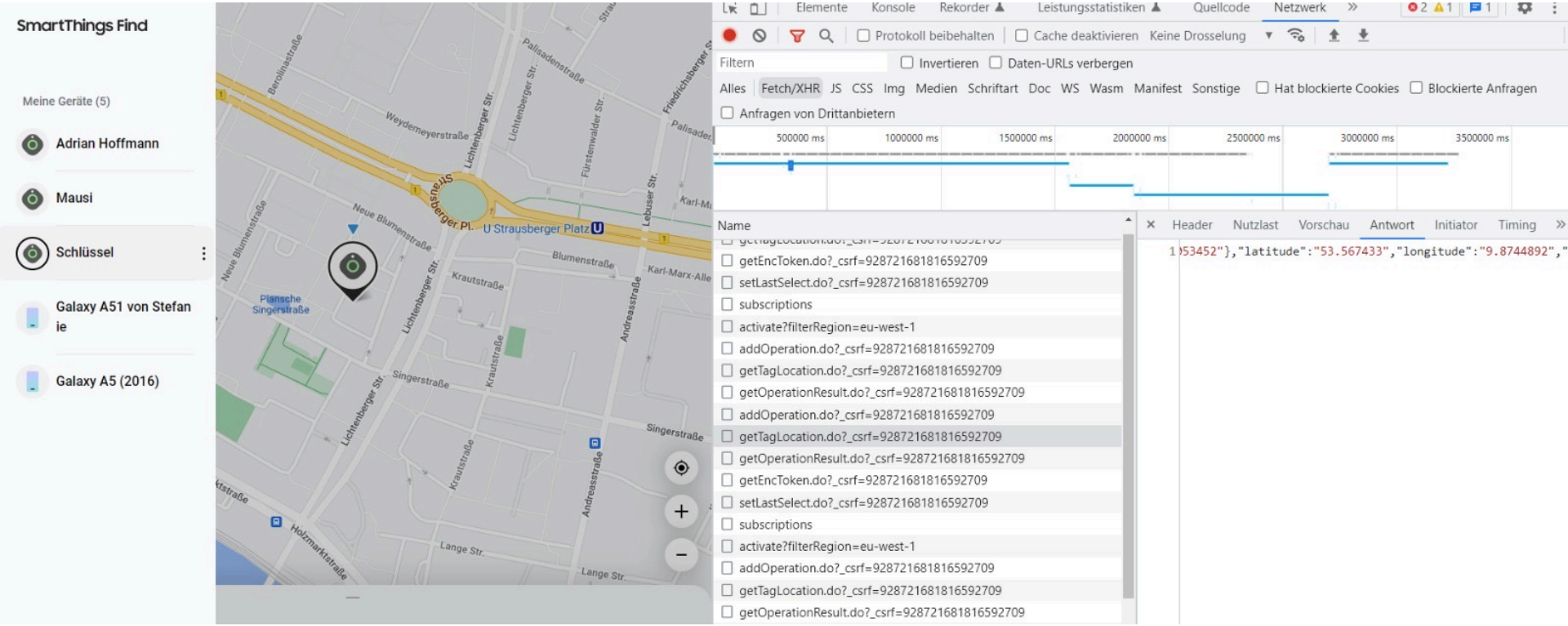
Pros:

- cheaper, no SIM-card needed
- longer battery life
- smaller and better to hide

***Cons*:**

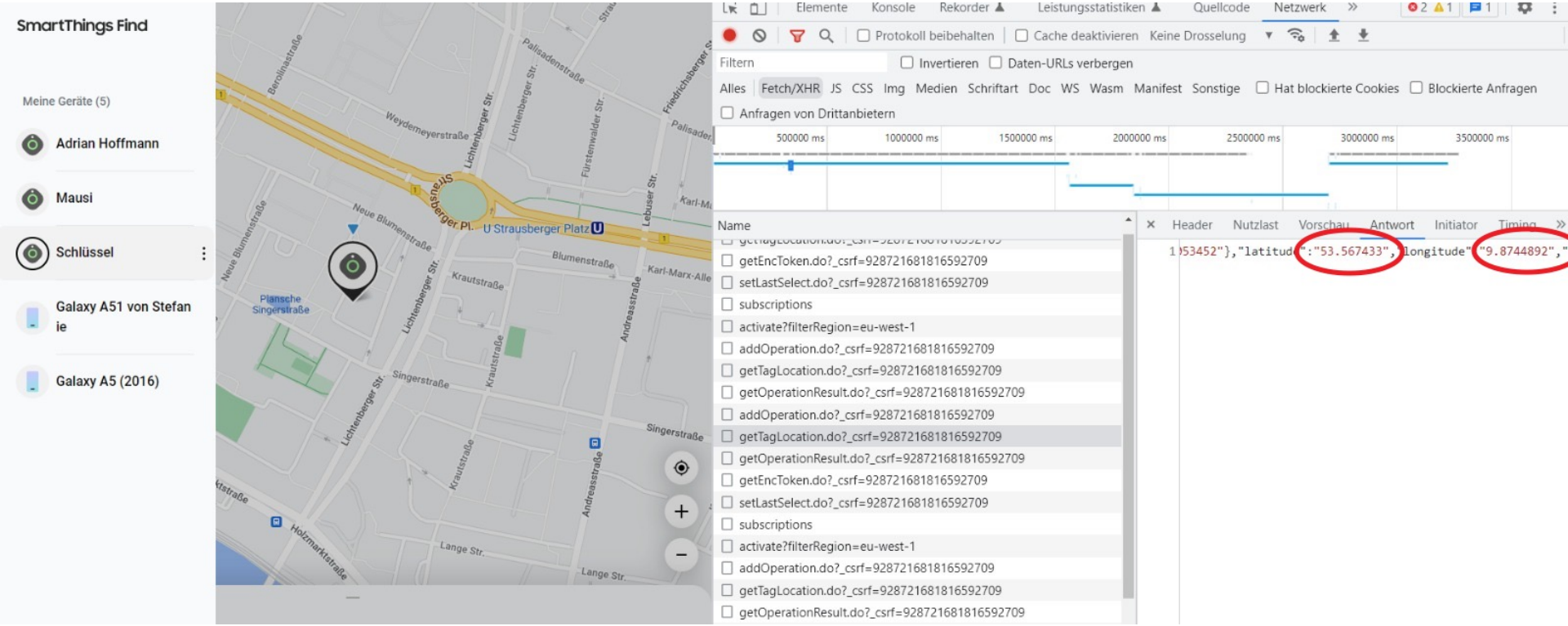
- People the device follows might get warned

What does it look like?



knopfloch tv

What does it look like?



knopfloch tv

What does it look like?

Select a Device (3)...

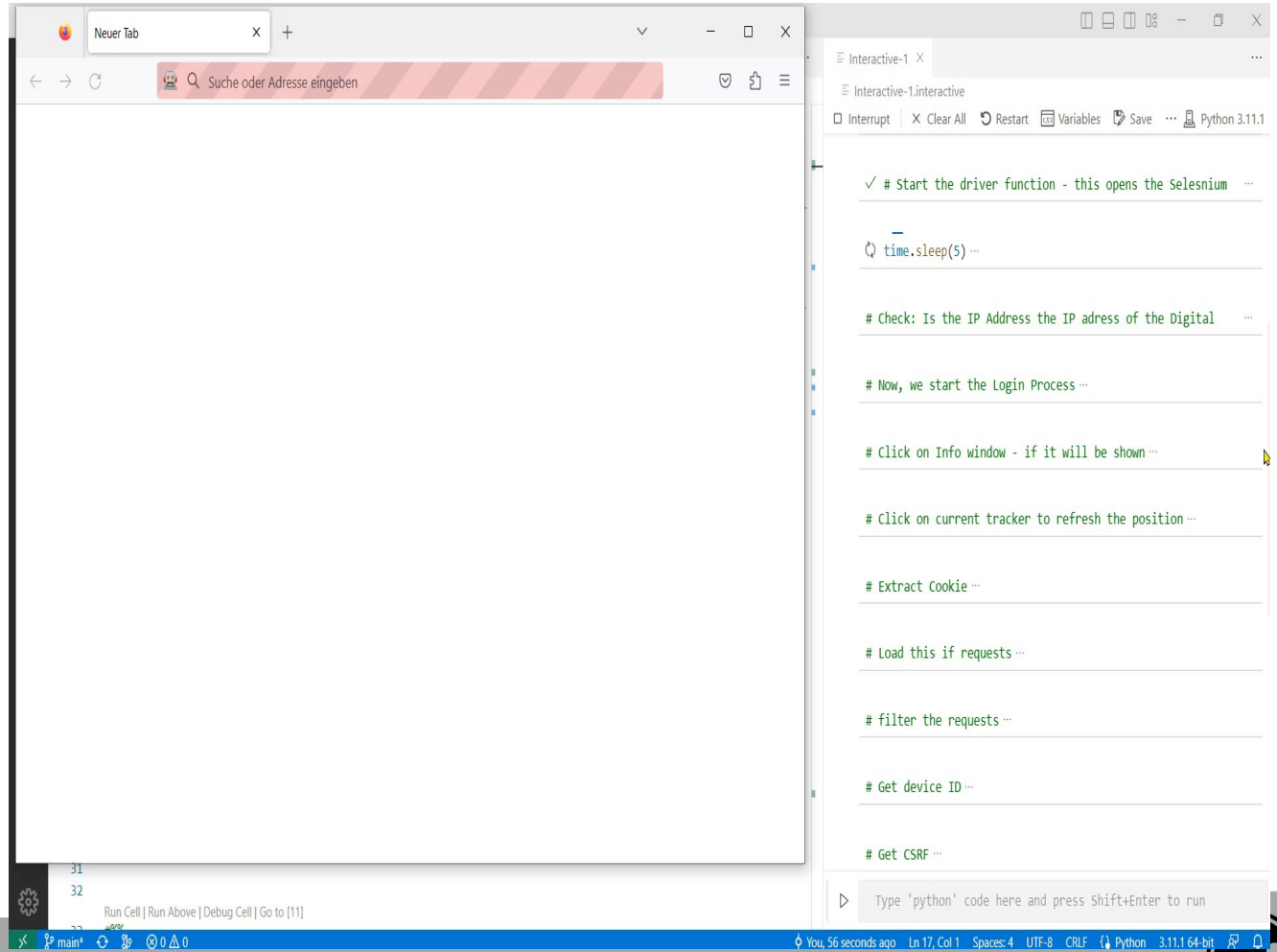
Device Label	Device ID
Adrian Hoffmann	f5f5fc1a-9ec9-4e67-abdd-c1dc15c0103d
Mausi	2d20cd3d-a1ee-4291-9227-d7427f2044c6
Schlüssel	21988bdb-f2fa-44a1-8c09-7444e5d8ef50

Status for device "Schlüssel"

Status: ONLINE (as of 18.4.2023, 14:20:01)

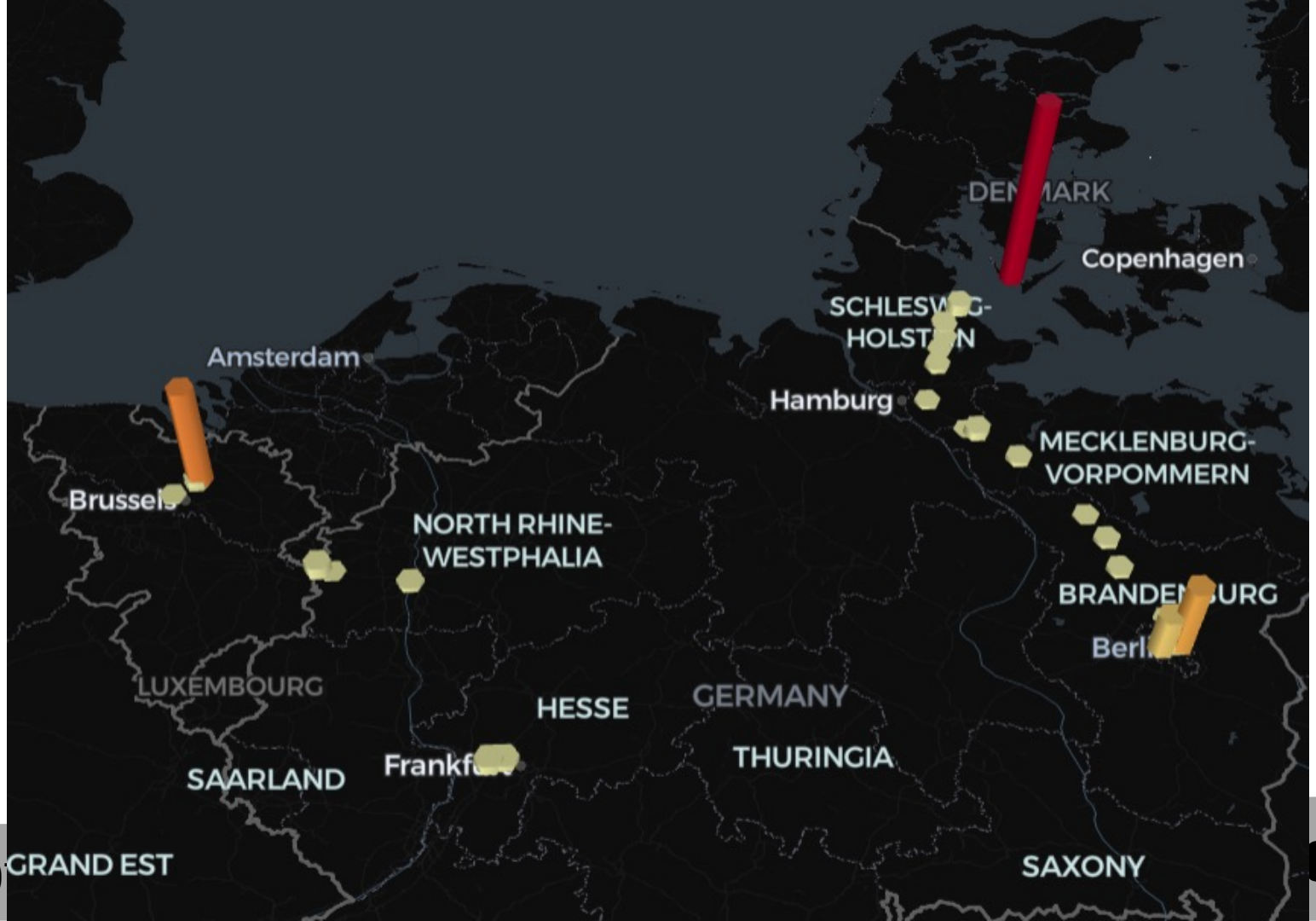
Component	Capability	Attribute	Value
main	tag.e2eEncryption	encryption	null
main	audioVolume	volume	null
main	tag.searchingStatus	searchingStatus	null
main	tag.tagStatus	connectedUserId	null
main	tag.tagStatus	tagStatus	null
main	tag.tagStatus	connectedDeviceId	null
main	geofence	enableState	null
main	geofence	geofence	null
main	geofence	name	null
main	alarm	alarm	null
main	tag.updatedInfo	connection	connected
main	tag.tagButton	tagButton	null
main	battery	battery	null
main	geolocation	method	null
main	geolocation	heading	null
main	geolocation	latitude	null
main	geolocation	accuracy	null
main	geolocation	altitudeAccuracy	null
main	geolocation	speed	null

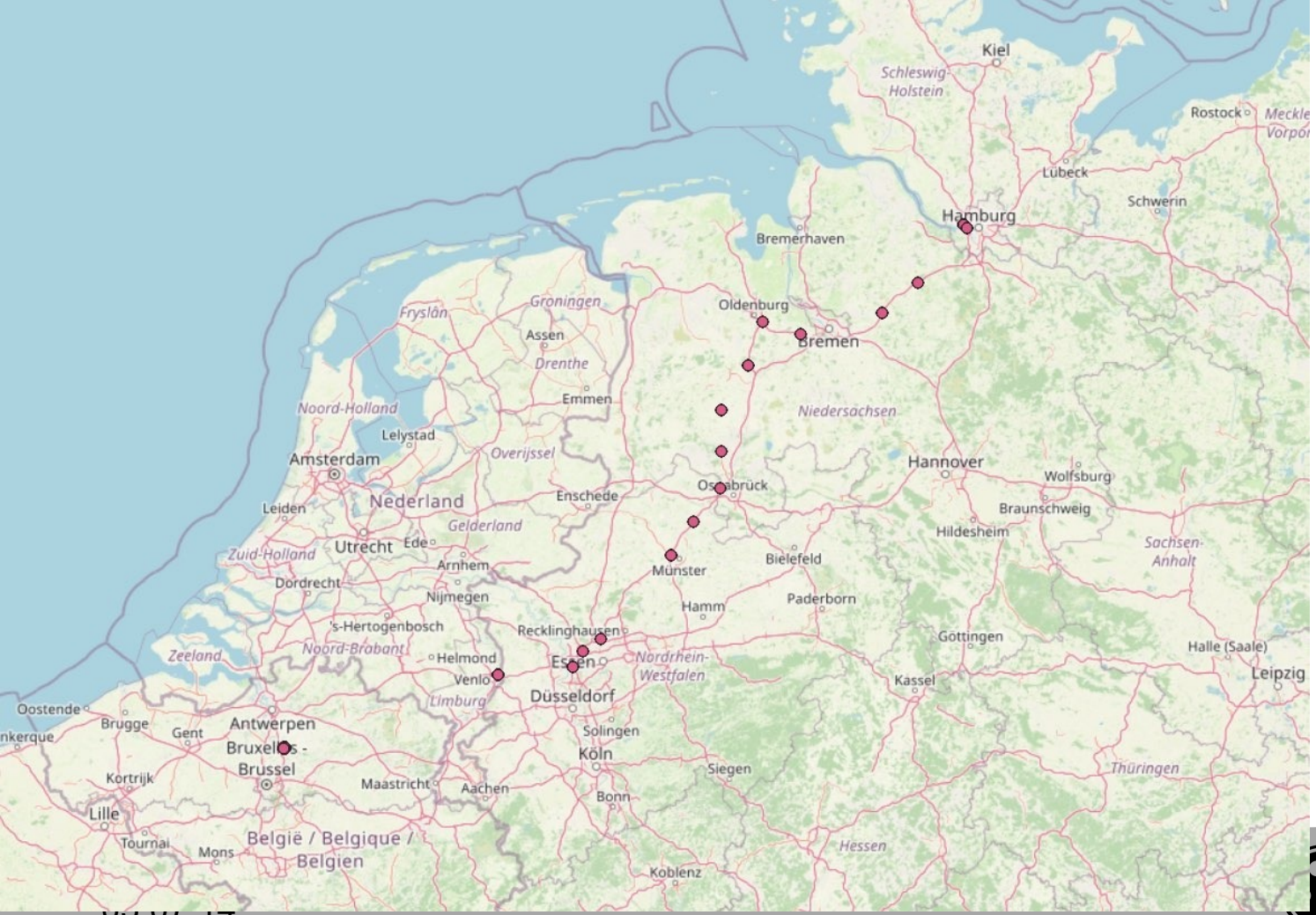
```
# Device 1

http --ignore-stdin https://smartthingsfind.samsung.com/device/setLastSelect.do? _csrf==${CSRF}
                                                  | jq --arg DATE "$(date +"%Y-%m-%d %H:%M:%S")" -r "
    .operation[0] | [\$DATE, (.longitude ), (.latitude), (.horizontalUncertainty),
    (.verticalUncertainty), (.locationType), (.oprnCrtDate)  ] ] | @csv" >> all.csv

```



knopfloch tv

```
"2023-05-29 19:09:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529190903",
"2023-05-29 19:10:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529191002",
"2023-05-29 19:11:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529191102",
"2023-05-29 19:12:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529191203",
"2023-05-29 19:13:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529191302",
"2023-05-29 19:14:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529191403",
"2023-05-29 19:15:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529191502",
"2023-05-29 19:16:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529191602",
"2023-05-29 19:17:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529191702",
"2023-05-29 19:18:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529191802",
"2023-05-29 19:19:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529191903",
"2023-05-29 19:20:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529192002",
"2023-05-29 19:21:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529192102",
"2023-05-29 19:22:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529192202",
"2023-05-29 19:23:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529192302",
"2023-05-29 19:24:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529192402",
"2023-05-29 19:25:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529192502",
"2023-05-29 19:26:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529192603",
"2023-05-29 19:27:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529192702",
"2023-05-29 19:28:01","10.525060332412842","54.84759829459622","6.0","6.0",,"20230529192802",
"2023-05-29 19:29:01","10.524851644587885","54.84741412964807","6.0","6.0",,"20230529192902",
"2023-05-29 19:30:01","10.524851644587885","54.84741412964807","6.0","6.0",,"20230529193002",
"2023-05-29 19:31:01","10.524851644587885","54.84741412964807","6.0","6.0",,"20230529193102",
"2023-05-29 19:32:01","10.524851644587885","54.84741412964807","6.0","6.0",,"20230529193202",
"2023-05-29 19:33:01","10.524851644587885","54.84741412964807","6.0","6.0",,"20230529193302",
"2023-05-29 19:34:01","10.524851644587885","54.84741412964807","6.0","6.0",,"20230529193403",
```


DENMARK
Copenhagen
SCHLESWIG-
HOLSTEIN
Amsterdam
Hamburg
MECKLENBURG-
VORPOMMERN
Brussels
NORTH RHINE-
WESTPHALIA
BRANDENBURG
Berlin
LUXEMBOURG
HESSE
GERMANY
Frankfurt
THURINGIA
SAARLAND
GRAND EST
SAXONY



Why Samsung and not Apple?

- **Probably broader distribution**
- **Easier to hide**
- **Sound can be easily disabled.**
- **Srcaping works!**

Learings and insights

- No signaling when connected phone is traveling together
- Works on highways
- Not always working on trains

Thank you – any questions left? Get in contact!

Marcus Lindemann

lindemann@autorenwerk.de **Twitter: @MarcusLindemann**

autoren(werk) GmbH & Co KG

Weydinger Str. 20-22

10178 Berlin

Germany

www.autorenwerk.com www.knopfloch.tv

knopfloch tv