

Geek speak !

Your favourite tool



Moderator : Ana Lutzky, Data Editor at AEF info
[@anouchka](https://twitter.com/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

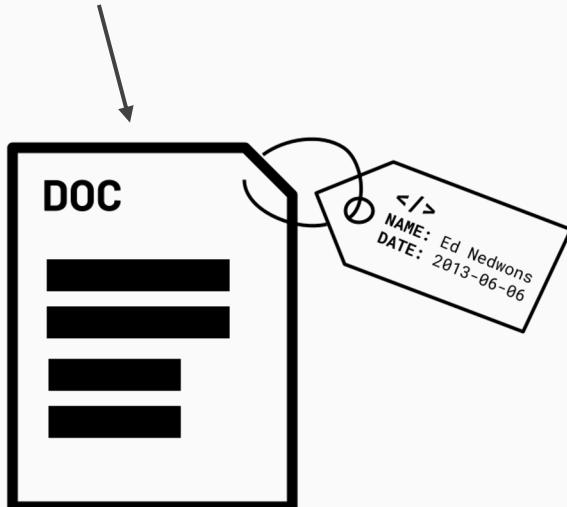
Handling Docs Safely

June 2023

Alex Pyrgiotis (@apyrgio)

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

⚠ Malicious documents
may contain malware



Is it still relevant?

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

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

Nation-state Hackers Target Journalists with Goldbackdoor Malware

Headlines from 2022 articles on malware attacks

Yeap.



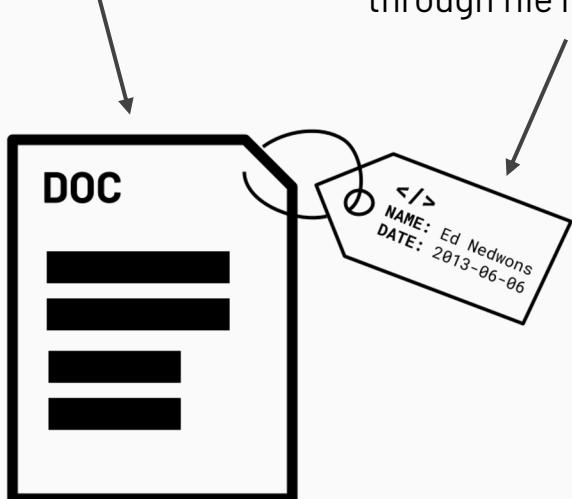
Dangerzone

<https://dangerzone.rocks>

.... 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.



Dangerzone

<https://dangerzone.rocks>

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>

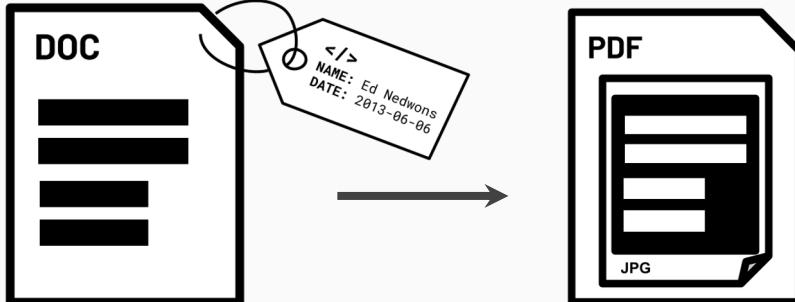


Dangerzone

<https://micahflee.com>

<https://freedom.press>

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

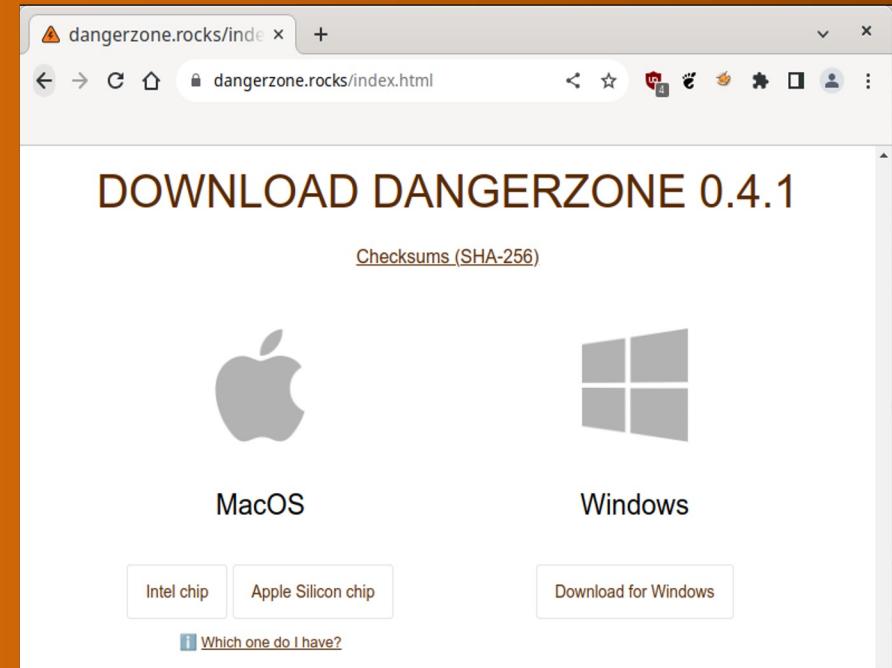
Windows, Mac & Linux



Dangerzone

How it works?

- Install Dangerzone in your computer



Dangerzone

How it works?

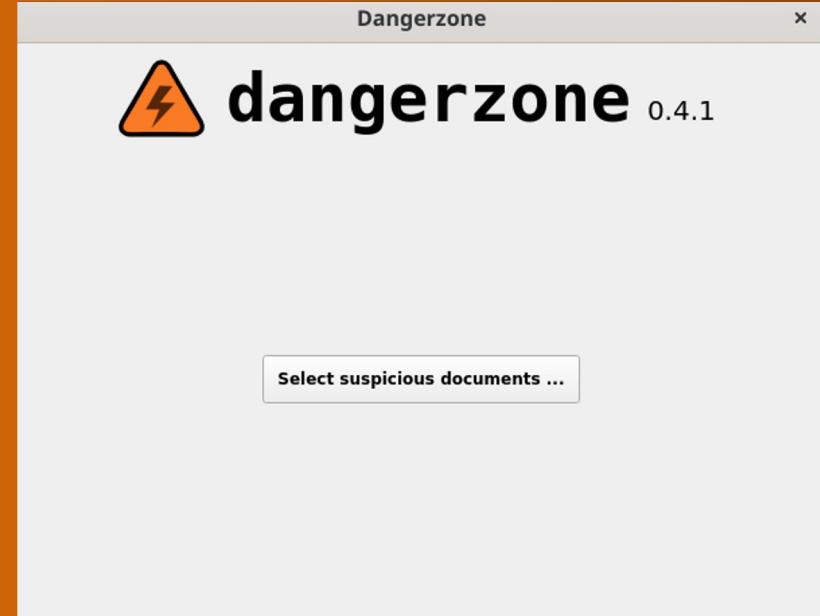
- Install Dangerzone in your computer
- Install Docker Desktop (MacOS/Win)



Dangerzone

How it works?

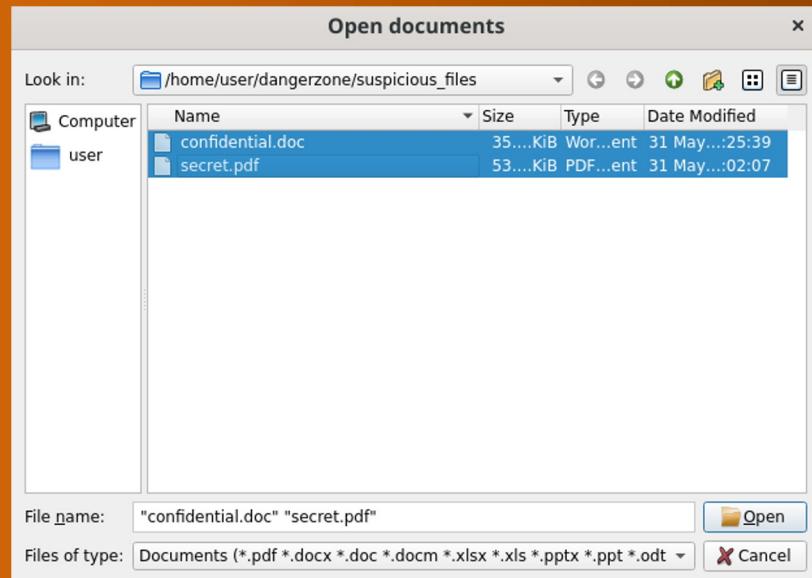
- Install Dangerzone in your computer
- Install Docker Desktop (MacOS/Win)
- Open the Dangerzone application



Dangerzone

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 



Dangerzone

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?



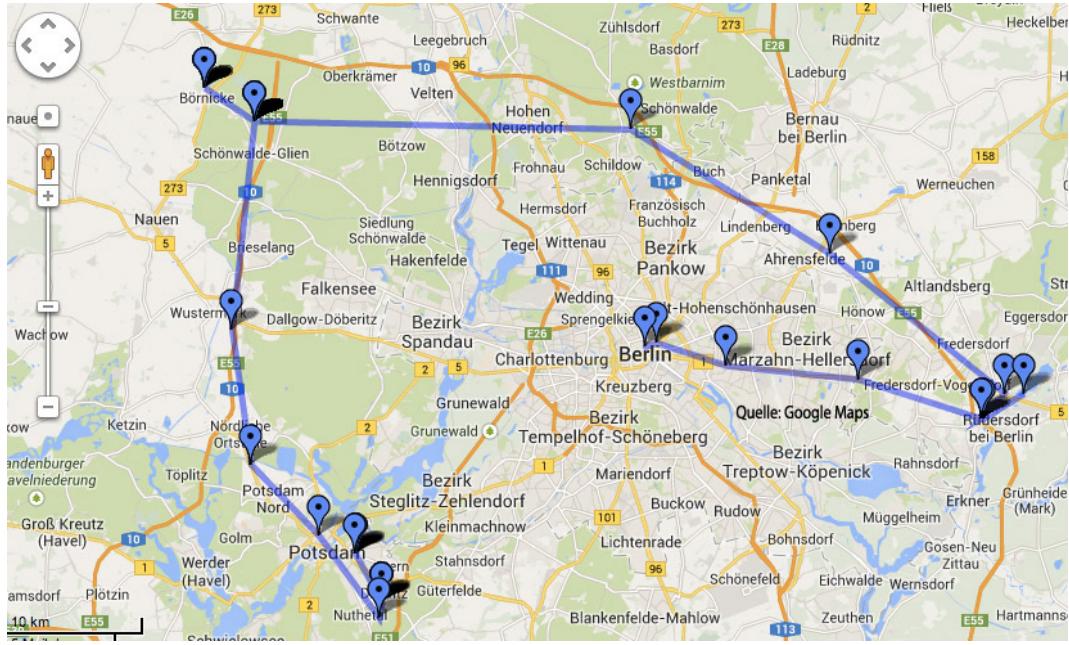
Dangerzone



Bluetooth tracking – first learnings

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

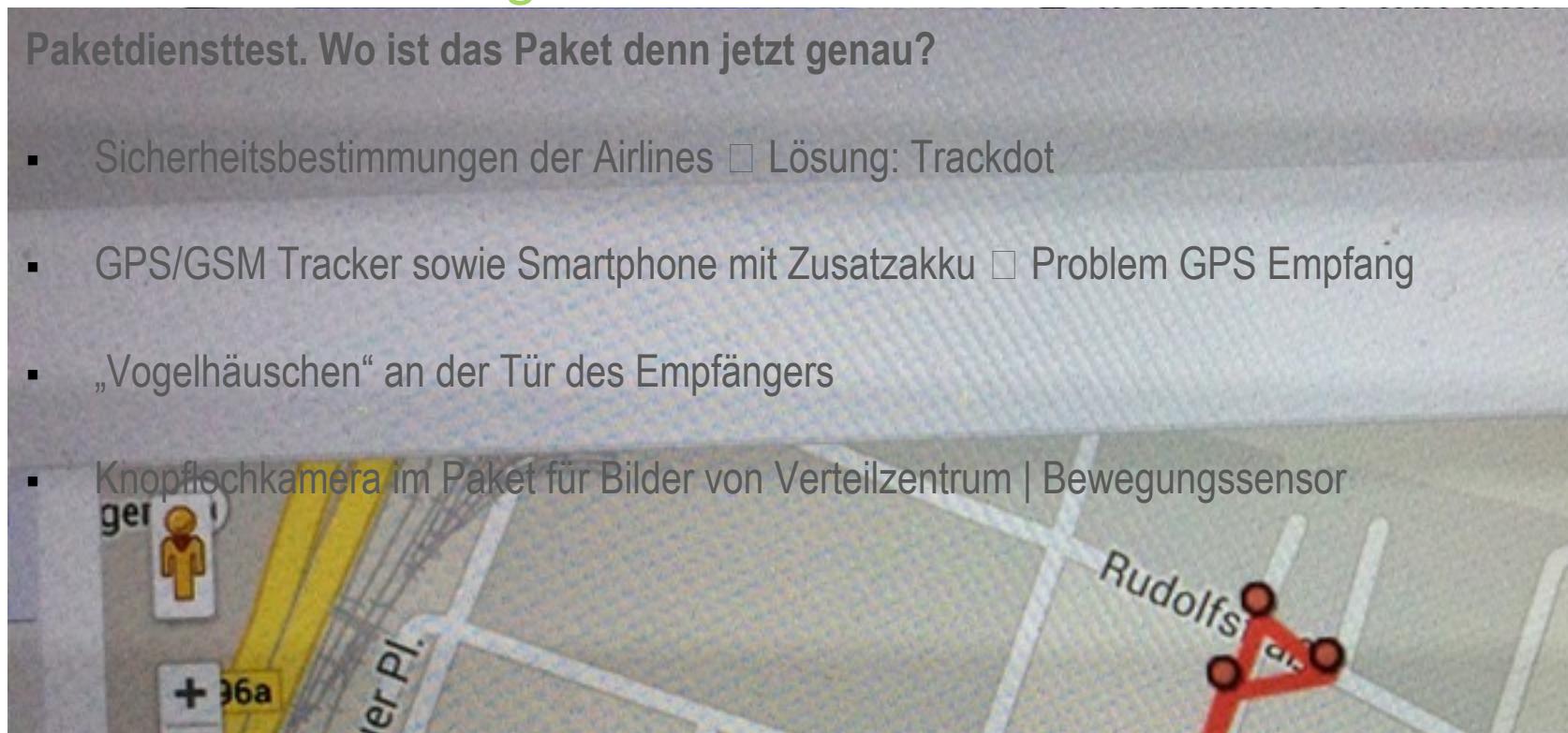
Video und Tracking 2



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



2018 – 2020: tracking electronic waste

The image is a composite of three panels. The left panel shows a close-up of hands assembling a black electronic component onto a white plastic frame. The middle panel is a map of Berlin and surrounding areas, showing a green line representing the path of a tracked object. A callout box provides specific tracking details. The right panel is a larger map of Brandenburg and parts of Berlin, also showing a green path and a callout box with tracking information.

Left Panel: A person's hands are shown assembling a black electronic component onto a white plastic frame. The ZDF logo is in the top left corner. The WISO logo is in the bottom left corner. The video player interface shows 15:14 | 42:10.

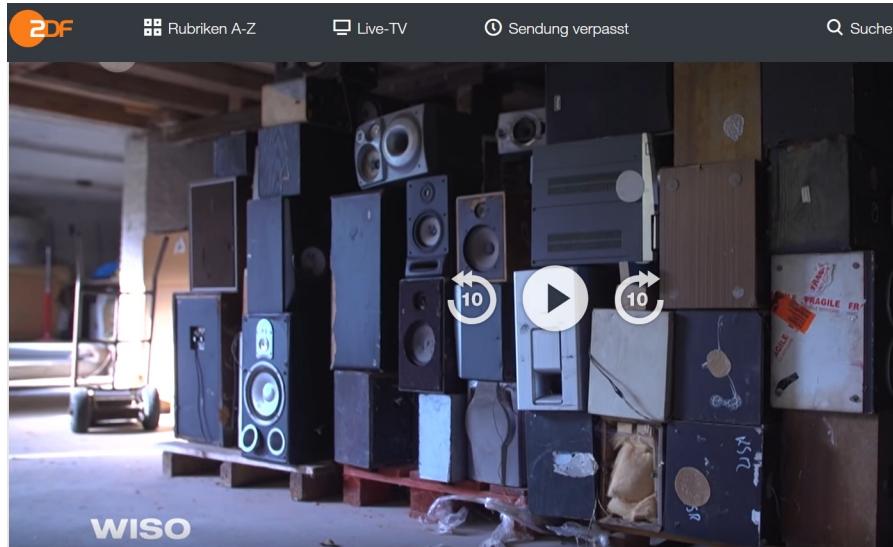
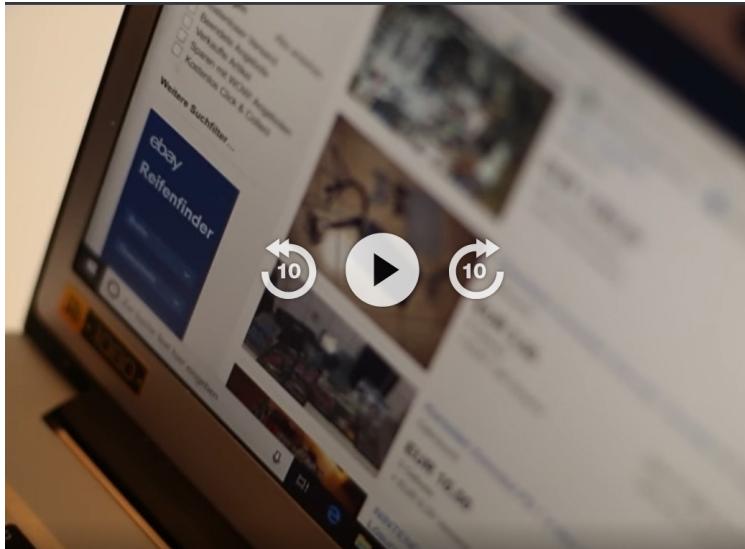
Middle Panel: A map of Berlin and surrounding areas. A green line tracks the movement of an object. A callout box displays the following information:
4 ON Delta LK209C-12301
2017-06-12 09:41:37
Latitude 52.46011, Long 13.52422
Lat52.54692,Long13.52422
Direction North, Speed 0.00km/h

Right Panel: A map of Brandenburg and parts of Berlin. A green line tracks the movement of an object. A callout box displays the following information:
4 On Board Alpha LK209C-33346
2017-07-25 06:08:42
Latitude 52.14201, Long 12.78912
Lat52.14201,Long12.78912
Direction Southwest, Speed 77.78km/h

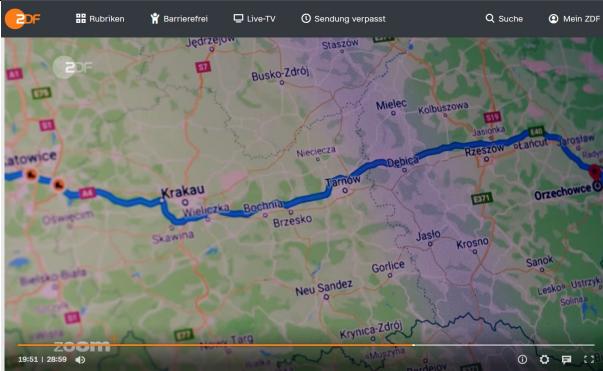
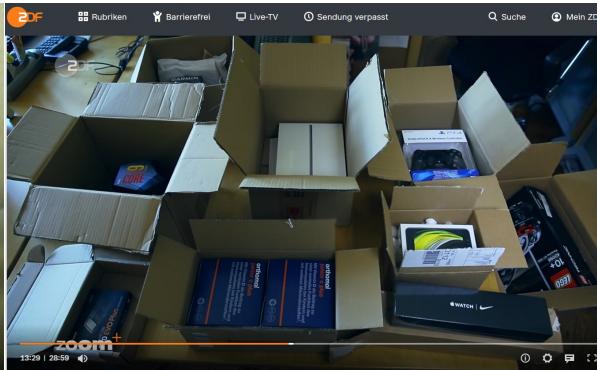
2018 – 2020: tracking electronic waste



2018 – 2020: tracking electronic waste



2020: investigating online fraud



Gadget currently 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 €



anlos liefern lassen
vorrätige Artikel im
le Store abholen



Kostenlose persönliche
Gravur



Kostenlose, einfache
Rückgabe



05.07.14

★★★★★ (2)

Samsung Galaxy Sm

€79.90

● IN STOCK, IMMEDIATELY READY FOR DELIVERY

1



Fixed delivery €4.95



Up

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?

The screenshot shows a web application interface. On the left, there's a sidebar titled "SmartThings Find" with a list of devices: "Meine Geräte (5)" including "Adrian Hoffmann", "Mausi", "Schlüssel", "Galaxy A51 von Stefan ie", and "Galaxy A5 (2016)". The main area displays a map of a city street with several green location markers. One marker is highlighted with a larger circle and a green dot, indicating its current position. The map includes street names like Berlinstraße, Weydemeyerstraße, Lichtenberger Str., Palisadenstraße, Friedrichsberger Str., Fürstenwalder Str., Lebuser Str., Karl-Marx-Allee, Neue Blumenstraße, Plänsche Singerstraße, Lichtenberger Str., Singerstraße, Krautstraße, Andressstraße, and Lange Str. A U-Bahn station "U Strausberger Platz" is also visible. To the right of the map is a browser's developer tools Network tab. The Network tab shows a list of requests with their names and CSRF tokens. One request is selected, showing its details: "Name: getTagLocation.do?_csrf=928721681816592709". The "Timing" section of the Network tab shows a timeline with several blue bars representing request durations. The "Header" and "Nutzlast" sections are also visible.

Name
getTagLocation.do?_csrf=928721681816592709
getEncToken.do?_csrf=928721681816592709
setLastSelect.do?_csrf=928721681816592709
subscriptions
activate?filterRegion=eu-west-1
addOperation.do?_csrf=928721681816592709
getTagLocation.do?_csrf=928721681816592709
getOperationResult.do?_csrf=928721681816592709
addOperation.do?_csrf=928721681816592709
getTagLocation.do?_csrf=928721681816592709
getOperationResult.do?_csrf=928721681816592709
getEncToken.do?_csrf=928721681816592709
setLastSelect.do?_csrf=928721681816592709
subscriptions
activate?filterRegion=eu-west-1
addOperation.do?_csrf=928721681816592709
getTagLocation.do?_csrf=928721681816592709
getOperationResult.do?_csrf=928721681816592709

What does it look like?

The image shows a screenshot of a web application interface. On the left, there is a map of a city area with several streets labeled in German, such as Berlinstraße, Weydemeyerstraße, Lichtenberger Str., Palisadenstraße, Friedrichsberger Str., Lebuser Str., Karl-Marx-Allee, Neue Blumenstraße, Plänsche Singerstraße, Lichtenberger Str., Singerstraße, Krautstraße, and Andrästraße. A green location marker with a blue arrow points to a specific spot on the map. On the right, a browser's developer tools Network tab is open, showing a list of network requests. One request, with the ID 1 X53452, is highlighted with a red circle around its response payload. The payload contains the JSON object: {"latitude": "53.567433", "longitude": "9.8744892", "...". The Network tab also includes a timeline at the top and various filter options.

Name	Header	Nutzlast	Vorschau	Antwort	Initiator	Timing
getTagLocation.do?_csrf=928721681816592709						
getEncToken.do?_csrf=928721681816592709						
setLastSelect.do?_csrf=928721681816592709						
subscriptions						
activate?filterRegion=eu-west-1						
addOperation.do?_csrf=928721681816592709						
getTagLocation.do?_csrf=928721681816592709						
getOperationResult.do?_csrf=928721681816592709						
addOperation.do?_csrf=928721681816592709						
getTagLocation.do?_csrf=928721681816592709						
getOperationResult.do?_csrf=928721681816592709						
getEncToken.do?_csrf=928721681816592709						
setLastSelect.do?_csrf=928721681816592709						
subscriptions						
activate?filterRegion=eu-west-1						
addOperation.do?_csrf=928721681816592709						
getTagLocation.do?_csrf=928721681816592709						
getOperationResult.do?_csrf=928721681816592709						

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

```
7 # Device 1
8
9 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
10
```

The screenshot shows a Jupyter Notebook interface running in a browser window. The browser title bar says "Neuer Tab". The search bar contains "Suche oder Adresse eingeben". The notebook has two visible cells:

```
✓ # Start the driver function - this opens the Selenium ...
    time.sleep(5) ...

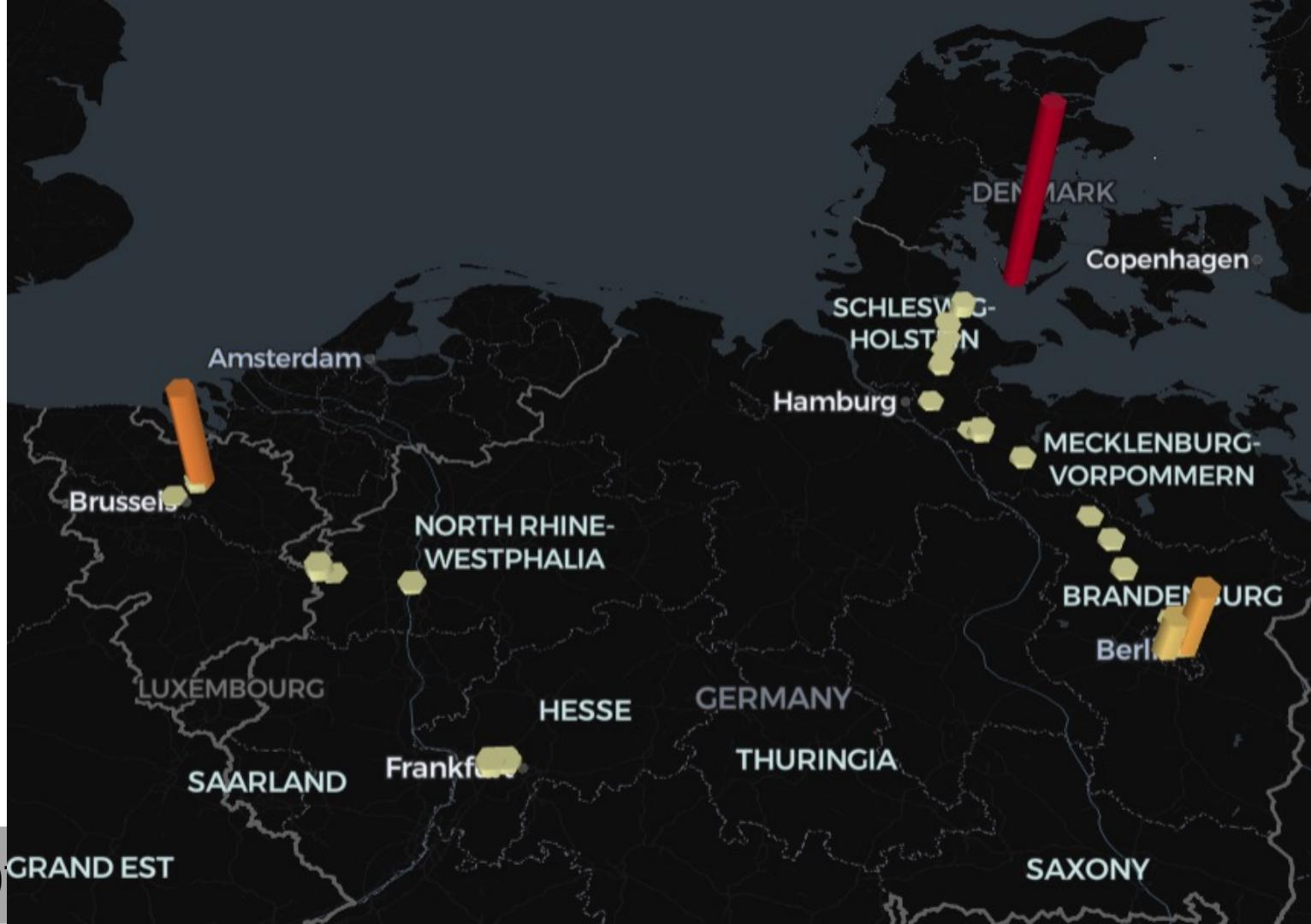
# Check: Is the IP Address the IP adress of the Digital ...
# Now, we start the Login Process ...
# Click on Info window - if it will be shown ...
# Click on current tracker to refresh the position ...
# Extract Cookie ...
# Load this if requests ...
# filter the requests ...
# Get device ID ...
# Get CSRF ...
```

Cell 31 and Cell 32 are visible at the bottom left. The status bar at the bottom shows "You, 56 seconds ago Ln 17 Col 1 Spaces: 4 UTF-8 CRLF Python 3.11.1 64-bit".

Type 'python' code here and press Shift+Enter to run

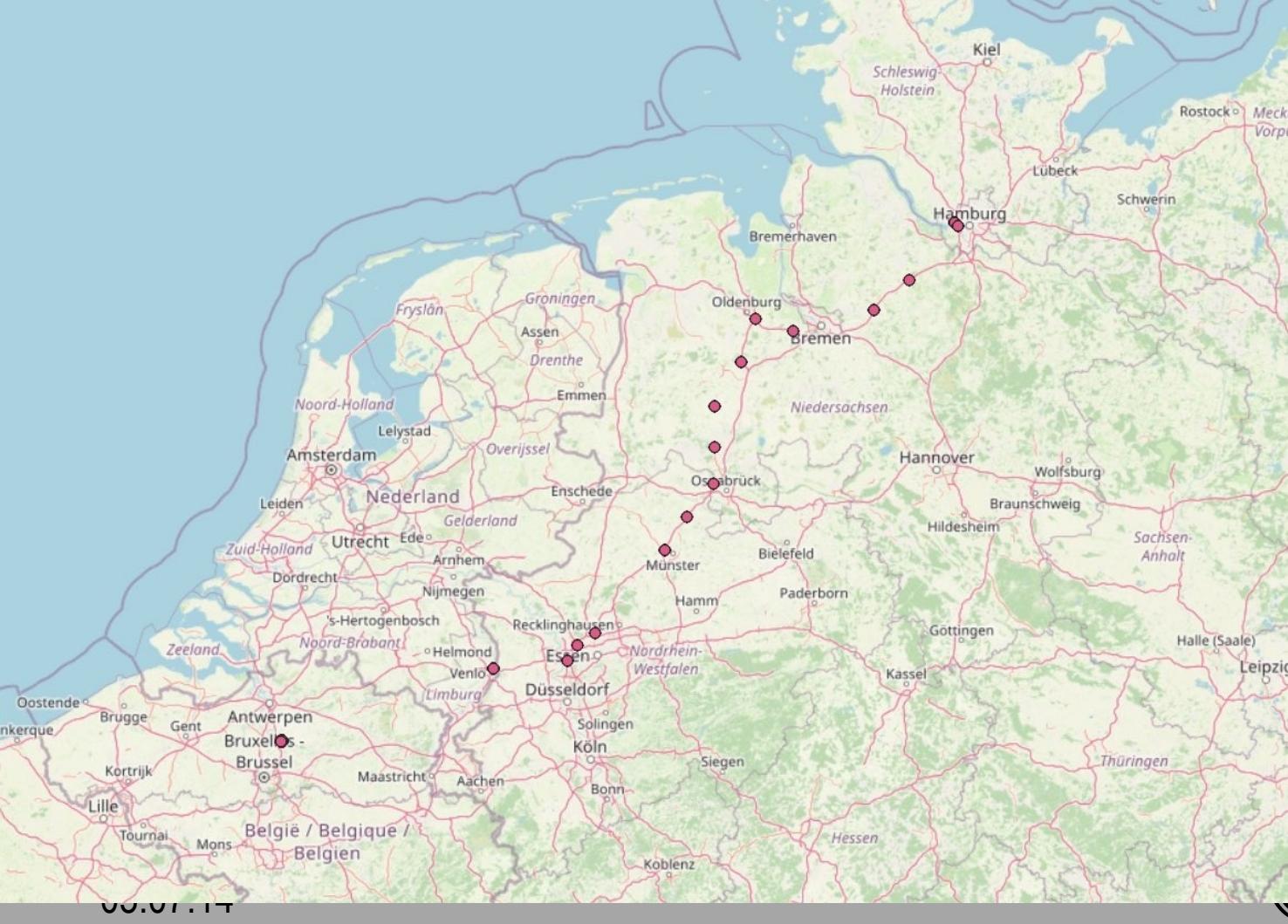


1	"2023-05-29 19:09:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529190903",
2	"2023-05-29 19:10:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529191002",
3	"2023-05-29 19:11:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529191102",
4	"2023-05-29 19:12:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529191203",
5	"2023-05-29 19:13:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529191302",
6	"2023-05-29 19:14:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529191403",
7	"2023-05-29 19:15:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529191502",
8	"2023-05-29 19:16:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529191602",
9	"2023-05-29 19:17:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529191702",
10	"2023-05-29 19:18:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529191802",
11	"2023-05-29 19:19:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529191903",
12	"2023-05-29 19:20:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529192002",
13	"2023-05-29 19:21:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529192102",
14	"2023-05-29 19:22:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529192202",
15	"2023-05-29 19:23:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529192302",
16	"2023-05-29 19:24:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529192402",
17	"2023-05-29 19:25:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529192502",
18	"2023-05-29 19:26:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529192603",
19	"2023-05-29 19:27:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529192702",
20	"2023-05-29 19:28:01", "10.525060332412842", "54.84759829459622", "6.0", "6.0",, "20230529192802",
21	"2023-05-29 19:29:01", "10.524851644587885", "54.84741412964807", "6.0", "6.0",, "20230529192902",
22	"2023-05-29 19:30:01", "10.524851644587885", "54.84741412964807", "6.0", "6.0",, "20230529193002",
23	"2023-05-29 19:31:01", "10.524851644587885", "54.84741412964807", "6.0", "6.0",, "20230529193102",
24	"2023-05-29 19:32:01", "10.524851644587885", "54.84741412964807", "6.0", "6.0",, "20230529193202",
25	"2023-05-29 19:33:01", "10.524851644587885", "54.84741412964807", "6.0", "6.0",, "20230529193302",
26	"2023-05-29 19:34:01", "10.524851644587885", "54.84741412964807", "6.0", "6.0",, "20230529193403",



05.0

och tv



00.07.17

Why Samsung and not Apple?

- Probably broader distribution
- Easier to hide
- Sound can be easily disabled.
- Scrapping 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

