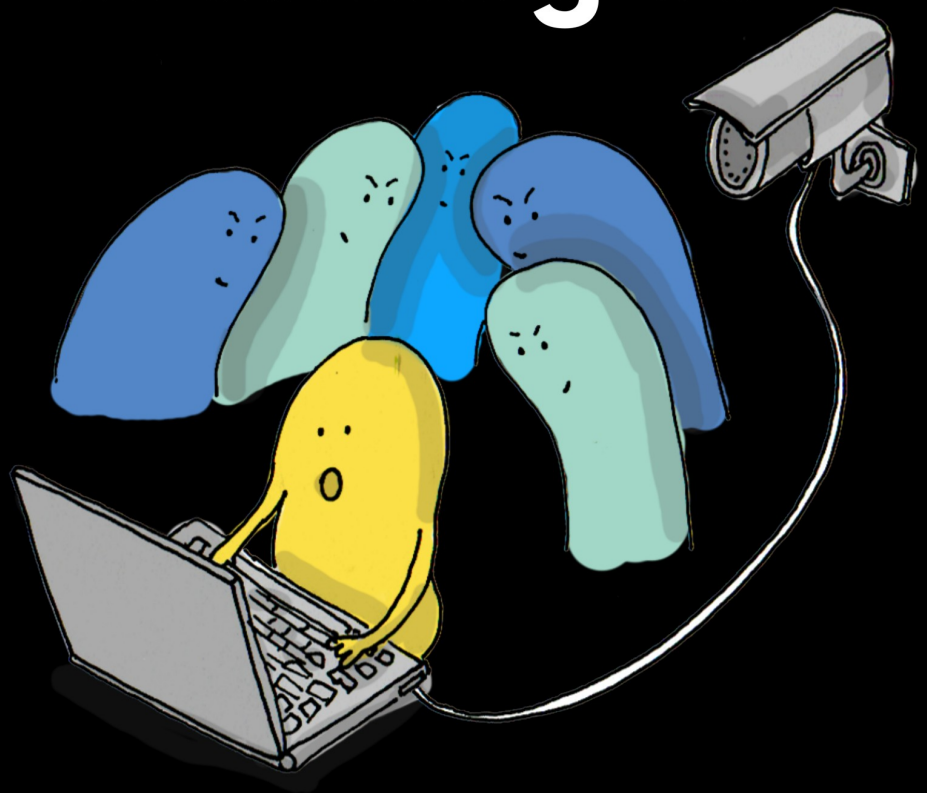
Watching them Watching us

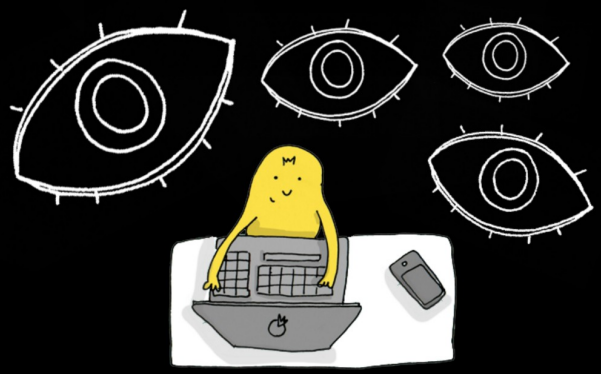


Konark Modi | @konarkmodi
Santiago Saavedra | @ssice
Sofía Prósper | @sofipros

github.com/cliqz-oss/local-sheriff

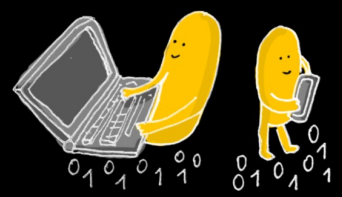
trackula.org

Top 5 trackers in Europe

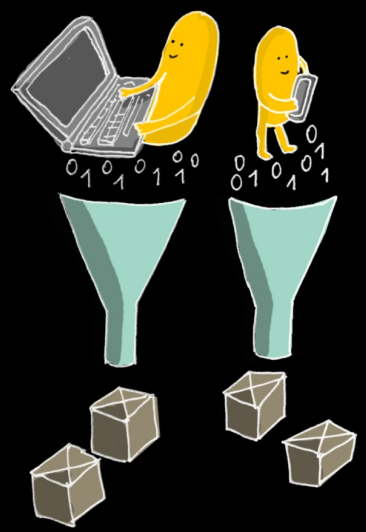


Source: whotracks.me from December 2018

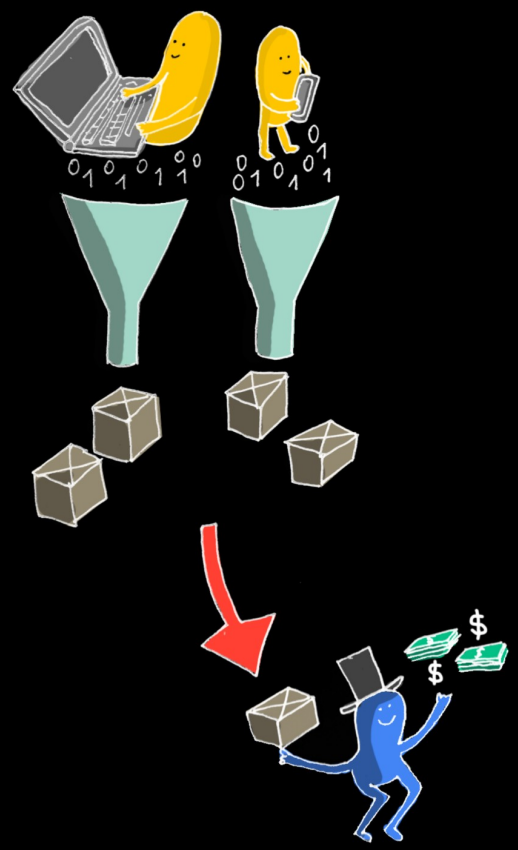
How does it work?



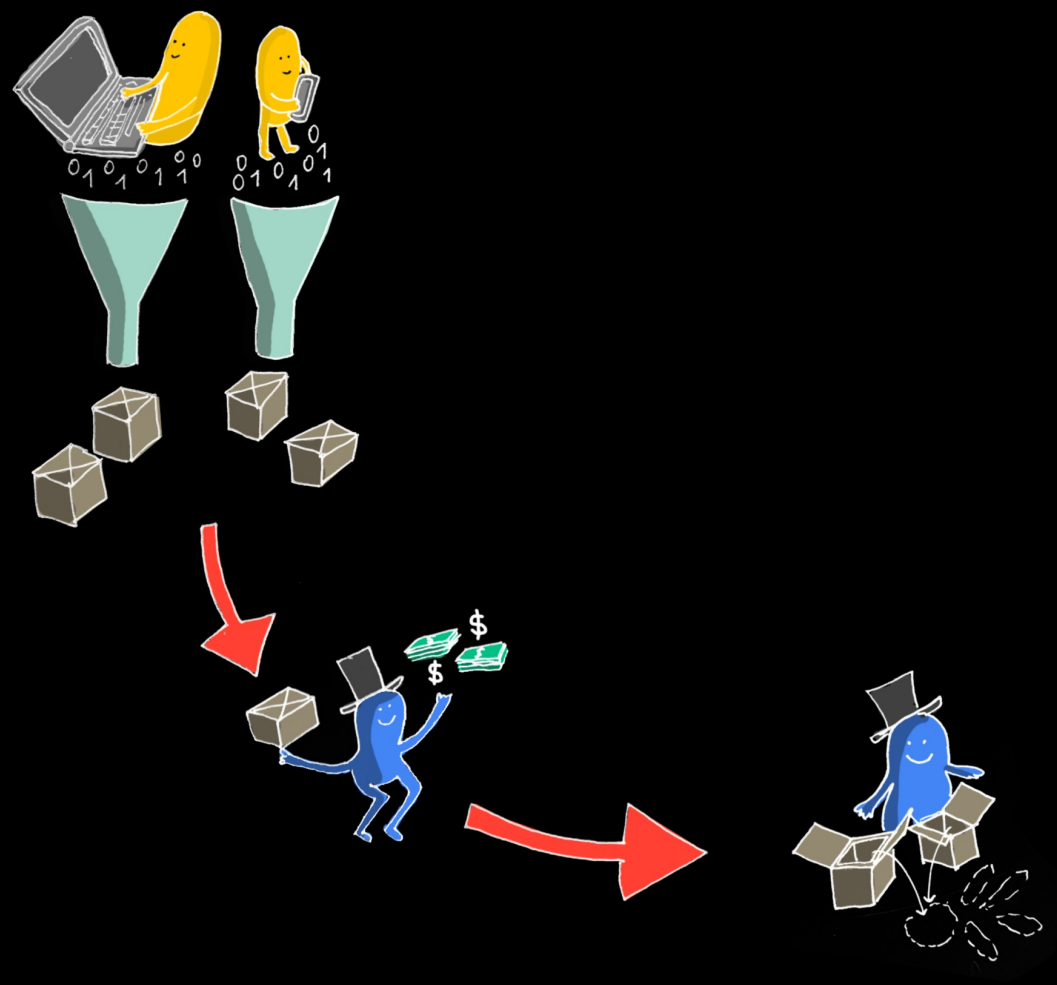
How does it work?



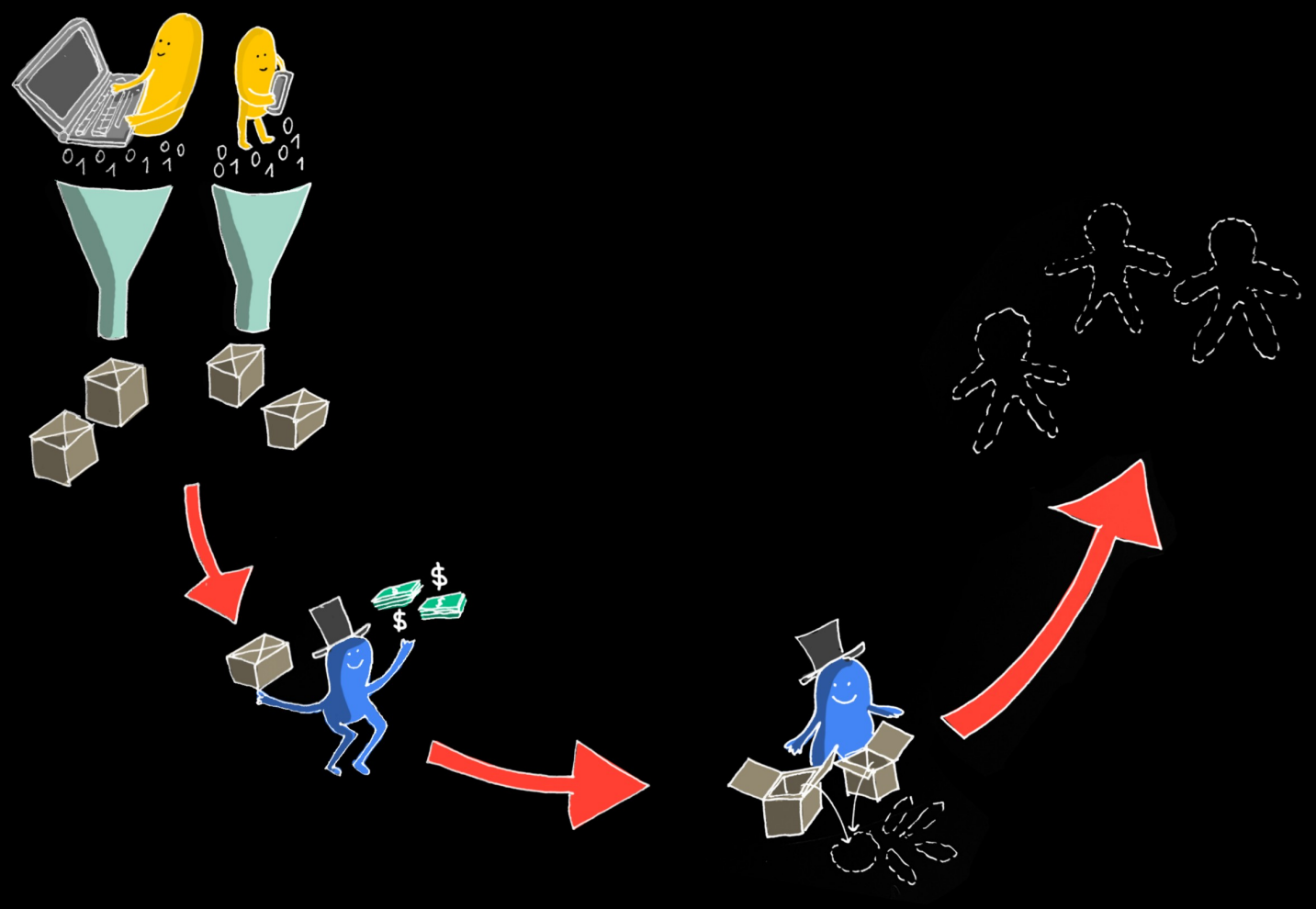
How does it work?



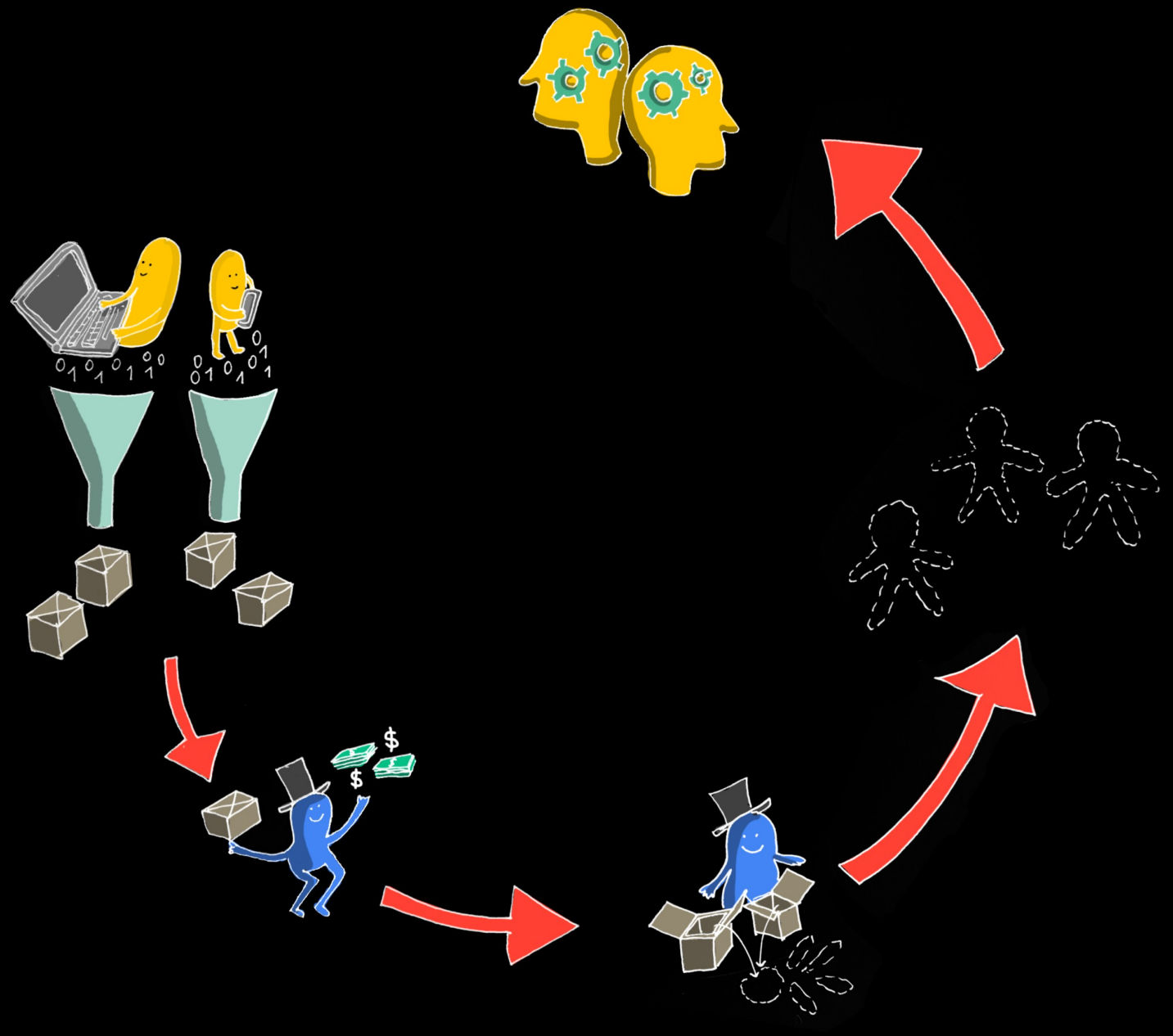
How does it work?



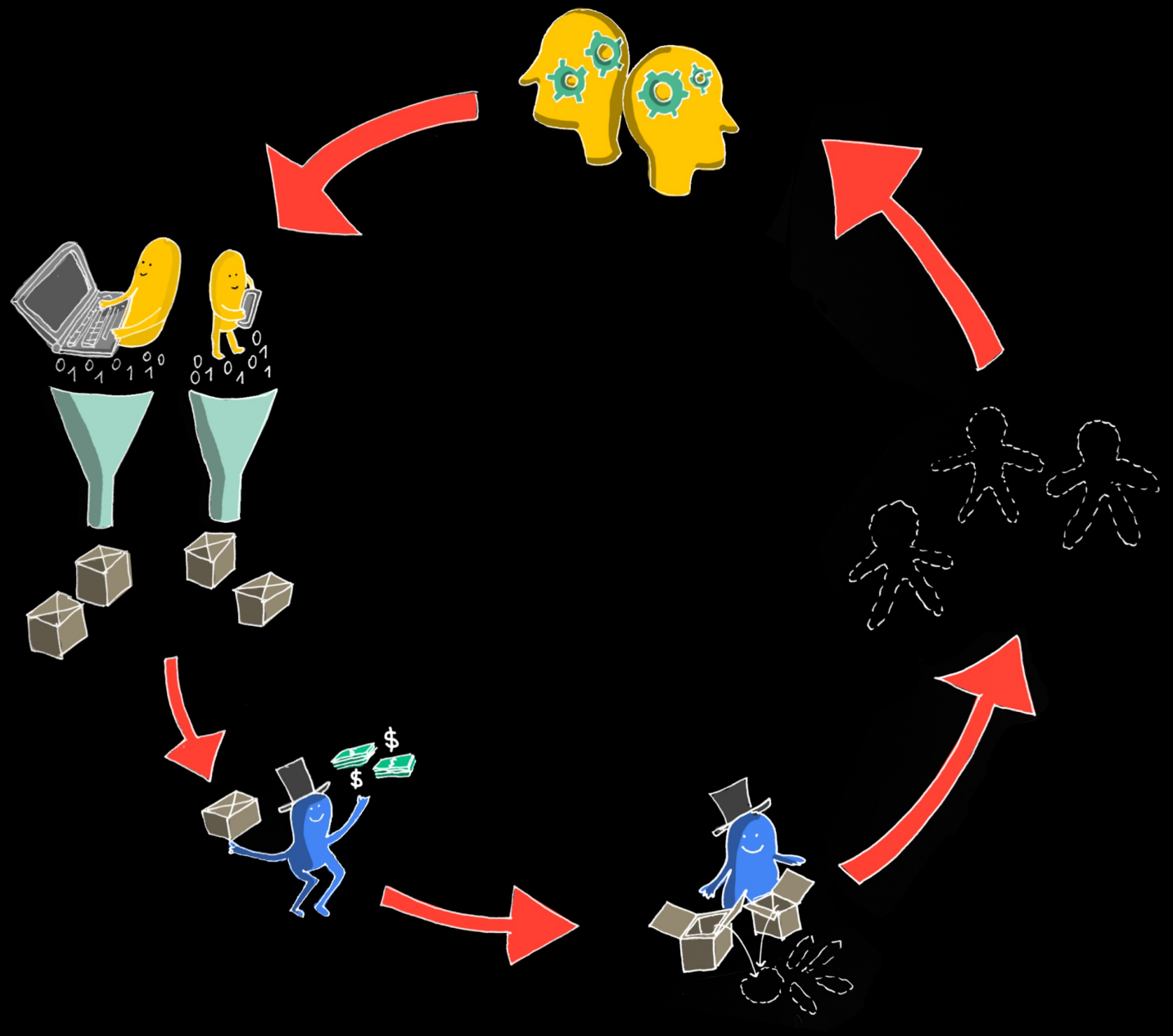
How does it work?



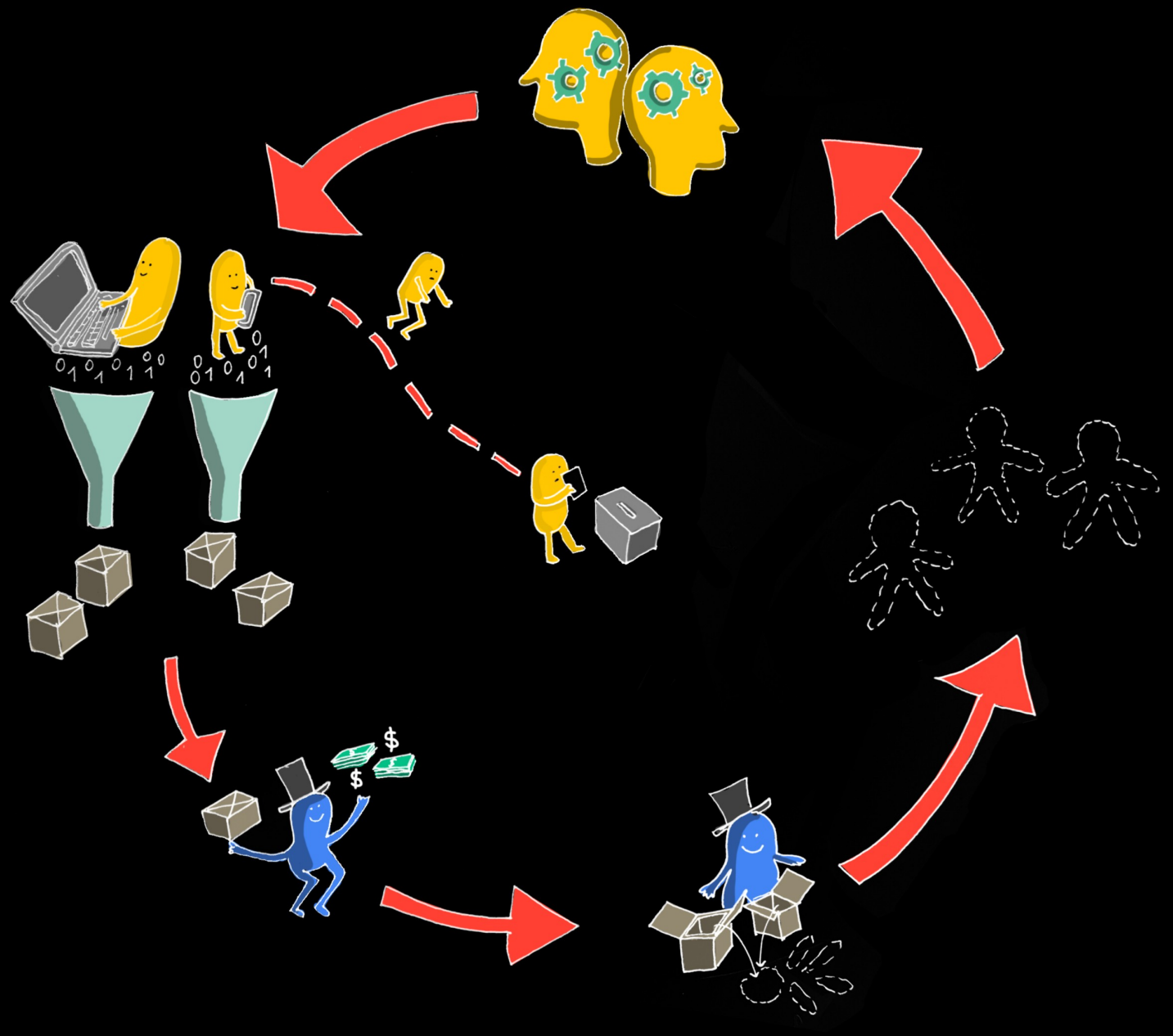
How does it work?

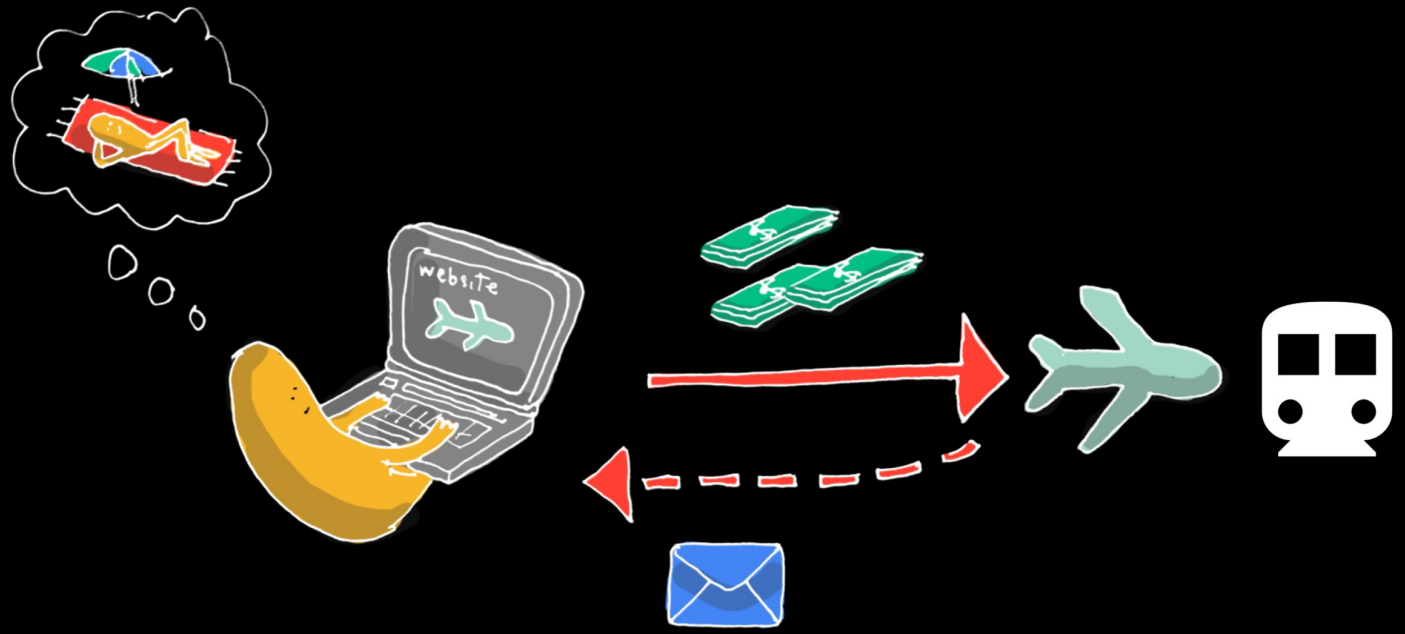


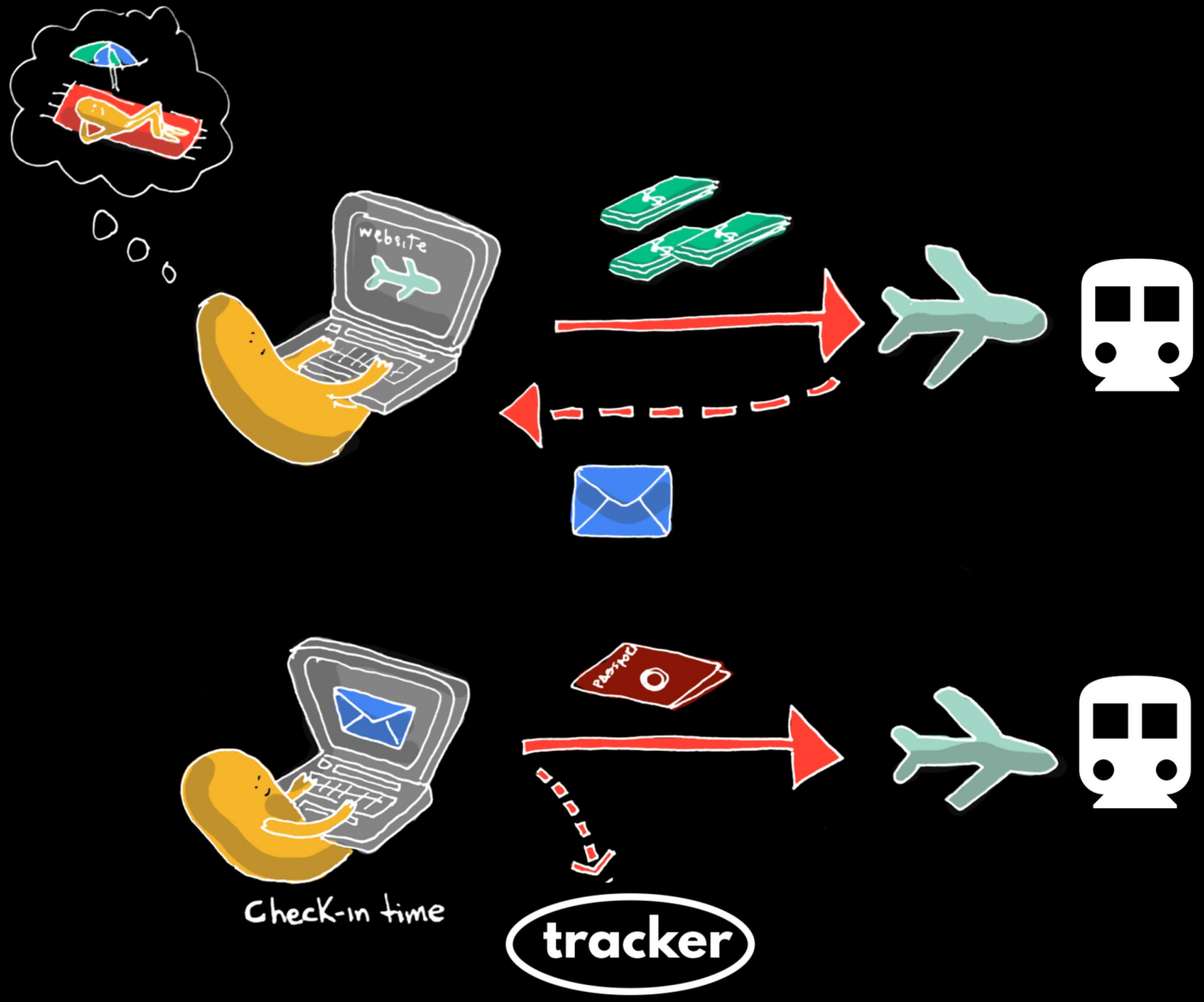
How does it work?



How does it work?




website

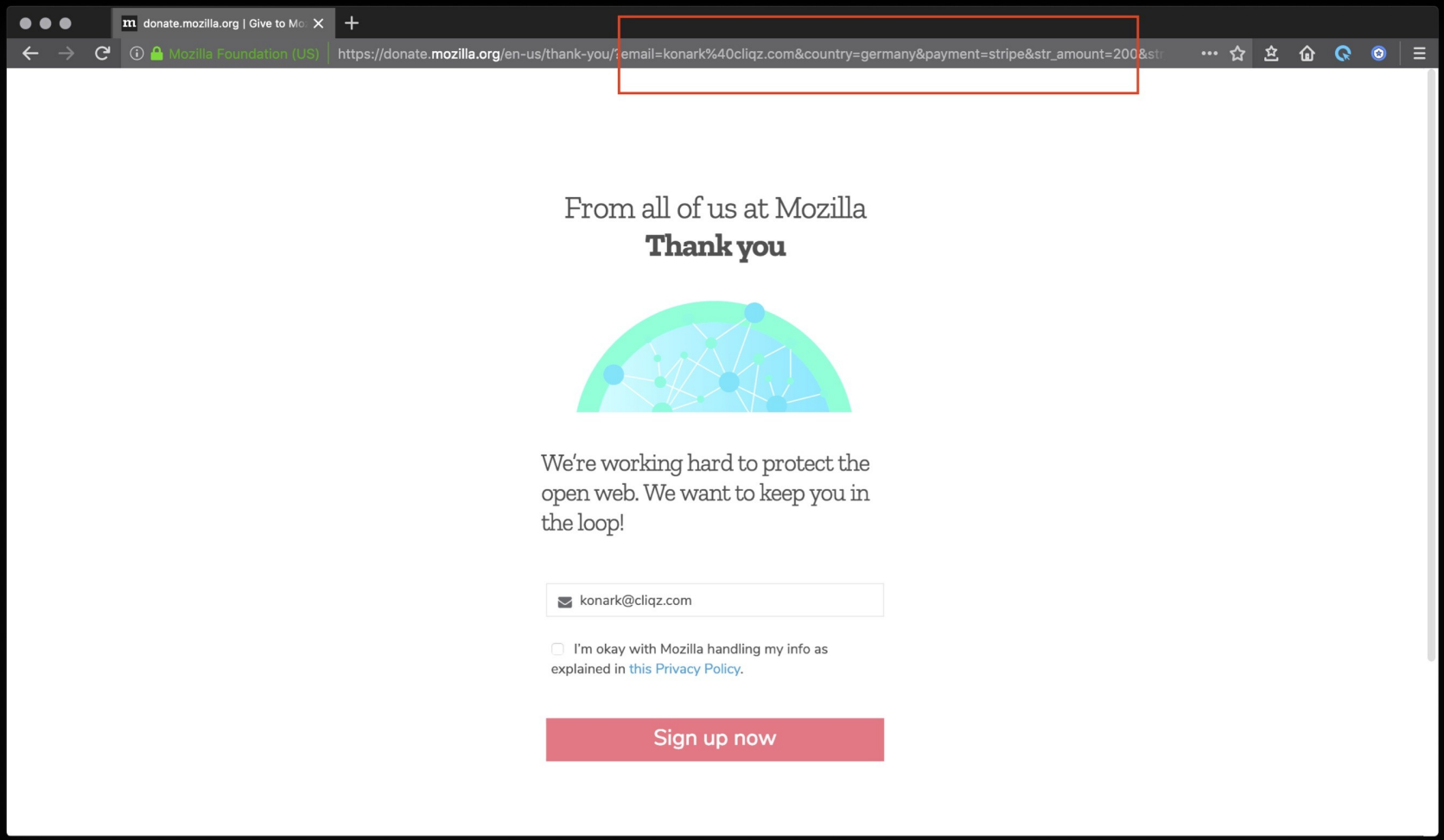

website
Check-in time
tracker

LOCAL SHERIFF

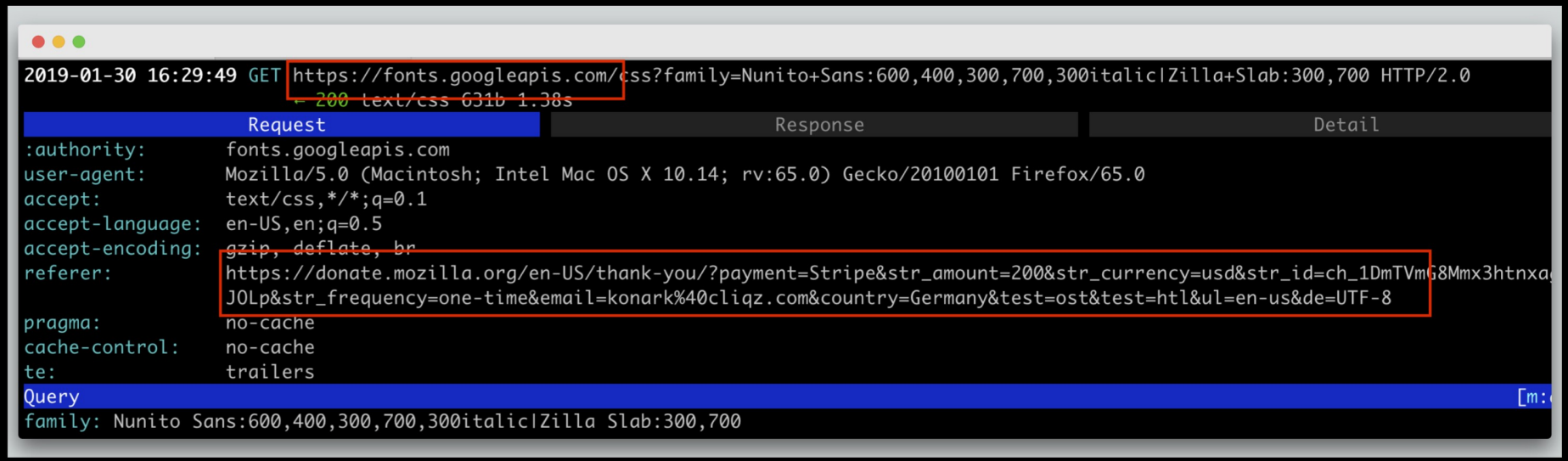
TELLTALE URL

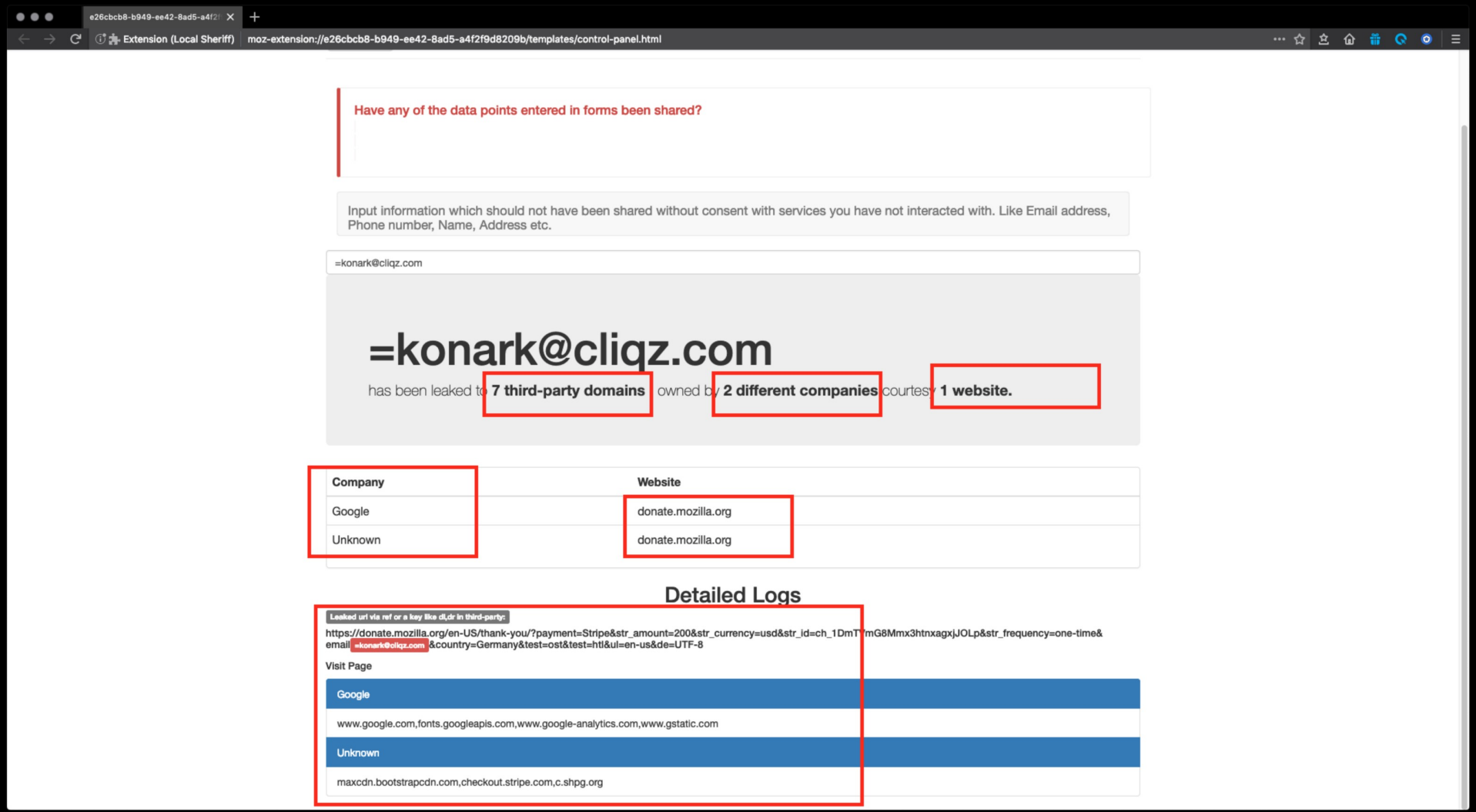
A URL which contains sensitive information or can lead to a page which contains sensitive information

EXAMPLE #1

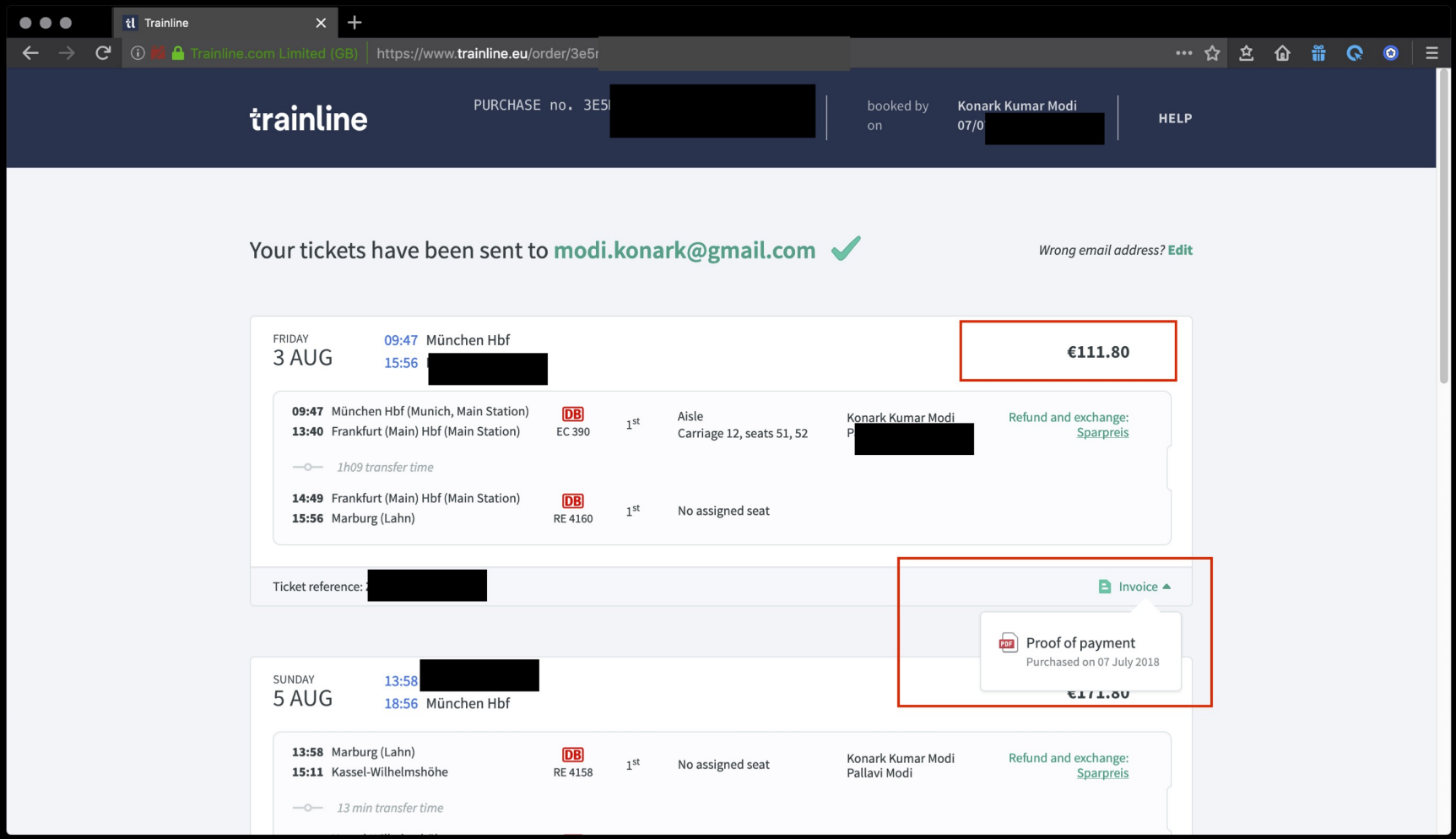

donate.mozilla.org | Give to Mo
Mozilla Foundation (US)
https://donate.mozilla.org/en-us/thank-you/?email=konark%40cliqz.com&country=germany&payment=stripe&str_amount=200&str
From all of us at Mozilla
Thank you
We're working hard to protect the open web. We want to keep you in the loop!
konark@cliqz.com
I'm okay with Mozilla handling my info as explained in this Privacy Policy.
Sign up now

IDENTIFYING LEAKS

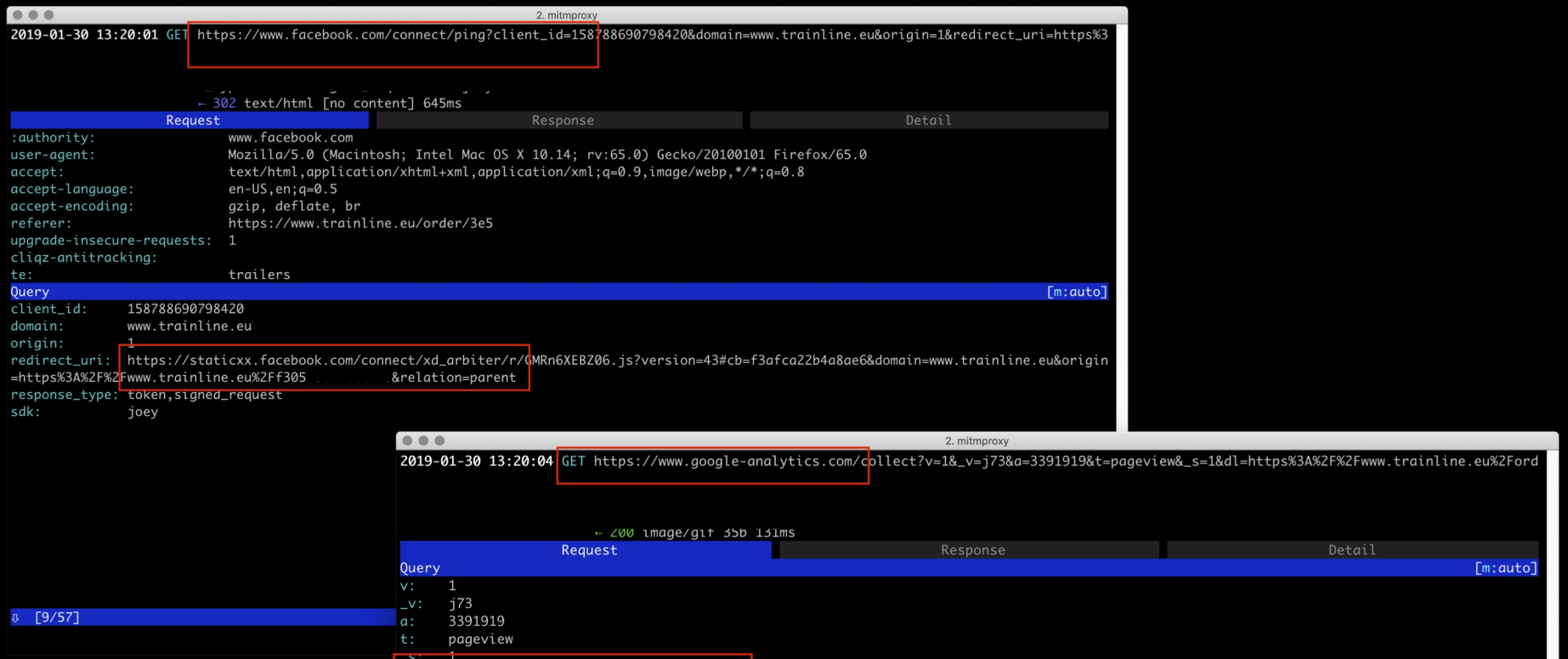


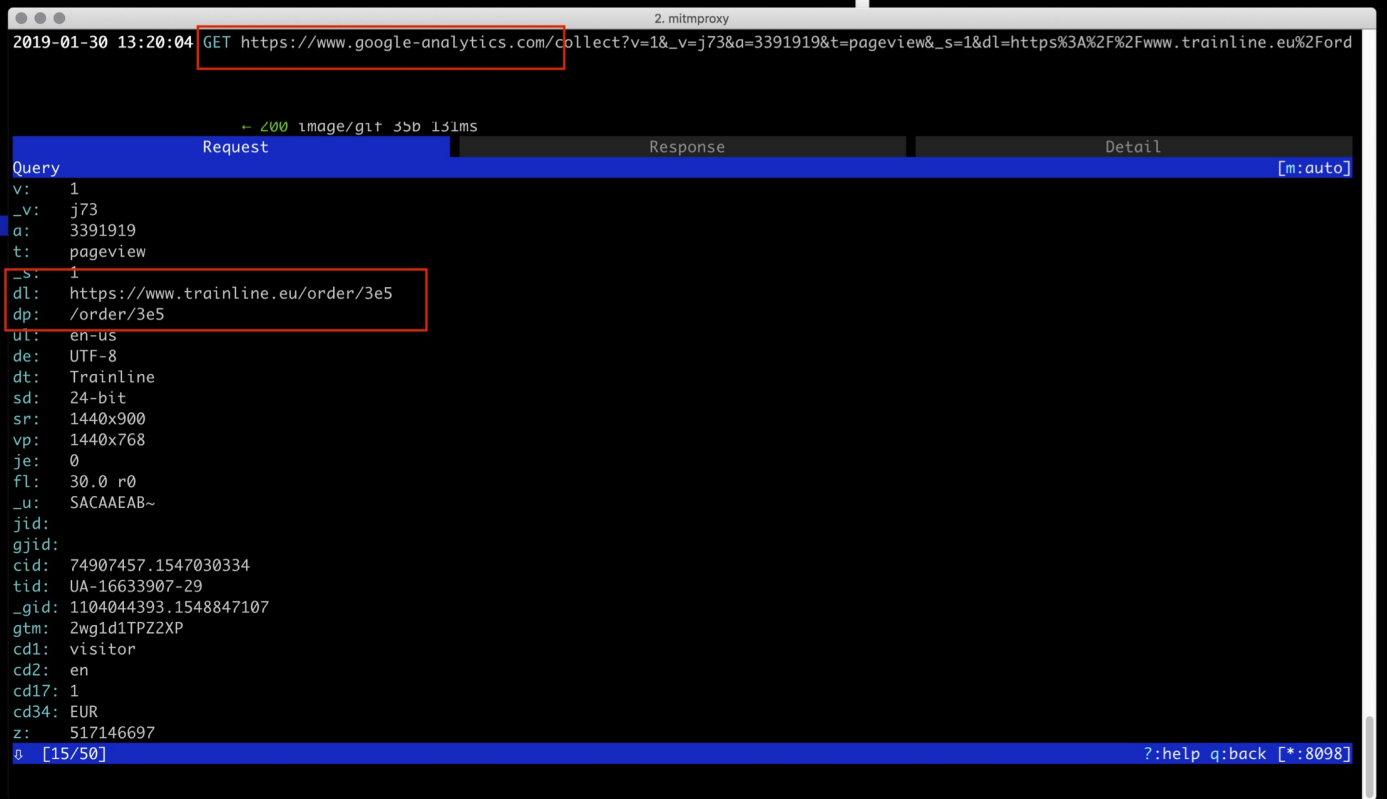

e26cbcb8-b949-ee42-8ad5-a4f2f
Extension (Local Sheriff)
moz-extension://e26cbcb8-b949-ee42-8ad5-a4f2f9d8209b/templates/control-panel.html
Have any of the data points entered in forms been shared?
Input information which should not have been shared without consent with services you have not interacted with. Like Email address, Phone number, Name, Address etc.
=konark@cliqz.com
=konark@cliqz.com
has been leaked to 7 third-party domains owned by 2 different companies courtesy 1 website.
Company
Website
Google
donate.mozilla.org
Unknown
donate.mozilla.org
Detailed Logs
Leaked url via ref or a key like dl,dr in third-party:
https://donate.mozilla.org/en-US/thank-you/?payment=Stripe&str_amount=200&str_currency=usd&str_id=ch_1DmT
mG8Mmx3htnxagxJOLp&str_frequency=one-time&
email
=konark@cliqz.com
&country=Germany&test=ost&test=htl&ul=en-us&de=UTF-8
Visit Page
Google
www.google.com,fonts.googleapis.com,www.google-analytics.com,www.gstatic.com
Unknown
maxcdn.bootstrapcdn.com,checkout.stripe.com,c.shpg.org

EXAMPLE #2


Trainline
Trainline.com Limited (GB)
https://www.trainline.eu/order/3e5r
trainline
PURCHASE no. 3E5[redacted]
booked by
on
Konark Kumar Modi
07/0[redacted]
HELP
Your tickets have been sent to modi.konark@gmail.com
Wrong email address? Edit
FRIDAY
3 AUG
09:47 München Hbf
15:56 [redacted]
€111.80
09:47 München Hbf (Munich, Main Station)
13:40 Frankfurt (Main) Hbf (Main Station)
DB
EC 390
1st
Aisle
Carriage 12, seats 51, 52
Konark Kumar Modi
P[redacted]
Refund and exchange:
Sparpreis
1h09 transfer time
14:49 Frankfurt (Main) Hbf (Main Station)
15:56 Marburg (Lahn)
DB
RE 4160
1st
No assigned seat
Ticket reference: [redacted]
Invoice
Proof of payment
Purchased on 07 July 2018
SUNDAY
5 AUG
13:58 [redacted]
18:56 München Hbf
€171.80
13:58 Marburg (Lahn)
15:11 Kassel-Wilhelmshöhe
DB
RE 4158
1st
No assigned seat
Konark Kumar Modi
Pallavi Modi
Refund and exchange:
Sparpreis
13 min transfer time

IDENTIFYING LEAKS





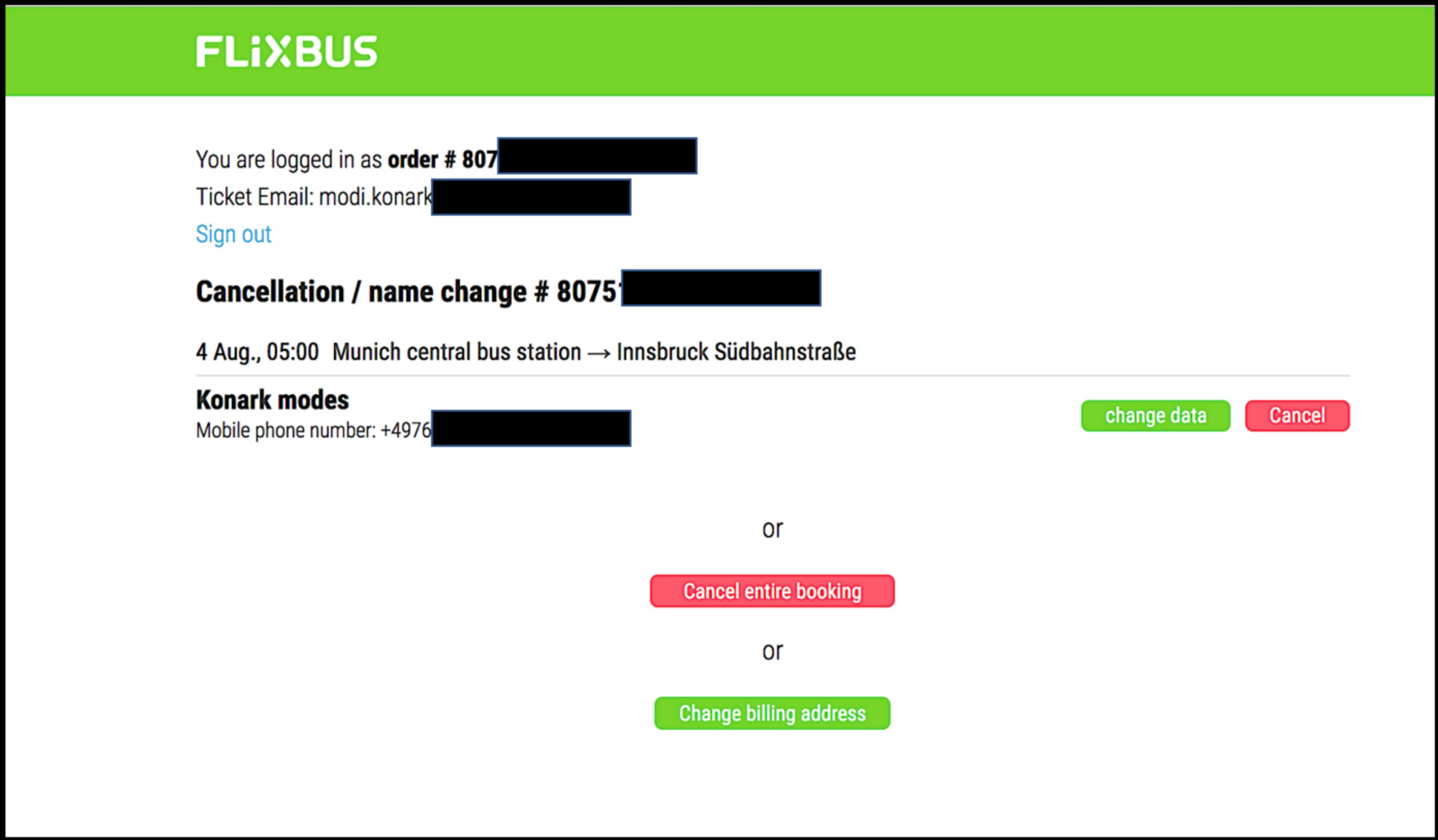
trainline.eu/order/3e5

trainline.eu/order/3e5

has been leaked to **17 third-party domains** , owned by **5 different companies** courtesy **1 website.**

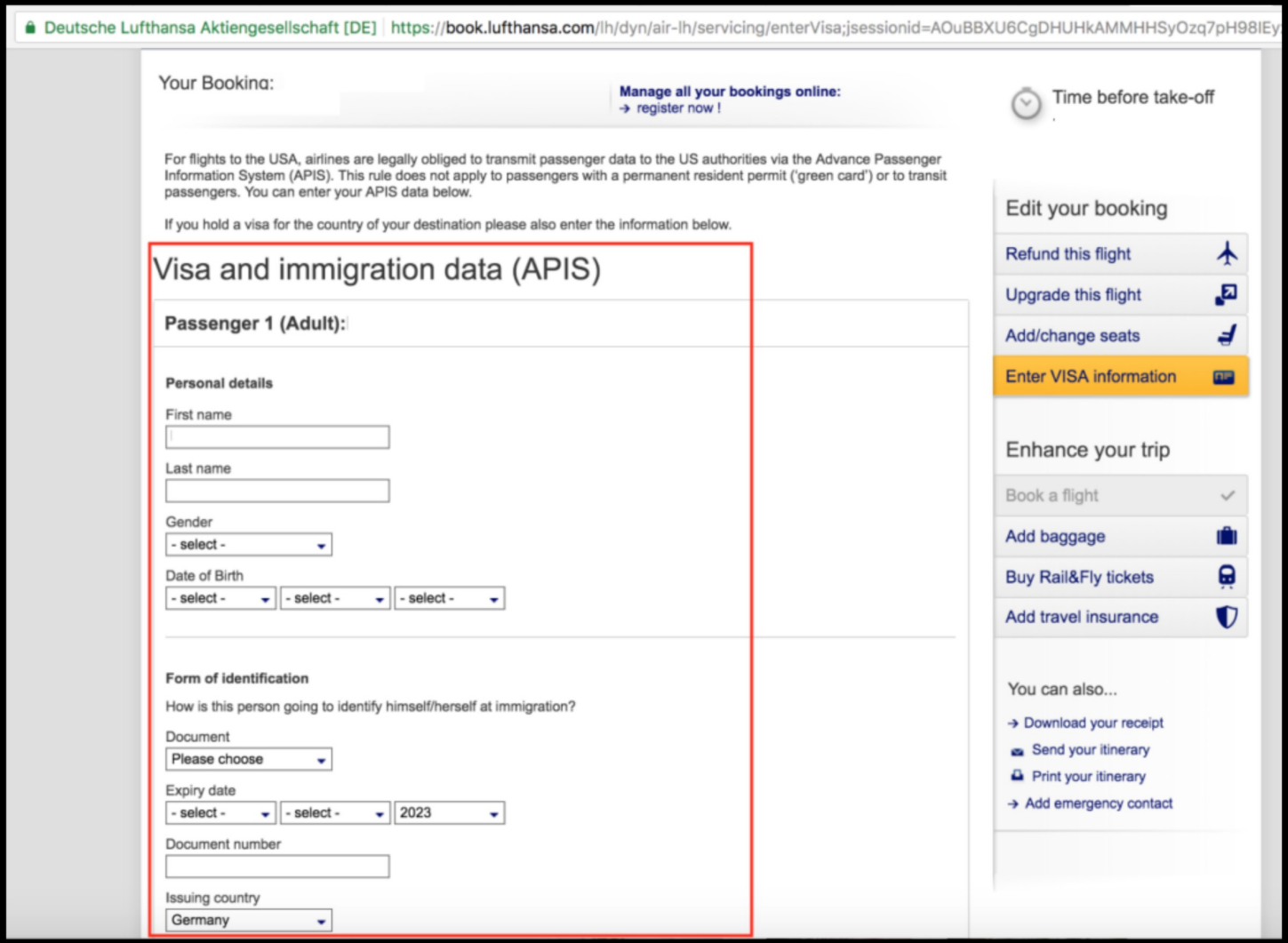
Company	Website
Facebook	www.trainline.eu
Google	www.trainline.eu
Microsoft	www.trainline.eu
ThreatMetrix	www.trainline.eu
New Relic	www.trainline.eu

EXAMPLE #3

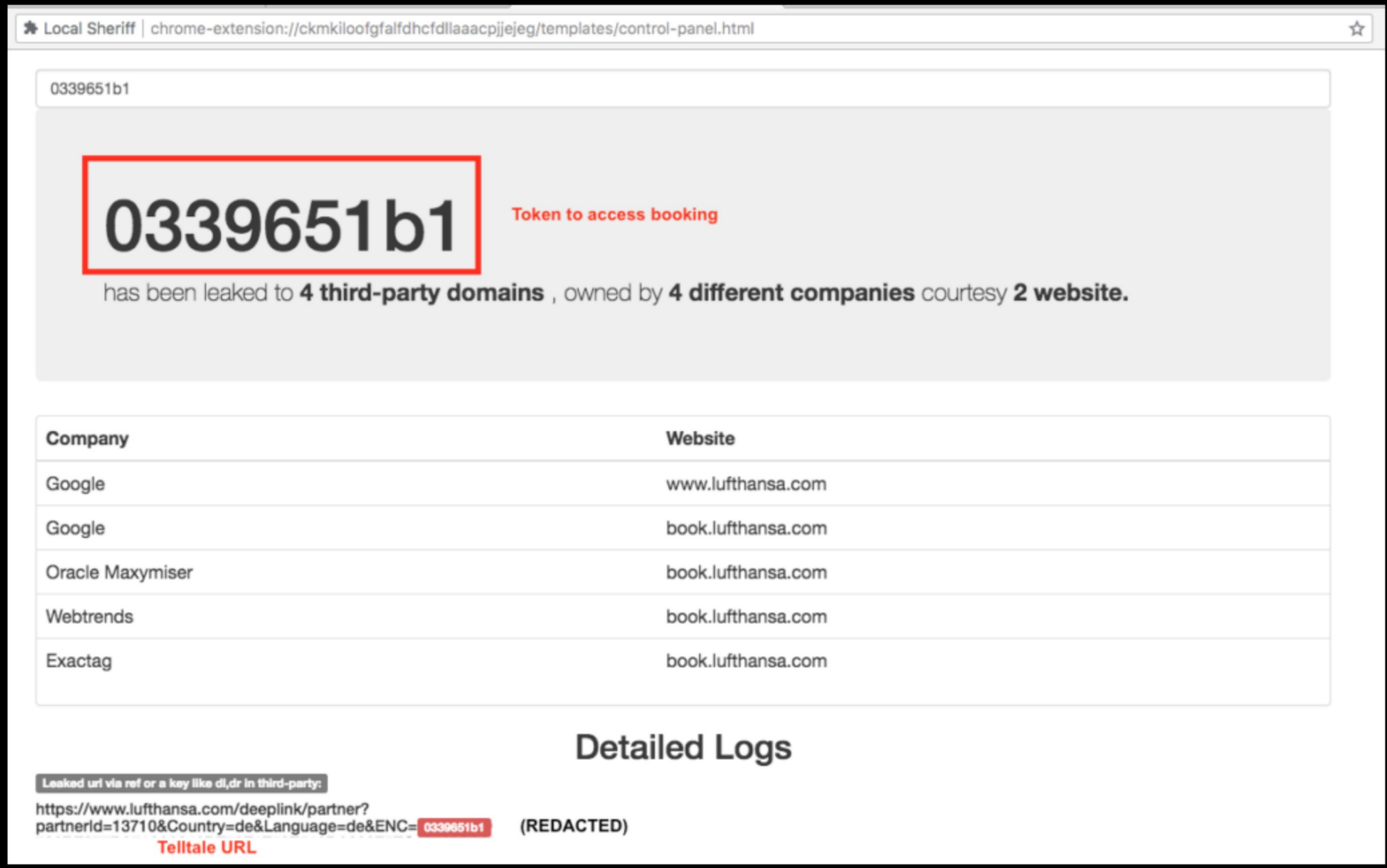

FLiXBUS
You are logged in as order # 807
Ticket Email: modi.konark
Sign out
Cancellation / name change # 8075
4 Aug., 05:00 Munich central bus station → Innsbruck Südbahnstraße
Konark modes
Mobile phone number: +4976
change data
Cancel
or
Cancel entire booking
or
Change billing address

IDENTIFYING LEAKS

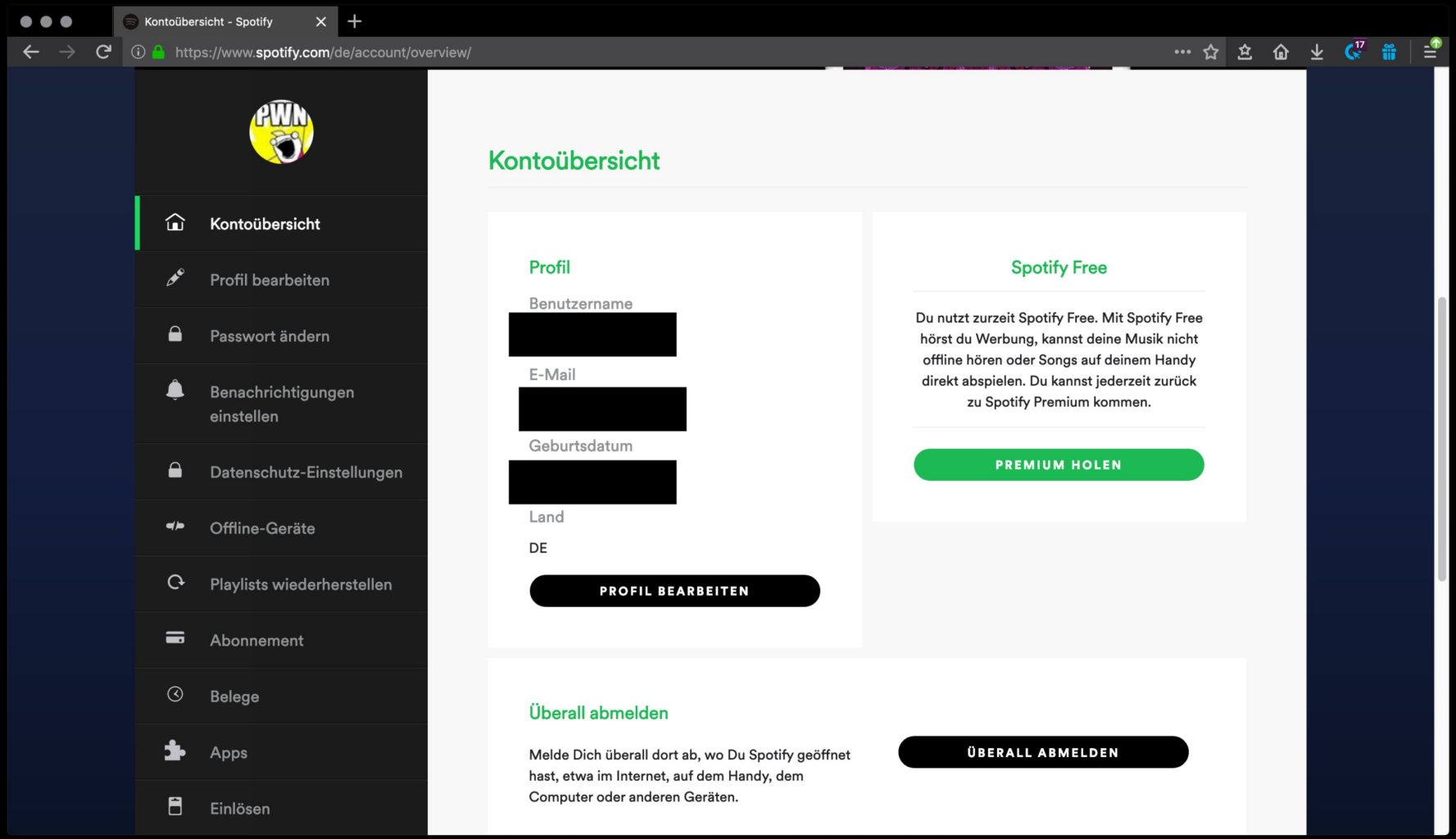
EXAMPLE #4


Deutsche Lufthansa Aktiengesellschaft [DE] https://book.lufthansa.com/lh/dyn/air-lh/servicing/enterVisa;jsessionid=AOuBBXU6CgDHUHkAMMHHSyOzq7pH98IEy
Your Booking:
Manage all your bookings online:
→ register now !
Time before take-off
For flights to the USA, airlines are legally obliged to transmit passenger data to the US authorities via the Advance Passenger Information System (APIS). This rule does not apply to passengers with a permanent resident permit ('green card') or to transit passengers. You can enter your APIS data below.
If you hold a visa for the country of your destination please also enter the information below.
Visa and immigration data (APIS)
Passenger 1 (Adult):
Personal details
First name
Last name
Gender
- select -
Date of Birth
- select - - select - - select -
Form of identification
How is this person going to identify himself/herself at immigration?
Document
Please choose
Expiry date
- select - - select - 2023
Document number
Issuing country
Germany
Edit your booking
Refund this flight
Upgrade this flight
Add/change seats
Enter VISA information
Enhance your trip
Book a flight
Add baggage
Buy Rail&Fly tickets
Add travel insurance
You can also...
→ Download your receipt
Send your itinerary
Print your itinerary
→ Add emergency contact

IDENTIFYING LEAKS



EXAMPLE #5

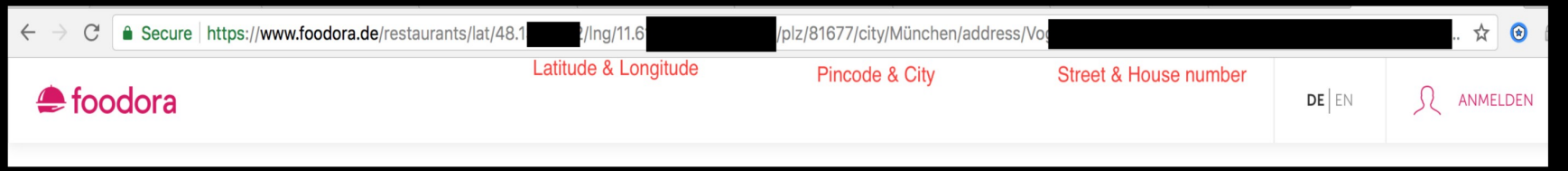

Kontoübersicht - Spotify
https://www.spotify.com/de/account/overview/
Kontoübersicht
Profil bearbeiten
Passwort ändern
Benachrichtigungen einstellen
Datenschutz-Einstellungen
Offline-Geräte
Playlists wiederherstellen
Abonnement
Belege
Apps
Einlösen
Kontoübersicht
Profil
Benutzername
E-Mail
Geburtsdatum
Land
DE
PROFIL BEARBEITEN
Spotify Free
Du nutzt zurzeit Spotify Free. Mit Spotify Free hörst du Werbung, kannst deine Musik nicht offline hören oder Songs auf deinem Handy direkt abspielen. Du kannst jederzeit zurück zu Spotify Premium kommen.
PREMIUM HOLEN
Überall abmelden
Melde Dich überall dort ab, wo Du Spotify geöffnet hast, etwa im Internet, auf dem Handy, dem Computer oder anderen Geräten.
ÜBERALL ABMELDEN

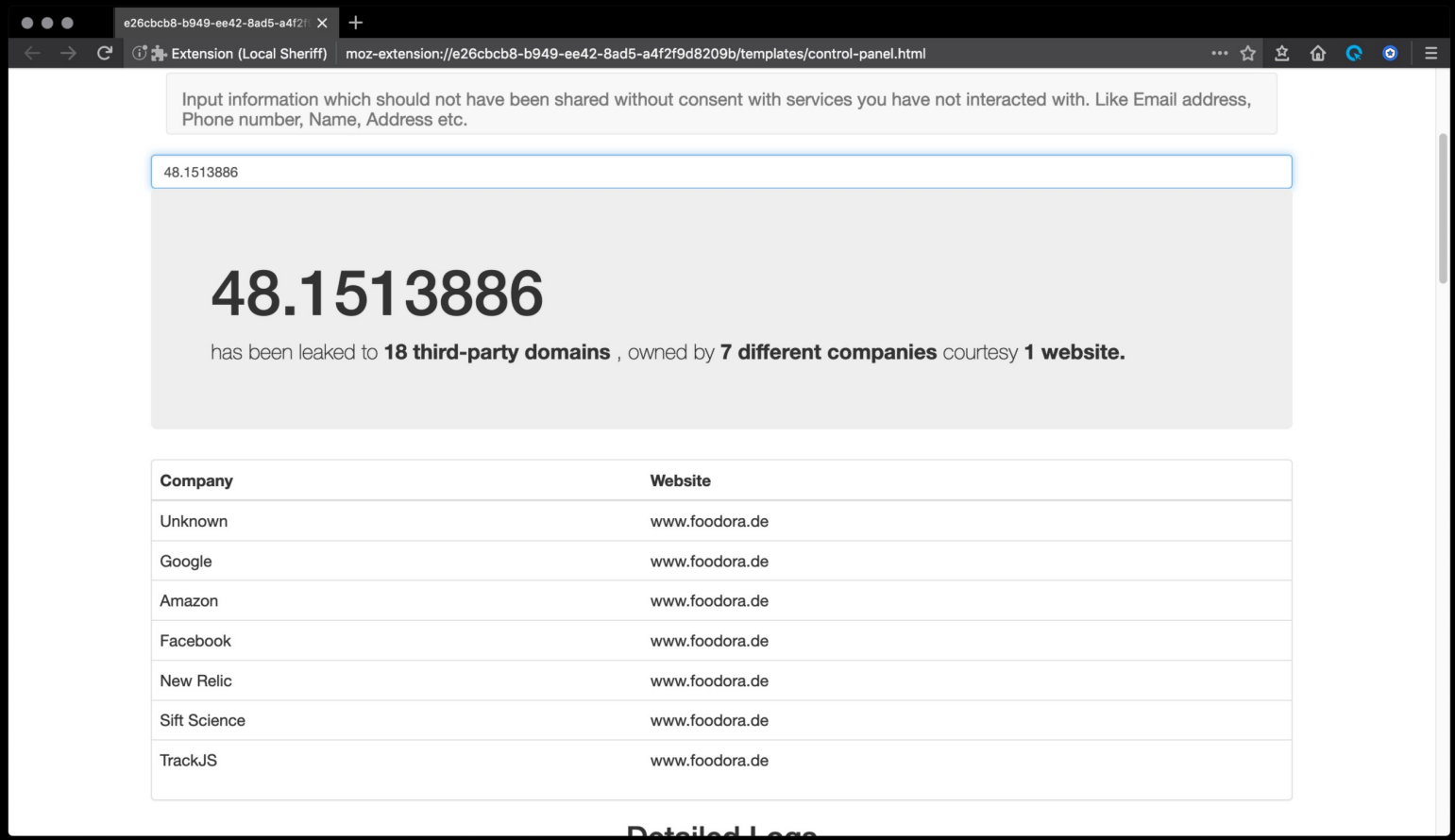
IDENTIFYING LEAKS

```
2018-03-18 03:27:23 GET https://sb.scorecardresearch.com/b?c1=2&c2=15654041&ns__t=1521340042970&ns_c=UTF-8&c8=Konto%C3%BCbersicht%20-%20Spoti
                        fy&c7=https%3A%2F%2Fwww.spotify.com%2Fde%2Faccount%2Foverview%2F%3Futm_source%3Dspotify%26utm_medium%3Dmenu%26utm_cam

                        ← 204 No Content [no content] 2.25s
                          Request                      Response                      Detail
Host:              sb.scorecardresearch.com
Connection:        keep-alive
User-Agent:        Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.146 Safari/537.36
                   OPR/52.0.2871.20 (Edition beta)
Accept:            image/webp,image/apng,image/*,*/*;q=0.8
Referer:           https://www.spotify.com/de/account/overview/?utm
                   =NAphCkkKDVNwb3RpZnktdXNlcnMSCmtvbmFyazMwMDMaA5g
                   UL4shIvIrpBMcA
Accept-Encoding:   gzip, deflate, br
Accept-Language:   en-GB,en-US;q=0.9,en;q=0.8
Cookie:            UID=17523a194187173be228dcg1521336255; UIDR=1521336255
Query                                                                                                                          [m:auto]
c1:    2
c2:    15654041
ns__t: 1521340042970
ns_c:  UTF-8
c8:    Kontoübersicht - Spotify
c7:    https://www.spotify.com/de/account/overview/?utm_source=sp
b3RpZnktdXNlcnMSCmtvbmFyazMwMDMaA5gBASUnxq1aMiIKCFqOQbXqyPevEhbhV
```

IDENTIFYING LEAKS






OH THE HORROR

RISKS OF TELLTALE URLS #1

Websites are carelessly leaking sensitive PII information to plethora of third-parties

RISKS OF TELLTALE URLS #2

- Websites are carelessly leaking sensitive PII information to plethora of third-parties
- Most often without users‘ consent

RISKS OF TELLTALE URLS #3

- Websites are carelessly leaking sensitive PII information to plethora of third-parties
- Most often without users‘ consent.

More dangerously: Without the websites realizing themselves.

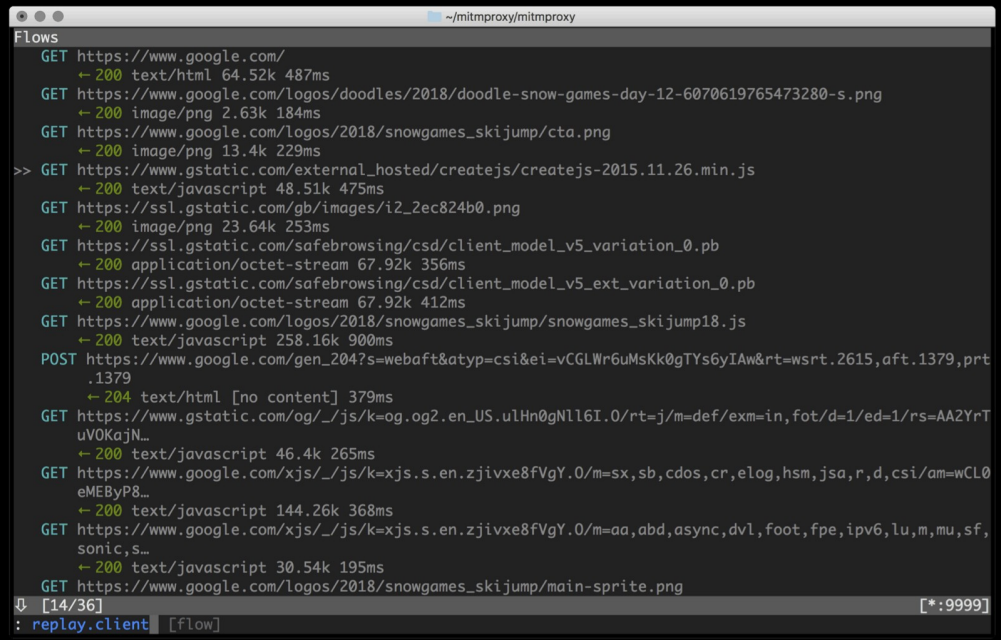
Protecting your details and protecting yourself against internet fraud

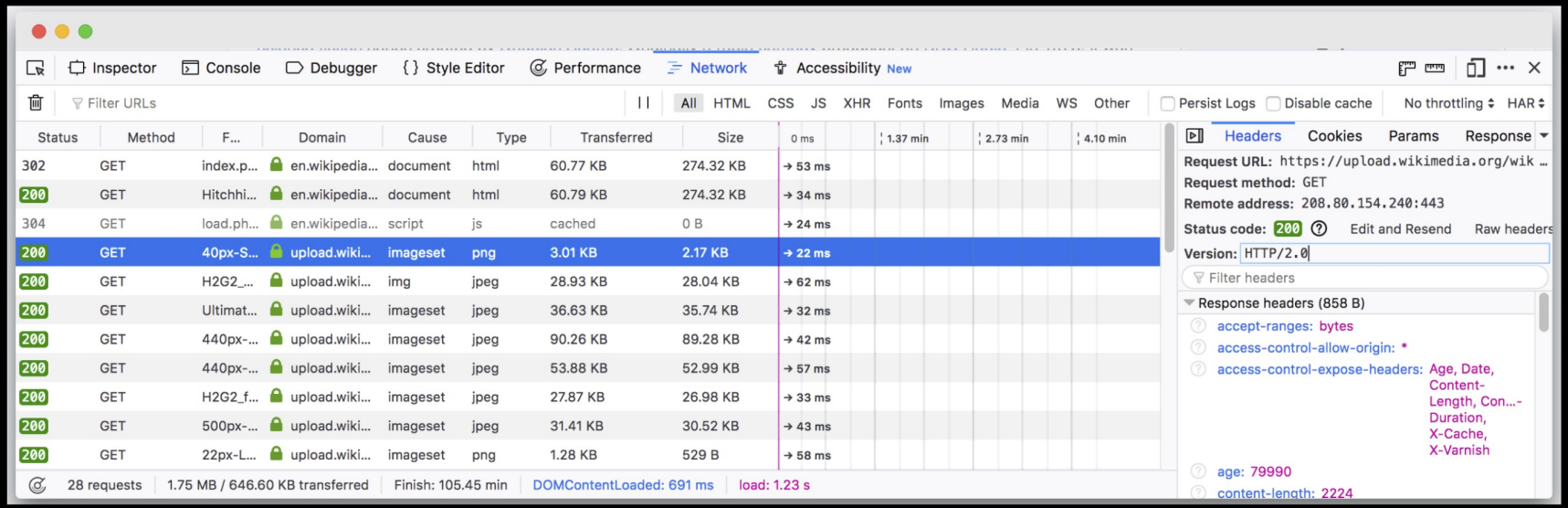
Here are some simple steps you can take to ensure your information is kept securely:

- Keep your booking reference confidential - upon making a booking a unique booking reference (also known as a PNR or Passenger Name Record) will appear on the email confirmation or ticket of each person in your booking. It is important that you keep your booking reference confidential at all times. Other persons may be able to access your booking details through our system if you disclose your booking reference to them.

	Third-party	Leaking via header	Leaking via Query Parameters
2	**boxever.com**	Referer	
3	**googletagmanager.com**	Referer	
4	**facebook.com**	Referer	DL
5	**facebook.net**	Referer	
6	**google-analytics.com**	Referer	DL, DR
7	**coremetrics**	Referer	UL, RF
8	**ads-twitter.com**	Referer	
9	**qubitproducts**	Referer	
10	**crazyegg.com**	Referer	
11	**ek.aero**	Referer	
12	**cloudfront**	Referer	

MISSING PIECE





EMPOWERING USERS'

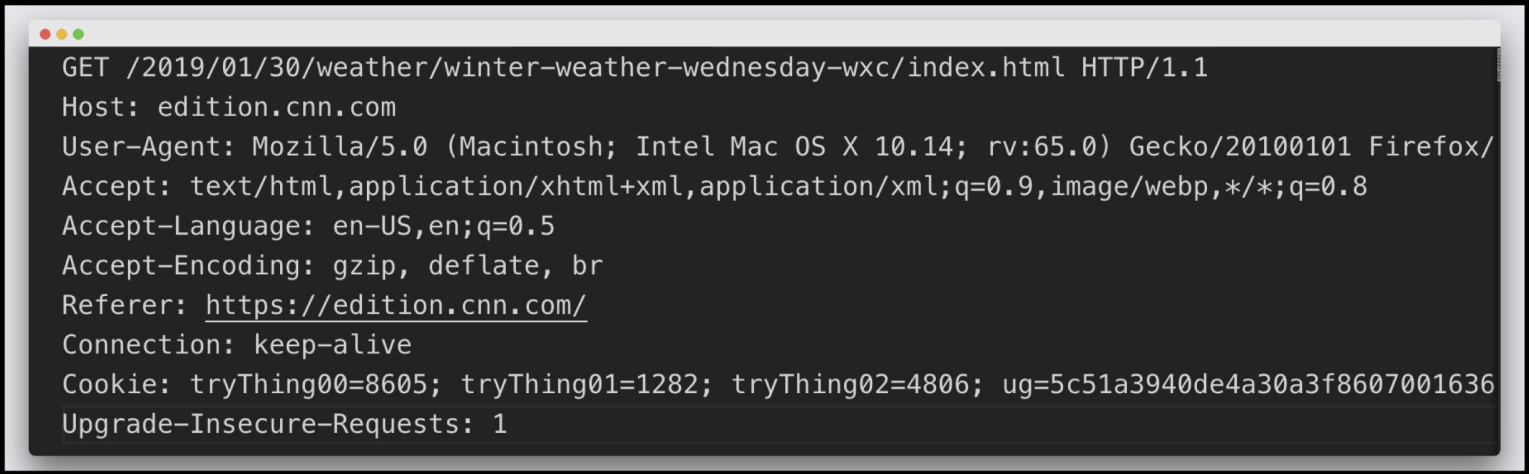
1. Easy to Install

2. Monitor & Store all data being exchanged while a user surfs the web.

3. Easy to identify which companies are behind tracking

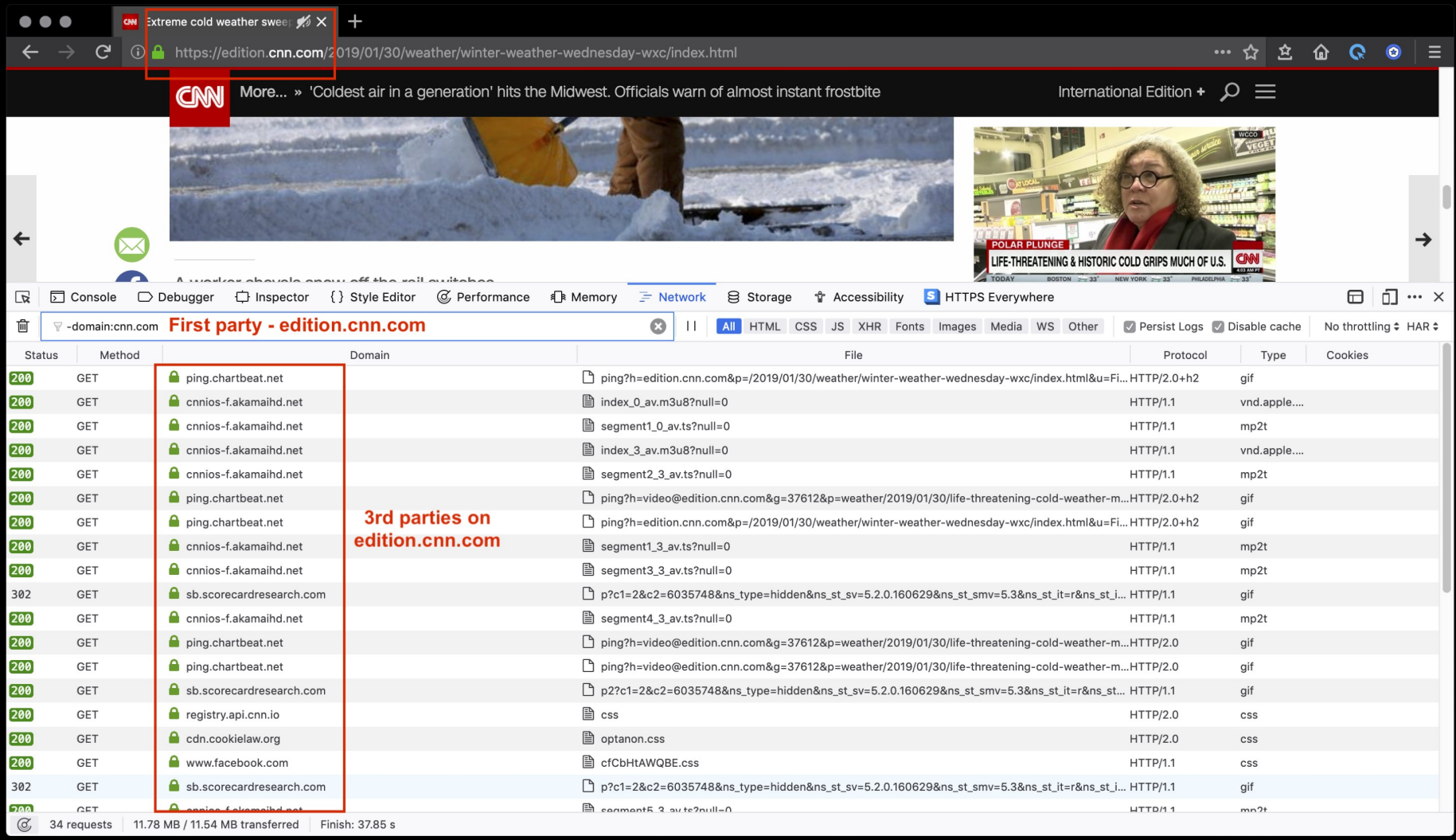
4. Search interface to find leaks

LOCAL SHERIFF



1. **Monitor all Webrequest that take place in the browser**
   https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/API/webRequest

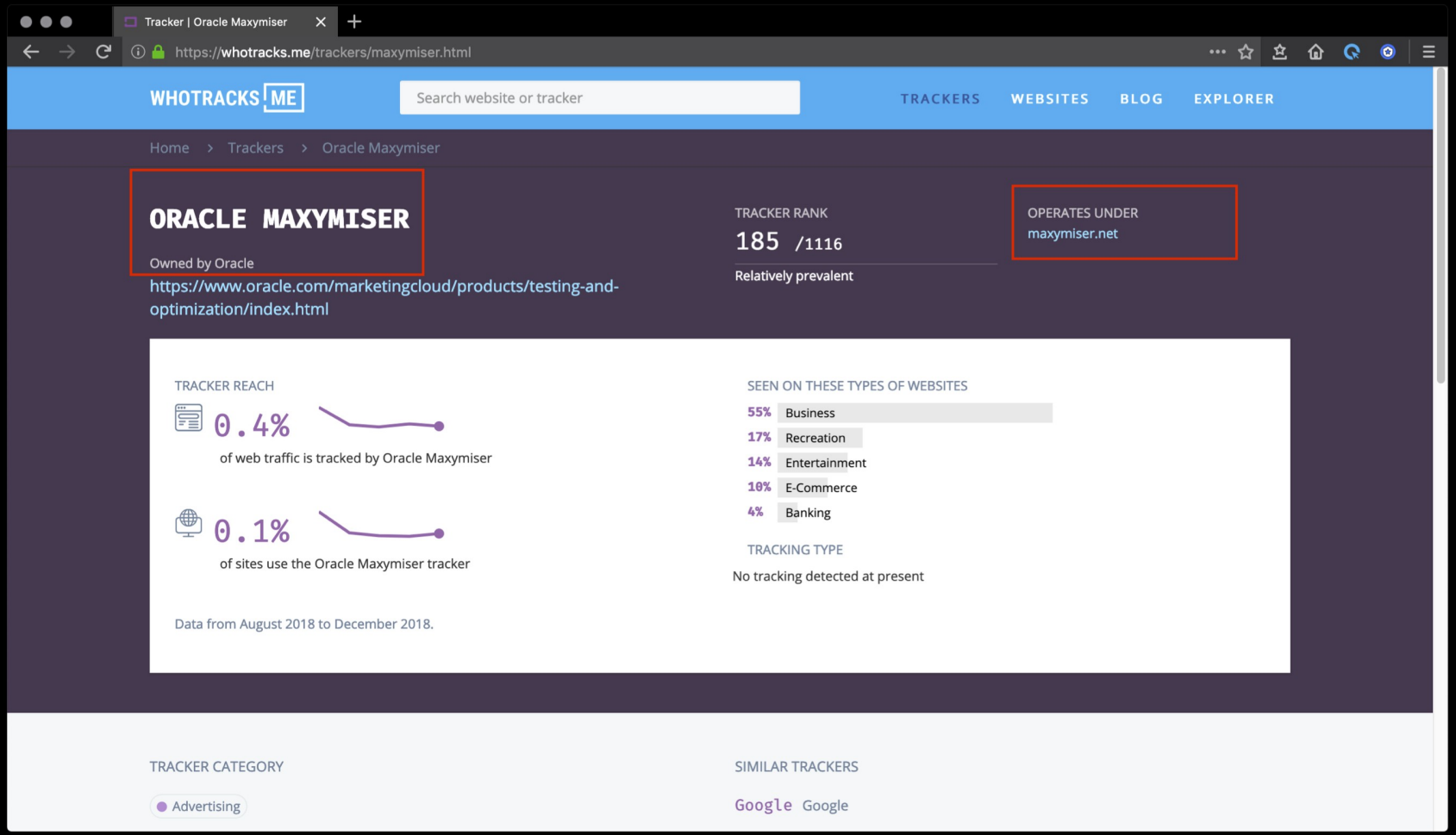
LOCAL SHERIFF



Status	Method	Domain	File	Protocol	Type	Cookies
200	GET	ping.chartbeat.net	ping?h=edition.cnn.com&p=/2019/01/30/weather/winter-weather-wednesday-wxc/index.html&u=Fi...	HTTP/2.0+h2	gif	
200	GET	cnnios-f.akamaihd.net	index_0_av.m3u8?null=0	HTTP/1.1	vnd.apple....	
200	GET	cnnios-f.akamaihd.net	segment1_0_av.ts?null=0	HTTP/1.1	mp2t	
200	GET	cnnios-f.akamaihd.net	index_3_av.m3u8?null=0	HTTP/1.1	vnd.apple....	
200	GET	cnnios-f.akamaihd.net	segment2_3_av.ts?null=0	HTTP/1.1	mp2t	
200	GET	ping.chartbeat.net	ping?h=video@edition.cnn.com&g=37612&p=weather/2019/01/30/life-threatening-cold-weather-m...	HTTP/2.0+h2	gif	
200	GET	ping.chartbeat.net	ping?h=edition.cnn.com&p=/2019/01/30/weather/winter-weather-wednesday-wxc/index.html&u=Fi...	HTTP/2.0+h2	gif	
200	GET	cnnios-f.akamaihd.net	segment1_3_av.ts?null=0	HTTP/1.1	mp2t	
200	GET	cnnios-f.akamaihd.net	segment3_3_av.ts?null=0	HTTP/1.1	mp2t	
302	GET	sb.scorecardresearch.com	p?c1=2&c2=6035748&ns_type=hidden&ns_st_sv=5.2.0.160629&ns_st_smv=5.3&ns_st_it=r&ns_st_i...	HTTP/1.1	gif	
200	GET	cnnios-f.akamaihd.net	segment4_3_av.ts?null=0	HTTP/1.1	mp2t	
200	GET	ping.chartbeat.net	ping?h=video@edition.cnn.com&g=37612&p=weather/2019/01/30/life-threatening-cold-weather-m...	HTTP/2.0	gif	
200	GET	ping.chartbeat.net	ping?h=video@edition.cnn.com&g=37612&p=weather/2019/01/30/life-threatening-cold-weather-m...	HTTP/2.0	gif	
200	GET	sb.scorecardresearch.com	p2?c1=2&c2=6035748&ns_type=hidden&ns_st_sv=5.2.0.160629&ns_st_smv=5.3&ns_st_it=r&ns_st...	HTTP/1.1	gif	
200	GET	registry.api.cnn.io	css	HTTP/2.0	css	
200	GET	cdn.cookielaw.org	optanon.css	HTTP/2.0	css	
200	GET	www.facebook.com	cfCbHtAWQBE.css	HTTP/1.1	css	
302	GET	sb.scorecardresearch.com	p?c1=2&c2=6035748&ns_type=hidden&ns_st_sv=5.2.0.160629&ns_st_smv=5.3&ns_st_it=r&ns_st_i...	HTTP/1.1	gif	

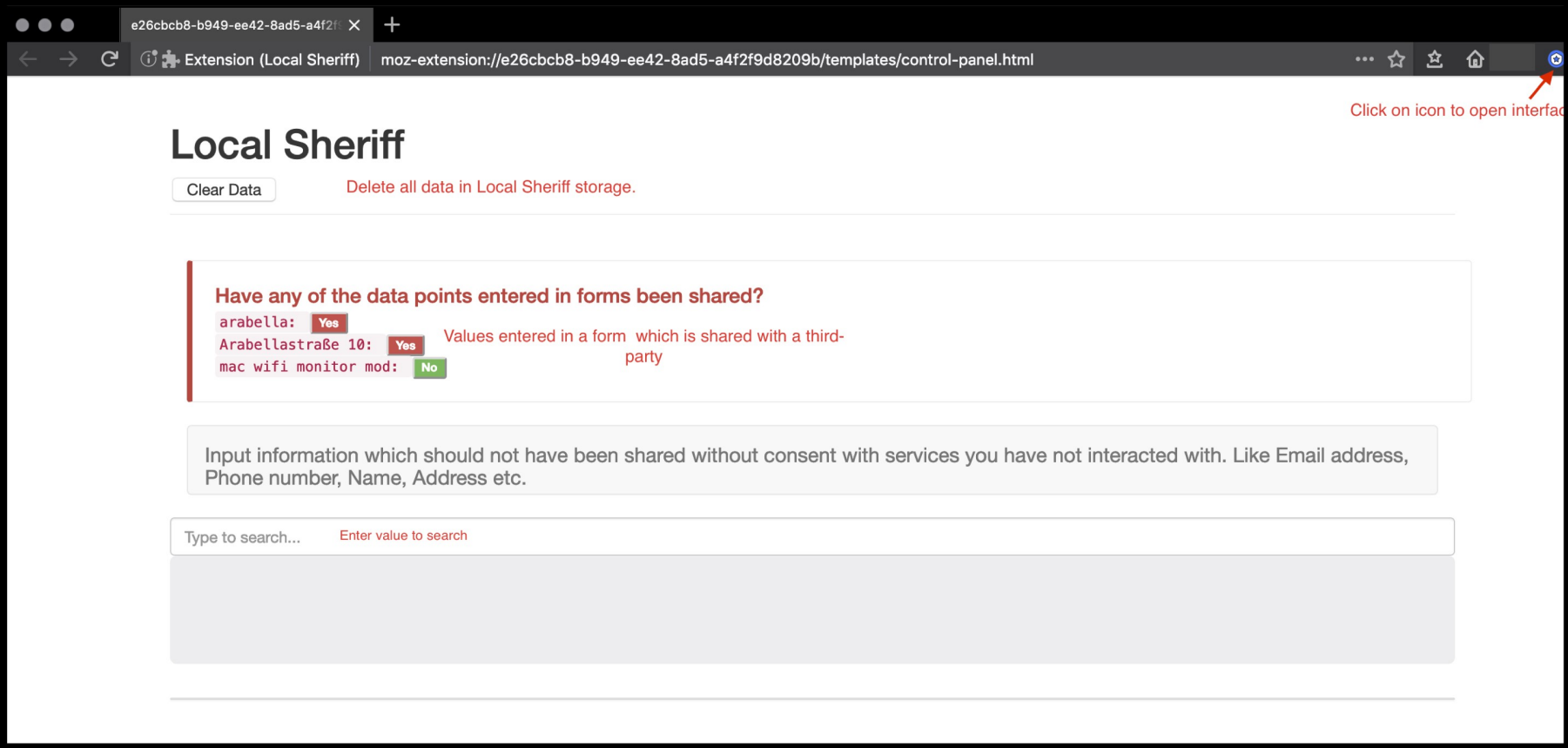
2. Classify as first party vs third-party

LOCAL SHERIFF



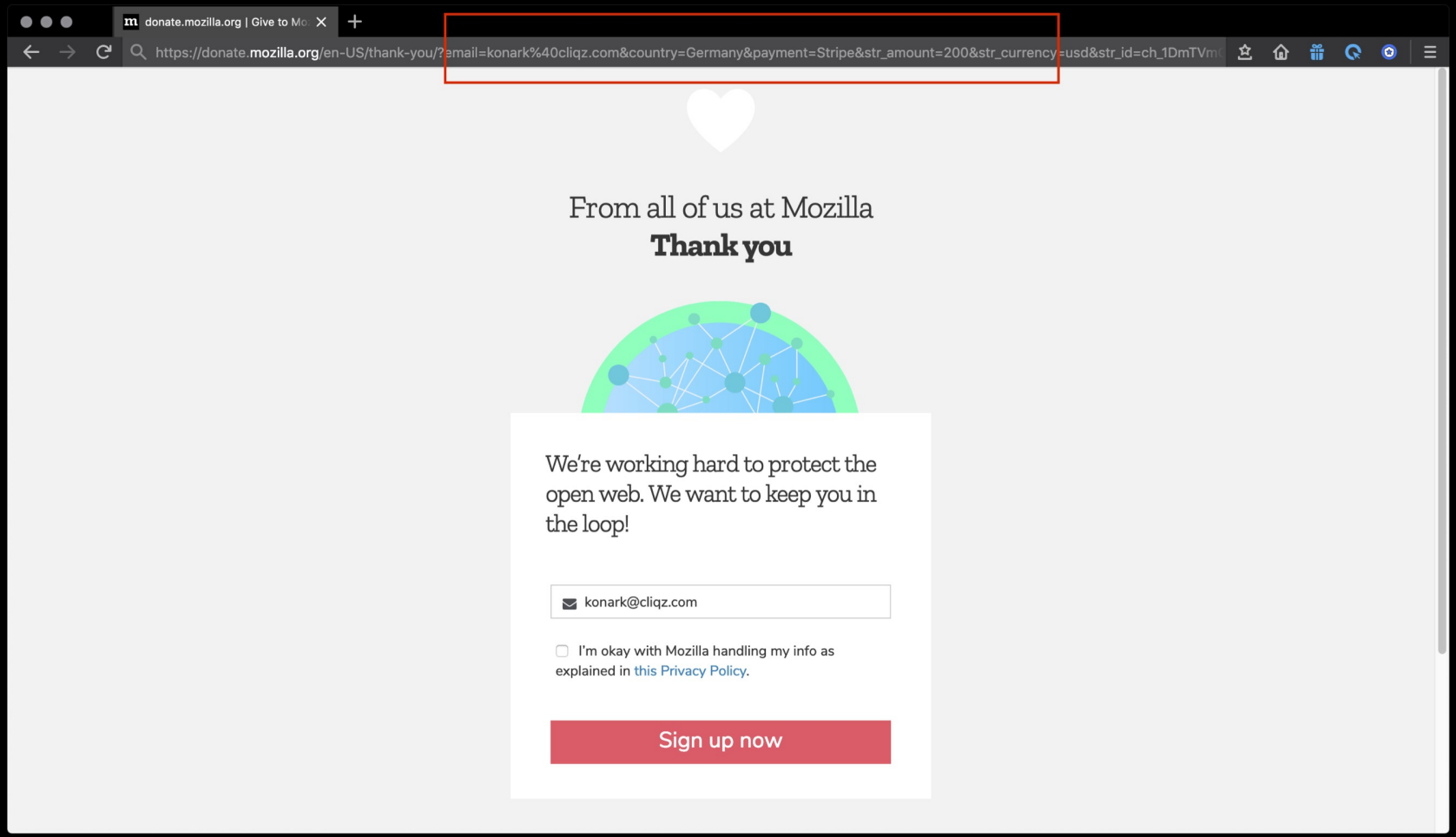
3. Locally shipped copy of hostnames to Companies
Source: https://whotracks.me
https://github.com/cliqz-oss/whotracks.me

LOCAL SHERIFF

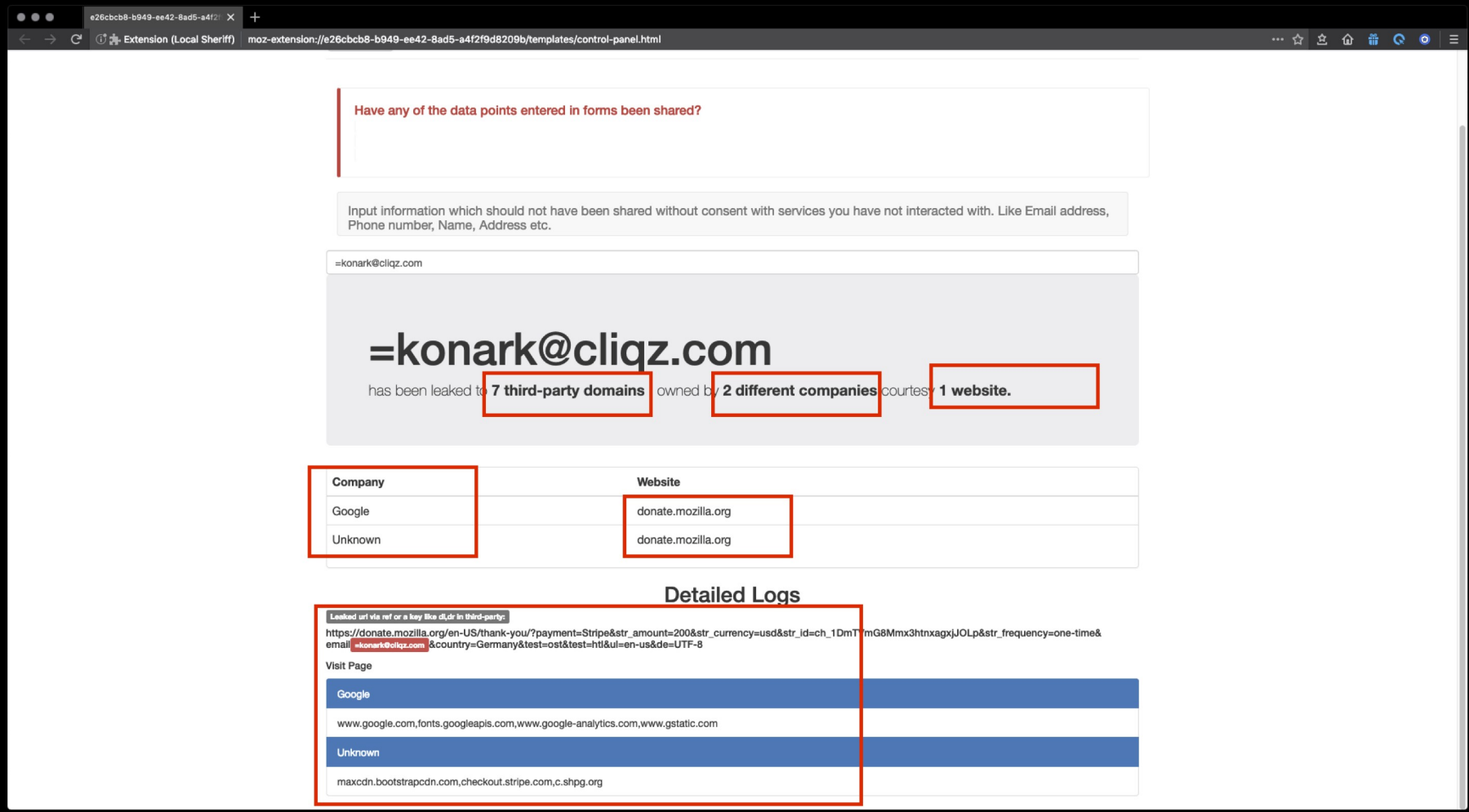


4. Search interface

LOCAL SHERIFF



LOCAL SHERIFF



LOCAL SHERIFF

facebook.com/tr

has been leaked to **1 third-party domains** , owned by **1 different companies** courtesy **4 website.**

Company	Website
Facebook	www.lieferando.de
Facebook	www.nytimes.com
Facebook	www.thetrainline.com
Facebook	www.trainline.eu

Also found `fr=0Sh6fFpK7USdFh0w3.` **in third-party urls courtesy shop.flixbus.de:**

https://www.facebook.com/tr/?id=803825069649082&ev=PixelInitialized&dl=https://shop.flixbus.de/search?departureCity=94&arrivalCity=1001&route=München-Innsbruck&rideDate=04.08.2018&adult=1&_locale=de&wt_eid=215272714130067272 2&wt_t=1531949797662&affiliate=(not+set),&_ga=2.144760631.221776319.1531949772-96041186.1527271413&rl=https://www.flixbus.de/&if=false&ts=1531949799661

`Cookie` `fr=0Sh6fFpK7USdFh0w3.`.Ba5J4E..Fsl.1.0.BbT7LM.

LOCAL SHERIFF

fr=0Sh6fFpK7USdFh0w3.

has been leaked to **2 third-party domains** , owned by **1 different companies** courtesy **11 website.**

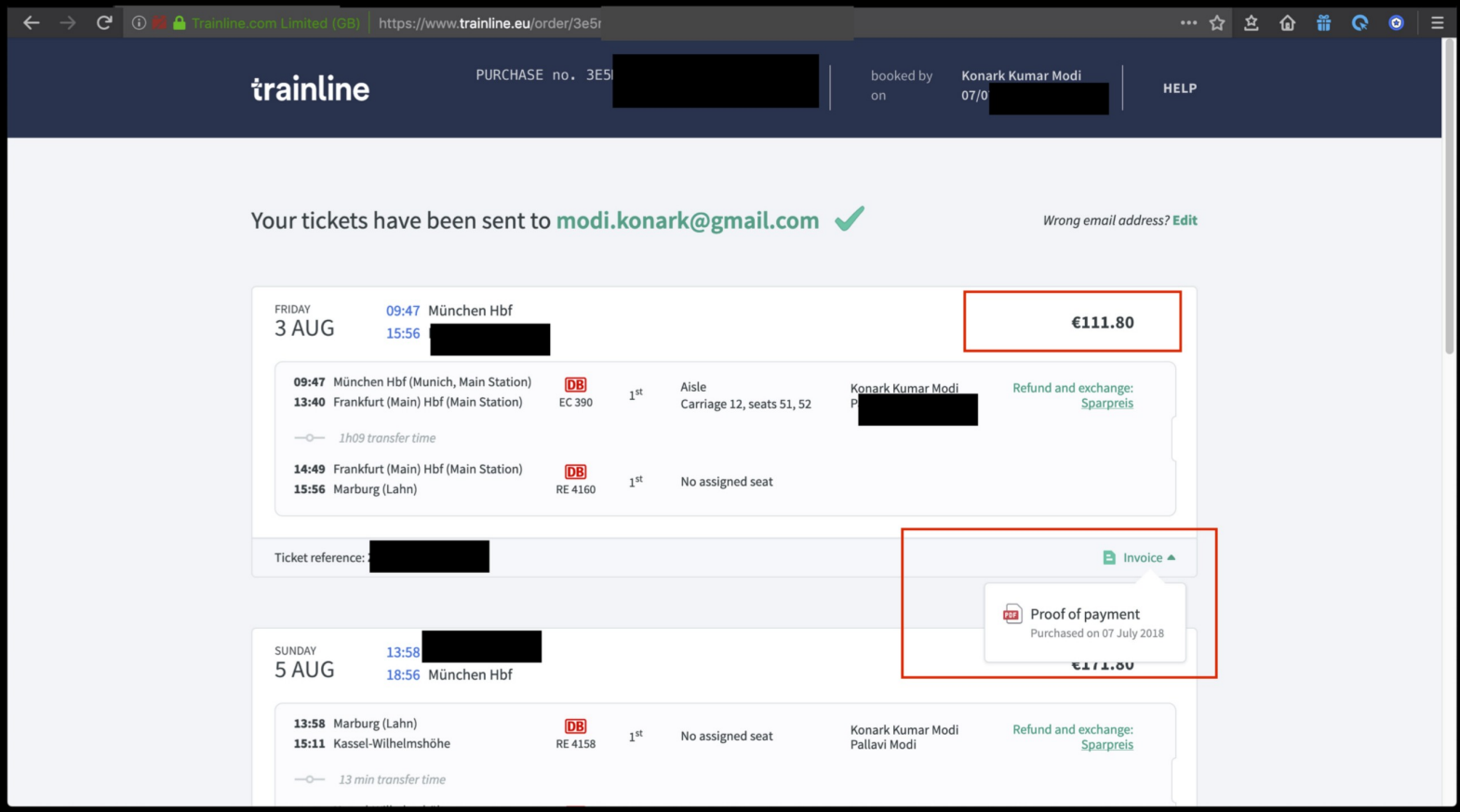
Company	Website
Facebook	www.flixbus.de
Facebook	shop.flixbus.de
Facebook	www.bild.de
Facebook	www.trainline.eu
Facebook	www.cleartrip.com
Facebook	www.foodora.com
Facebook	www.foodora.de
Facebook	edition.cnn.com
Facebook	www.nytimes.com
Facebook	www.c-and-a.com
Facebook	www.macworld.com

LOCAL SHERIFF

Also found `fr=0Sh6fFpK7USdFh0w3.` in third-party urls courtesy www.trainline.eu:

https://www.facebook.com/tr/?id=1674453146124987&ev=PageView&dl=https://www.trainline.eu/order/4a83[redacted]se&ts=1532015667057&sw=1440&sh=900&v=2.8.21&r=stable&ec=0&o=28&it=1532015666967

Cookie `fr=0Sh6fFpK7USdFh0w3.`.Ba5J4E..Fsl.1.0.BbT7LM.

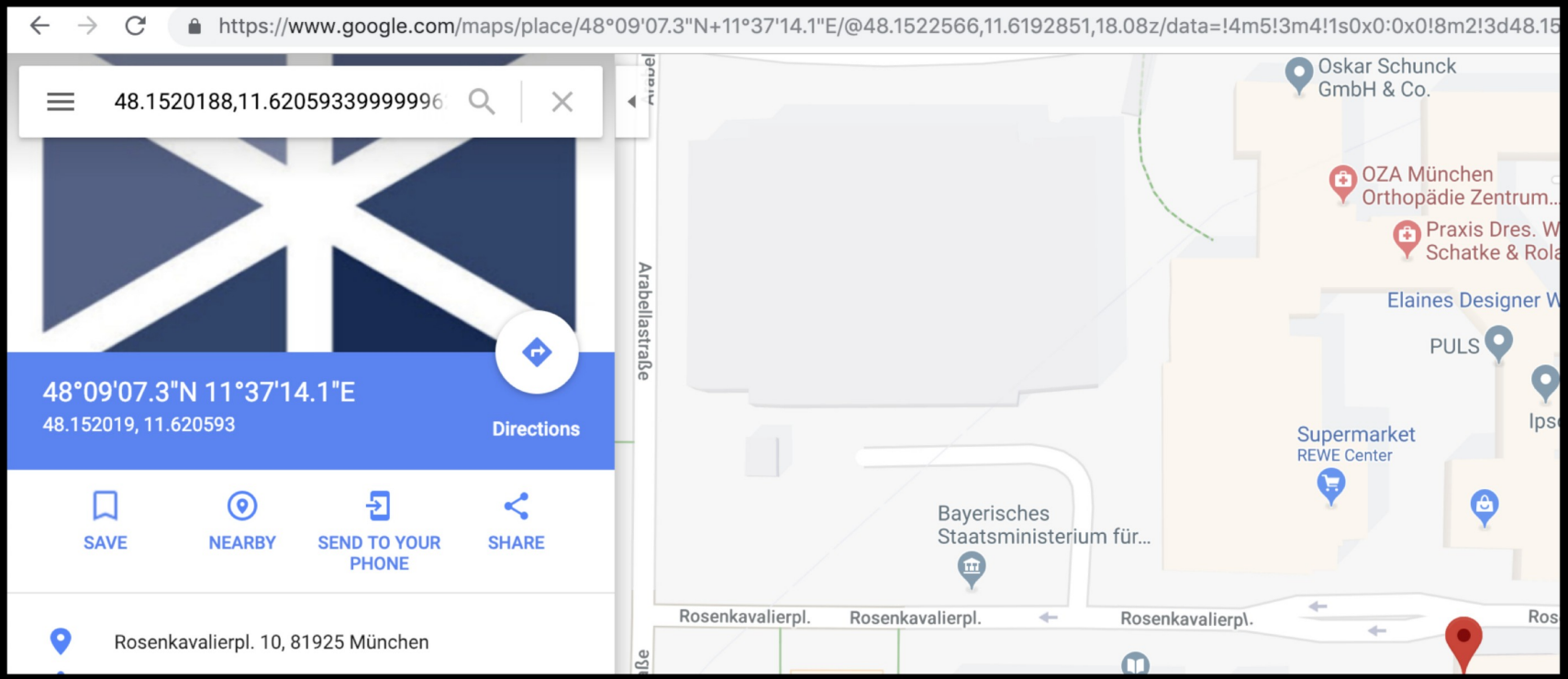


LOCAL SHERIFF

Also found `fr=0Sh6fFpK7USdFh0w3.` in third-party urls courtesy www.foodora.de:

https://www.facebook.com/tr/?id=1611247079118723&ev=PageView&dl=https://www.foodora.de/restaurants/lat/48.1520188/lng/11.620593399999962/plz/81925/city/München/address/Rosenkavalierpl.%2010%2C%2081925%20M%C3%BCnchen%2C%20Deutschland/Rosenkavalierplatz/10&rl=https://www.foodora.com/&if=false&ts=1536244957700&sw=1280&sh=800&v=2.8.26&r=stable&ec=4&o=28&it=1536244944545

Cookie `fr=0Sh6fFpK7USdFh0w3.`.Ba5J4E..FuR.1.0.BbkTy8.



URL	Cookie
www.bild.d	**fr=**0Sh6fFpK7USdFh0w3.
edition.cnn.com	**fr=**0Sh6fFpK7USdFh0w3.
www.trainline.eu/order/3e5<Redacted>	**fr=**0Sh6fFpK7USdFh0w3.
www.foodora.de/en/restaurants/lat/48.1520188/lng/11.620593399999962/plz/81925/city/München/address/	**fr=**0Sh6fFpK7USdFh0w3.

Analytics Backend

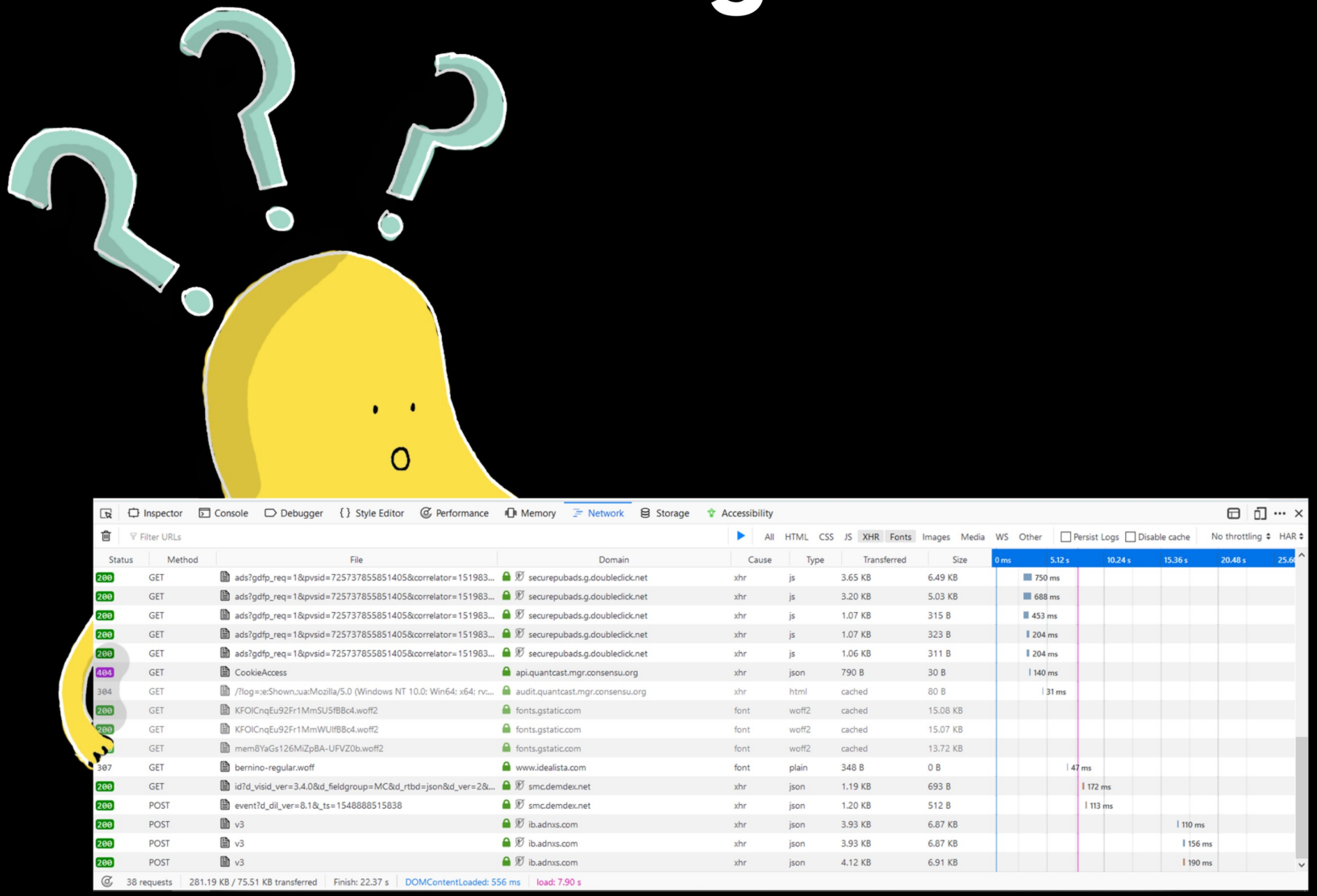
Audit tool

PLATFORMS

https://github.com/cliqz-oss/local-sheriff

https://github.com/cliqz-oss/local-sheriff#app-store-links

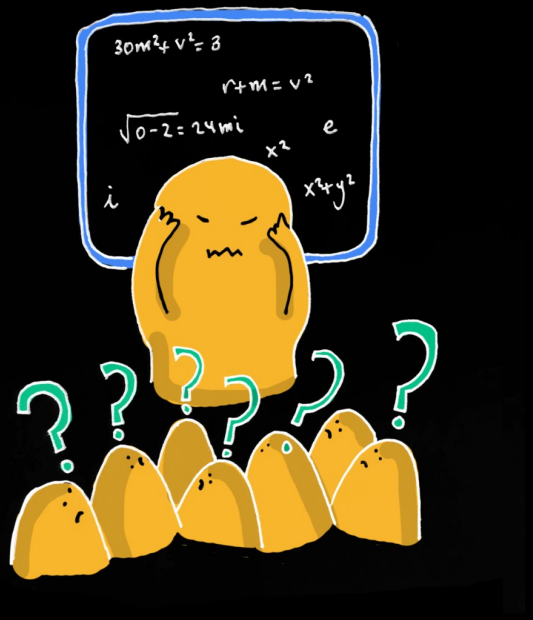
How to explain the problem to an average user?

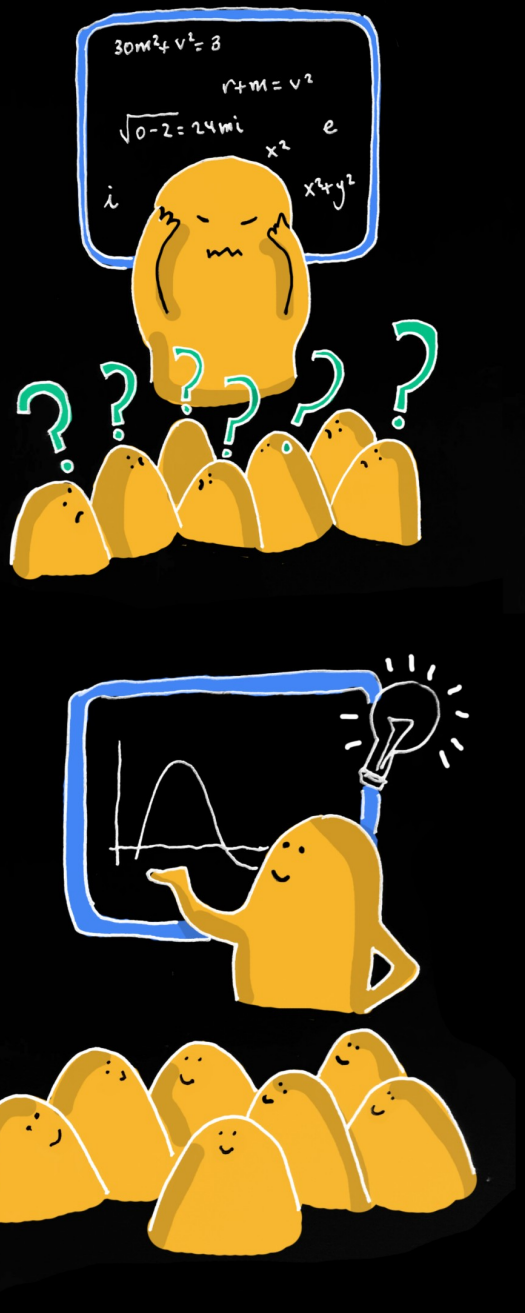


TRACKULA


MEDIALAB PRADO
DataLab
Migraciones
VISUALIZAR'17
15-30 septiembre
porCausa
Investigación y periodismo


VISUALIZARIT
TRACKULA


30m²+v²=3
r+m=v²
√0-2=24mi
e
x²
i
x²+y²


$30m^2 + v^2 = 3$
$r + m = v^2$
$\sqrt{0-2} = 24mi$
x^2
e
i
$x^2 + y^2$

Lightbeam for Firefox

VISUALIZATION

Graph

DATA

Save Data

Reset Data

Give Us Feedback

DATA GATHERED SINCE
SEP 29 2017

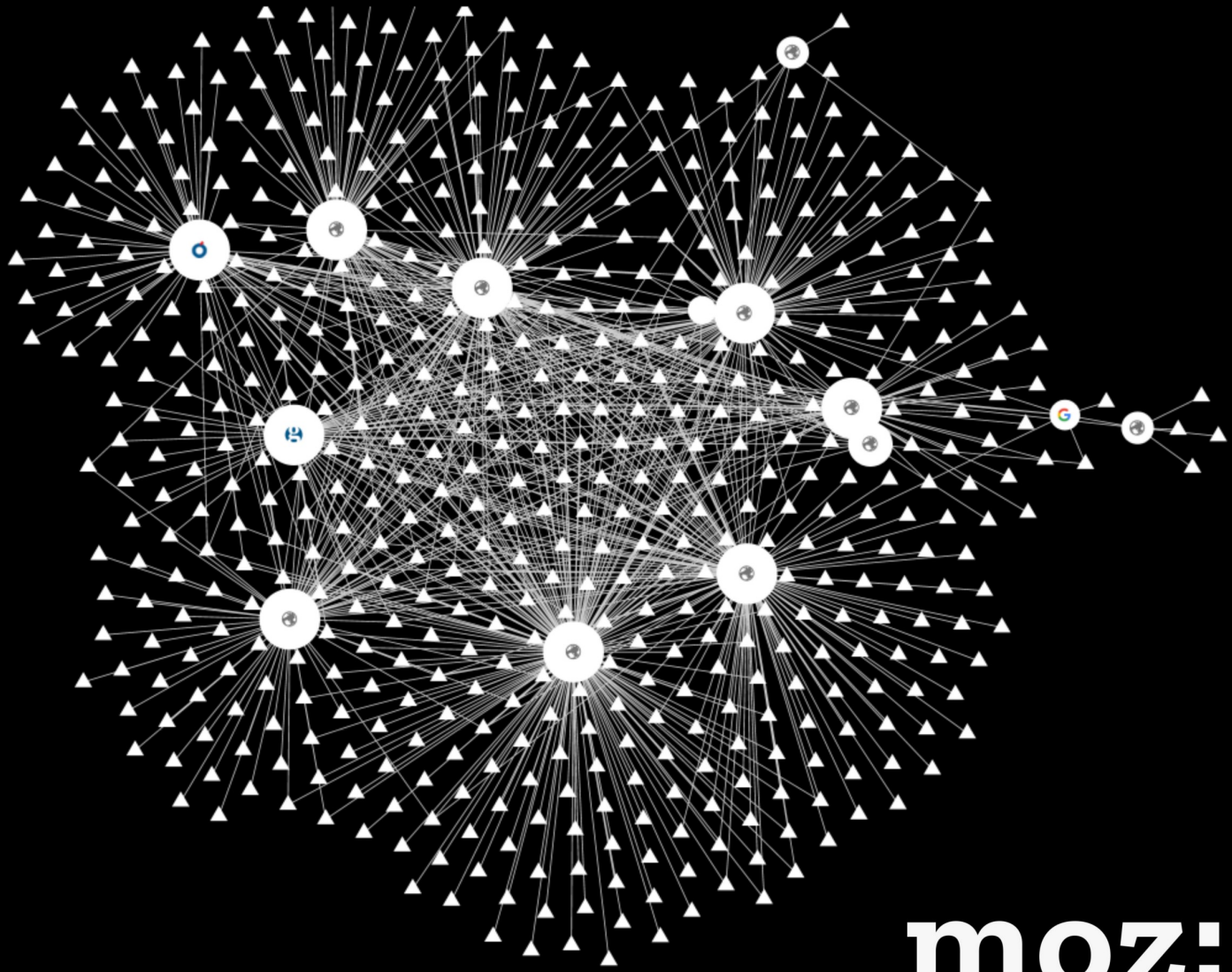
YOU HAVE VISITED
15 SITES

YOU HAVE CONNECTED WITH
545 THIRD PARTY SITES

TRACKING PROTECTION OFF

Recent Site

GRAPH VIEW



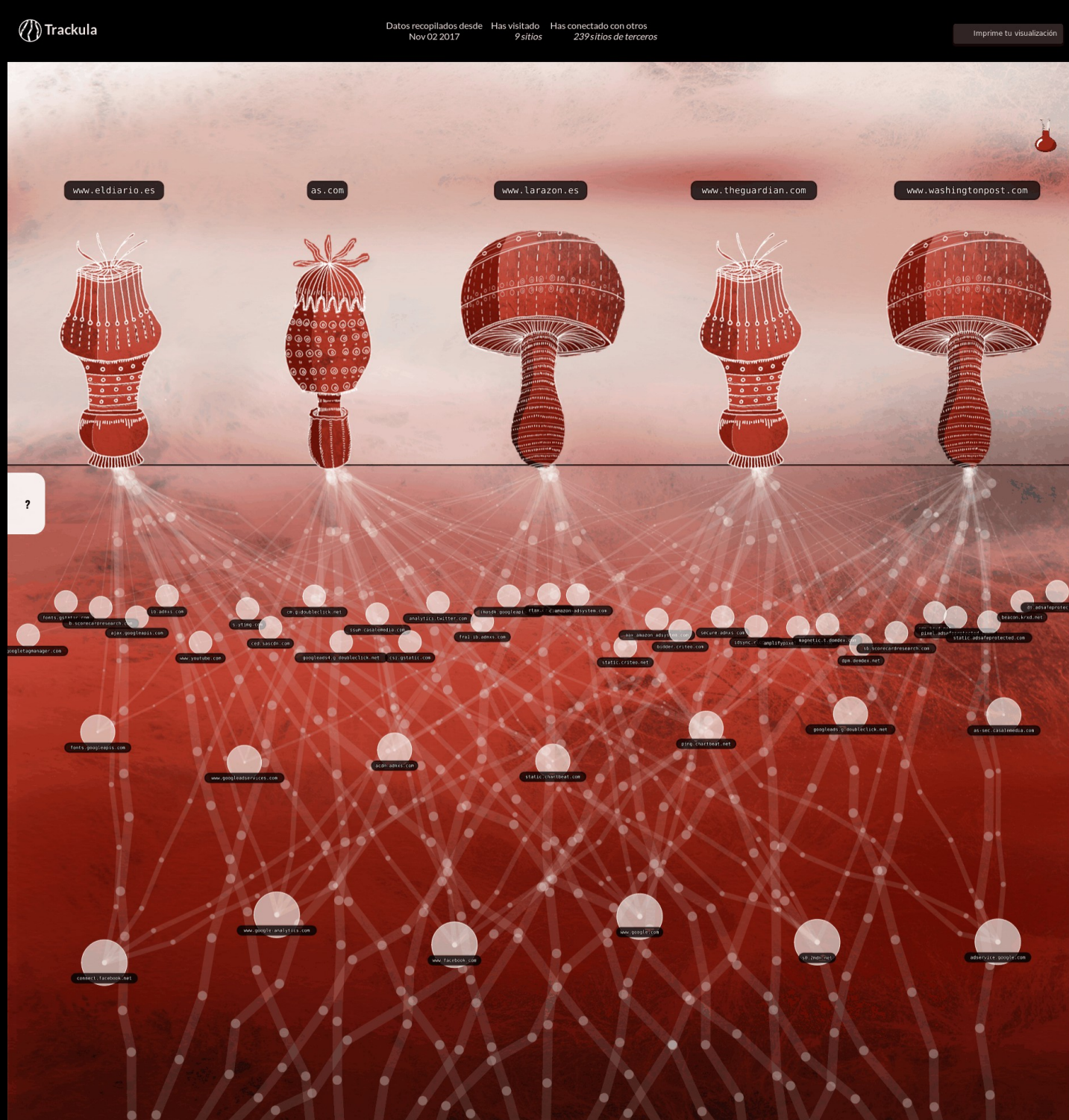
moz://a

World known

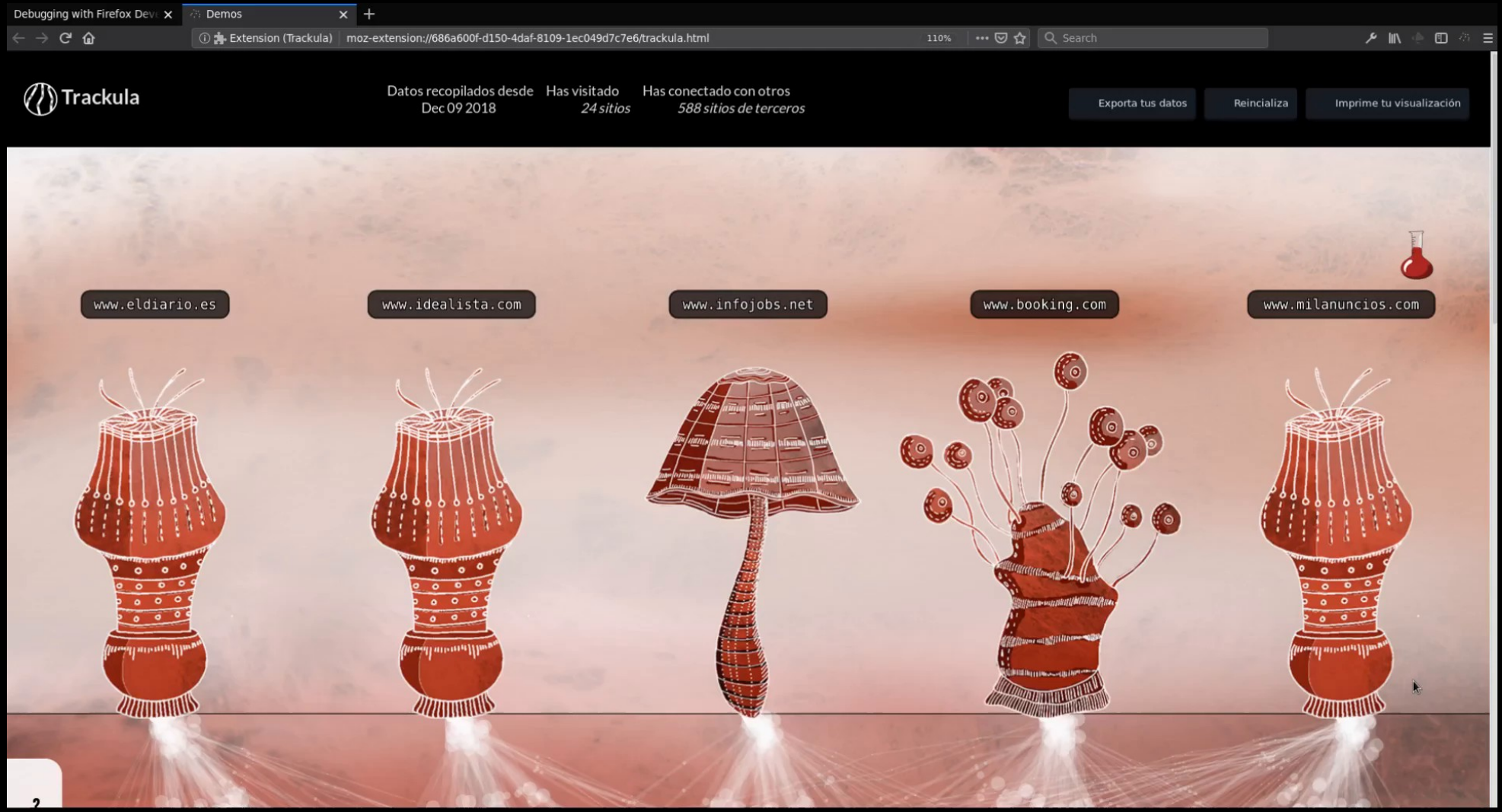
(visited websites)

Underworld

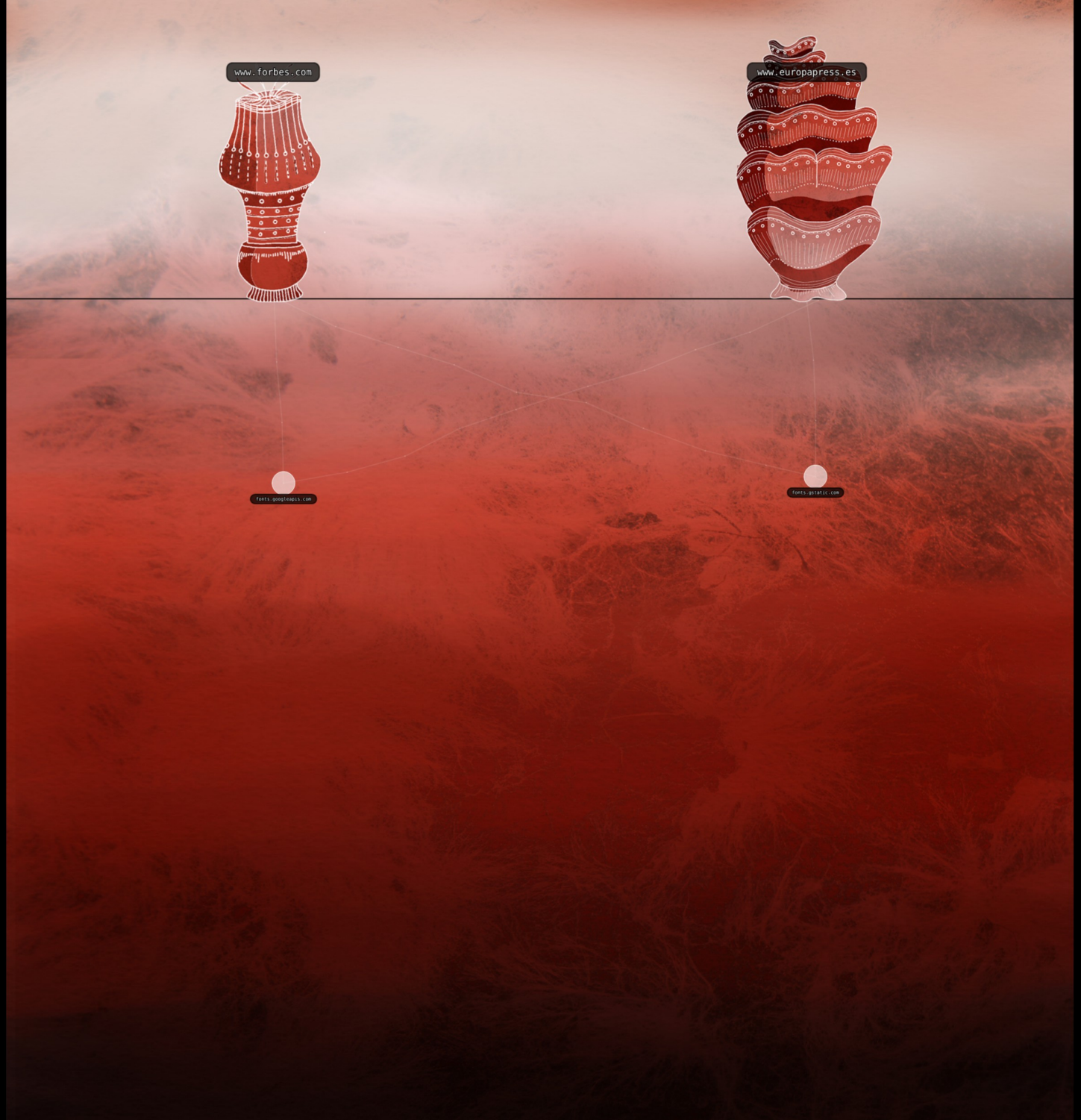
(third parties involved)



Video demo not available on the PDF version.
The video is available at:
`https://assets.trackula.org/2019-trackula-plugin-usage.mp4`


Debugging with Firefox Deve
Demos
Extension (Trackula)
moz-extension://686a600f-d150-4daf-8109-1ec049d7c7e6/trackula.html
110%
Search
Trackula
Datos recopilados desde
Dec 09 2018
Has visitado
24 sitios
Has conectado con otros
588 sitios de terceros
Exporta tus datos
Reincializa
Imprime tu visualización
www.eldiario.es
www.idealista.com
www.infojobs.net
www.booking.com
www.milanuncios.com

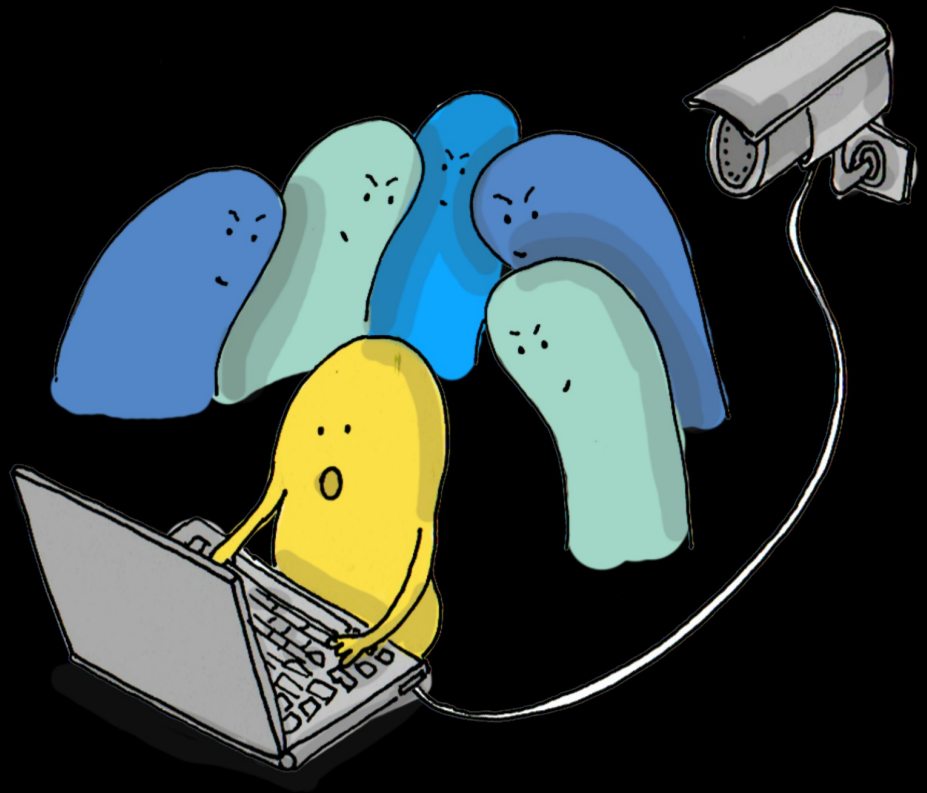

forbes.com
www.dhs.gov
www.trainline.de
www.takeaway.com
www.europapress.es
js-agent.newrelic.com
bam.nr-data.net
www.googletagmanager.com
bat.bing.com
fonts.googleapis.com
fonts.gstatic.com
googleads.g.doubleclick.net
www.facebook.com
www.google.com
www.google.be
connect.facebook.net
adservice.google.com
stats.g.doubleclick.net


www.forbes.com
www.europapress.es
fonts.googleapis.com
fonts.gstatic.com

FUTURE WORK

- Local Sheriff: notify user of form data leaked
- Local Sheriff as a privacy analysis “engine”
- Lower-level language (wasm); HAR support
- Trackula as a UI and client of Local Sheriff
- Sharing technology for GDPR compliance

Questions?



Konark Modi | @konarkmodi
Santiago Saavedra | @ssice
Sofía Prósper | @sofipros

github.com/cliqz-oss/local-sheriff

trackula.org