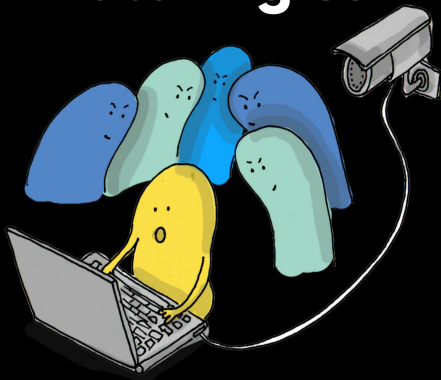


Watching them Watching us



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



github.com/cliqz-oss/local-sheriff



trackula.org

Top 5 trackers in Europe

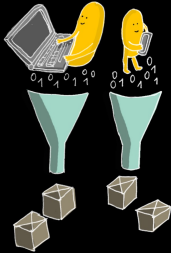


Source: *whotracks.me* from December 2018

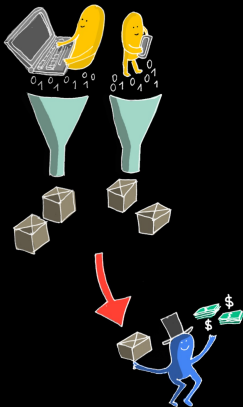
How does it work?



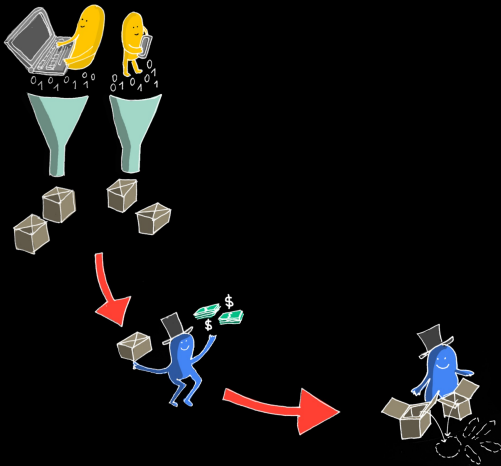
How does it work?



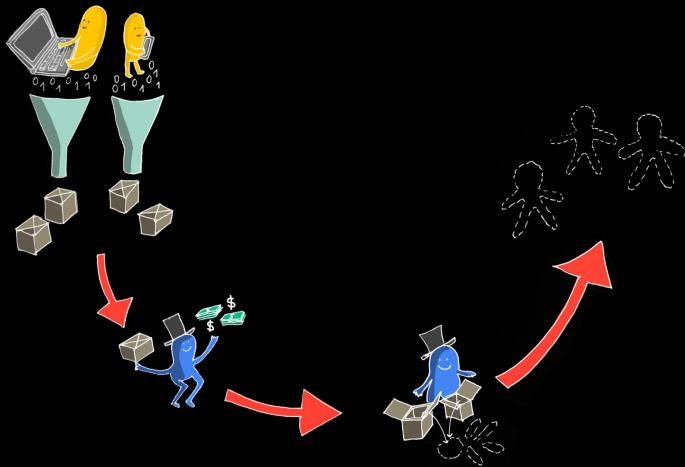
How does it work?



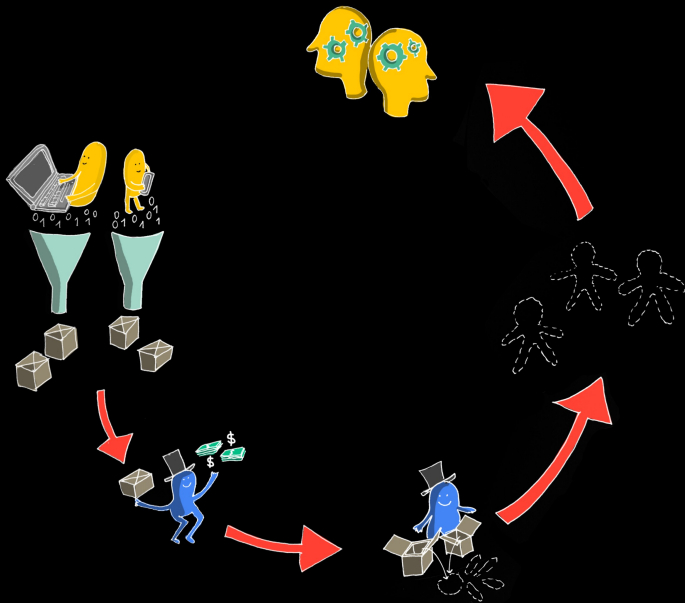
How does it work?



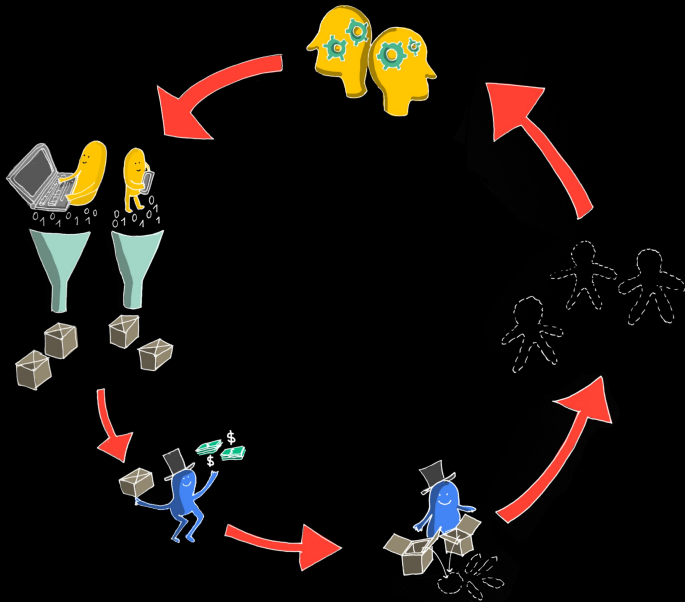
How does it work?



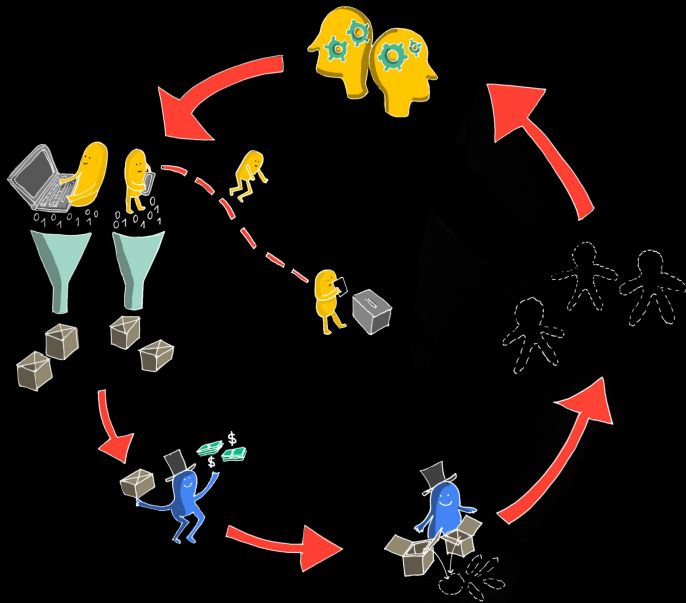
How does it work?

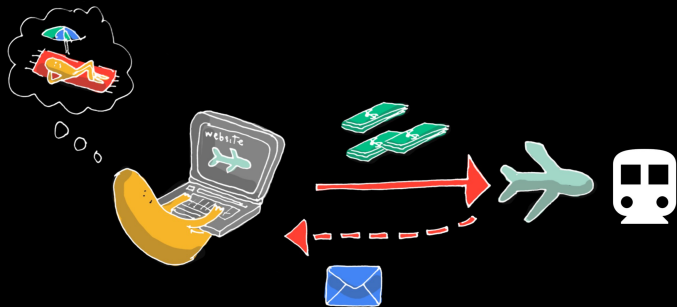


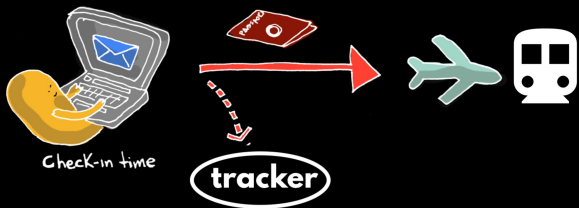
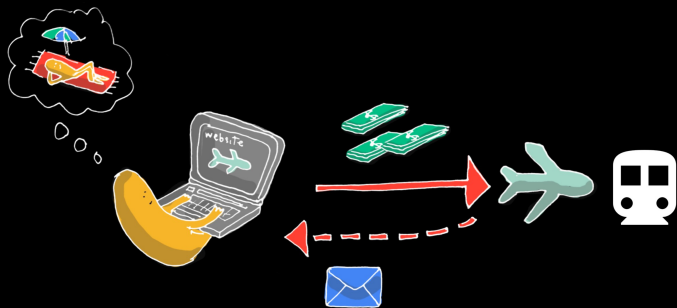
How does it work?



How does it work?









**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 Mozilla Foundation (US) | https://donate.mozilla.org/en-us/thank-you/?email=konark%40cliqz.com&country=germany&payment=stripe&str_amount=200&str_currency=USD

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

2019-01-30 16:29:49 GET https://fonts.googleapis.com/css?family=Nunito+Sans:600,400,300,700,300italic|Zilla+Slab:300,700 HTTP/2.0

200 text/css 631b 1.38s

Request	Response	Detail
:authority:	fonts.googleapis.com	
user-agent:	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:65.0) Gecko/20100101 Firefox/65.0	
accept:	text/css,*/*;q=0.1	
accept-language:	en-US,en;q=0.5	
accept-encoding:	gzip, deflate, br	
referrer:	https://donate.mozilla.org/en-US/thank-you/?payment=Stripe&str_amount=200&str_currency=usd&str_id=ch_1DmTVmG8Mmx3htnxaJ0lp&str_frequency=one-time&email=konark%40cliqz.com&country=Germany&test=ost&test=htl&ul=en-us&de=UTF-8	
pragma:	no-cache	
cache-control:	no-cache	
te:	trailers	
Query		[m]
family: Nunito Sans:600,400,300,700,300italic Zilla Slab:300,700		

EXAMPLE #2

tl Trainline

Trainline.com Limited (GB) | https://www.trainline.eu/order/3e5r

...

☆

🏠

🔍

🔄

⚙️

☰

trainline

PURCHASE no. 3ES [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
15:56

München Hbf
[REDACTED]

€111.80

09:47 München Hbf (Munich, Main Station)

13:40 Frankfurt (Main) Hbf (Main Station)

— 1h09 transfer time

14:49 Frankfurt (Main) Hbf (Main Station)

15:56 Marburg (Lahn)

DB

EC 390

1st

Aisle
Carriage 12, seats 51, 52

Konark Kumar Modi
[REDACTED]

Refund and exchange:
[Sparpreis](#)

DB

RE 4160

1st

No assigned seat

Ticket reference: [REDACTED]

Invoice

Proof of payment

Purchased on 07 July 2018

€111.80

SUNDAY
5 AUG

13:58
18:56

[REDACTED]
München Hbf

13:58 Marburg (Lahn)

15:11 Kassel-Wilhelmshöhe

— 13 min transfer time

DB

RE 4158

1st

No assigned seat

Konark Kumar Modi
Pallavi Modi

Refund and exchange:
[Sparpreis](#)

IDENTIFYING LEAKS

```
2019-01-30 13:20:01 GET https://www.facebook.com/connect/ping?client_id=158788690798420&domain=www.trainline.eu&origin=I&redirect_uri=https%3A%2F%2Fwww.trainline.eu%2F3e5

- 302 text/html [no content] 645ms

Request Response Detail
:authority: www.facebook.com
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14; rv:65.0) Gecko/20100101 Firefox/65.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate, br
referer: https://www.trainline.eu/order/3e5
upgrade-insecure-requests: 1
cliqz-antitracking:
te: trailers

Query
client_id: 158788690798420 [m:auto]
domain: www.trainline.eu
origin: I
redirect_uri: https://staticxx.facebook.com/connect/xd_arbiter/r/UMRn6XE8Z06.js?version=43#cb=f3afca22b4a8ae6&domain=www.trainline.eu&origin=https%3A%2F%2Fwww.trainline.eu%2F3e5 &relation=parent
response_type: token,signed_request
sdk: joey
```

```
2019-01-30 13:20:04 GET https://www.google-analytics.com/collect?v=1&_v=j73&a=3391919&t=pageview&_s=1&dl=https%3A%2F%2Fwww.trainline.eu%2Forder/3e5

- 200 image/gif 550 15ms

Query Request Response Detail [m:auto]
v: 1
_v: j73
a: 3391919
t: pageview
dl: https://www.trainline.eu/order/3e5
dp: /order/3e5
ut: en-us
de: UTF-8
ds: Trainline
sd: 24-bit
sr: 1440x900
vp: 1440x768
je: 0
fl: 30.0 r0
_u: SACAAEAB~
jid:
gid:
cid: 74907457.1547030334
tid: UA-16633907-29
_gid: 1104044393.1548847107
gtm: 2wgldlTP22XP
cd1: visitor
cd2: en
cd17: 1
cd34: EUR
z: 517146697
[15/50] ? :help q:back [*:8098]
```

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

Request URL: <https://fonts.googleapis.com/css?family=PT+Sans+Narrow:400,700>

Request Method: GET

Status Code:  200

Remote Address: [2a00:1450:4001:821::200a]:443

Referrer Policy: no-referrer-when-downgrade

▶ Response Headers (15)

▼ Request Headers

⚠ Provisional headers are shown

Referer: [https://shop.flixbus.de/rebooking/mobile/auth?orderId=807\[REDACTED\]h=54xfy6dhecns52d\[REDACTED\]iscnjqdwu91q990](https://shop.flixbus.de/rebooking/mobile/auth?orderId=807[REDACTED]h=54xfy6dhecns52d[REDACTED]iscnjqdwu91q990)

EXAMPLE #4

Deutsche Lufthansa Aktiengesellschaft [DE] <https://book.lufthansa.com/lh/dyn/air-lh/servicing/enterVisa?sessionId=AOuBBXU6CgDHUHKAMMH5yOzq7pH98IEy>

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

Local Sheriff | chrome-extension://ckmkilooftgfaifdhcfdllaacp[ejeg/templates/control-panel.html]

☆

0339651b1

0339651b1

Token to access booking

has been leaked to **4 third-party domains** , owned by **4 different companies** courtesy **2 website**.

Company	Website
Google	www.lufthansa.com
Google	book.lufthansa.com
Oracle Maxymiser	book.lufthansa.com
Webtrends	book.lufthansa.com
Exactag	book.lufthansa.com

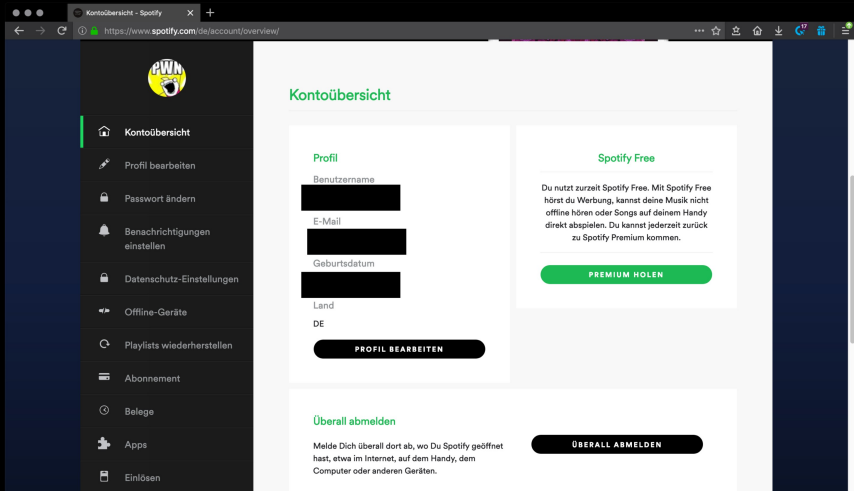
Detailed Logs

Leaked via ref or a key like d,dr in third-party:

<https://www.lufthansa.com/deeplink/partner?partnerid=13710&Country=de&Language=de&ENC=0339651b1> (REDACTED)

Telltale URL

EXAMPLE #5



IDENTIFYING LEAKS

2018-03-18 03:27:23 GET https://sb.scorecardresearch.com/b?c1=28&c2=15654041&ns_t=1521340042970&ns_c=UTF-8&c=Konto%C3%BCbersicht%20-%20Spoti
fy&c7=https%3A%2F%2Fwww.spotify.com%2Fde%2Faccount%2Foverview%2F%3Futm_source%3Dspotify%26utm_medium%3Dmenu%26utm_c

← 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_source=NAphCkkKDVNwb3RpZnktZnXlcnMSCmtvbMfyazMwMDMaA5G 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: Kontoubersicht - Spotify

c7: https://www.spotify.com/de/account/overview/?utm_source=sp_b3RpZnktcXNlcnMSCmtvbmFyazMwMDMaA5qBASUnxq1aMiIKCFaQ0bXqYpEvEhbh

IDENTIFYING LEAKS

Secure | [https://www.foodora.de/restaurants/lat/48.1\[REDACTED\]/lng/11.6\[REDACTED\]/plz/81677/city/München/address/Vo\[REDACTED\]](https://www.foodora.de/restaurants/lat/48.1[REDACTED]/lng/11.6[REDACTED]/plz/81677/city/München/address/Vo[REDACTED])

Latitude & Longitude Pincode & City Street & House number

foodora DE | EN ANMELDEN

Extension (Local Sheriff) moz-extension://e26cbcb8-b949-ee42-8ad5-e4f219d8209b/templates/control-panel.html

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.

48.1513886

48.1513886

has been leaked to **18 third-party domains** , owned by **7 different companies** courtesy **1 website**.

Company	Website
Unknown	www.foodora.de
Google	www.foodora.de
Amazon	www.foodora.de
Facebook	www.foodora.de
New Relic	www.foodora.de
Sift Science	www.foodora.de
TrackJS	www.foodora.de

Detailed Log

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

crazyegg doubleclick facebook
google-analytics qubityahoo

ads-twitter aero appdynamics bing booking boxever bstatic captcha cartrawler cloudfront
coremetrics crazyegg ek eu-appdynamics facebook fly
getyourguide google-analytics googletagmanager imigix qubit qubitproducts

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.

	Leaking via header	Leaking via Query Parameters
1 Third-party		
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

```
Flows
GET https://www.google.com/
  → 200 text/html 64.52k 487ms
GET https://www.google.com/logos/doodles/2018/doodle-snow-games-day-12-6070619765473280-s.png
  → 200 image/png 2.63k 184ms
GET https://www.google.com/logos/2018/snowgames-skipjump/cta.png
  → 200 image/png 13.4k 229ms
→ GET https://www.gstatic.com/external_hosted/createsjs/createsjs-2015.11.26.min.js
  → 200 text/javascript 48.51k 475ms
GET https://ssl.gstatic.com/gb/images/i2_2ec824b0.png
  → 200 image/png 23.64k 253ms
GET https://ssl.gstatic.com/safebrowsing/csd/client_model_v5_variation_0.pb
  → 200 application/octet-stream 67.92k 356ms
GET https://ssl.gstatic.com/safebrowsing/csd/client_model_v5_ext_variation_0.pb
  → 200 application/octet-stream 67.92k 412ms
GET https://www.google.com/logos/2018/snowgames-skipjump/snowgames-skipjump18.js
  → 200 text/javascript 258.16k 900ms
POST https://www.google.com/gen_204?sw=baft&atyp=c&ie=vcGLWp6uMskK0gTYs6yIAm&rt=wsrt.2615,oft.1379,prt.1379
  → 204 text/html [no content] 379ms
GET https://www.gstatic.com/gg/_/js/k=og.2.en_US.ulIn0gNl16I.0/rt=j/m=def/ex=win,fof/d=1/ed=1/rs=AAZYrT
uVOKajNL
  → 200 text/javascript 46.4k 265ms
GET https://www.google.com/xjs/_/js/k=xjs.s.en.zjlvx8fVgY.0/m=sx,sb,cdo,s,cr,elog,hsm,jso,r,d,ci/am=CL0
eMEByP8_
  → 200 text/javascript 144.26k 368ms
GET https://www.google.com/xjs/_/js/k=xjs.s.en.zjlvx8fVgY.0/m=aa,abd,async,dv1,foof,fpe,ipw6,lu,n,mu,sf,
sonic,s-
  → 200 text/javascript 30.54k 195ms
GET https://www.google.com/logos/2018/snowgames-skipjump/main-sprite.png
  → 200 image/png 1.28k 529B
[14/36] [*:9999]
replay_client [flow]
```

Status	Method	F...	Domain	Cause	Type	Transferred	Size	0 ms	1.87 ms	2.73 ms	4.10 ms
302	GET	index.p...	en.wikipedia...	document	html	60.77 KB	274.32 KB	→ 53 ms			
200	GET	Hitchhi...	en.wikipedia...	document	html	60.79 KB	274.32 KB	→ 34 ms			
304	GET	load.ph...	en.wikipedia...	script	js	cached	0 B	→ 24 ms			
200	GET	40px-s...	upload.wiki...	imageset	png	3.01 KB	2.17 KB	→ 32 ms			
200	GET	H2G2_...	upload.wiki...	img	jpeg	28.93 KB	28.04 KB	→ 62 ms			
200	GET	Ultimat...	upload.wiki...	imageset	jpeg	36.63 KB	35.74 KB	→ 32 ms			
200	GET	440px...	upload.wiki...	imageset	jpeg	90.26 KB	89.28 KB	→ 42 ms			
200	GET	440px...	upload.wiki...	imageset	jpeg	53.88 KB	52.99 KB	→ 67 ms			
200	GET	H2G2_f...	upload.wiki...	imageset	jpeg	27.87 KB	26.98 KB	→ 33 ms			
200	GET	500px...	upload.wiki...	imageset	jpeg	31.41 KB	30.52 KB	→ 43 ms			
200	GET	22px-L...	upload.wiki...	imageset	png	1.28 KB	529 B	→ 58 ms			
28 requests 1.75 MB / 846.60 KB transferred Finish: 105.45 min DOMContentLoaded: 691 ms load: 1.23 s											

Inspector Console Debugger Style Editor Performance Network Accessibility New

Filter URLs

Headers Cookies Params Response

Request URL: https://upload.wikimedia.org/wik...
Request method: GET
Remote address: 208.88.154.248:443
Status code: 200 Edit and Resend Raw headers
Version: HTTP/2.0

Filter headers

Response headers (858 B)

accept-ranges: bytes
access-control-allow-origin: *
access-control-expose-headers: Age, Date, Content-Length, Con...
Duration, X-Cache, X-Varnish
age: 79990
content-length: 2224

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



```
GET /2019/01/30/weather/winter-weather-wednesday-wxc/index.html HTTP/1.1
Host: edition.cnn.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:65.0) Gecko/20100101 Firefox/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://edition.cnn.com/
Connection: keep-alive
Cookie: tryThing00=8605; tryThing01=1282; tryThing02=4806; ug=5c51a3940de4a30a3f8607001636
Upgrade-Insecure-Requests: 1
```

- 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

More... » 'Coldest air in a generation' hits the Midwest. Officials warn of almost instant frostbite

International Edition +

First party - edition.cnn.com

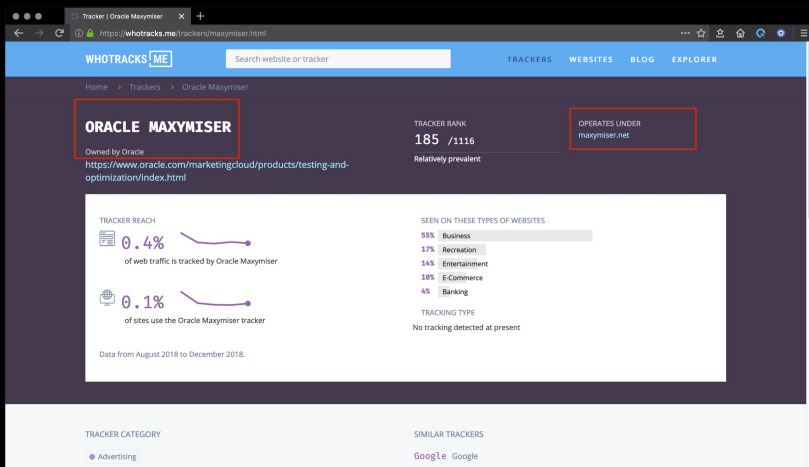
3rd parties on edition.cnn.com

Status	Method	Domain	File	Protocol	Type	Cookies
200	GET	ping.chartbeat.net	ping7h=edition.cnn.com&p=2019/01/30/weather/winter-weather-wednesday-wxc/index.html&u=FL...	HTTP/2.0+h2	gif	
200	GET	cnrrios-f.akamaihd.net	index_0_av.m3u8?null=0	HTTP/1.1	vnd.apple...	
200	GET	cnrrios-f.akamaihd.net	segment1_0_av.ts?null=0	HTTP/1.1	mp2t	
200	GET	cnrrios-f.akamaihd.net	index_3_av.m3u8?null=0	HTTP/1.1	vnd.apple...	
200	GET	cnrrios-f.akamaihd.net	segment2_3_av.ts?null=0	HTTP/1.1	mp2t	
200	GET	ping.chartbeat.net	ping7h=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	ping7h=edition.cnn.com&p=2019/01/30/weather/winter-weather-wednesday-wxc/index.html&u=FL...	HTTP/2.0+h2	gif	
200	GET	cnrrios-f.akamaihd.net	segment1_3_av.ts?null=0	HTTP/1.1	mp2t	
200	GET	cnrrios-f.akamaihd.net	segment3_3_av.ts?null=0	HTTP/1.1	mp2t	
302	GET	sb.scorecardresearch.com	p7c1=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	cnrrios-f.akamaihd.net	segment4_3_av.ts?null=0	HTTP/1.1	mp2t	
200	GET	ping.chartbeat.net	ping7h=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	ping7h=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	p27c1=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.cookiecutter.org	optanon.css	HTTP/2.0	css	
200	GET	www.facebook.com	rcfbHAWQBE.css	HTTP/1.1	css	
302	GET	sb.scorecardresearch.com	p7c1=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	cnrrios-f.akamaihd.net	segment5_3_av.ts?null=0	HTTP/1.1	mp2t	

34 requests 11.78 MB / 11.54 MB transferred Finish: 37.85 s

2. Classify as first party vs third-party

LOCAL SHERIFF

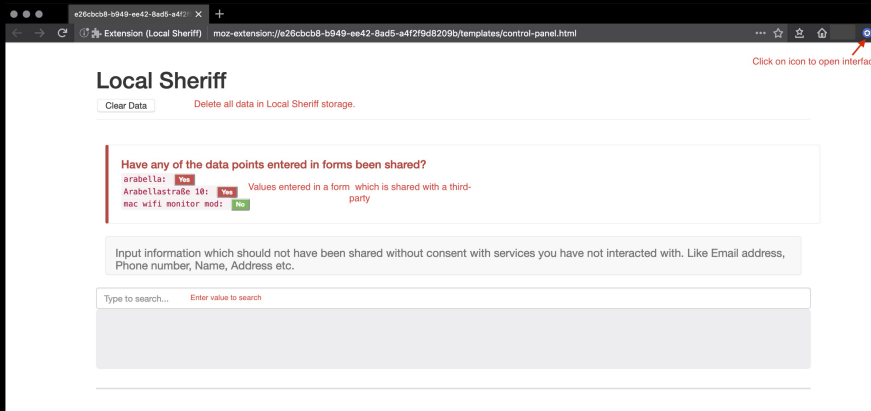


3. Locally shipped copy of hostnames to Companies

Source: <https://whotracks.me>

<https://github.com/cliqz-oss/whotracks.me>

LOCAL SHERIFF



4. Search interface

LOCAL SHERIFF

donate.mozilla.org | Give to Mozilla

https://donate.mozilla.org/en-US/thank-you/?email=konark%40clqz.com&country=Germany&payment=Stripe&str_amount=200&str_currency=usd&str_id=ch_1DmTVm

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!

☐ I'm okay with Mozilla handling my info as explained in [this Privacy Policy](#).

Sign up now

LOCAL SHERIFF

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 of **1 website.**

Company	Website
Google	donate.mozilla.org
Unknown	donate.mozilla.org

Detailed Logs

Tested all data set or a few the data is: **third party**
konark@cliqz.com
https://donate.mozilla.org/en-US/thank-you/?payment=stripe&tr_amount=200&tr_currency=usd&tr_id=ch_1DmTm28MmxzhxagxJOLp&tr_frequency=one-time&email=konark@cliqz.com&country=Germany&test=on&test=rd&tr=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	

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=2152727141300672722&wt_t=1531949797662&affiliate=\(not+set\),&_ga=2.144760631.221776319.1531949772-96041186.1527271413&rl=https://www.flixbus.de/&if=false&ts=1531949799661](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=2152727141300672722&wt_t=1531949797662&affiliate=(not+set),&_ga=2.144760631.221776319.1531949772-96041186.1527271413&rl=https://www.flixbus.de/&if=false&ts=1531949799661)

Cookie **tr=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]&ts=1532015667057&sw=1440&sh=900&v=2.8.21&r=stabl`
`e&ec=0&o=28&it=1532015666967`

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

The screenshot shows the trainline website interface. At the top, the trainline logo is on the left, and the purchase details are in the center: "PURCHASE no. 3ES [REDACTED] booked by Konark Kumar Modi on 07/07 [REDACTED]". A "HELP" link is on the right. Below the header, a message states: "Your tickets have been sent to modi.konark@gmail.com ✓". A link "Wrong email address? Edit" is provided. The main content area displays two tickets. The first ticket is for Friday, 3 AUG, from München Hbf to Marburg (Lahn) via Frankfurt (Main) Hbf. It shows a price of €111.80. The second ticket is for Sunday, 5 AUG, from Marburg (Lahn) to München Hbf. A "Ticket reference: [REDACTED]" is shown. A red box highlights the "Invoice" and "Proof of payment" section, which includes a PDF icon, the text "Proof of payment", "Purchased on 07 July 2018", and the amount "€ 111.80".

trainline PURCHASE no. 3ES [REDACTED] booked by Konark Kumar Modi on 07/07 [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) 15:56 Marburg (Lahn)

EC 390 1st Aisle Carriage 12, seats 51, 52 Konark Kumar Modi [REDACTED] Refund and exchange: Sparpreis

— 1h09 transfer time

14:49 Frankfurt (Main) Hbf (Main Station) 15:56 Marburg (Lahn)

RE 4180 1st No assigned seat

Ticket reference: [REDACTED]

SUNDAY 5 AUG 13:58 [REDACTED] 18:56 München Hbf

13:58 Marburg (Lahn) 15:11 Kassel-Wilhelmshöhe

RE 4138 1st No assigned seat Konark Kumar Modi Pallavi Modi Refund and exchange: Sparpreis

— 13 min transfer time

Invoice Proof of payment Purchased on 07 July 2018 € 111.80

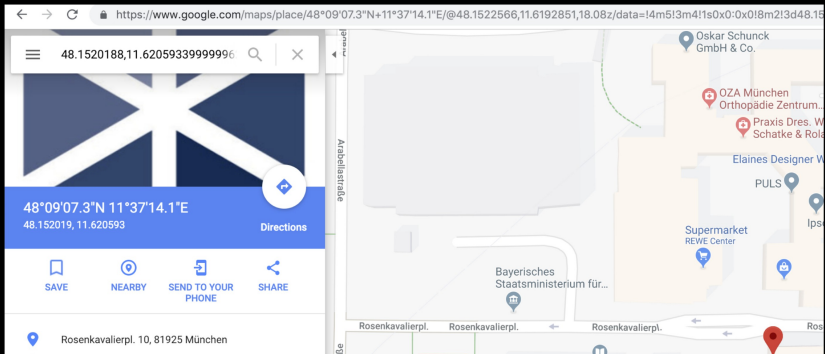
LOCAL SHERIFF

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/Ing/11.620593399999962/plz/81925/city/München/address/Rosenkavali
erpl.%2010%2C%2081925%20M%C3%BCnchen%2C%20Deutschland/Rosenkavaliplatz/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=153624494545

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



• URL

- www.bild.d
- edition.cnn.com
- www.trainline.eu/order/3e5<Redacted>
- www.foodora.de/en/restaurants/lat/48.1520188/Ing/11.620593399999962/plz/81925/city/München/address/

• Cookie

- [fr=0Sh6fFpK7USdFh0w3.](#)
- [fr=0Sh6fFpK7USdFh0w3.](#)
- [fr=0Sh6fFpK7USdFh0w3.](#)
- [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?



The screenshot shows the Network tab of a web browser's developer tools. The 'Filter URLs' field is empty. The table lists 38 requests. The first request is a GET to 'api/getby_wq=10pwid=725737855851455&correlation=151983...' from 'securepubads.g.doubleclick.net'. A yellow arrow points to this first request. The table has columns for Status, Method, File, Domain, Cause, Type, Transferred, Size, and Time. The 'Time' column shows a waterfall chart for the first few requests.

Status	Method	File	Domain	Cause	Type	Transferred	Size	Time
200	GET	api/getby_wq=10pwid=725737855851455&correlation=151983...	securepubads.g.doubleclick.net	xhr	js	3.65 KB	6.49 KB	750 ms
200	GET	api/getby_wq=10pwid=725737855851455&correlation=151983...	securepubads.g.doubleclick.net	xhr	js	3.20 KB	5.03 KB	688 ms
200	GET	api/getby_wq=10pwid=725737855851455&correlation=151983...	securepubads.g.doubleclick.net	xhr	js	1.07 KB	315 B	493 ms
200	GET	api/getby_wq=10pwid=725737855851455&correlation=151983...	securepubads.g.doubleclick.net	xhr	js	1.07 KB	323 B	284 ms
200	GET	api/getby_wq=10pwid=725737855851455&correlation=151983...	securepubads.g.doubleclick.net	xhr	js	1.06 KB	311 B	284 ms
200	GET	CookieAccess	api.quantcast.mgr.consensu.org	xhr	json	790 B	30 B	140 ms
200	GET	/log-wsDown-usaMozilla5.0 (Windows NT 10.0; Win64; x64; rv:...	audit.quantcast.mgr.consensu.org	xhr	html	cached	80 B	30 ms
200	GET	8FOCnqdu8H1MnWU9R8Bok.wv02	fbntrgstatic.com	font	woff2	cached	15.08 KB	
200	GET	8FOCnqdu8H1MnWU9R8Bok.wv02	fbntrgstatic.com	font	woff2	cached	15.07 KB	
200	GET	memH9Gin12MzQp8A-UPV20k.wv02	fbntrgstatic.com	font	woff2	cached	15.72 KB	
200	GET	barreno-regular.woff	www.idealista.com	font	plain	348 B	0 B	147 ms
200	GET	idRe_vist_ver=3.4.0&id_feldgroup=MC&id_rsbvjon&id_ver=2&...	smc.demdes.net	xhr	json	1.19 KB	693 B	1102 ms
200	POST	eventId_all_ver=5.18_ts=1548888515838	smc.demdes.net	xhr	json	1.20 KB	512 B	1110 ms
200	POST	v5	lbadns.com	xhr	json	3.93 KB	6.87 KB	1110 ms
200	POST	v5	lbadns.com	xhr	json	3.93 KB	6.87 KB	1106 ms
200	POST	v5	lbadns.com	xhr	json	4.12 KB	6.91 KB	1180 ms

38 requests 201.19 KB / 75.51 KB transferred / 6 min 22.37 s / DOMContentLoaded 506 ms / load 7.90 s

TRACKULA



MEDIALAB
PRADO



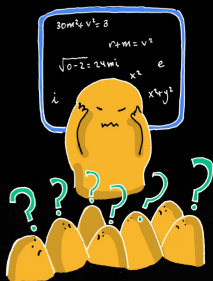
DataLab

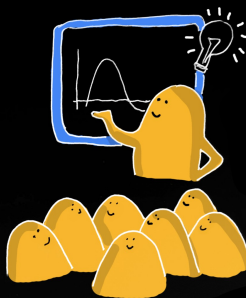
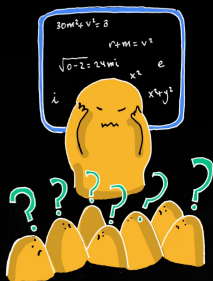
Migraciones VISUALIZAR'17

15-30 septiembre

porCausa
investigación y periodismo







VISUALIZATION

 Graph

DATA

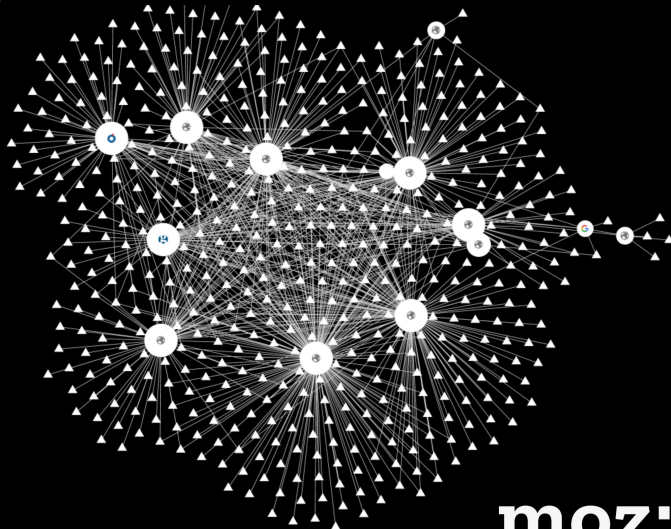
 Save Data

 Reset Data

 [Give Us Feedback](#)

Recent Site

GRAPH VIEW



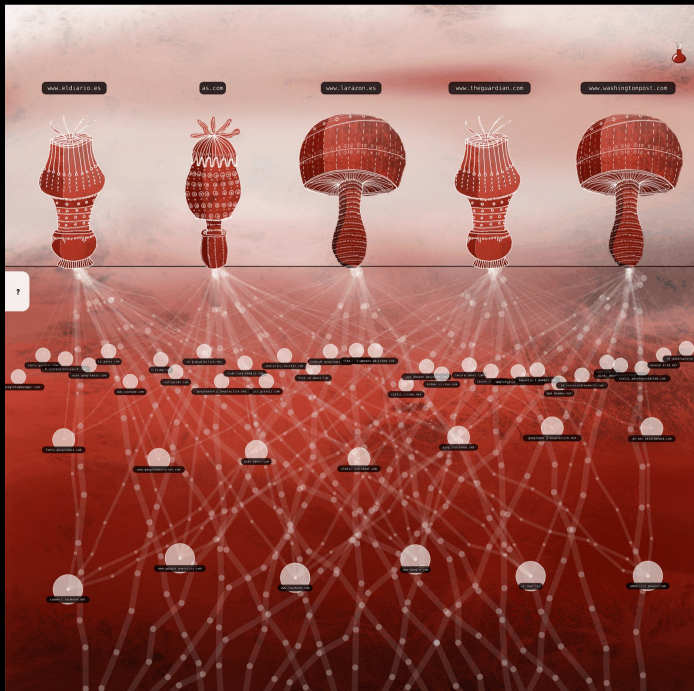
moz://a

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>



Datos recopilados desde Dec 09 2018
Has visitado 24 sitios
Has conectado con otros 588 sitios de terceros

Exporta tus datos

Reinicializa

Imprime tu visualización

www.eldiario.es

www.idealista.com

www.infojobs.net

www.booking.com

www.milanuncios.com



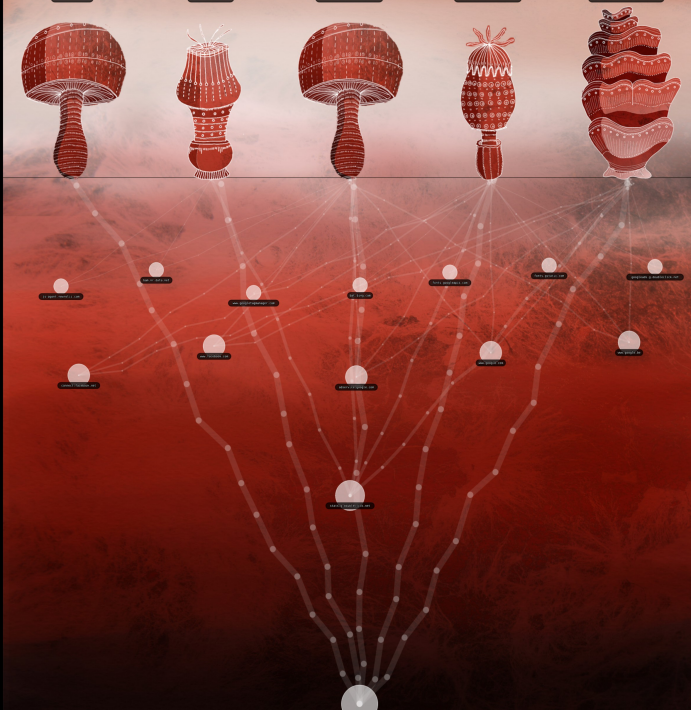
forbes.com

www.dhs.gov

www.trainline.de

www.Takeaway.com

www.eurjopapress.es



www.forbes.com



www.eurapress.es



www.gutenberg.org



www.gutenberg.org

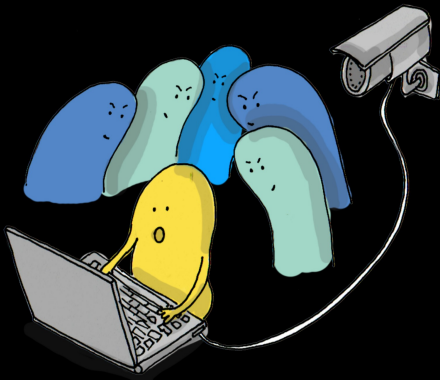


FUTURE WORK



- 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