

Theft and doxxing

The (two) most unethical things I've done at work

My first job out of university

- Security consultant
 - Pentesting
 - Code reviews
 - Forensics
 - Incident response
 - Tools development
 - Miscellaneous ← We are here
- Small Stockholm based company
 - Bought by Finnish Nixu in 2017 (RIP)

That time I stole a company

Let's set the scene

- The client
 - A Stockholm based company (X, the owner)
- The subject
 - A US based company (Y, the subsidiary)
- The background
 - X bought Y
 - Some slight strain with old management

The mission

1. Retrieve a copy of all data controlled by Y
2. They must not suspect anything

The plan

- X claims they want to do a security review of Y
- Fly over to US
- Perform a security review of the company
- Steal all files from on-premise servers
- Steal all data from cloud-based mail server

The execution

- Very welcoming at the office
- Gave me my own room
- Got access to main file server
 - Started dumping everything to hard drives
- Email server password
 - Panic!
- Bandwidth email server <--> Sweden low
 - Offload to local AWS server
 - Transfer back to Sweden over 2 weeks

The anonymous blogger

The \$100M company

- The client
 - Tech startup
 - “disrupting” a very conservative field
 - Valued at ~\$100M
 - Preparing for a sale
- The issue
 - Anonymous blog
 - Trash talking the company
 - Worried about affecting valuation before sale

The blog

- Wordpress.com hosted
- RSS feed
 - Exact timestamp
- About 10 posts
 - ~3 month timespan
- Knowledge of the field



```
▼<rss xmlns:atom="http://www.w3.org/2005/Atom" version="2.0">
  ▼<channel>
    <title>Zeta-Two.com</title>
    <description>My blog about technology, security and life. </description>
    <link>https://zeta-two.com/</link>
    <atom:link href="https://zeta-two.com/feed.xml" rel="self" type="application/rss+xml"/>
    <pubDate>Mon, 23 Dec 2019 14:31:38 +0100</pubDate>
    <lastBuildDate>Mon, 23 Dec 2019 14:31:38 +0100</lastBuildDate>
    <generator>Jekyll v3.8.5</generator>
  ▼<item>
    <title>SecurityFest 2019 - Software Obfuscation with LLVM</title>
    ▼<description>
      <p>At the end of May, I gave a presentation at <a href="https://securityfest.com/">Se
```

The emails

- Emails to employees
- Around publication
- Company website
 - “Our team” page “/team”

HTTP access logs

- Timestamp
 - Path
 - User agent
-
- Turned on full header logging

GeoIP access logs

- Kibana
- GeoIP
- Limited info

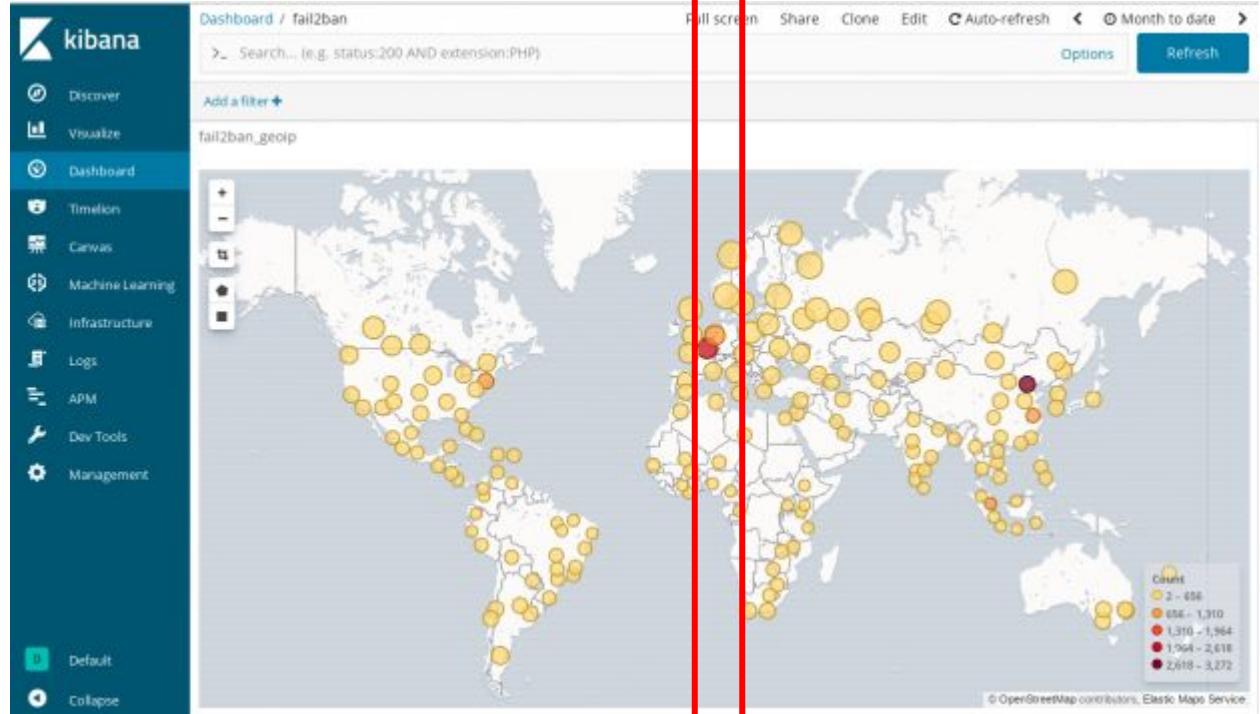


Finding out the timezone

	A	B	C	D	E	F	G
1	UTC-3	UTC-2	UTC-1	UTC	UTC+1	UTC+2	UTC+3
2	04.02.00	05.02.00	06.02.00	07.02.00	08.02.00	09.02.00	10.02.00
3	05.25.00	06.25.00	07.25.00	08.25.00	09.25.00	10.25.00	11.25.00
4	13.37.00	14.37.00	15.37.00	16.37.00	17.37.00	18.37.00	19.37.00
5	14.13.00	15.13.00	16.13.00	17.13.00	18.13.00	19.13.00	20.13.00
6	16.02.00	17.02.00	18.02.00	19.02.00	20.02.00	21.02.00	22.02.00
7	16.41.00	17.41.00	18.41.00	19.41.00	20.41.00	21.41.00	22.41.00
8	17.51.00	18.51.00	19.51.00	20.51.00	21.51.00	22.51.00	23.51.00
9	18.21.00	19.21.00	20.21.00	21.21.00	22.21.00	23.21.00	00.21.00
10	19.01.00	20.01.00	21.01.00	22.01.00	23.01.00	00.01.00	01.01.00

GeoIP + Time Zone

- Kibana
- GeoIP
- ~100 IP addresses



GeoIP + Time stamps + Team page

- All IP addresses from suspect TZ +/- 1
- Who visited “/team”
- Within 2 hours of publication

~10 IP addresses

GeoIP + Time stamps + Team page + Intersect

- All IP addresses from suspect TZ +/- 1
- Who visited “/team”
- Within 2 hours of publication
- For every post

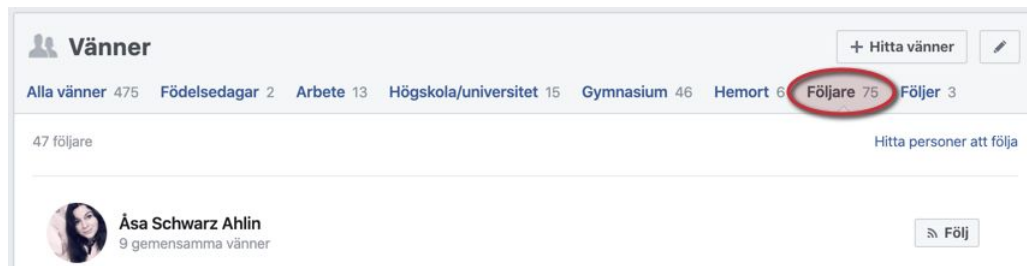
1 IP address!

Suspect profiling

- No crime → no help from law enforcement
- Check full headers logs for IP
- Google Analytics static between events
 - Hypothesis: not using “Incognito Mode”
- A lot of people use Facebook
 - Hypothesis: logged in to FB in same browser

Click-jacking deanonymization

- Facebook “follow” feature
- Follow != friend
 - Asymmetric
- Can embed button
 - Iframe + CSS + JS
- Javascript file
 - Served to specific IP



Box Count

Button Count

Button



Hur kan vi hjälpa dig?

 Sök bland symptom

Mest sökta just nu:



Förnya recept



Eksem



Stress



Coronavirus

[Se alla besvär och symptom](#)

Hur kan vi hjälpa dig?

 Sök bland symptom

Mest sökta just nu:



Förnya recept



Eksem



Stress



Coronavirus

[Se alla besvär och symptom](#)



**A FEW
MOMENTS LATER**



A new follower


The image shows a Facebook 'Vänner' (Friends) page. At the top, there's a header with a person icon and the word 'Vänner'. To the right of the header are two buttons: '+ Hitta vänner' and a pencil icon. Below the header is a navigation bar with several tabs: 'Alla vänner 475', 'Födelsedagar 2', 'Arbete 13', 'Högskola/universitet 15', 'Gymnasium 46', 'Hemort 6', 'Följare 75', and 'Följer 3'. The 'Följare 75' tab is highlighted with a red circle. Below the navigation bar, it says '47 följare' on the left and 'Hitta personer att följa' on the right. The main content area shows a list of followers. The first follower is 'Åsa Schwarz Ahlin' with a profile picture of a woman and the text '9 gemensamma vänner'. To the right of her name is a button with a plus icon and the word 'Följ'. The second follower is 'Abderaman Moad' with a profile picture of a man. This entire entry is circled in red.

Vänner + Hitta vänner

Alla vänner 475 Födelsedagar 2 Arbete 13 Högskola/universitet 15 Gymnasium 46 Hemort 6 **Följare 75** Följer 3

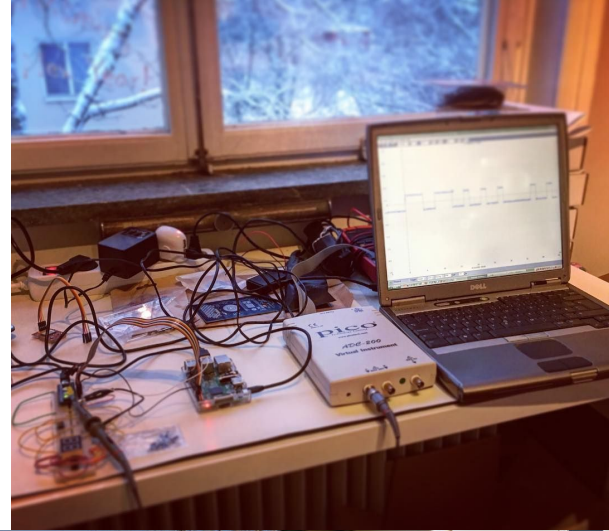
47 följare Hitta personer att följa

 **Åsa Schwarz Ahlin**
9 gemensamma vänner 

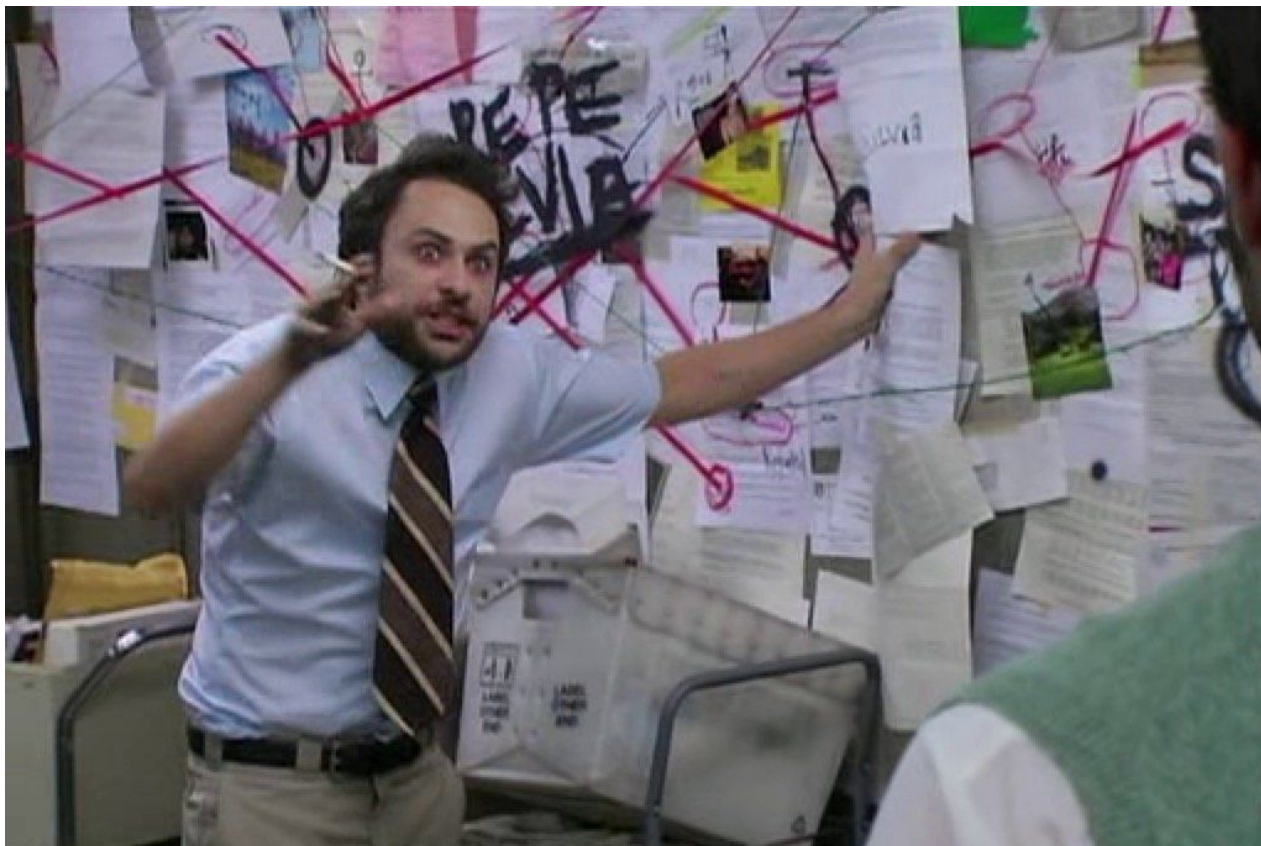
 **Abderaman Moad**

Aftermath

- Verify identity
 - Public records
 - Facebook profile
 - Photos from apartment
 - Cross-reference Google Street View
- Find motive
 - Nothing obvious



About a week of



Then finally

- Family business
 - Same field
 - ...but good relations with them
- The plot twist
 - Professional text analysis
 - The autistic son

Thank you!