VISUALIZATION FOR IT-SECURITY

L. Aaron Kaplan (kaplan@cert.at)

http://CERT.AT

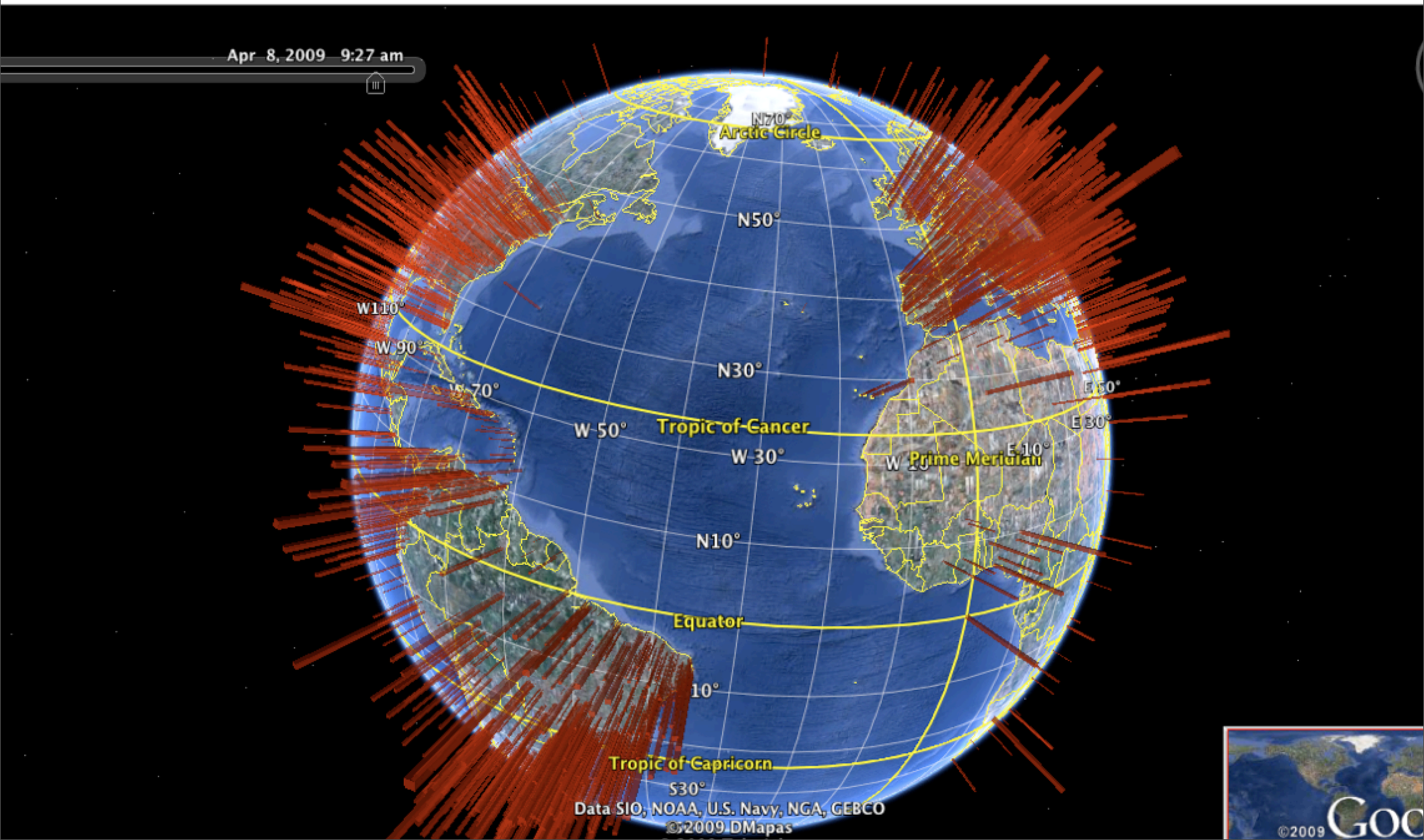
OVERVIEW

CERT.at

- Motivation
- Target Group
- 5 Minutes of design background for techies
- Tools
- DNSviz and Flows

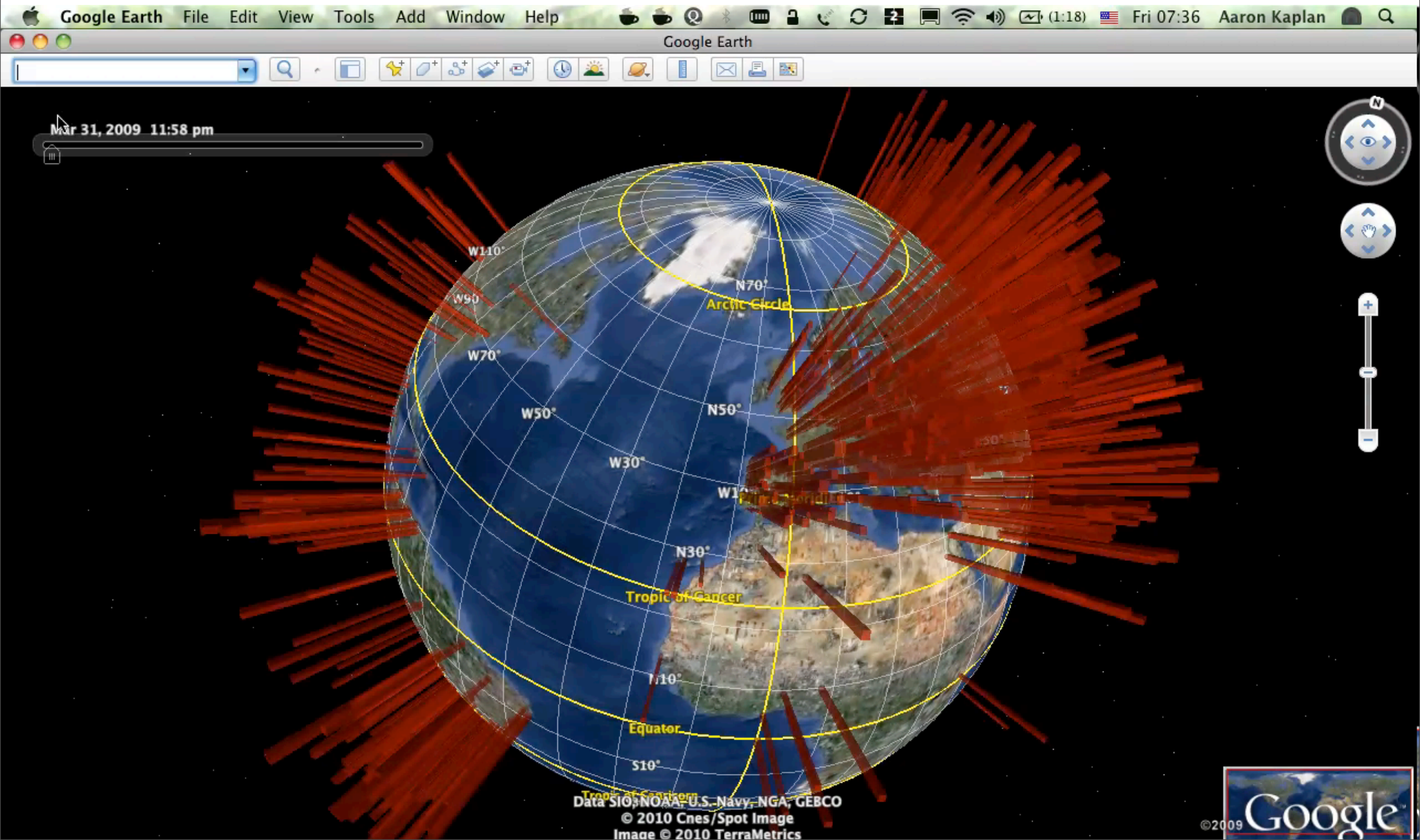
Why am I holding this talk?

Why am I holding this talk?



Why am I holding this talk?

CERT.at



Why am I holding this talk?

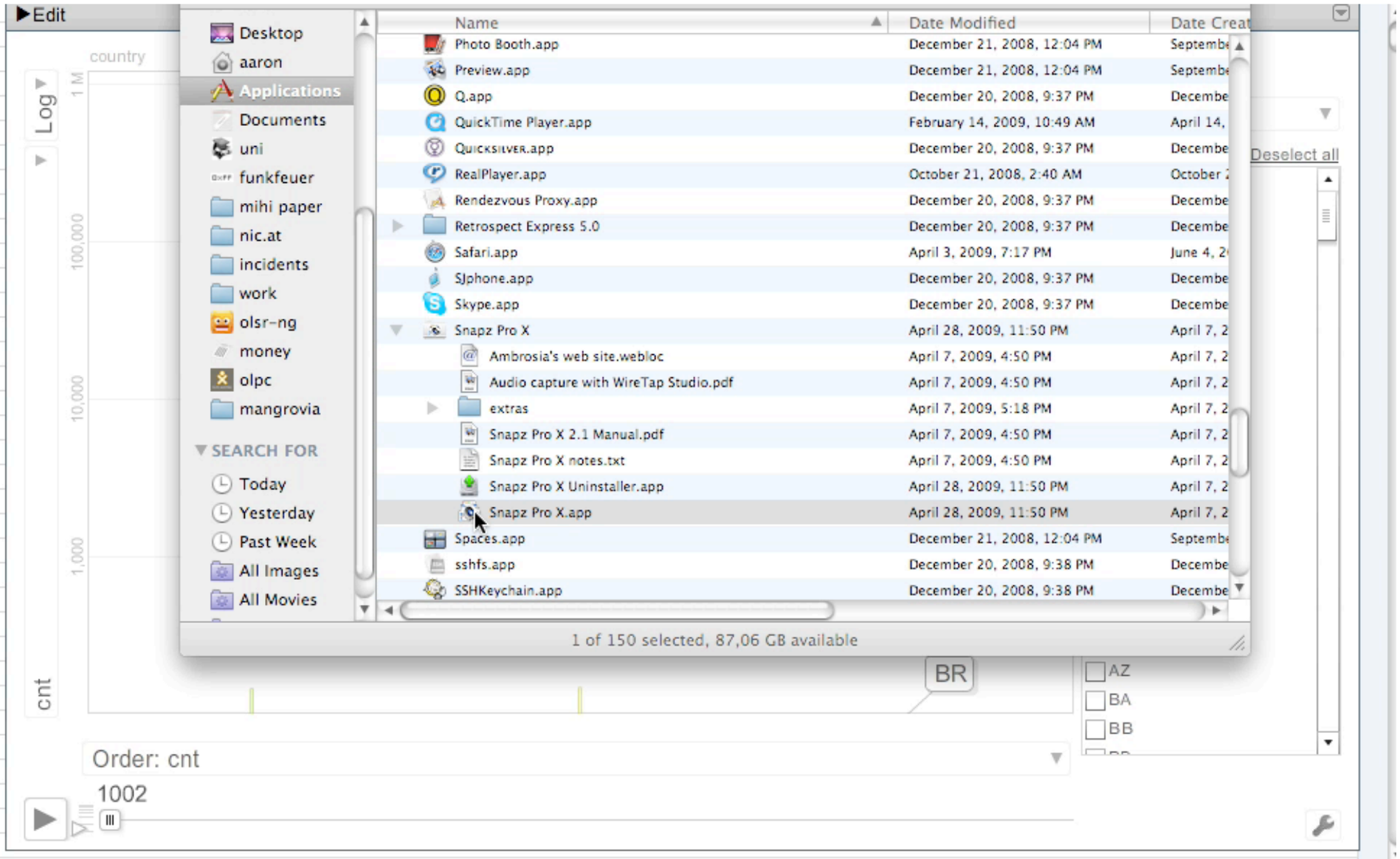
Why am I holding this talk?

Why am I holding this talk?

CERT.at

	country	date	cnt	cnt2
2	MX	1000	4	1
3	KR	1001	2	1
4	BR	1002	2	1
5	VE	1003	1	1
6	CA	1004	1	1
7	KH	1005	1	1
8	RO	1006	1	1
9	TT	1007	1	1
10	RU	1008	1	1
11	PK	1009	1	1
12	AR	1010	1	1
13	ES	1011	1	1
14	CN	1012	1	1
15	US	1013	1	1
16	PH	1014	1	1
17	EC	1015	1	1
18	CN	1016	762166	1
19	BR	1017	644646	1
20	RU	1018	582881	1
21	VN	1019	255845	1
22	UA	1020	245734	1
23	IN	1021	233908	1
24	KR	1022	230627	1
25	ID	1023	210525	1
26	IT	1024	177121	1
27	ES	1025	171711	1
28	PH	1026	153319	1
29	US	1027	150700	1
30	TH	1028	132307	1
31	RO	1029	111490	1
32	TW	1030	103898	1
33	MY	1031	93251	1
34	AR	1032	84714	1
35	VE	1033	84454	1

Add Sheet | Sheet 1 | Gadget1



Overview

CERT.at

- What will you get out of it?
  - Quick IT–security visualization skills with 5 tools
  - Understanding the basic visualization cycle
  - Initial good results in < 1 day
  - Really good results in 10+ years ;–)

CERT.at, Austria

CERT.at, Austria

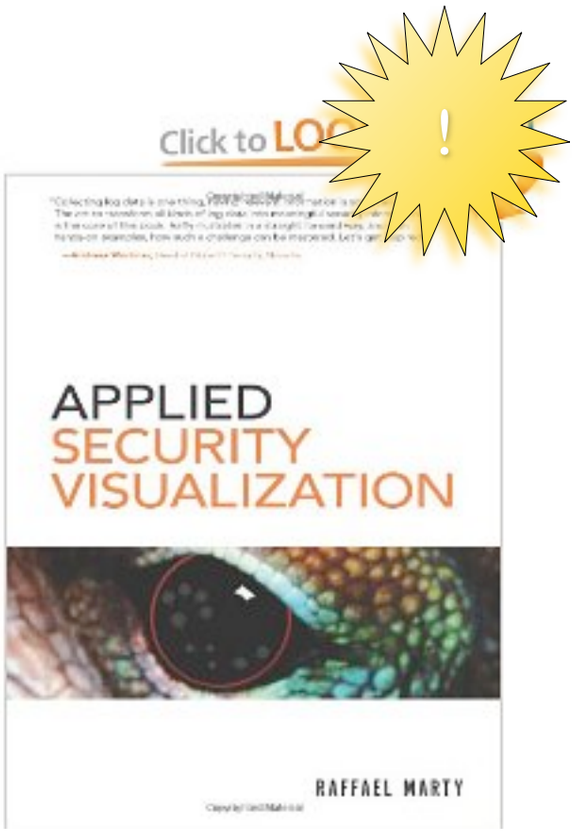
- CERT.at is part of **NIC.at**, the Austrian domain registry. CERT.at is the national CERT
- Austria is in **Europe**, but we definitely like the friends from **AUSCert** and down under
- Vienna, Austria is where we will have our next **FIRST conference 2011**
- **German** is spoken in Austria
- Our neighbouring countries are: Hungary, Slovenia, Germany, Switzerland, Slovakia, Czech Republic, Italy, Liechtenstein

OVERVIEW

CERT.at

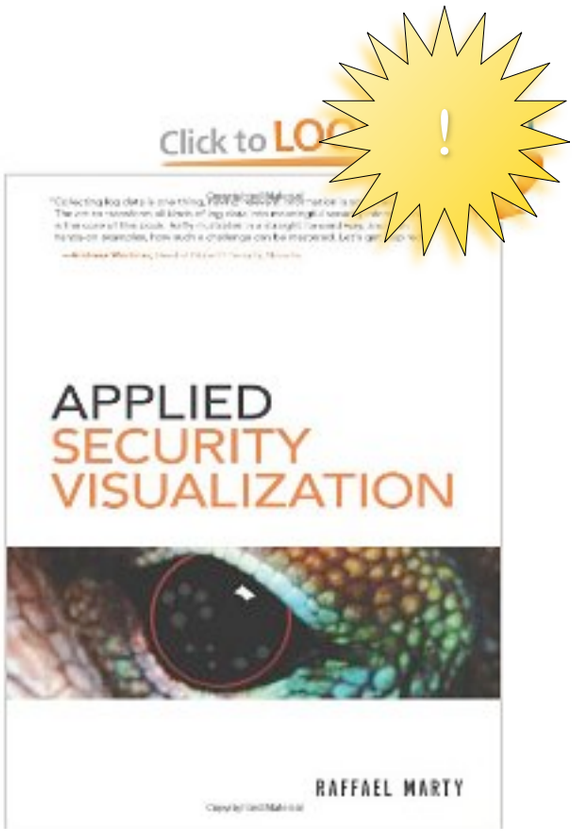
- Motivation
- Target Group
- 5 Minutes of design background for techies
- Tools
- DNSviz and Flows

Motivation



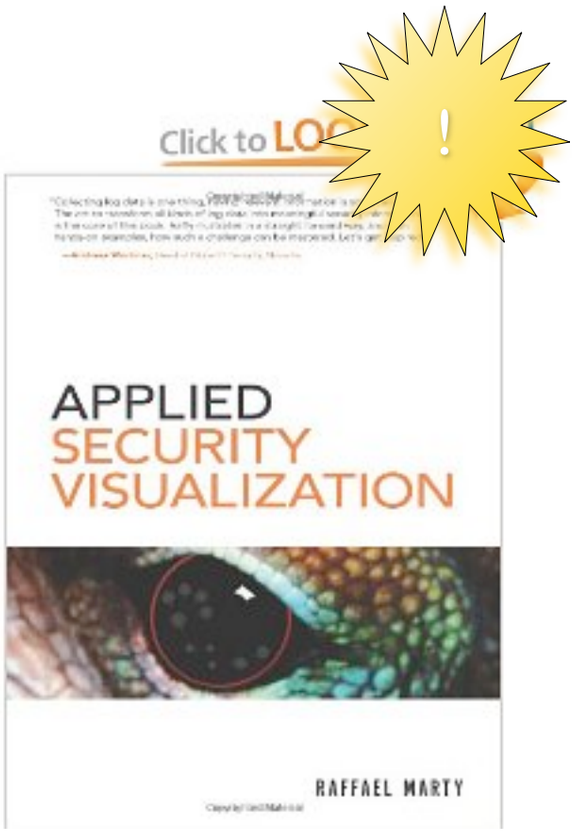
Motivation

- “A picture is worth 1000 log records” (R. Marty)



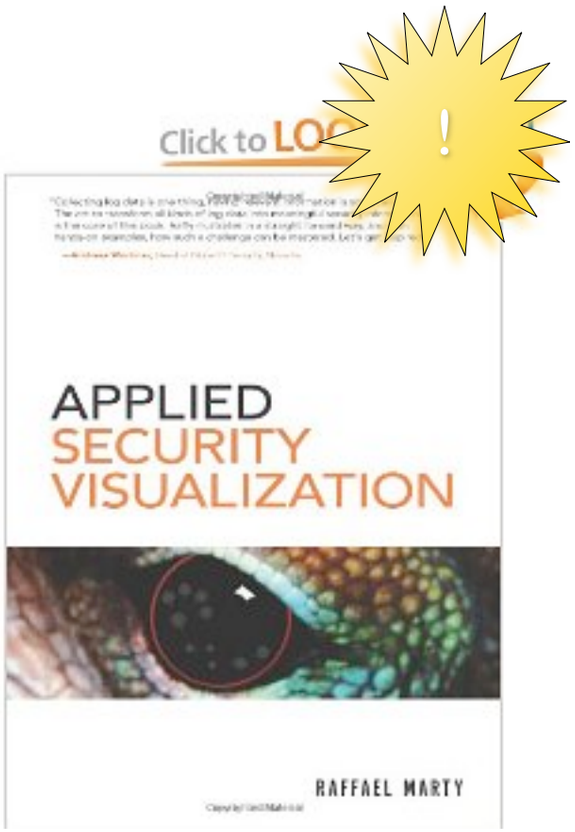
Motivation

- “A picture is worth 1000 log records” (R. Marty)
- We have too much data, info explosion



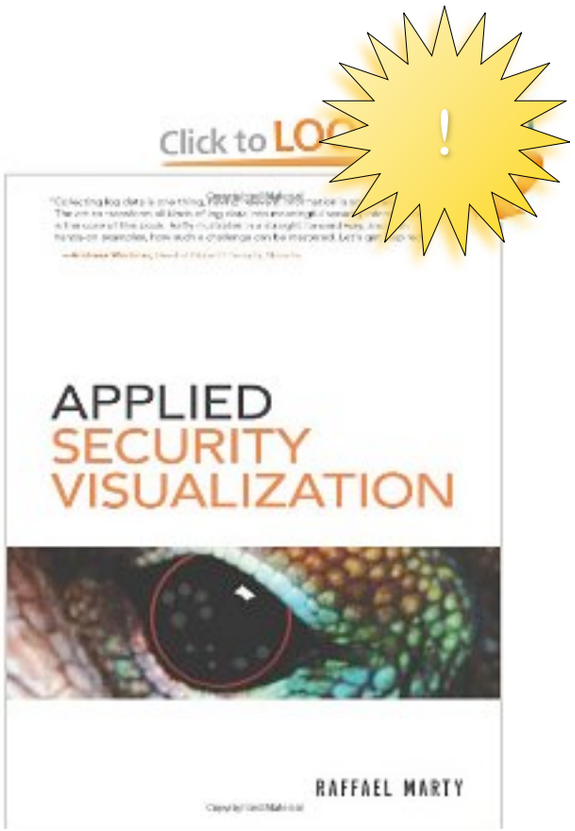
Motivation

- “A picture is worth 1000 log records” (R. Marty)
- We have too much data, info explosion
- **High broadband path to your brain**



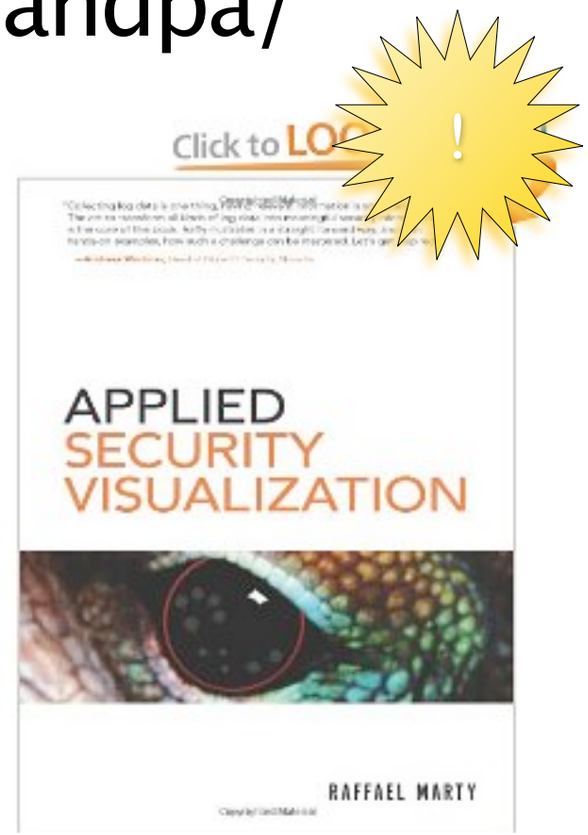
Motivation

- “A picture is worth 1000 log records” (R. Marty)
- We have too much data, info explosion
- **High broadband path to your brain**
- People “get it”



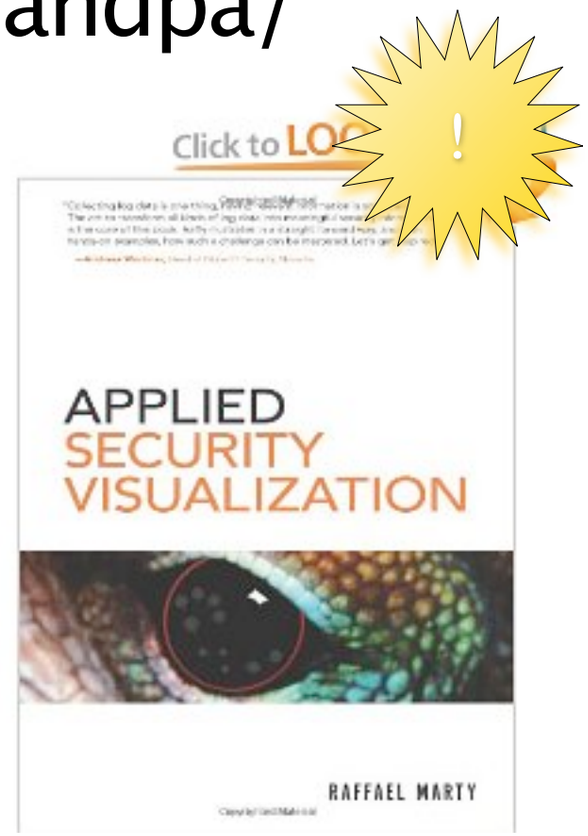
Motivation

- “A picture is worth 1000 log records” (R. Marty)
- We have too much data, info explosion
- **High broadband path to your brain**
- People “get it”
- Visualization can explain it all to your grandpa/father/mother/partner...



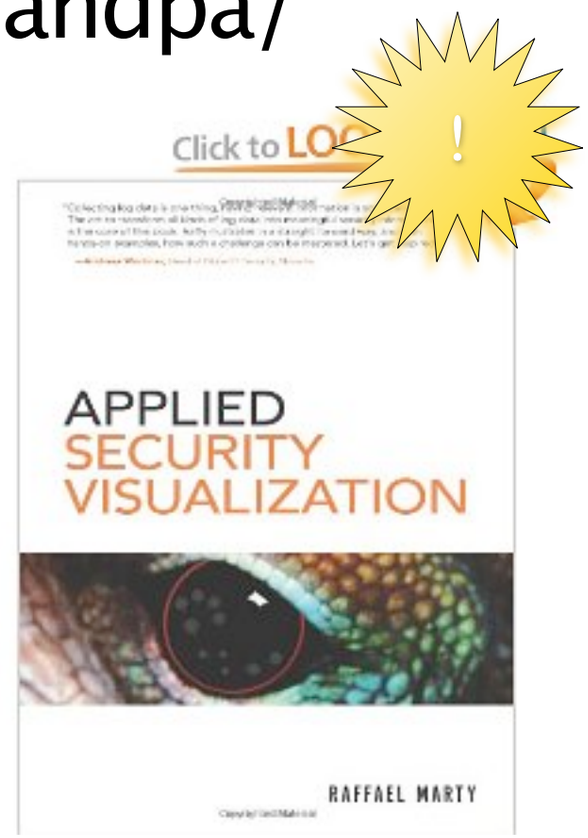
Motivation

- “A picture is worth 1000 log records” (R. Marty)
- We have too much data, info explosion
- **High broadband path to your brain**
- People “get it”
- Visualization can explain it all to your grandpa/father/mother/partner...
- ... and helps them understand that you need to save the internet first



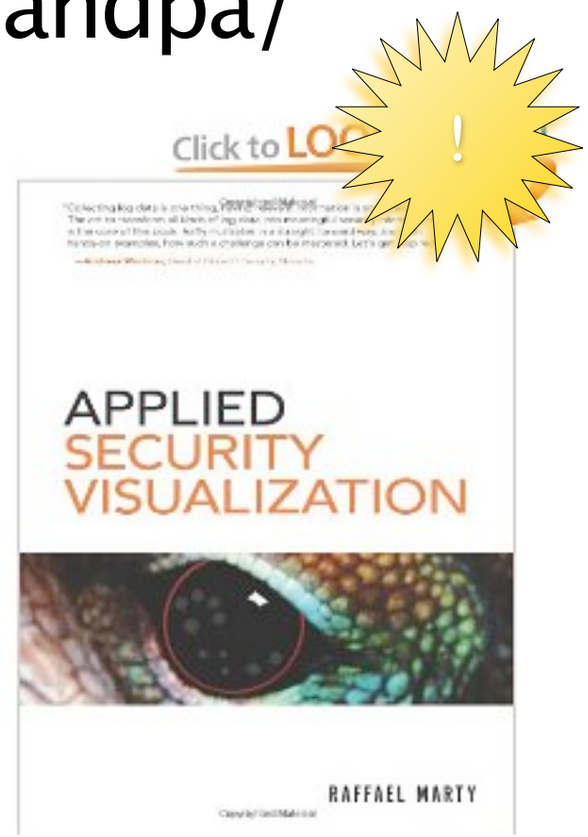
Motivation

- “A picture is worth 1000 log records” (R. Marty)
- We have too much data, info explosion
- **High broadband path to your brain**
- People “get it”
- Visualization can explain it all to your grandpa/father/mother/partner...
- ... and helps them understand that you need to save the internet first
- gives new insights –> explore data



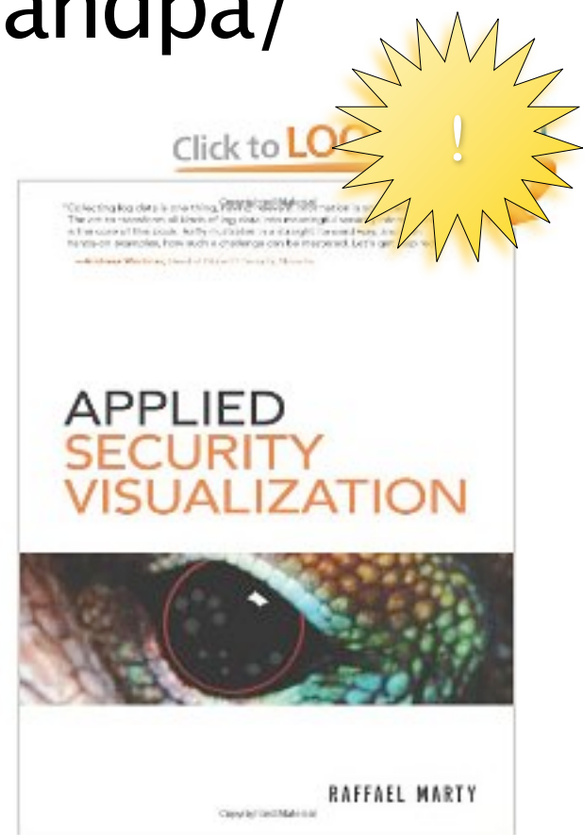
Motivation

- “A picture is worth 1000 log records” (R. Marty)
- We have too much data, info explosion
- **High broadband path to your brain**
- People “get it”
- Visualization can explain it all to your grandpa/father/mother/partner...
- ... and helps them understand that you need to save the internet first
- gives new insights –> explore data
- gives us an overview



Motivation

- “A picture is worth 1000 log records” (R. Marty)
- We have too much data, info explosion
- **High broadband path to your brain**
- People “get it”
- Visualization can explain it all to your grandpa/father/mother/partner...
- ... and helps them understand that you need to save the internet first
- gives new insights –> explore data
- gives us an overview
- **sells your services**



OVERVIEW

- Motivation
- Target Group
- 5 Minutes of design background for techies
- Tools
- DNSviz and Flows

Target groups

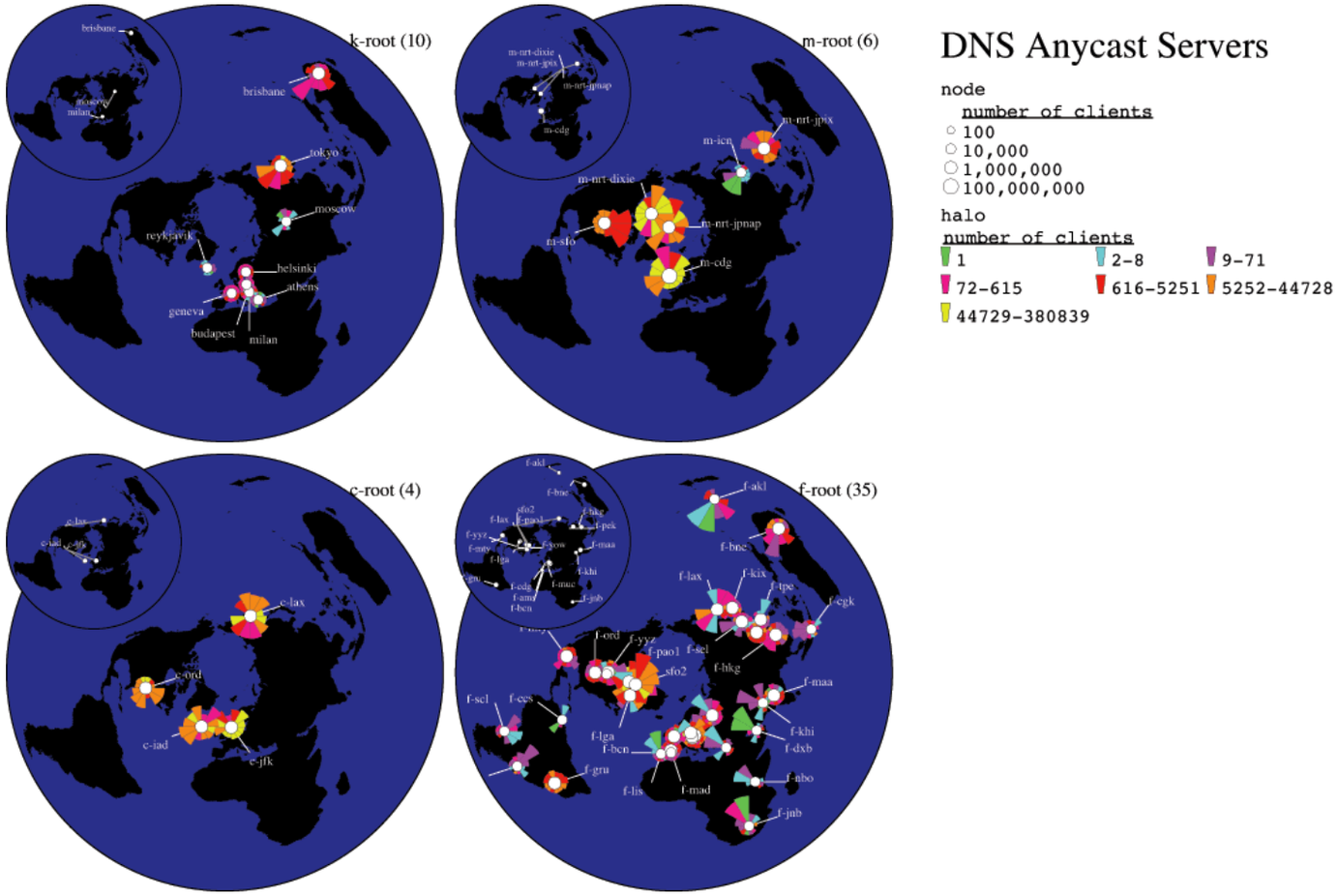
- Users
- Management, Sales, Politicians

- Operational staff
- Researchers

Target groups

- Users
- Management, Sales, Politicians

- Operational staff
- Researchers



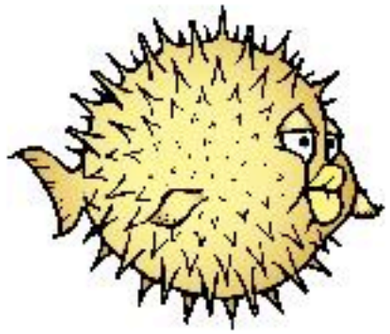
source: CAIDA.org

Target groups

- Users
- Management, Sales, Politicians

- Operational staff
- Researchers

Conficker Eye Chart

F-Secure. F-Secure.	SecureWorks®	TREND MICRO™
		

OVERVIEW

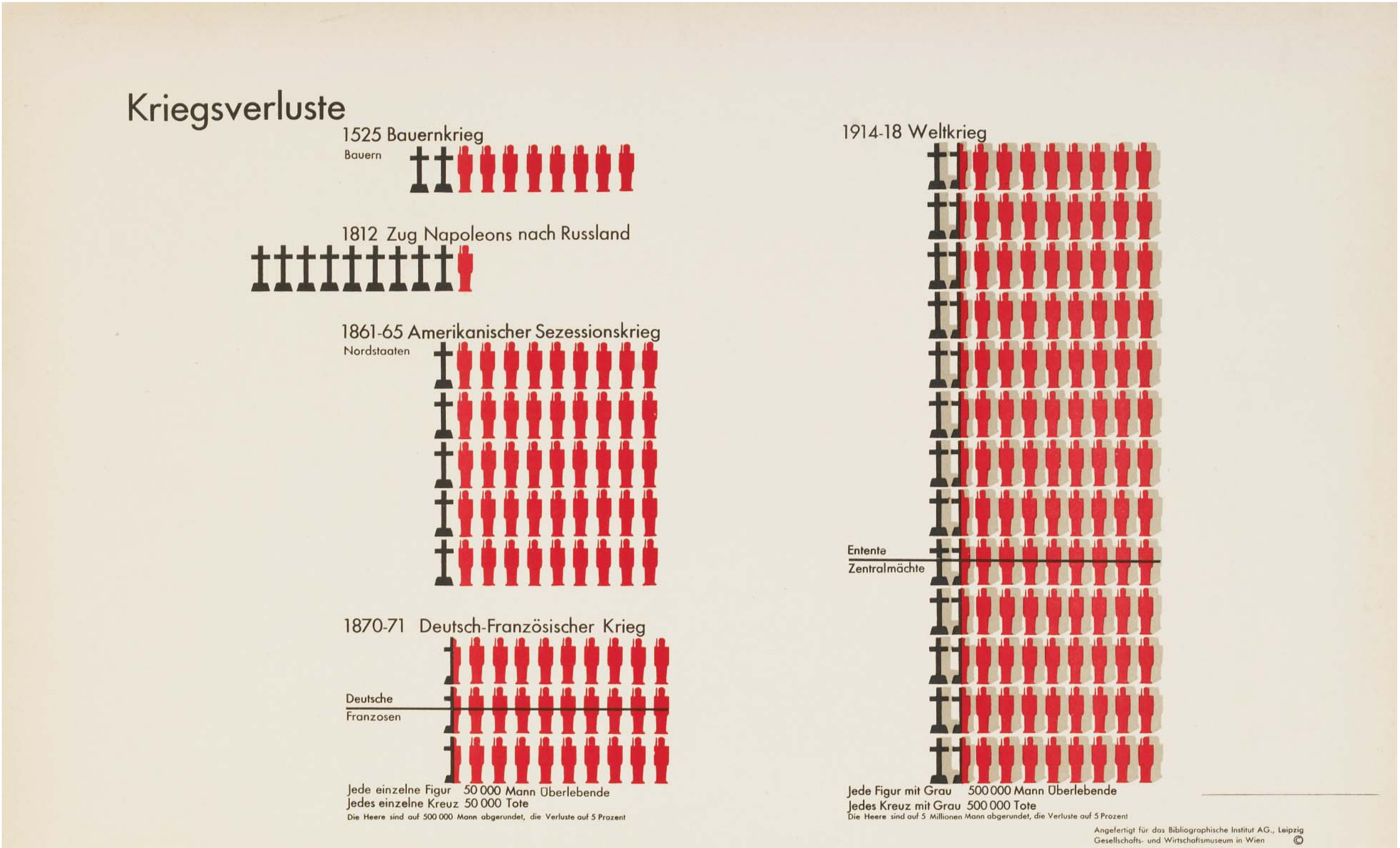
- Motivation
- Target Group
- 5 Minutes of design background for techies
- Tools
- DNSviz and Flows

Some design background

- One of the leading persons in the field right now: **Edward Tufte**

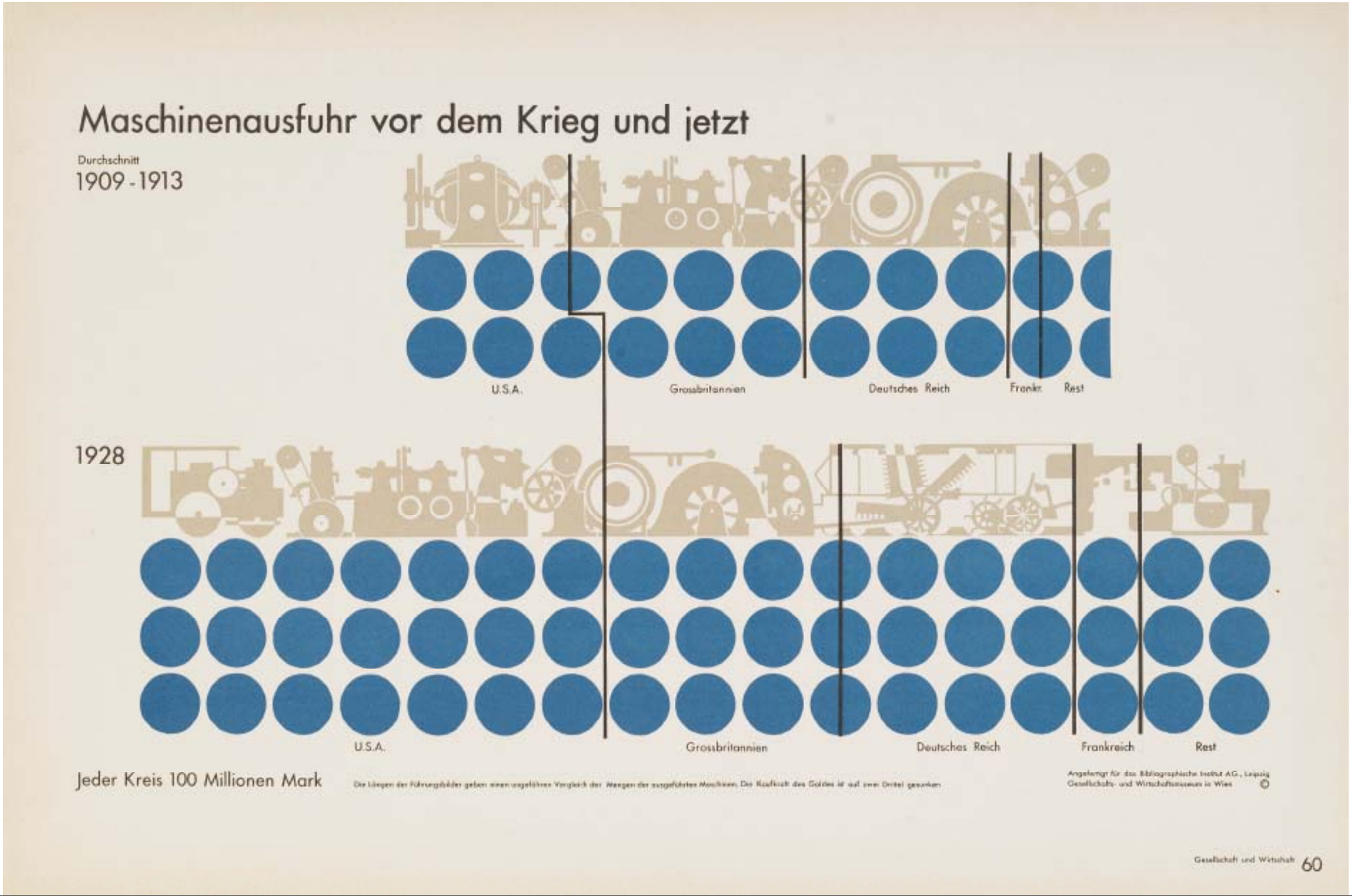
- Learned a lot from **Otto Neurath**: “Isotypes” in Vienna in the early 1900s
- First invention of “**icons**”. Idea: educate the illiterate working class population in Europe w.r.t basic economics relationships

Otto Neurath's Isotype

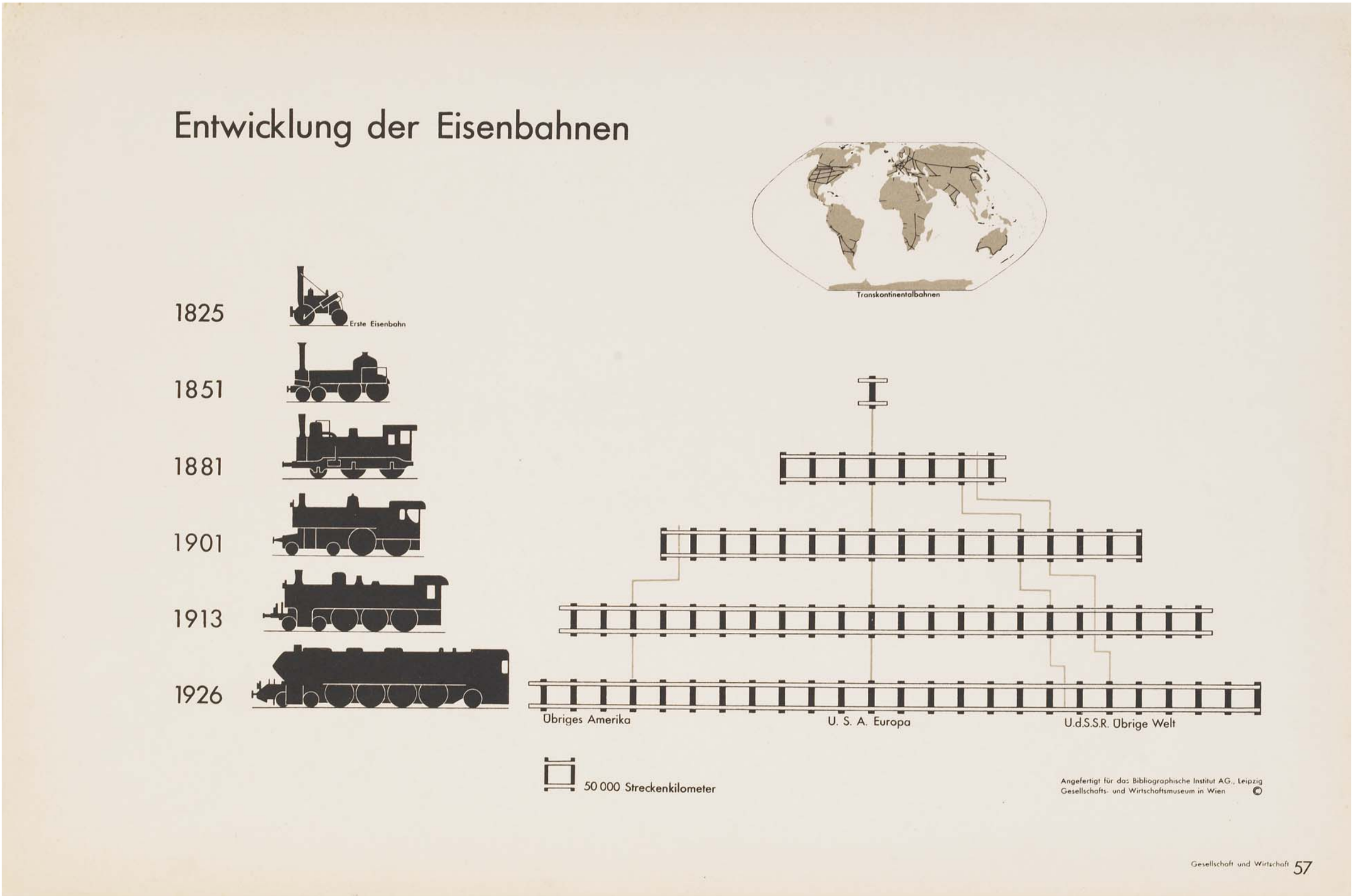


Otto Neurath's Isotype

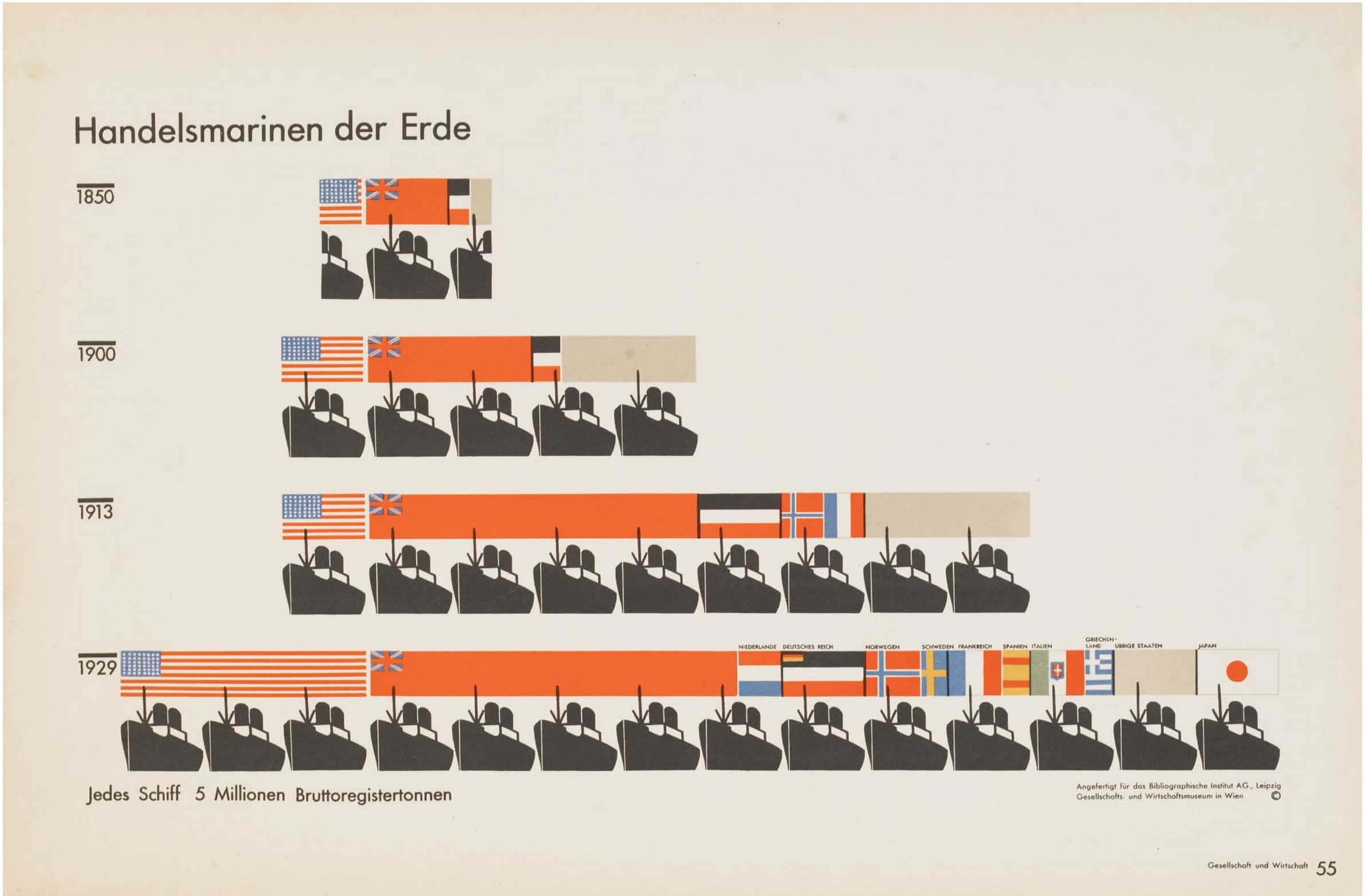
Otto Neurath's Isotype



Otto Neurath's Isotype

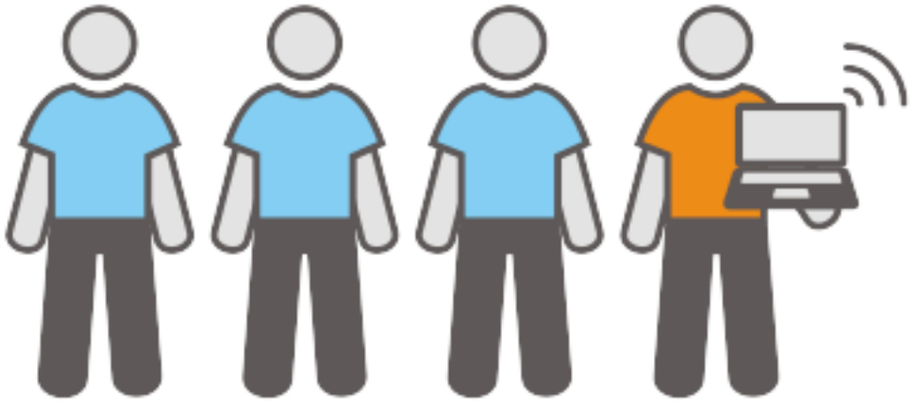


Otto Neurath's Isotype



Otto Neurath's Isotype

Modern day examples



How many people are connected to the internet?

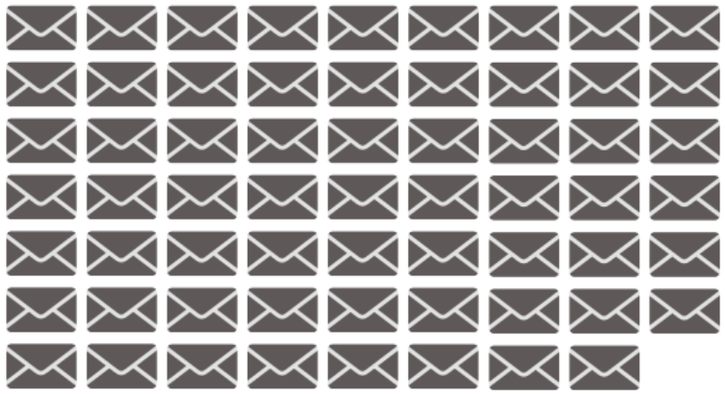
In 2009, we had approximately 6,767,805,208 people on the earth

from those, 1,802,330,457 have internet access which makes it 26.6% or one quarter of the world population.

(source: http://www.internetworldstats.com/stats.htm)

Modern day examples

Handling, sending, receiving and filtering out spam



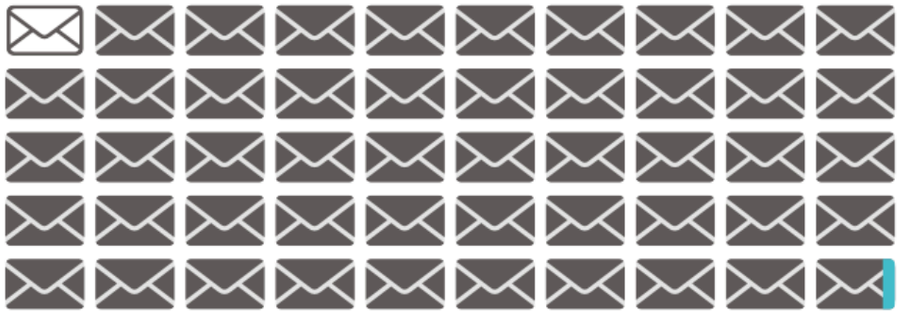
Each mail represents 1 trillion spam mails

takes up the power of 2.4 million US houses

Each house represents 100 000 US houses

or 1 nuclear power plant

An average nuclear power plant produces 2500 Mwatts



Good Emails 2%

Spam 98%

Orders from Spam 0,02%

US household **per month**

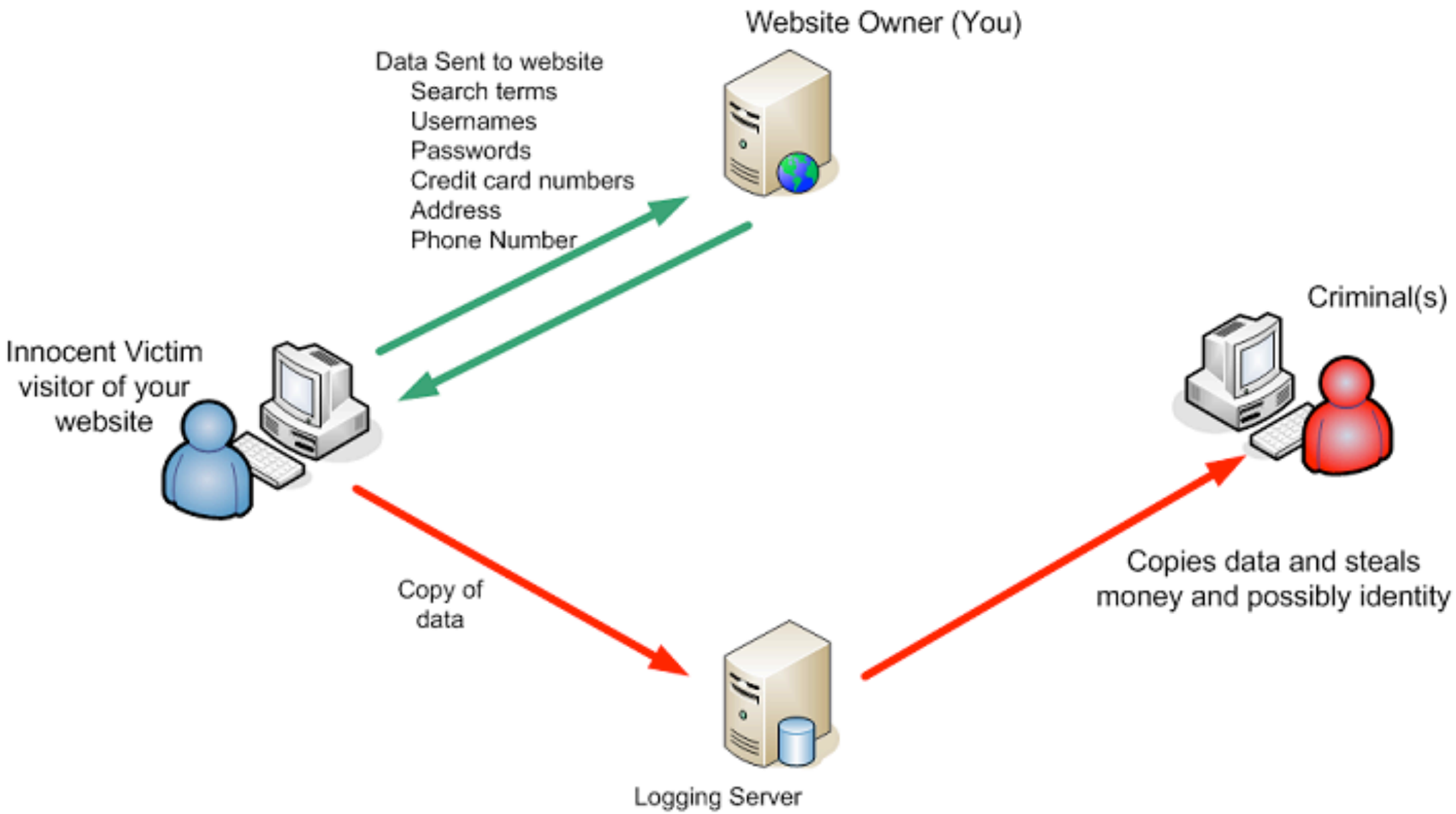
$ Each sign represents $1000

spammer **per day**

waste of resources by spam and a spammer's income

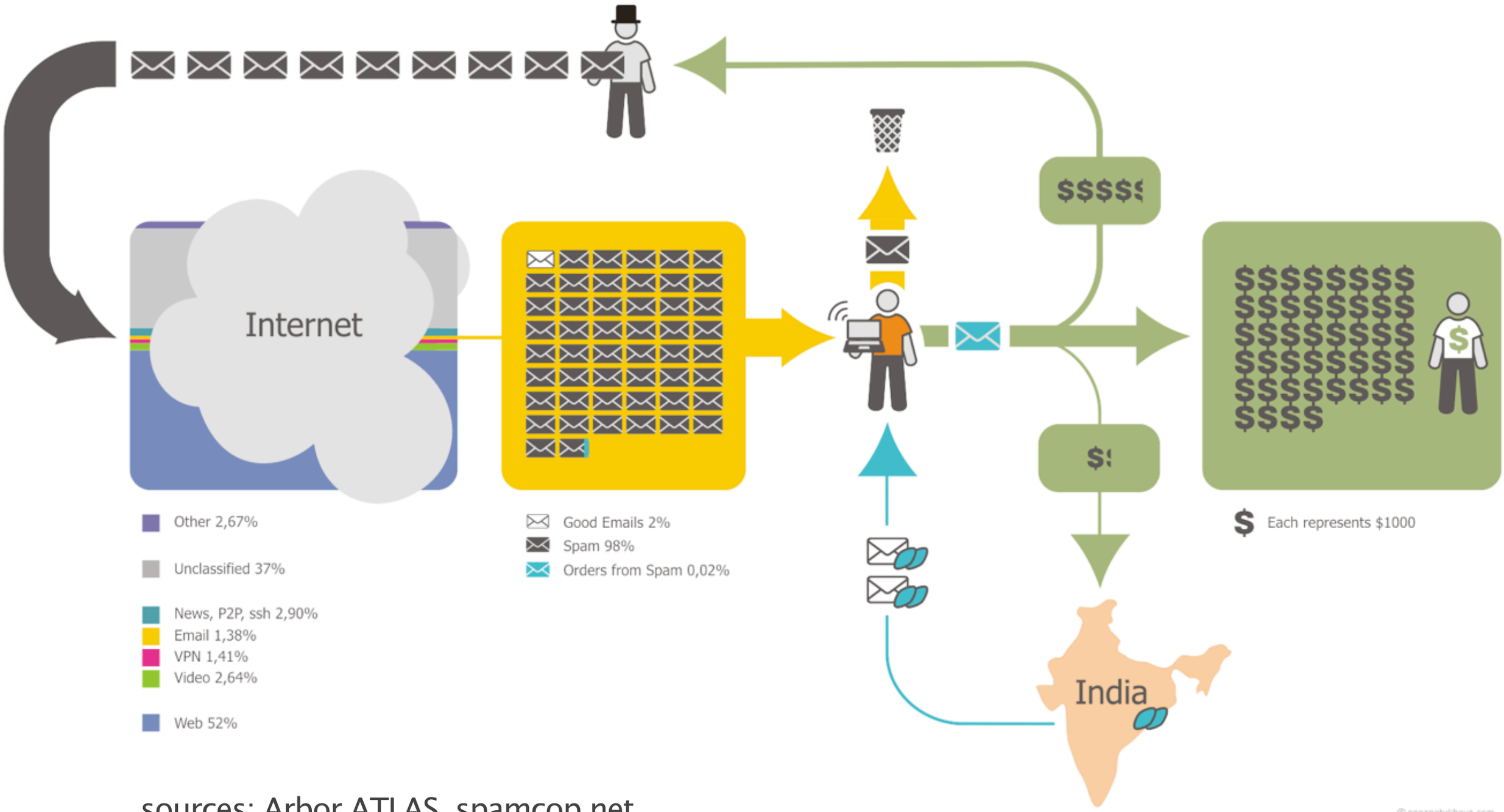
(source: McAffee CO2 Impact of Spam + NY Times)

Making users understand IT security



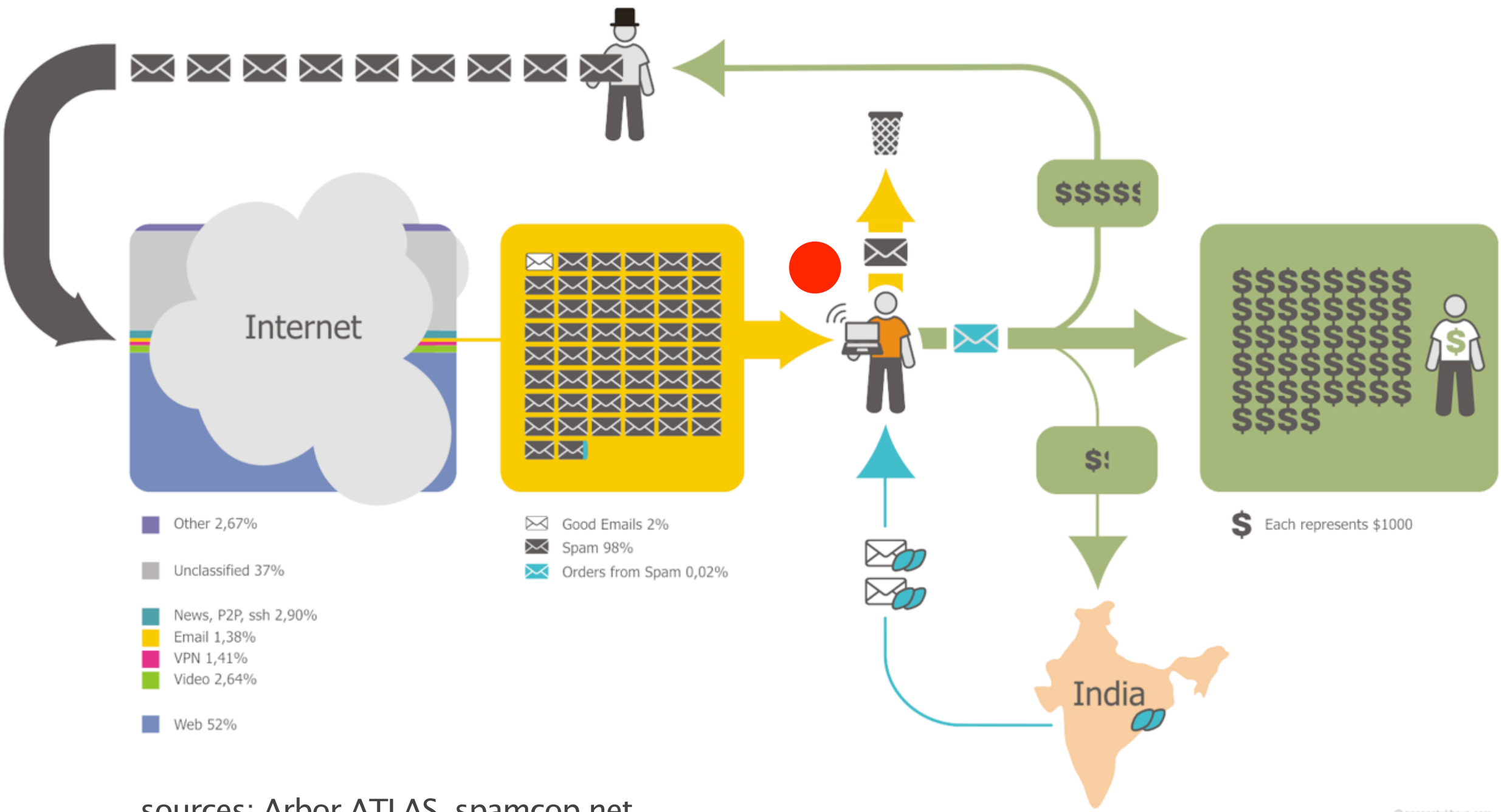
source: AusCERT http://www.auscert.org.au/9536

Making users understand IT security



sources: Arbor ATLAS, spamcop.net

Making users understand IT security



sources: Arbor ATLAS, spamcop.net

OVERVIEW

- Motivation
- Target Group
- 5 Minutes of design background for techies
- Tools
- DNSviz and Flows

TOOLS

CERT.at

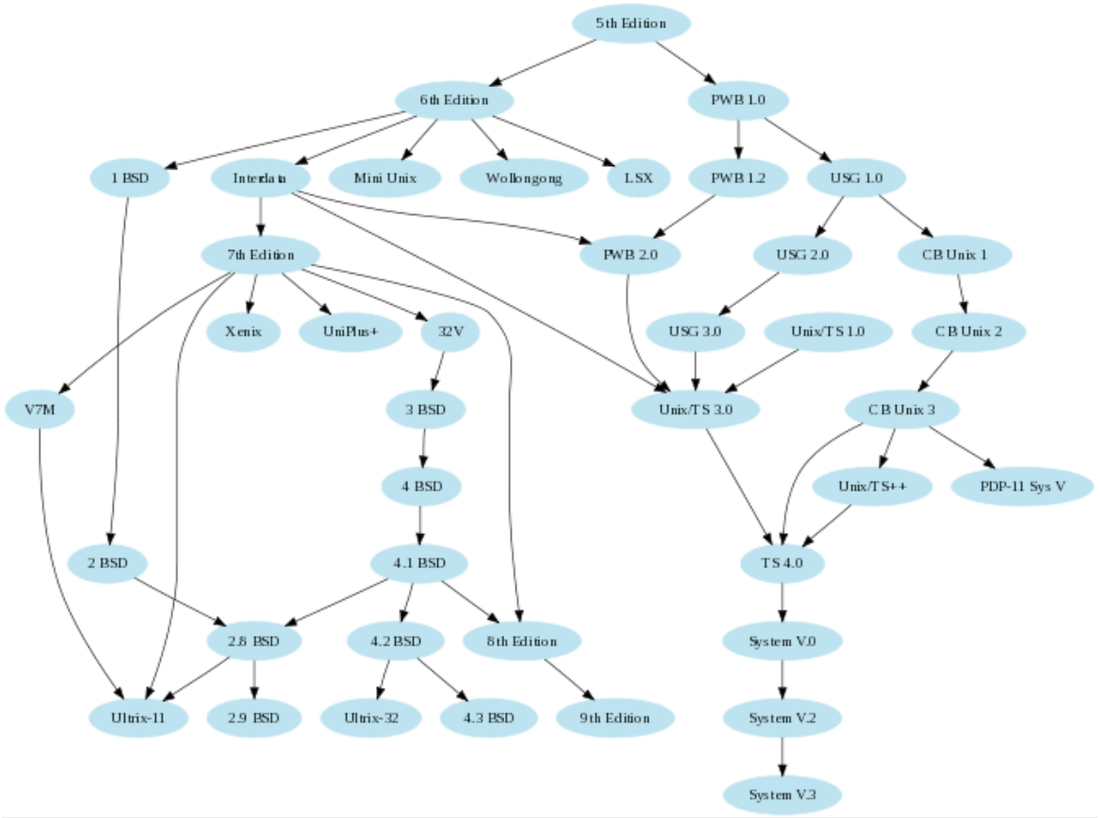
- Graphviz
- Maxmind GeoIP
- Logster
- Unix wizardry
- Google Earth
- Gapminder
- Processing.org
- Outlook: Davix

Graphviz

- based on research @ AT&T Labs
- Syntax:

```
digraph {
  A -> B;
  A -> C [label="foo"];
}
```

```
dot -T png -o out.png \
   inputfile.dot
```



Maxmind GeoIP

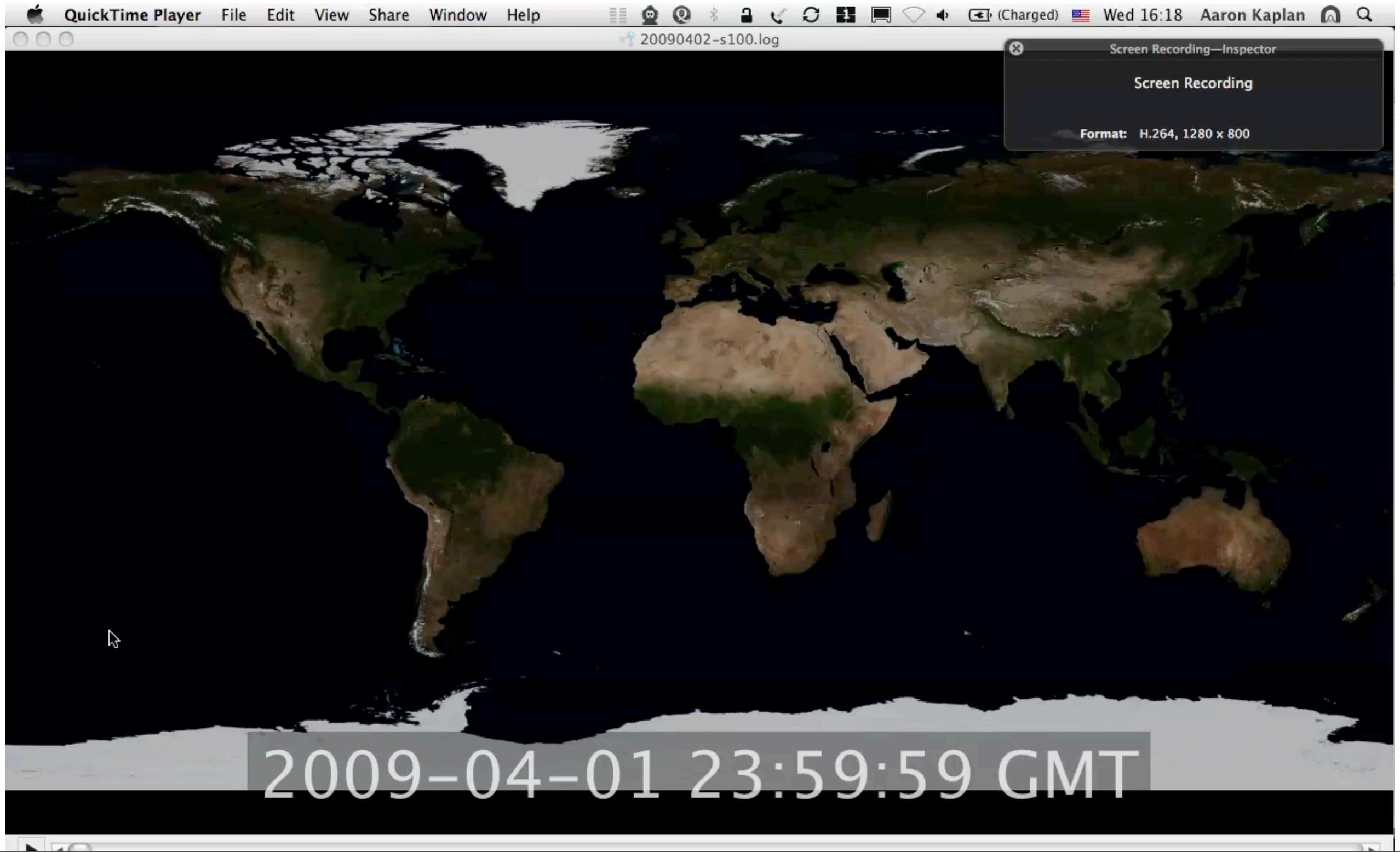
- http://maxmind.com
- cityLite DB is usually enough

```
my $gi = Geo::IP->open("/home/aaron/GeoLiteCity.dat",
GEOIP_STANDARD);
# ------------------ functions ------------------
# input : ip
# output: array [countrycode, city, lat, lon]
sub ip2geolocate {
    my $ip = $_[0];
    my @ret;
    my $record = $gi->record_by_name("$ip");
    @ret = ( $record->latitude , $record->longitude) ;
    return(@ret);
}
```

Tools: Logster

- Logster by Clarified Networks
- Input format: Apache log file format
- output: movie. Can screen capture

Tools: Logster



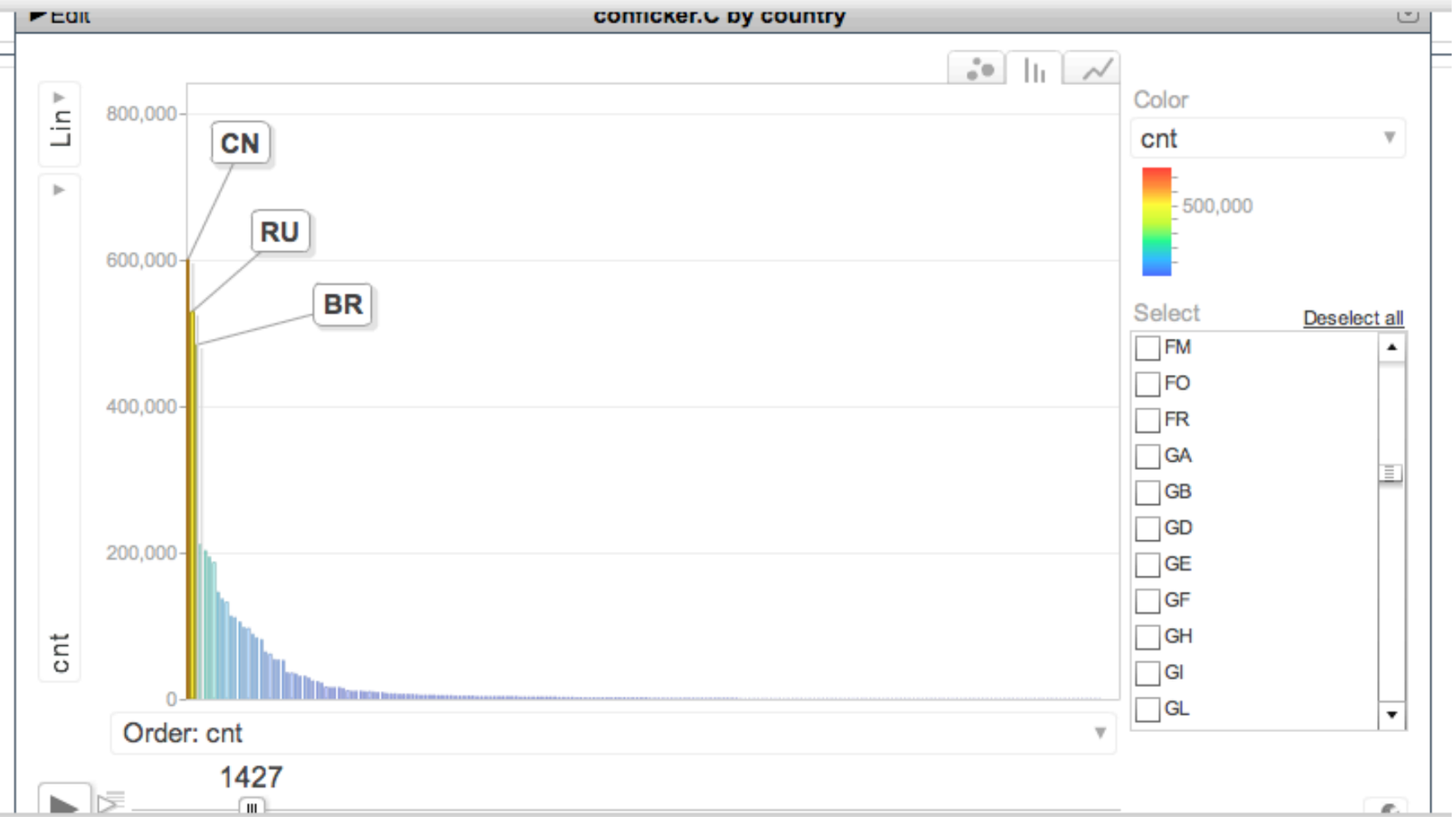
Tools: Gapminder

Google docs conficker hits by country

Autosaved on 3:31 PM GMT+02:00

File Edit View Insert Format Form Tools Help

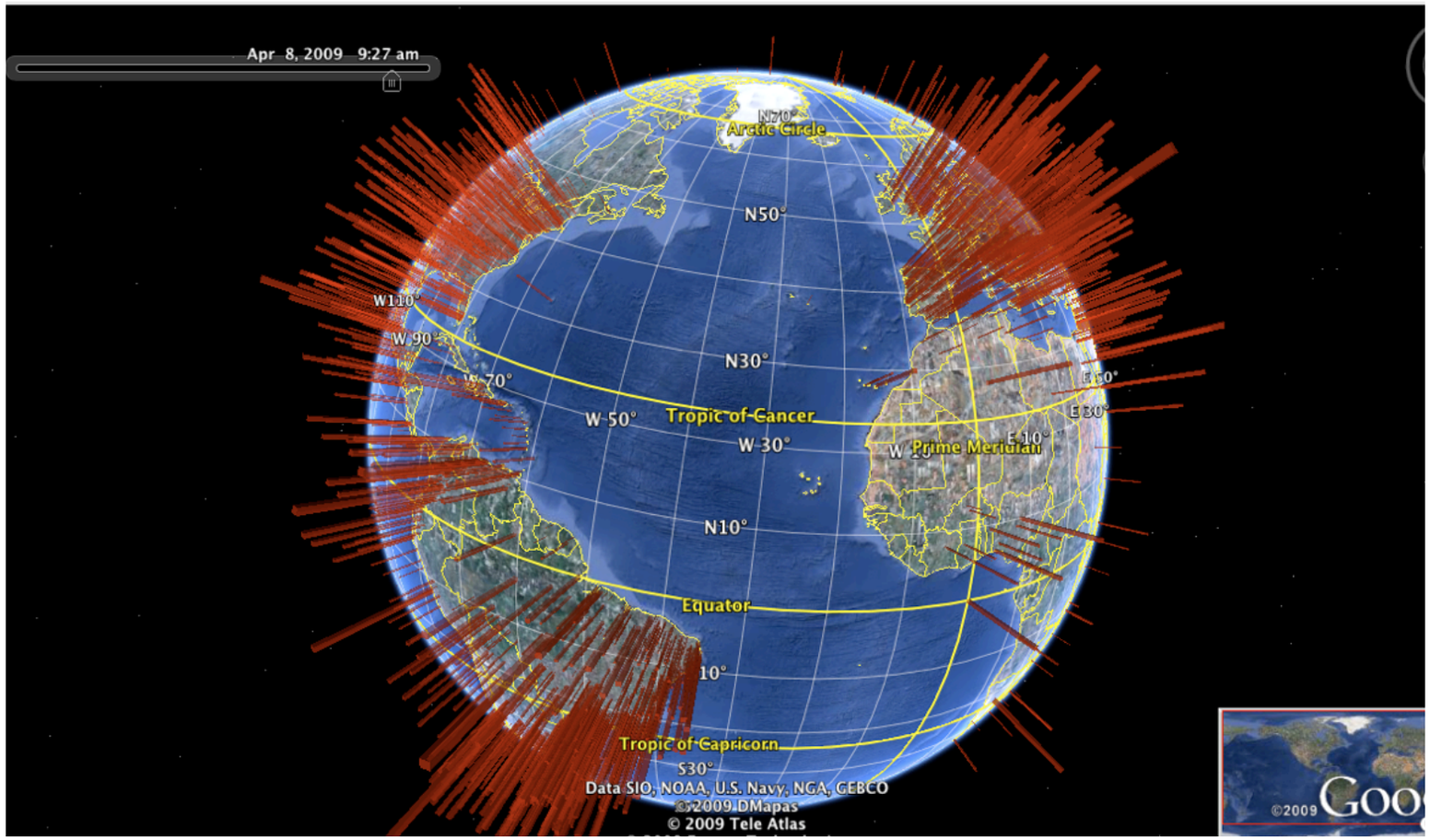
	country	date	cnt	cnt2
2	MX	1000	4	1
3	KR	1001	2	1
4	BR	1002	2	1
5	VE	1003	1	1
6	CA	1004	1	1
7	KH	1005	1	1
8	RO	1006	1	1
9	TT	1007	1	1
10	RU	1008	1	1
11	PK	1009	1	1
12	AR	1010	1	1
13	ES	1011	1	1
14	CN	1012	1	1
15	US	1013	1	1
16	PH	1014	1	1
17	EC	1015	1	1
18	CN	1016	762166	1
19	BR	1017	644646	1
20	RU	1018	582881	1
21	VN	1019	255845	1
22	UA	1020	245734	1
23	IN	1021	233908	1
24	KR	1022	230627	1
25	ID	1023	210525	1
26	IT	1024	177121	1



Add Sheet | Sheet 1 | software piracy

Tools: Google Earth

- format: KML. Well documented.
- Head section
- Placemarks



Tools: Unix filters

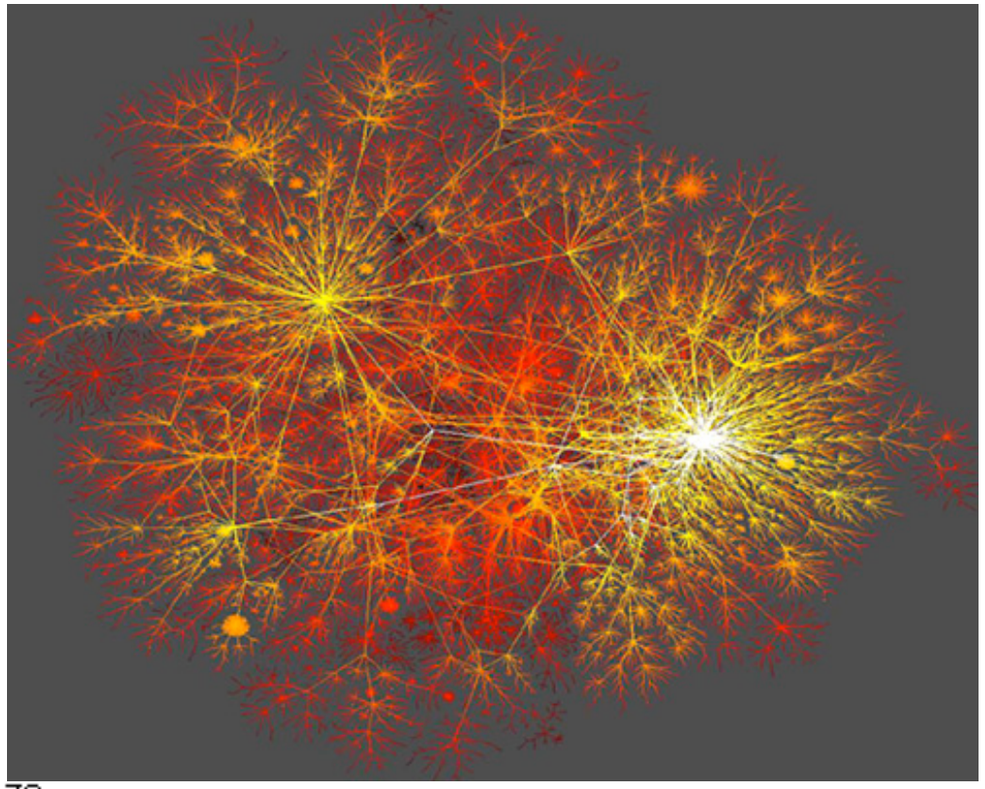
- Use Unix tools to quickly get a grasp of the trends

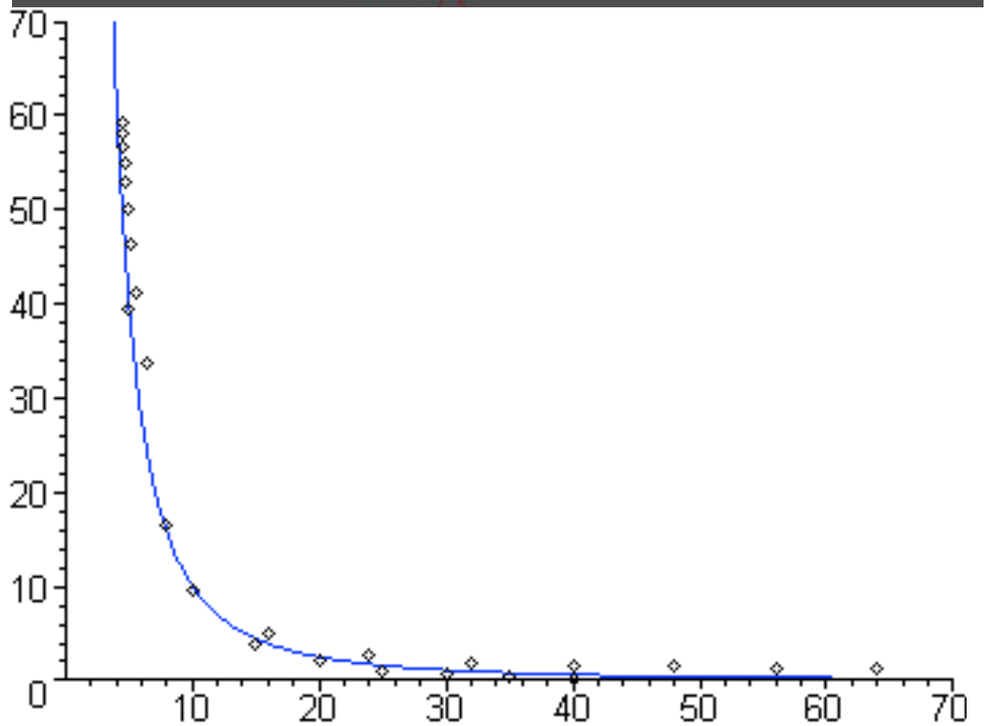
- cut –d “;” –f 5 | sort | uniq –c | sort –rn
- gnuplot

plot “myfile.csv” using 1 with boxes

Scale-freeness

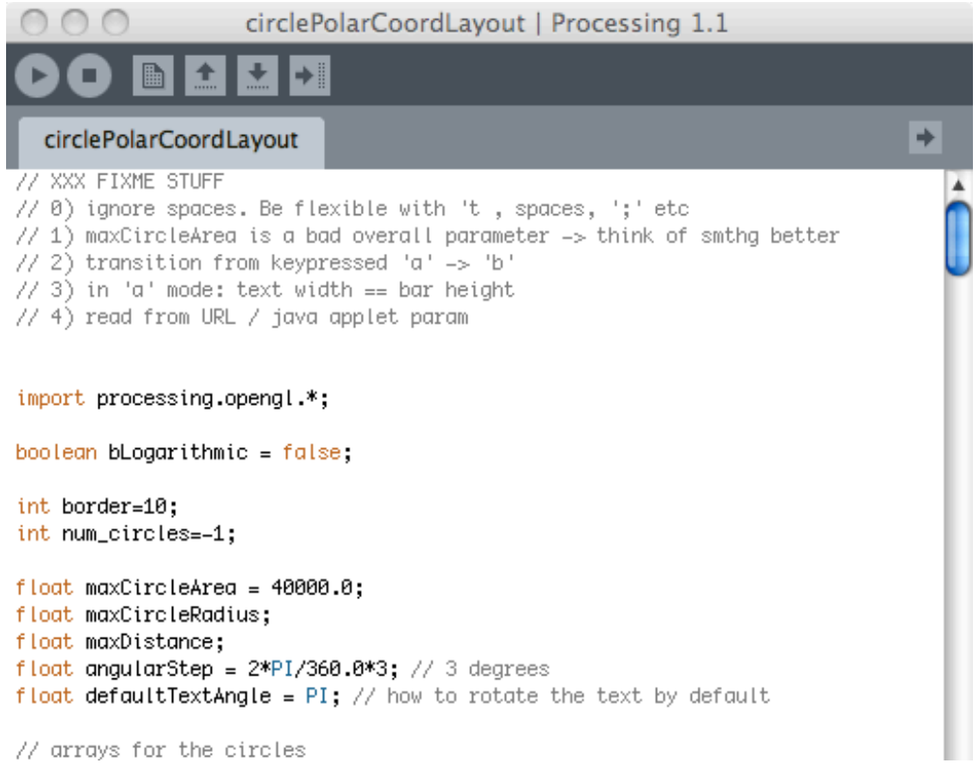
- Albert-László Barabási made them famous.
- Some property is distributed by an inverse power law formula:
  $P(k) \sim 1/k^{\gamma}$ $(2 < \gamma < 3)$
- “fractal”
- “internet-ish”
- “biological”
- “not again-ish”



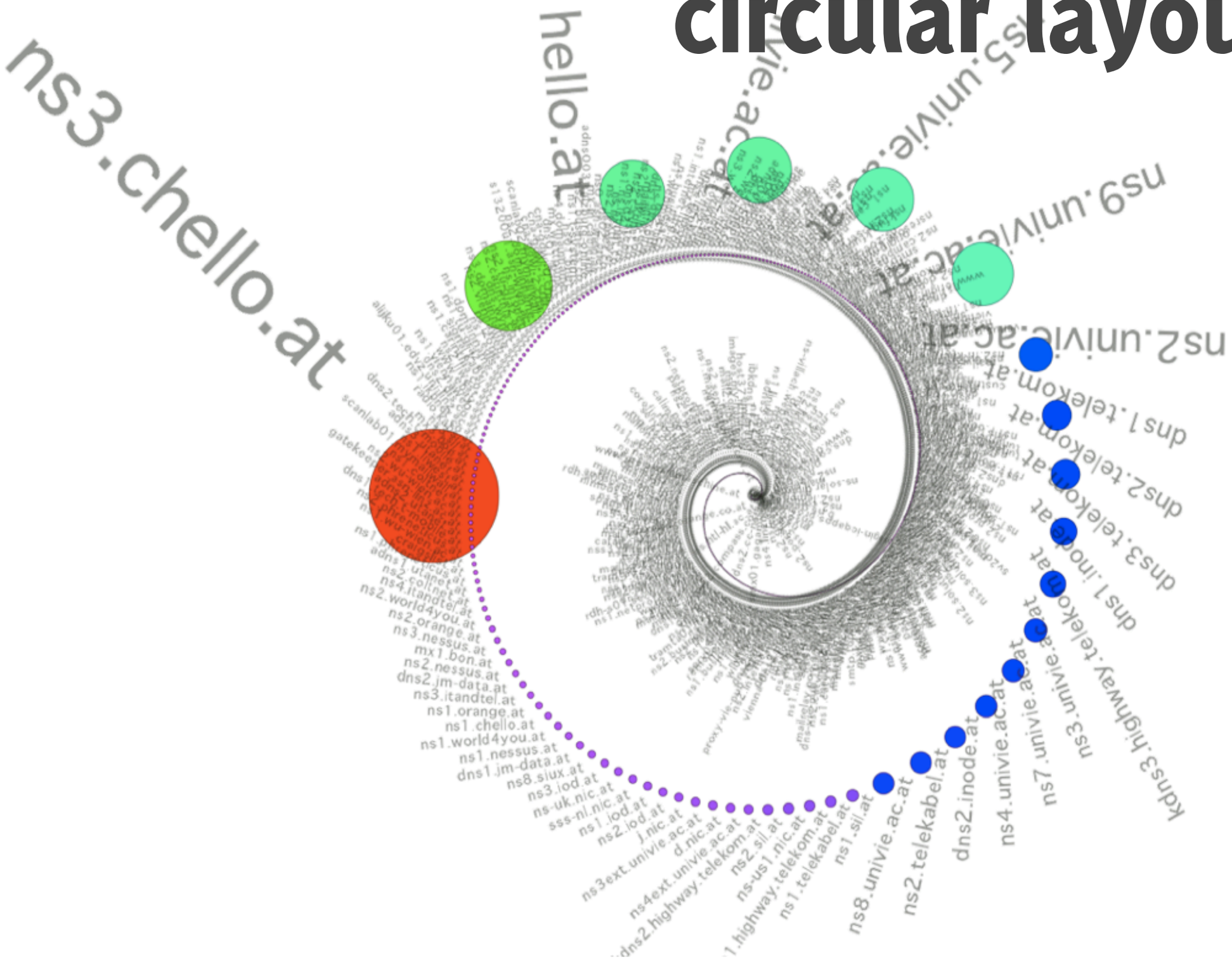


TOOLS: Processing.org

- Invented by Ben Fry, Casey Reas @MIT
- Basic idea: easy IDE for Java 3D/OpenGL programing. Lots of examples, openprocessing.org
- Includes a rich API:
  - sockets
  - DB connections
  - serial I/O
  - sound, etc.



Processing example: circular layout

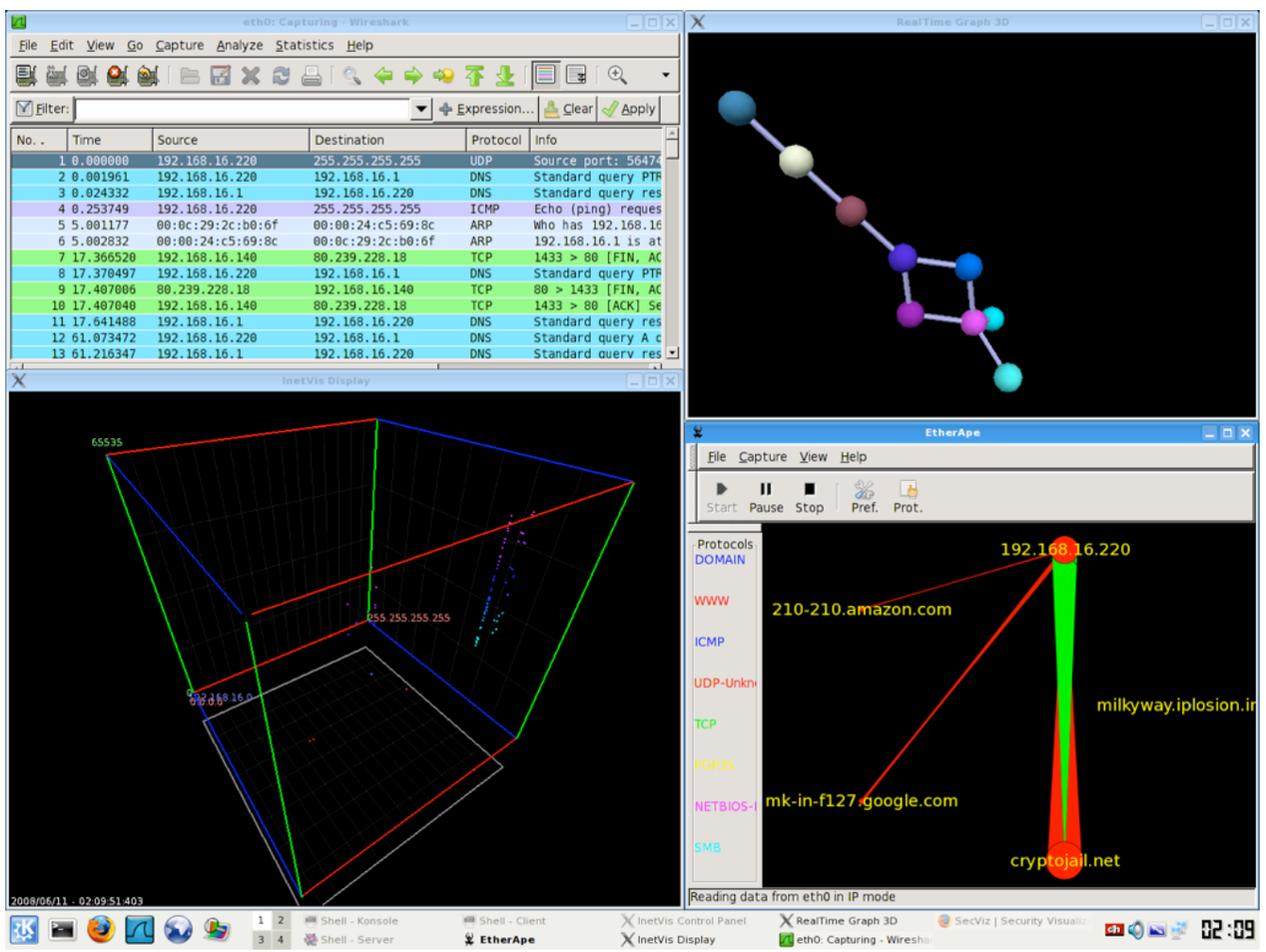


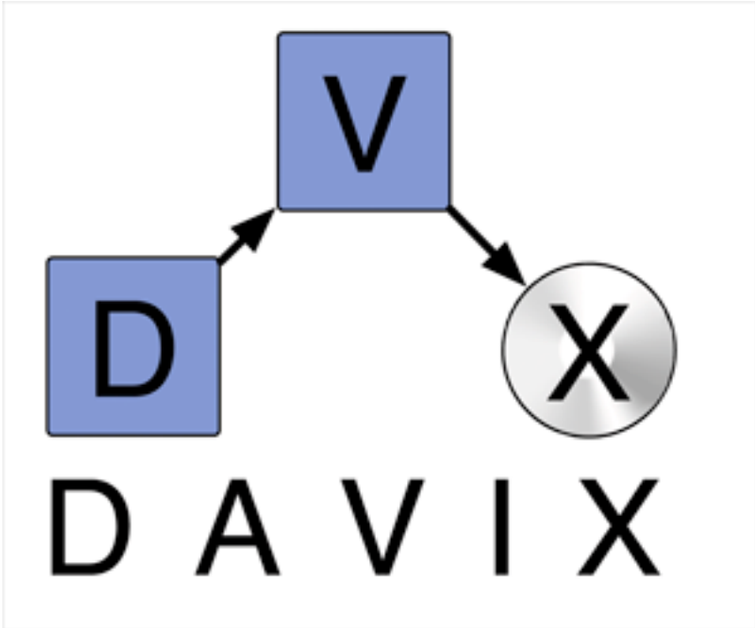
Other processing Examples

- Esfera
- Registrymon

Outlook: DAVIX

- ISO image on http://www.secviz.org



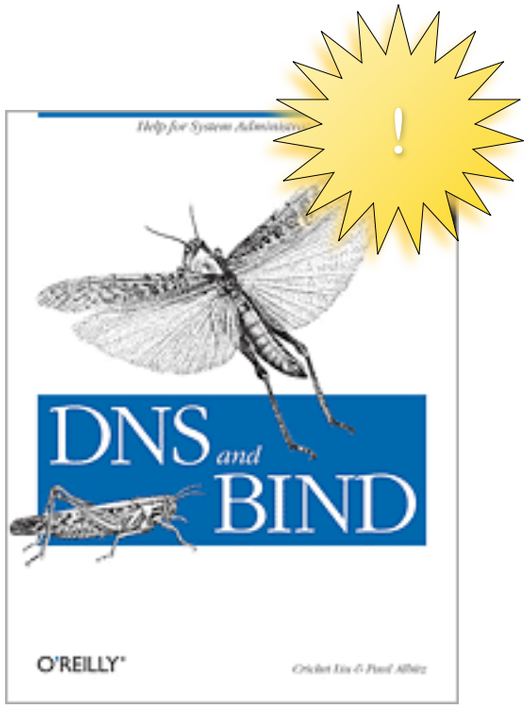


OVERVIEW

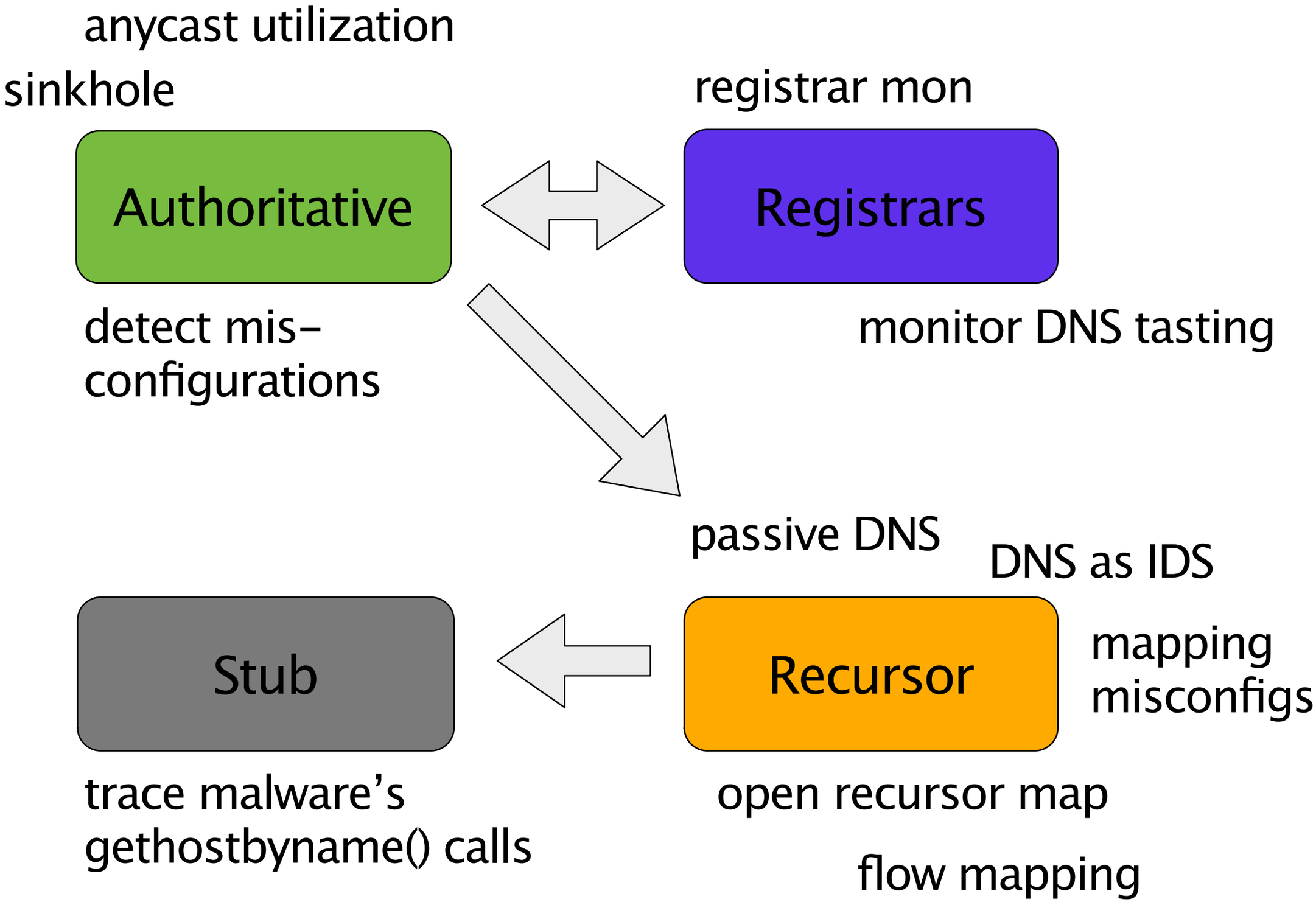
- Motivation
- Target Group
- 5 Minutes of design background for techies
- Tools
- DNSviz and Flows

DNS

DNS



DNS for IT security viz



Idea list DNS and IT security viz

- Authoritative Nameservers:
  - you don't see much at the authoritative NS
  - TTLs are wrong
  - other misconfigurations
  - But – idea: Spam for a newly registered domain should be a spike. But can we filter it out from the noise?
  - Anycast effectiveness (c.f. CAIDA paper)
  - **Sinkholing** works!

Idea list DNS and IT security viz

- Registry / Registrars:
  - from registry's perspective: track your resellers. How "clean" is a registrar?
  - monitor DNS tasting. Find domain catchers.
- Recursors:
  - passive DNS
  - DNS "netflow" ("passive DNS++")
  - DNS as IDS (<– Google talk today!)
  - log/visualize localhost/bogus/bogon answers!
  - fastflux
  - monitor TXT record answers
  - map (maliciously) open recursors

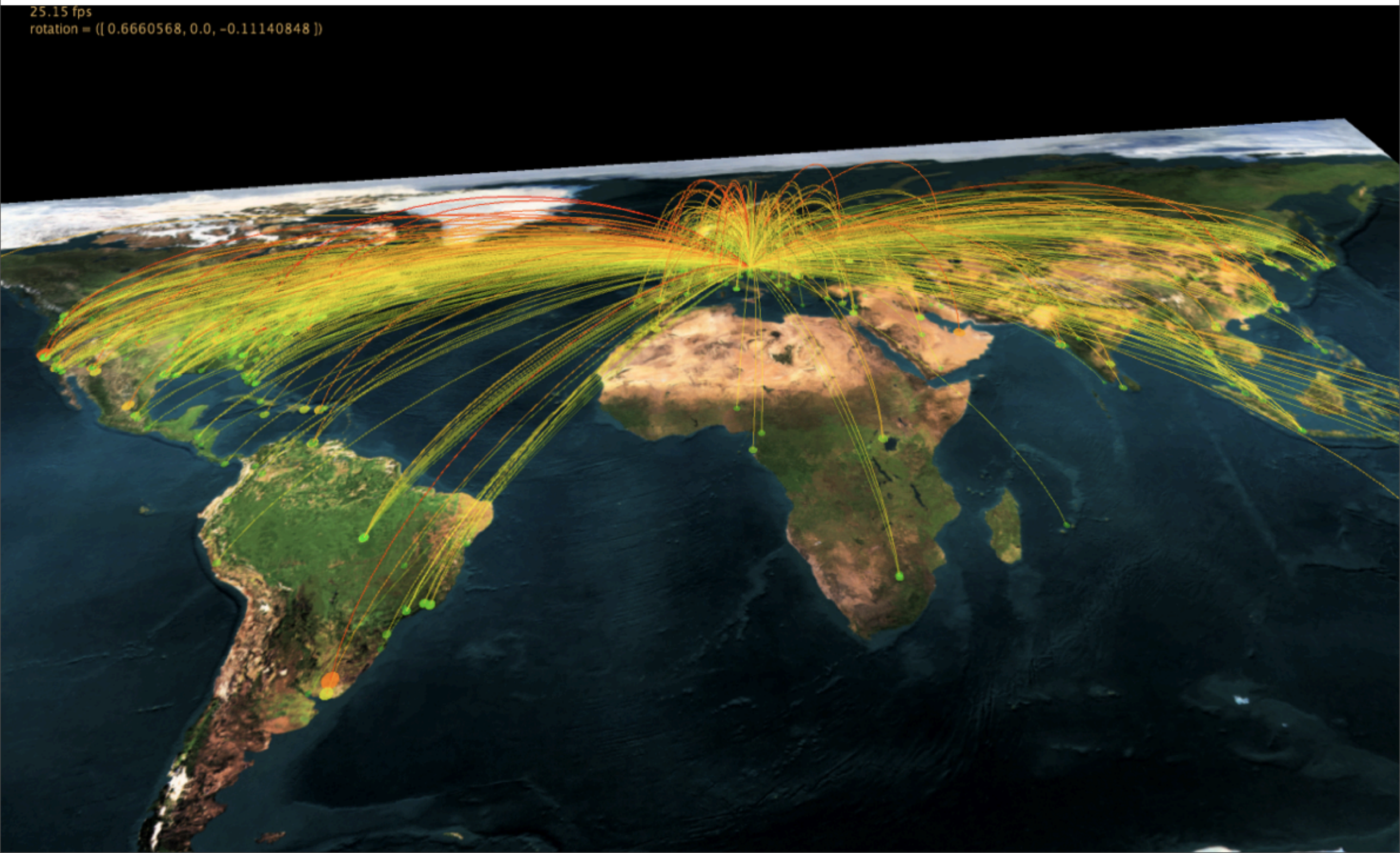
Idea list DNS and IT security viz

- Stub resolvers:
  - trace malware's gethostbyname() syscalls (Minibis)
  - idea: outgoing FW + logster for the stub / PC

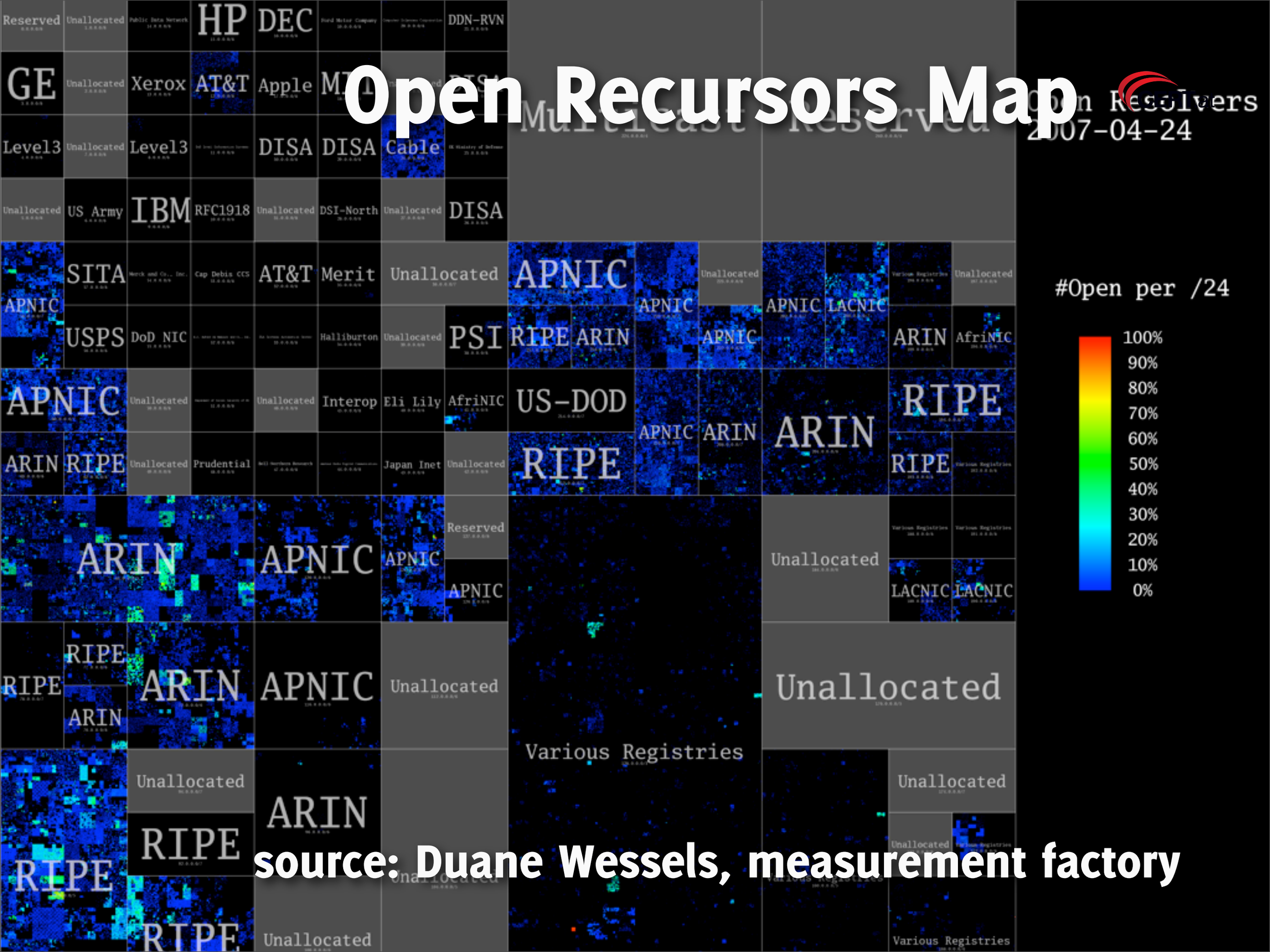
DNS netflow example

- Done in Processing
- data: tcpdump –ni eth0 port 53 and src = ...
- filter out local queries
- find all nameservers which are queried
- aggregate(!) + transform via perl script to...
- format:
  lat srcip; lon srcip; lat dstip; lon dstip; amount
- aggregation factor:
  - aaron@lair:~$ wc –l outgoing–without–ports.txt
    - 100000 outgoing–without–ports.txt
  - aaron@lair:~$ wc –l flows–lat–lon.txt
    - 28948 flows–lat–lon.txt
- source code demo?

DNS netflow



Open Recursors Map



source: Duane Wessels, measurement factory

SIG? Data exchange?

annapetukhova.com, processing.org, Otto Neurath

annapetukhova.com, processing.org, Otto Neurath