i’m wes.. i’m here to help you share data.

collectiveintel.org

china is going to steel
all your warez.

your bios is phoning home.

all of our natural gas pipes are going to blow up no one can hack in their sleep...

... and be on the look out for some guy who works for “twitter” who might be trying to bump ugglies with your mobile ... then send all my info to nigerian scammers who will try to get  me to fly to europe so they can haz all my monies...

we’re screwed.

# whoami

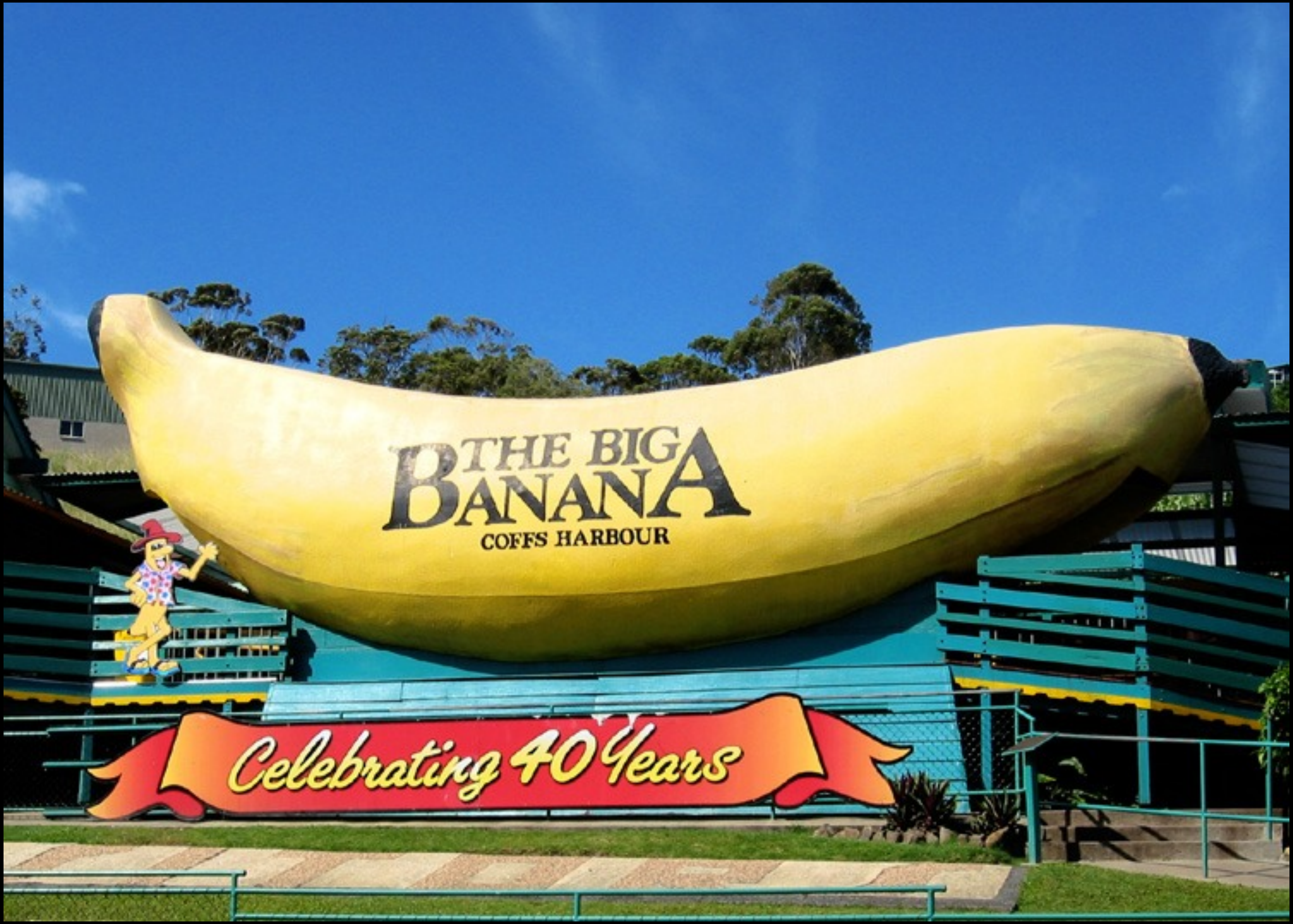
- we’re the north american .edu CSIRT
- we operate a large (very active) trust community
- we build tools (CIF)
- we travel, foster relationships (here i am!)
- we drink beer (it’s not a good talk, unless your hung-over)

# some context

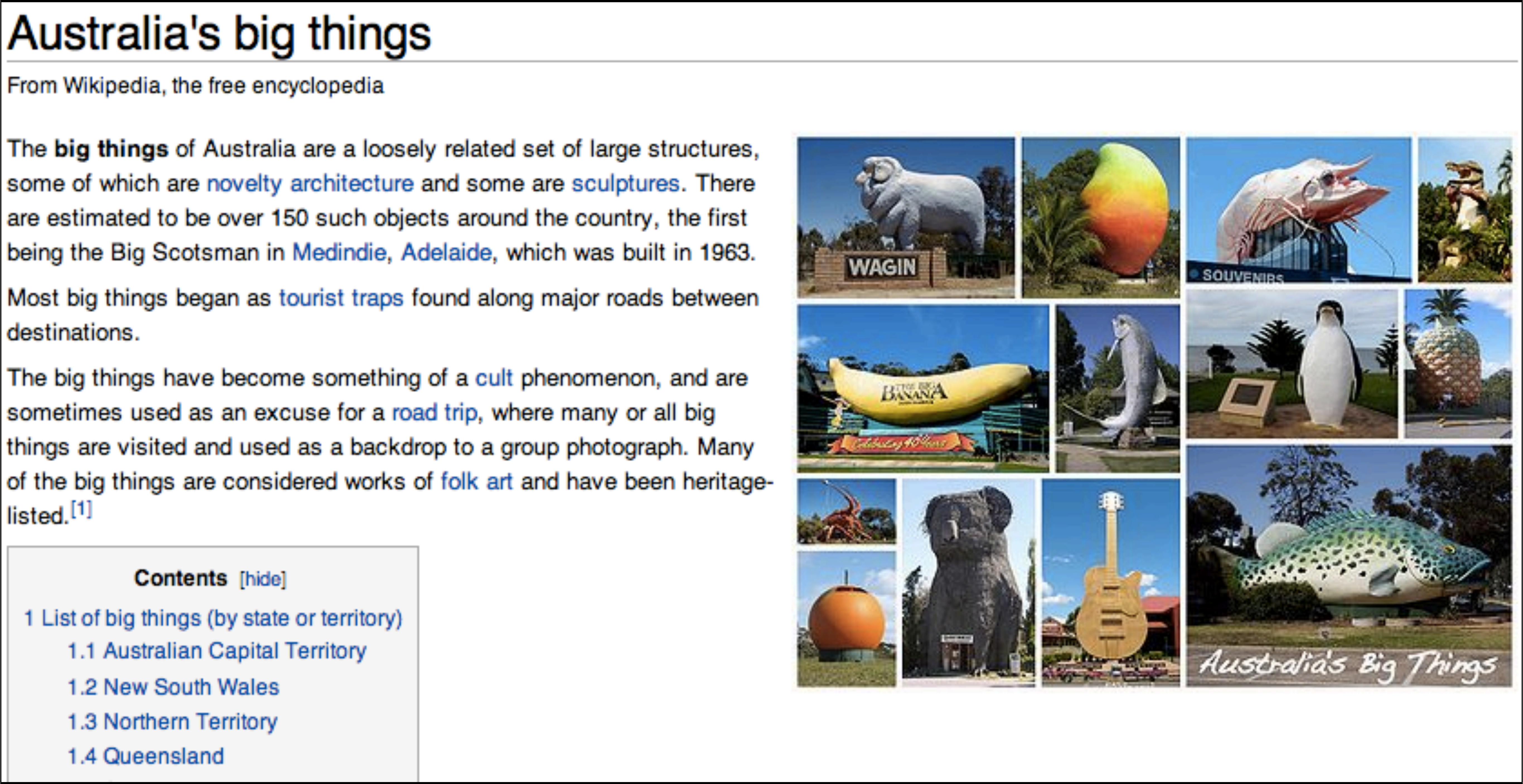
- mostly north america (few scattered throughout other english speaking countries)
- mega v4 and v6 allocations
- mega connectivity (10G - 100G), inter-continental
- BYOD: since the beginning of the inter-webs.
- culturally diverse (students, staff, operations, regions, etc)

# big-data: solved!
# now what do i do?

# (the next ten years)


THE BIG
BANANA
COFFS HARBOUR
Celebrating 40 Years

Trident Fish Bar @ The Big Prawn
Fresh Prawns & Oysters • Fish & C
Seafood Packs • Burgers • Local Coffee



# Australia's big things

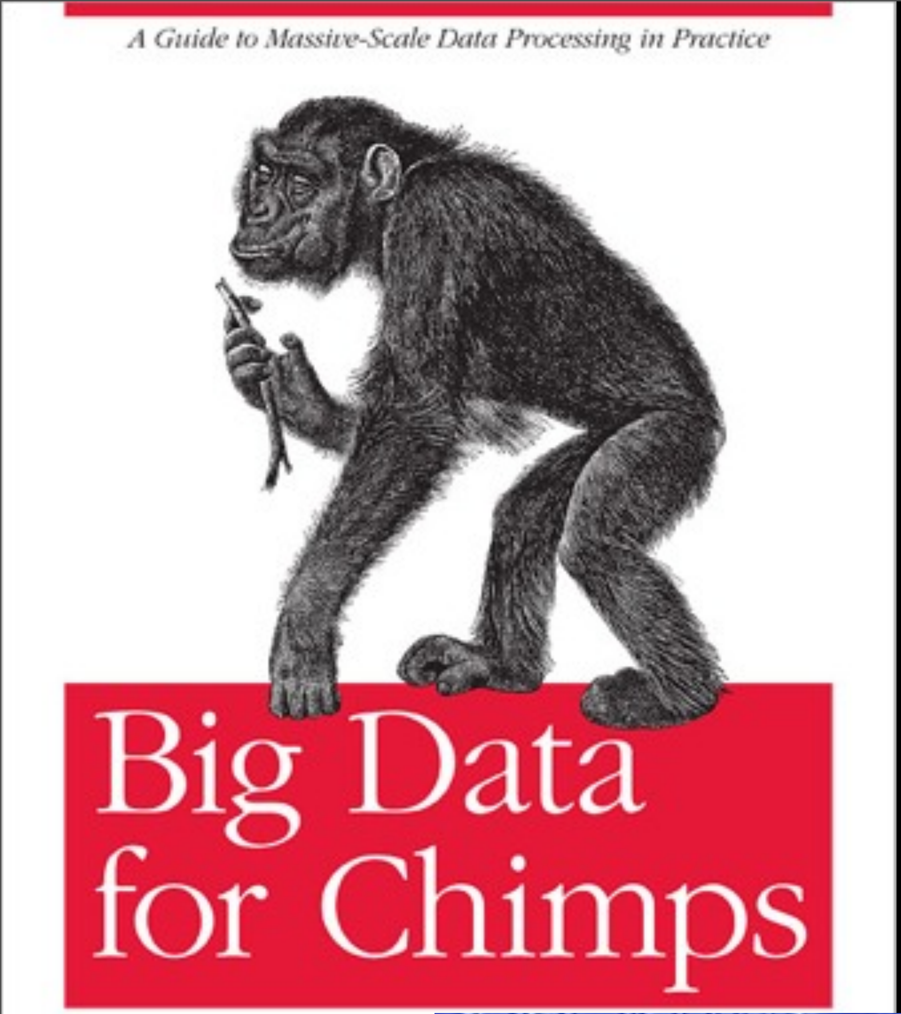
From Wikipedia, the free encyclopedia

The **big things** of Australia are a loosely related set of large structures, some of which are novelty architecture and some are sculptures. There are estimated to be over 150 such objects around the country, the first being the Big Scotsman in Medindie, Adelaide, which was built in 1963.

Most big things began as tourist traps found along major roads between destinations.

The big things have become something of a cult phenomenon, and are sometimes used as an excuse for a road trip, where many or all big things are visited and used as a backdrop to a group photograph. Many of the big things are considered works of folk art and have been heritage-listed.[1]

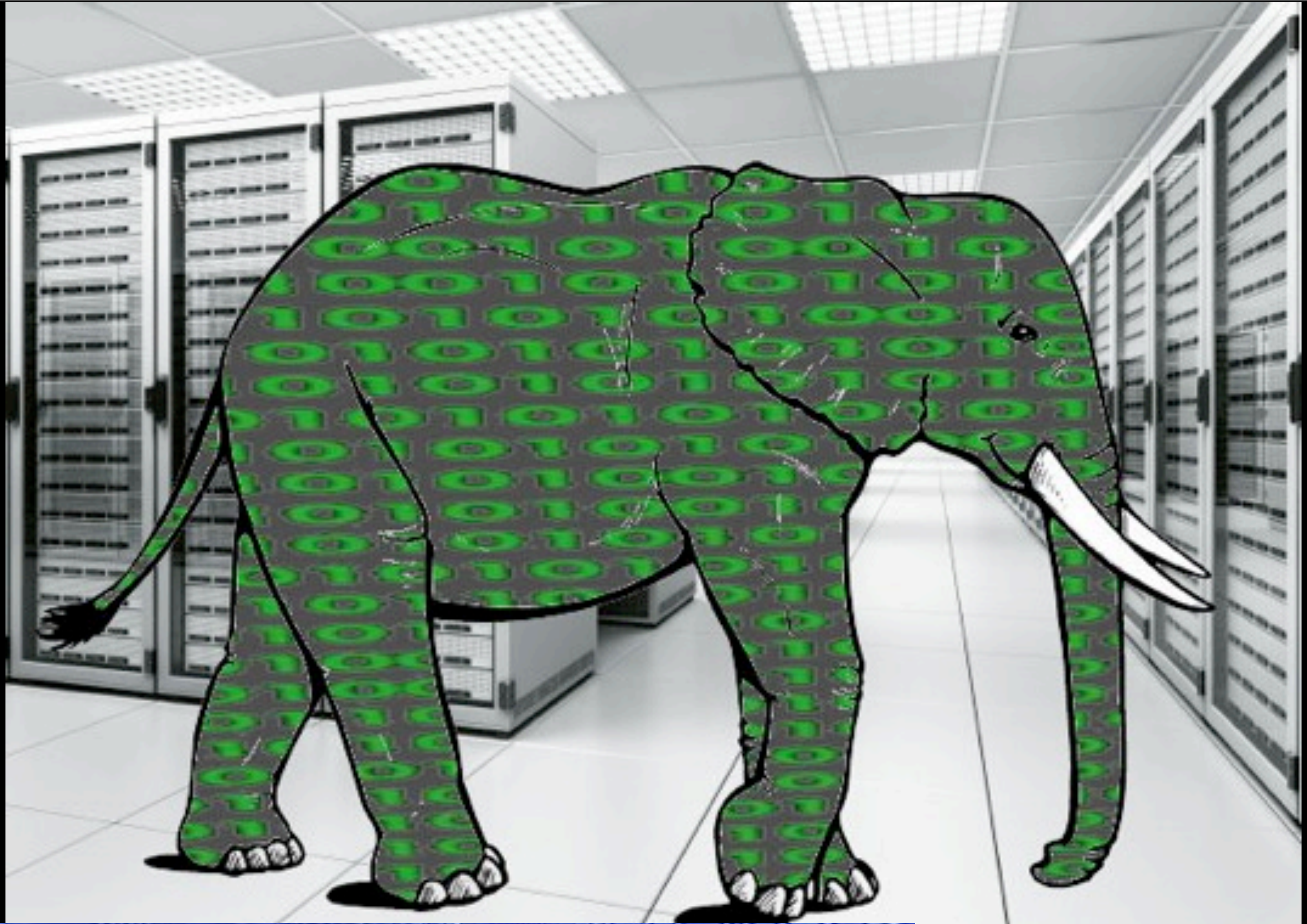
**Contents** [hide]

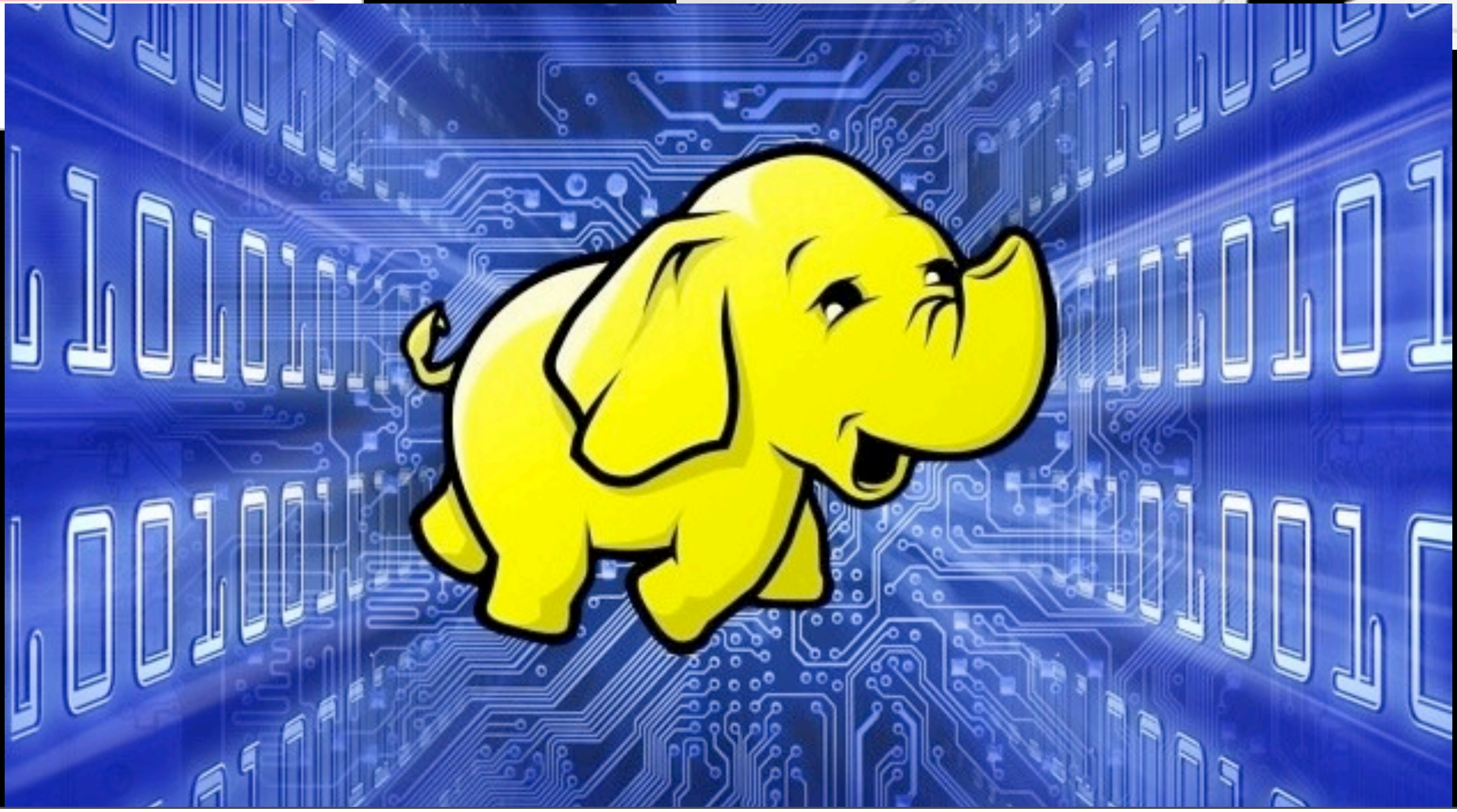


A Guide to Massive-Scale Data Processing in Practice

Big Data for Chimps

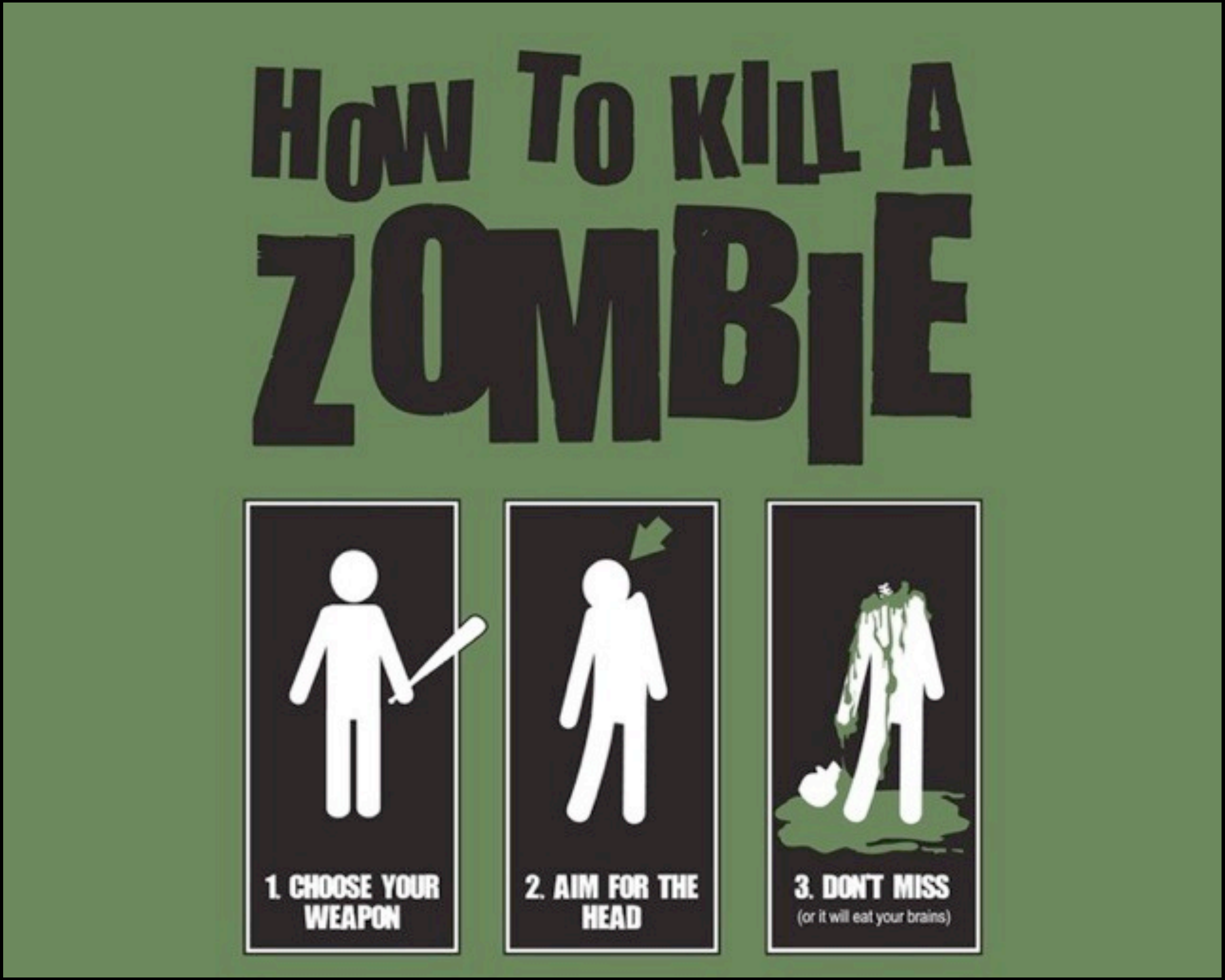
O'REILLY

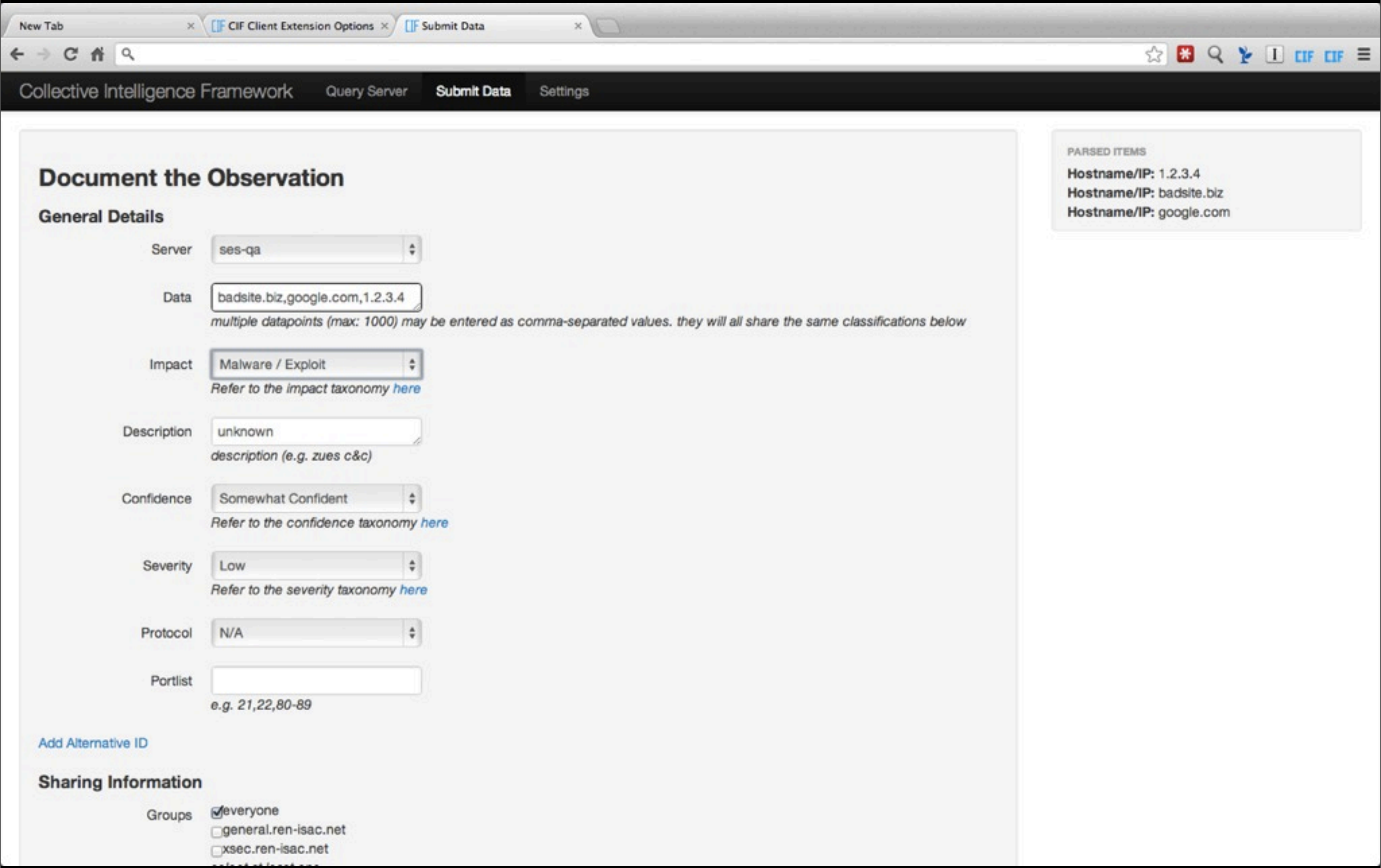




wait, what about the last ten years?

# collectiveintel.org




New Tab
CIF Client Extension Options
Submit Data
Collective Intelligence Framework
Query Server
Submit Data
Settings

## Document the Observation

### General Details

Server: ses-qa

Data: badsite.biz,google.com,1.2.3.4

*multiple datapoints (max: 1000) may be entered as comma-separated values. they will all share the same classifications below*

Impact: Malware / Exploit

*Refer to the impact taxonomy here*

Description: unknown

*description (e.g. zues c&c)*

Confidence: Somewhat Confident

*Refer to the confidence taxonomy here*

Severity: Low

*Refer to the severity taxonomy here*

Protocol: N/A

Portlist:

*e.g. 21,22,80-89*

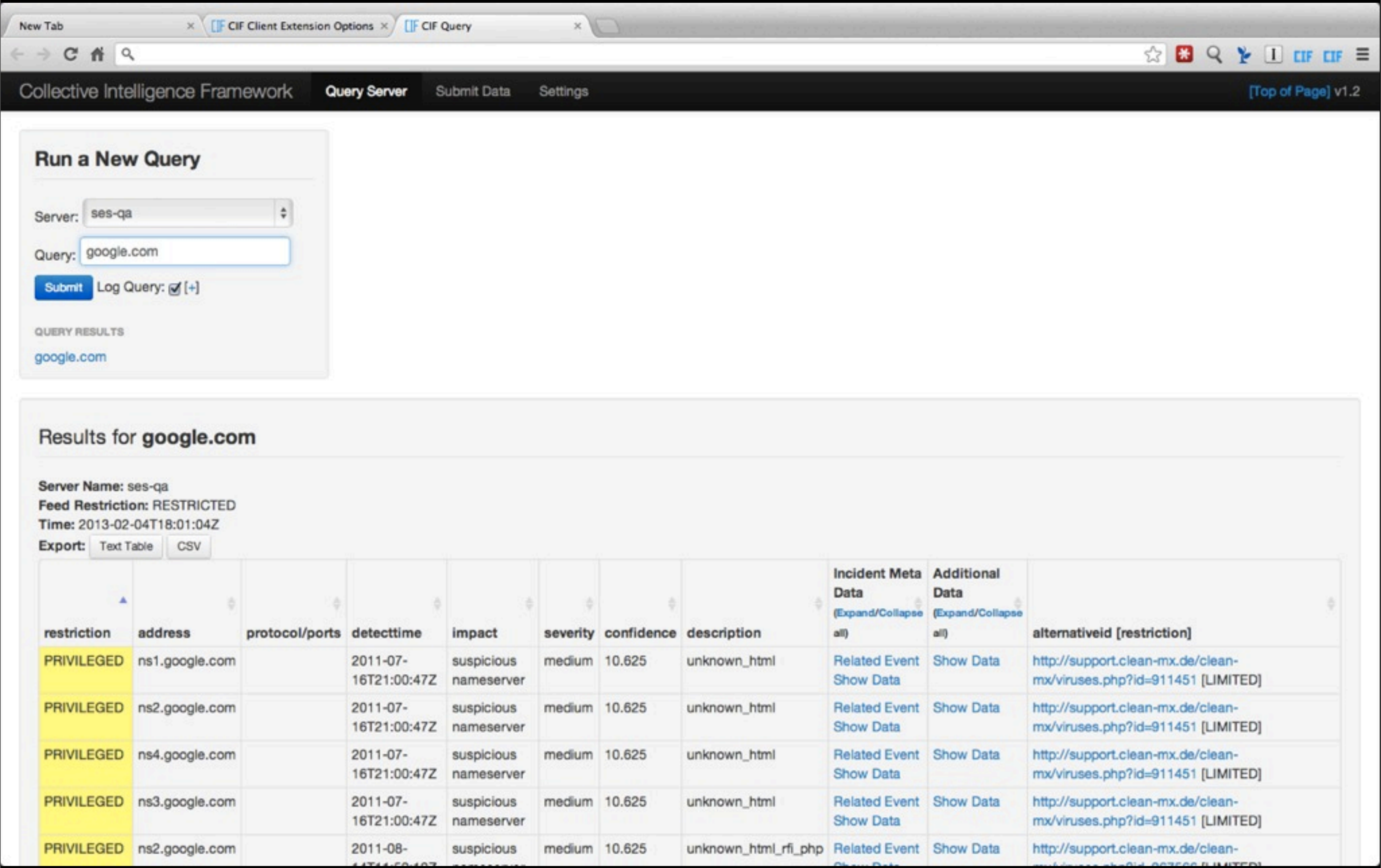
Add Alternative ID

### Sharing Information

Groups:
☑ everyone
□ general.ren-isac.net
□ xsec.ren-isac.net

PARSED ITEMS

**Hostname/IP:** 1.2.3.4
**Hostname/IP:** badsite.biz
**Hostname/IP:** google.com



## Run a New Query

Server: ses-qa

Query: google.com

Submit Log Query: ☑ [+]

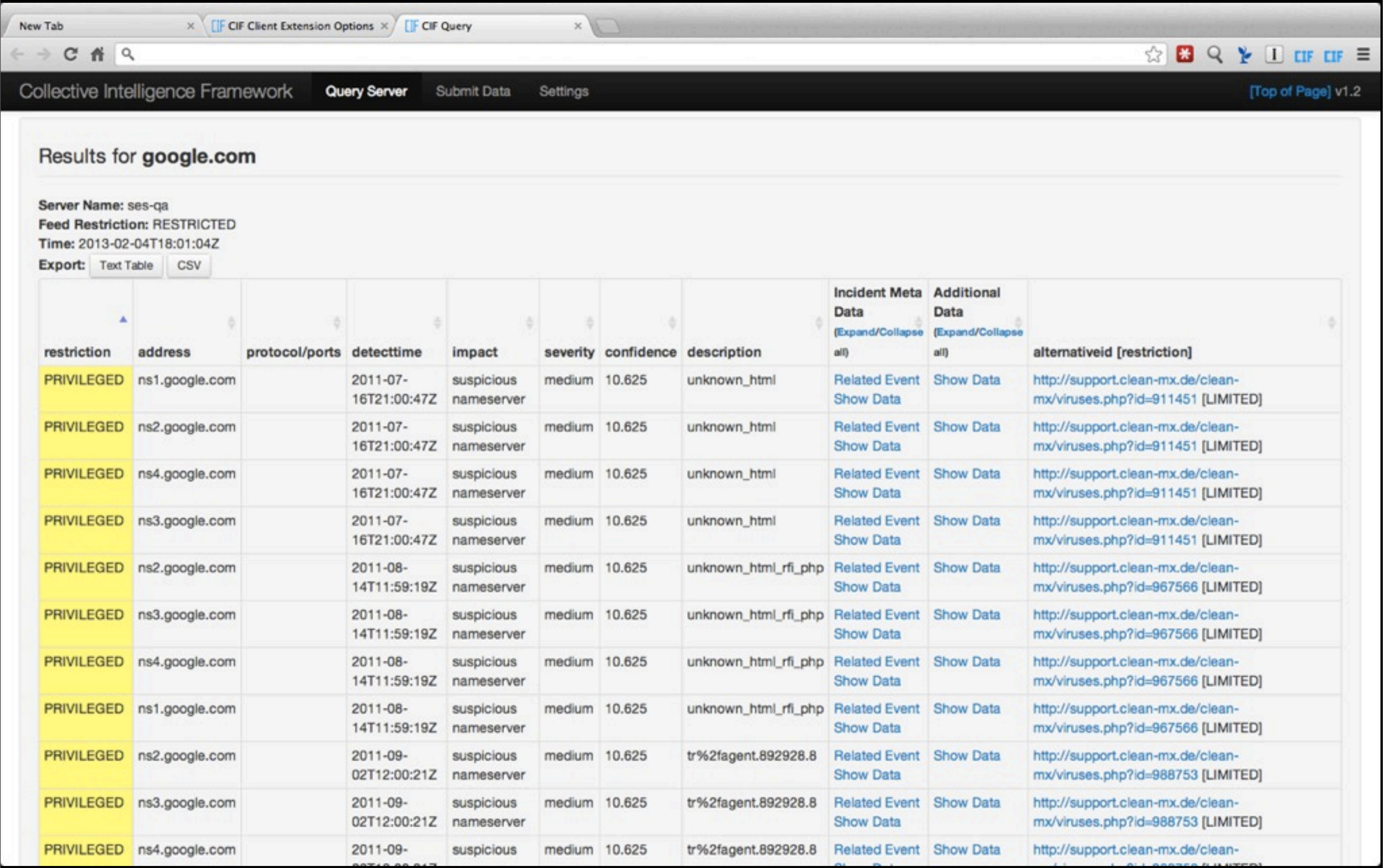
QUERY RESULTS

google.com

## Results for **google.com**

**Server Name:** ses-qa
**Feed Restriction:** RESTRICTED
**Time:** 2013-02-04T18:01:04Z
**Export:** Text Table CSV

| restriction | address | protocol/ports | detecttime | impact | severity | confidence | description | Incident Meta Data (Expand/Collapse all) | Additional Data (Expand/Collapse all) | alternativeid [restriction] |
|---|---|---|---|---|---|---|---|---|---|---|
| PRIVILEGED | ns1.google.com | | 2011-07-16T21:00:47Z | suspicious nameserver | medium | 10.625 | unknown_html | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=911451 [LIMITED] |
| PRIVILEGED | ns2.google.com | | 2011-07-16T21:00:47Z | suspicious nameserver | medium | 10.625 | unknown_html | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=911451 [LIMITED] |
| PRIVILEGED | ns4.google.com | | 2011-07-16T21:00:47Z | suspicious nameserver | medium | 10.625 | unknown_html | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=911451 [LIMITED] |
| PRIVILEGED | ns3.google.com | | 2011-07-16T21:00:47Z | suspicious nameserver | medium | 10.625 | unknown_html | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=911451 [LIMITED] |
| PRIVILEGED | ns2.google.com | | 2011-08- | suspicious | medium | 10.625 | unknown_html_rfi_php | Related Event | Show Data | http://support.clean-mx.de/clean- |



Results for **google.com**

**Server Name:** ses-qa
**Feed Restriction:** RESTRICTED
**Time:** 2013-02-04T18:01:04Z
**Export:** Text Table CSV

| restriction | address | protocol/ports | detecttime | impact | severity | confidence | description | Incident Meta Data (Expand/Collapse all) | Additional Data (Expand/Collapse all) | alternativeid [restriction] |
|---|---|---|---|---|---|---|---|---|---|---|
| PRIVILEGED | ns1.google.com | | 2011-07-16T21:00:47Z | suspicious nameserver | medium | 10.625 | unknown_html | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=911451 [LIMITED] |
| PRIVILEGED | ns2.google.com | | 2011-07-16T21:00:47Z | suspicious nameserver | medium | 10.625 | unknown_html | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=911451 [LIMITED] |
| PRIVILEGED | ns4.google.com | | 2011-07-16T21:00:47Z | suspicious nameserver | medium | 10.625 | unknown_html | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=911451 [LIMITED] |
| PRIVILEGED | ns3.google.com | | 2011-07-16T21:00:47Z | suspicious nameserver | medium | 10.625 | unknown_html | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=911451 [LIMITED] |
| PRIVILEGED | ns2.google.com | | 2011-08-14T11:59:19Z | suspicious nameserver | medium | 10.625 | unknown_html_rfi_php | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=967566 [LIMITED] |
| PRIVILEGED | ns3.google.com | | 2011-08-14T11:59:19Z | suspicious nameserver | medium | 10.625 | unknown_html_rfi_php | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=967566 [LIMITED] |
| PRIVILEGED | ns4.google.com | | 2011-08-14T11:59:19Z | suspicious nameserver | medium | 10.625 | unknown_html_rfi_php | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=967566 [LIMITED] |
| PRIVILEGED | ns1.google.com | | 2011-08-14T11:59:19Z | suspicious nameserver | medium | 10.625 | unknown_html_rfi_php | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=967566 [LIMITED] |
| PRIVILEGED | ns2.google.com | | 2011-09-02T12:00:21Z | suspicious nameserver | medium | 10.625 | tr%2fagent.892928.8 | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=988753 [LIMITED] |
| PRIVILEGED | ns3.google.com | | 2011-09-02T12:00:21Z | suspicious nameserver | medium | 10.625 | tr%2fagent.892928.8 | Related Event<br>Show Data | Show Data | http://support.clean-mx.de/clean-mx/viruses.php?id=988753 [LIMITED] |
| PRIVILEGED | ns4.google.com | | 2011-09- | suspicious | medium | 10.625 | tr%2fagent.892928.8 | Related Event | Show Data | http://support.clean-mx.de/clean- |

next 24 months.

# imagine a “box”

- that worked like google personalized search
- that not just read, but understood your email and favorite blogs
- that communicated seamlessly with your network infrastructure (firewalls, IDS, name-servers, etc) in real-time
- that could be peered with your close, trusted, partners “box” to exchange information

# now imagine that “box”

- leveraged existing science intelligence analytics (bio, chem, etc) to analyze the data
- could handle trillions of observations per day (netflow, passive dns, log flow, etc)
- magically manipulated your infrastructure into mitigating attacks on the fly

and... was an open and free framework

Skynet DEVELOPMENT TEAM

# we already know how to do this...

- pick a messaging framework (zeromq, xmpp, http, smtp, pigeon, horse, donkey, camel, hobbit..)
- pick a storage framework (hadoop, cassandra, sql, sqlite, clay tablets)
- pick a normalization protocol (iodef, csv, etc)
- pick an msg/api spec (protobuf, rest, soap)

pretend for a minute you've got all that in-house, what's next?

# information sharing is really all about...

- messaging
- storage
- analytics
- communication
- scale
- warfare
- economics
- trust
- people
- culture

# information sharing is really all about...

- peering.

# peering.

- cultural barriers (easy: requires only beer)
- language barriers (easy: requires beer and google)
- trust barriers (harder: requires more beer)
- scale barriers (harder: requires more beer)
- protocol barriers (hard: requires, hard-liquor, hangovers, etc)
- legal barriers (easy: they work for you)

# where we fail

- most [international] information sharing communities are great aggregators of internally shared information
- most cross-hub action happens by those who are in many communities
- we’re actually just inhibiting the data-sharing process

# peering.

- this is really a “BGP” problem
- it’s been solved before
- it’s been completely screwed up before
- where the wizards stay up late? the origins of the internet....

# peering.

- Jabber (XMPP)
- SMTP
- Skype
- SMS/iMessage
- Torrents
- BGP

- BBS / Forums
- Prodigy
- AOL
- CompuServe
- IRC
- Google+/Talk
- ICQ!!!!!

# peering.

- teh Facebook is a social platform for connecting you with your ~~friends~~ parents?
- teh LinkedIn is a social platform for connecting you with your friends who have money and would be dumb enough to hire someone like you
- teh google plus is a social platform for security peeps who have no desire for Facebook shenanigans

# peering.

- AusCERT is a social platform for connecting Australian security professionals
- the APWG is a social platform for connecting e-crime researchers
- the REN-ISAC is a social platform for connecting american security professionals in education

# you should be thinking...

- if you're not already doing automated data-sharing, why not?
- does your current infrastructure support automated data-sharing?
- have you executed information sharing agreements with your partners?

# you should be thinking...

- peers need to build trust (we’re not just pushing packets)
- peers need to travel (here i am!)
- peers need to leave their ego’s at the door

# end-game

- cross sector coordination
- cross culture coordination
- change in economics