Creating Wi-Fi NSA monitoring station

Milan Gabor

#/viris[# *]

Ljubljana::0x7E0

Blast from the past

Security BSides Ljubljana #BSidesLjubljana

« Talk: Low-Tech High-Intensity Phishing Attacks on Slovenian Banks (Gorazd Božič)

BSidesLjubljana tickets »

Talk: Invisible packets (Milan Gabor & Danijel Grah) | February 18th, 2015

Abstract:
This talk will be about packets that are constantly flying around us. Main focus will be on Wi-Fi. We will look into the coverage of wireless signal in the area of Ljubljana, show some statistic about access points and what is visible with simple equipment for few dollars. Techniques will be discussed on how to attack access points and clients and how to defend them. We will demonstrate how to be online for free in the area of Ljubljana all the time. Additionally we will touch state of the art of data exfiltration techniques and secret channels.

Bio:
Milan Gabor is a Founder and CEO of Viris, Slovenian company specialized in information security. He is security professional, pen-tester and researcher. Milan is a distinguished and popular speaker on information security. He has previously been invited to speak at various events at different IT conferences in Slovenia and loves to talk to IT students at different Universities. He also does trainings regarding ethical hacking. He is always on a hunt for new and uncovered things and he really loves and enjoys his job.

Danijel Grah has a Bachelor degree in Computer Science at the University of Ljubljana, Slovenia. He is a Security Consultant at Viris for some time and is involved in penetration testing, security reviews, programming, consulting and research. He has deep understanding into threats, vulnerabilities and trends. He likes to practice Information Security in everyday life. Danijel is devoted to his work, open minded, enjoys new challenges and he never stops studying.

#BSidesLjubljana

Date: 12th March 2015
Venue: Poligon creative centre, Ljubljana, Slovenia

Menu

- Call for papers
- Capture The Flag
- Schedule
- Sponsors
- Talks
- Tickets
- Venue
- Workshops

Recent Posts

- Oh my god all the tickets have gone!!
- First round of free ticket sold out
- BSidesLjubljana tickets
- Talk: Invisible packets (Milan Gabor & Danijel Grah)
- Talk: Low-Tech High-Intensity Phishing Attacks on Slovenian Banks (Gorazd Božič)

Twitter

#bsidesljubljana

BSidesHN - H...
@BSidesHN

@_FellMoon @revision_party Looking forward to see you in Hannover next week Garlef!

OUR
TERMS
PLEASE
READ
Wi
Fi

HOW IT STARTED

Agenda

insert into elasticsearch (E) logstash (L) kibana (K) values

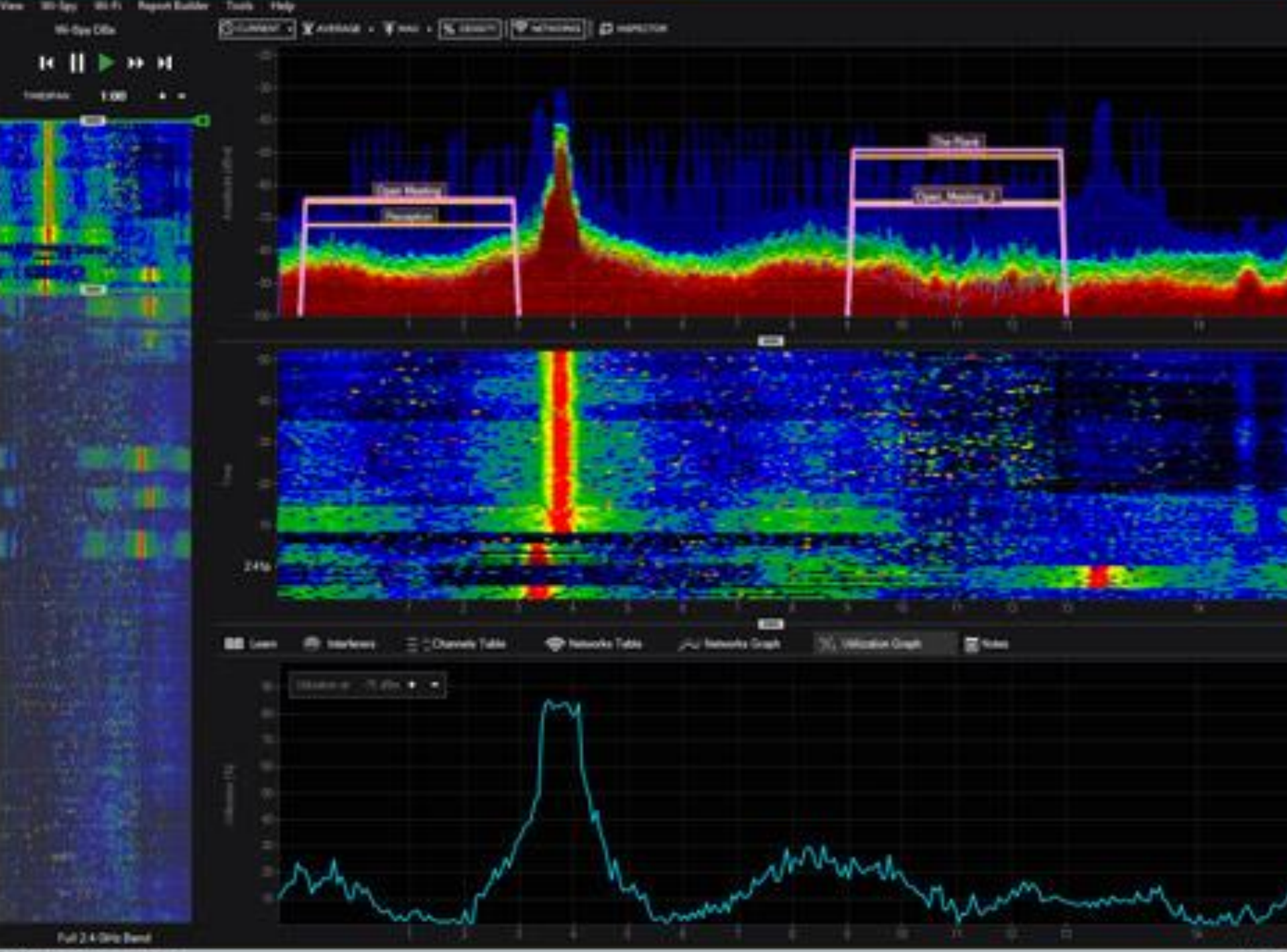
select * from Wi-fi packets;

create view

where Bigdata = strange patterns

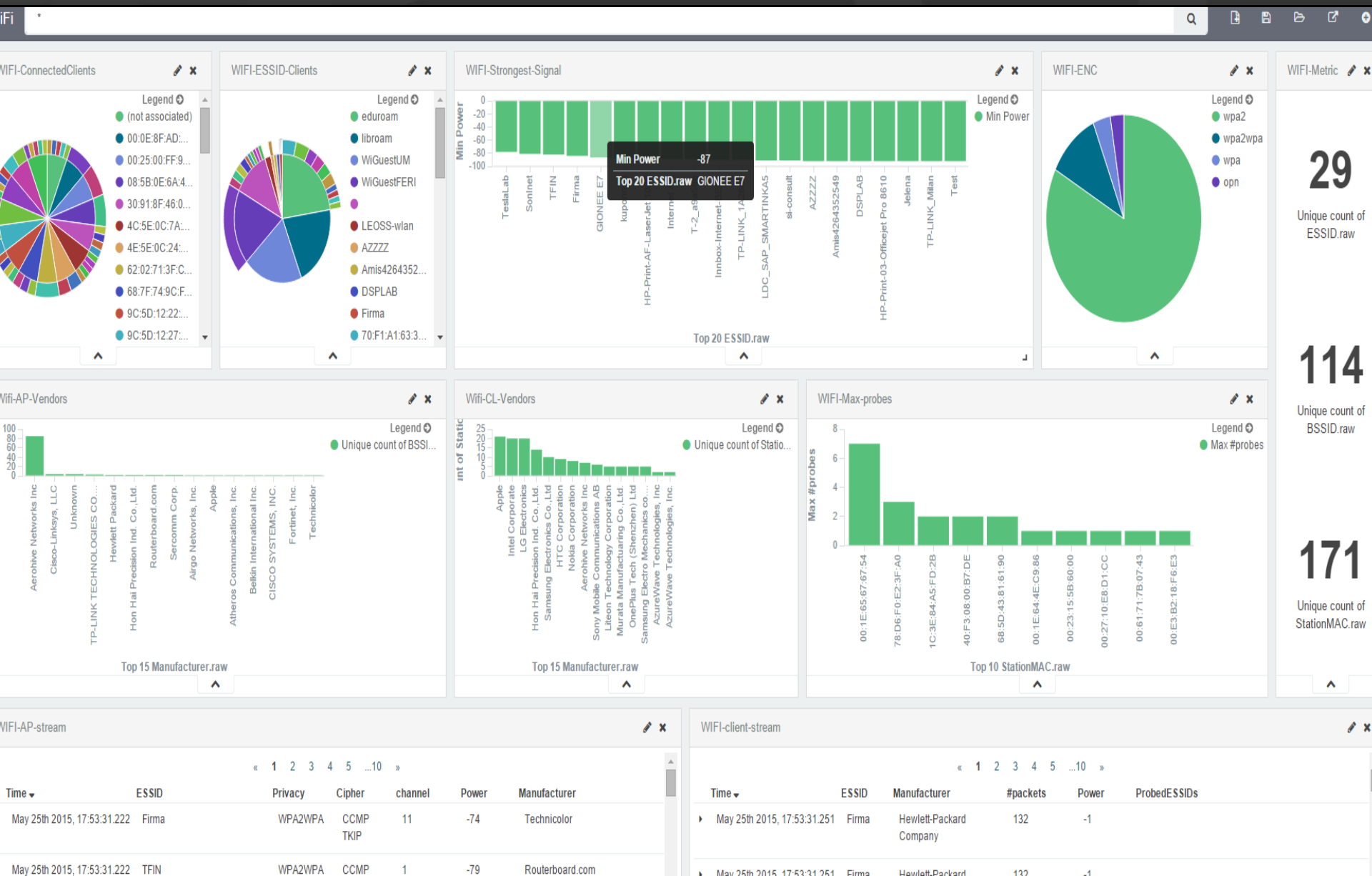
++ Ideas;

problem
problem
problem
problem
problem
problem
problem
problem
problem
problem
problem
solution

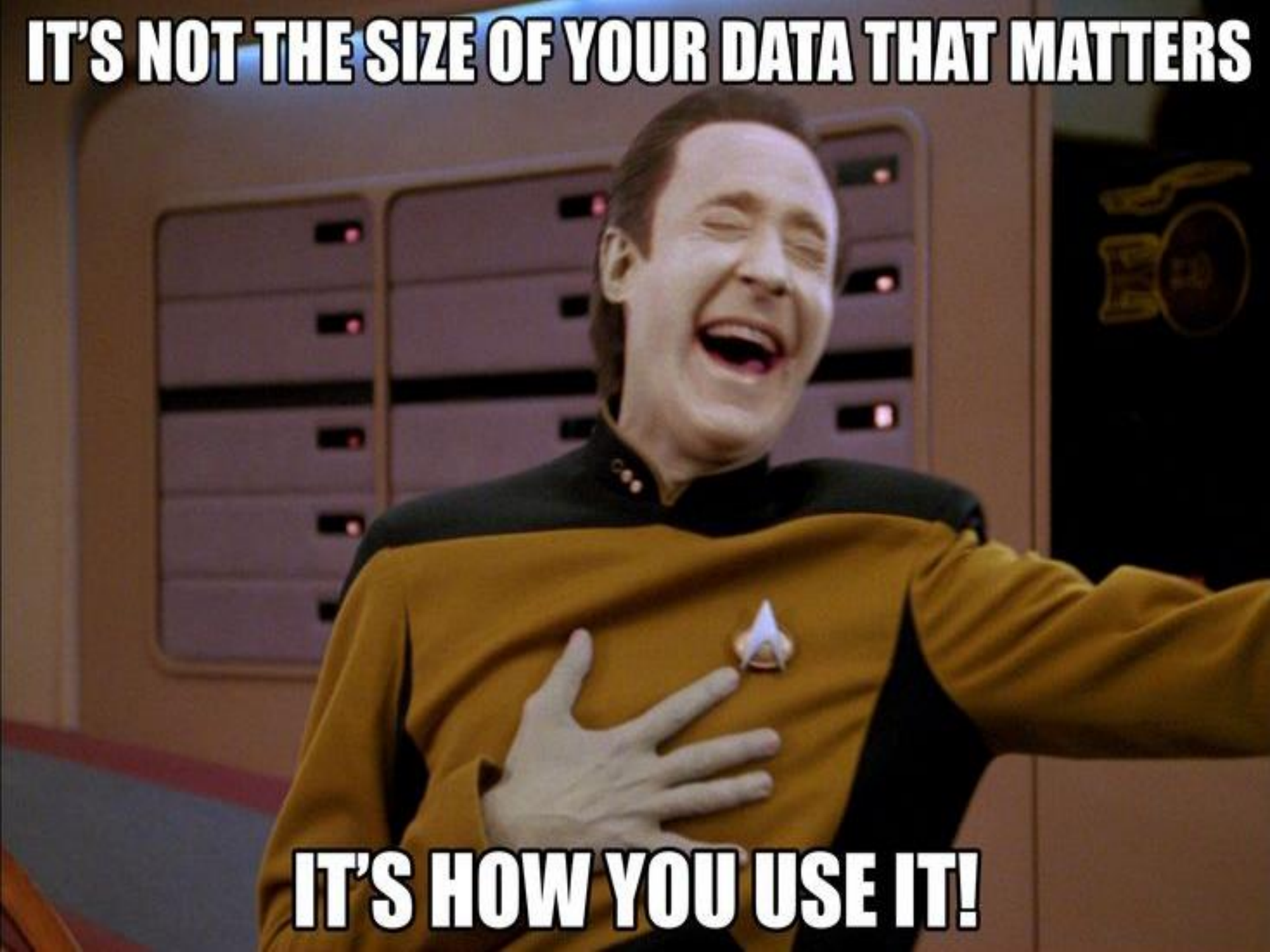

View
Wi-Spy
Wi-Fi
Report Builder
Tools
Help
Wi-Spy DBx
Open Meeting
Reception
The Park
Open Meeting 2
Lines
Interferers
Channels Table
Networks Table
Networks Graph
Utilization Graph
Notes
Full 2.4 GHz Band

FREE
WiFi
AVAILABLE
Solve this for
WiFi Password
$f(x) = a_0 + \sum_{n=1}^{\infty} \left(a_n \cos \frac{n\pi x}{L} + b_n \sin \frac{n\pi x}{L}\right)$

Transformation



computing
semi-structured
algorithms
classification
govern
complexity
collection
data
storage
set
a/b
parallel
technology
regression
statistics
sharing
methodology
trend
complex
quintillion
big
data
billion
millions
devices
visualiza
cameras
permutations
ex
insights
networks
mpp
time series analysis
information
traditional
finance
business
information
large
private
sector
velocity


IT'S NOT THE SIZE OF YOUR DATA THAT MATTERS
IT'S HOW YOU USE IT!

WELCOME TO
REALITY
ENJOY THE JOURNEY

```
CH  6 ][ Elapsed: 1 min ][ 2010-07-18 14:53

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:1B:11:91:70:BA    0   2       34        0    0   6  54 . WEP  WEP         Cortesi
00:1F:C6:51:63:9C    0   0        4       14    0   6  54   WEP  WEP         CONY
00:19:5B:8A:1C:F6    0   0        9        0    0   6  54 . WEP  WEP         samissions2
00:1B:FC:6B:6B:76    0   0       22      470    6   6  54   WEP  WEP         CONSTANZA1
00:15:E9:E1:F6:23    0  63      212        0    0   6  54 . WEP  WEP         www.conocechile.c
00:0F:3D:5A:CE:42    0   6       92        4    0   6  54 . WEP  WEP         REDRSM
00:02:CF:95:55:EB    0  39      344        2    0   6  54 . WEP  WEP         PABLO
00:22:B0:43:4E:C7    0  35      270        0    0   6  54 . WEP  WEP         vecinos
00:A0:C5:F9:D8:C2    0  49      394        0    0   6  11   WEP  WEP         Pilar
00:1B:11:90:82:E4    0  37      381        0    0   6  54 . WEP  WEP         learn
00:02:CF:95:47:EA    0  48      377        0    0   6  54 . WEP  WEP         loretito
00:18:39:71:F9:78    0   3       60        3    0   6  54   WEP  WEP         Fabulosa
00:21:91:4D:84:6E    0  43      344        0    0   6  54e  WEP  WEP         QQ
00:1F:33:2F:1B:E8    0   0       34        0    0   6  54e  WEP  WEP         RoomApart
00:1B:11:24:D3:91    0  38      400        5    0   6  54 . WEP  WEP         samissions
00:1F:C6:71:D1:9A    0  38      132     4603   47   6  54   WEP  WEP         natcam
00:17:9A:5A:BA:E1    0   0        4        0    0   6  54 . WEP  WEP         buenavista5
00:17:9A:62:EF:11    0   0        6        0    0   6  54 . WEP  WEP         jorge
00:02:CF:95:55:BD    0   0        4        0    0   6  54 . WEP  WEP         Casa
00:1A:73:B4:00:74    0   0        0        2    0 133  -1   WEP  WEP         <length:  0>

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   2C:A8:35:A8:6B:9D    0    0 - 2      0        5  morazan,Rep. Dominicana
(not associated)   00:23:7A:D9:0A:81    0    0 - 2      0        1  Defran
(not associated)   0C:EE:E6:9E:36:54    0    0 - 1      0        1  cpereira
(not associated)   00:19:7E:42:1E:81    0    0 - 1      0        1  XPA
(not associated)   00:04:23:8C:76:45    0    0 - 1      0        5
(not associated)   00:1B:77:00:D3:2E    0    0 - 1      0        1
```

nas | Execute SQL

be	toDS	fromDS	moreFragments	retry	powerMgmt	moreData	protectedFrame	ord	durationId	addr1	addr2	addr3
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
	1	0	0	0	1	0	0	0	314	BC:AE:C5:C3:5E:01	44:94:FC:12:61:BE	BC:AE:C5:C3:5E:01
	0	0	0	0	0	0	0	0	0	FF:FF:FF:FF:FF:FF	BC:AE:C5:C3:5E:01	BC:AE:C5:C3:5E:01
	0	0	0	0	0	0	0	0	0	FF:FF:FF:FF:FF:FF	B0:C5:54:86:5E:88	B0:C5:54:86:5E:88
	0	0	0	0	0	0	0	0	0	FF:FF:FF:FF:FF:FF	BC:AE:C5:C3:5E:01	BC:AE:C5:C3:5E:01
	1	0	0	0	0	0	0	0	314	BC:AE:C5:C3:5E:01	44:94:FC:12:61:BE	BC:AE:C5:C3:5E:01
	0	0	0	0	0	0	0	0	0	FF:FF:FF:FF:FF:FF	B0:C5:54:86:5E:88	B0:C5:54:86:5E:88
	0	0	0	0	0	0	0	0	0	FF:FF:FF:FF:FF:FF	BC:AE:C5:C3:5E:01	BC:AE:C5:C3:5E:01
	0	0	0	0	0	0	0	0	0	FF:FF:FF:FF:FF:FF	B0:C5:54:86:5E:88	B0:C5:54:86:5E:88
	0	0	0	0	0	0	0	0	0	FF:FF:FF:FF:FF:FF	BC:AE:C5:C3:5E:01	BC:AE:C5:C3:5E:01
	0	0	0	0	0	0	0	0	0	FF:FF:FF:FF:FF:FF	B0:C5:54:86:5E:88	B0:C5:54:86:5E:88
	1	0	0	0	1	0	0	0	314	BC:AE:C5:C3:5E:01	44:94:FC:12:61:BE	BC:AE:C5:C3:5E:01
	0	0	0	0	0	0	0	0	0			
	0	0	0	0	0	0	0	0	314			
	0	0	0	0	0	0	0	0	0			
	0	0	0	0	0	0	0	0	314			
	0	0	0	0	0	0	0	0	0			
	0	0	0	0	0	0	0	0	0			
	1	0	0	0	0	0	0	0	314			
	0	0	0	0	0	0	0	0	0			
	0	0	0	0	0	0	0	0	0			
	0	0	0	0	0	0	0	0	0			
	1	0	0	0	0	0	0	0	314			
	0	0	0	0	0	0	0	0	0			

WE CAN DO IT!

Programming

Where do we start?

A Great Combination

Hardware

> Your favorite Alfa card/s

> USB cable/s ☺

> Power

> Big screen

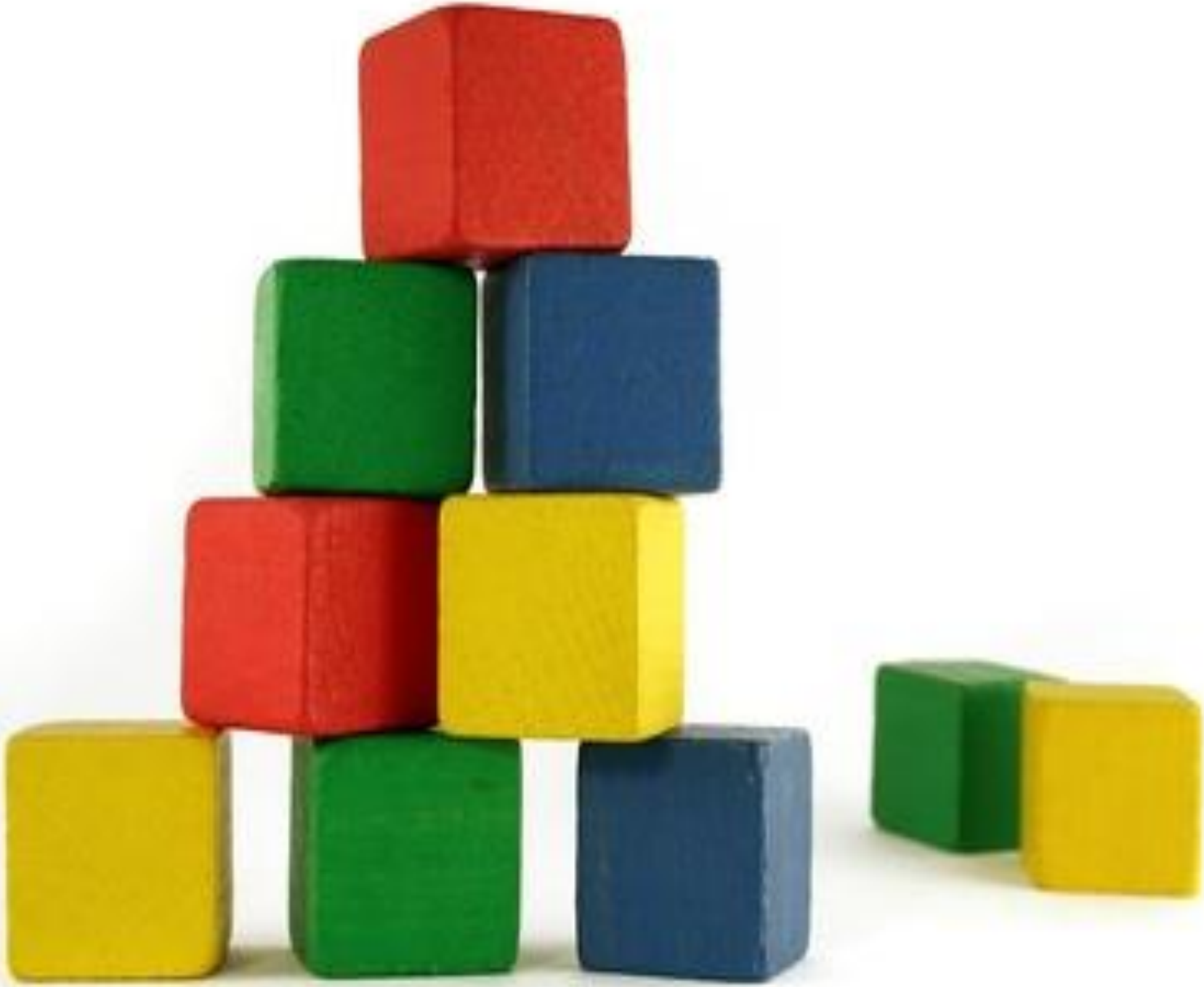
#/viris[ ]

Software

- You favourite OS (Linux, Mac, Win*)
- Keep in mind, that you might get into some challenges with one component, but there are some solutions

environment

data



ELK stack

kibana | Discover | Visualize | Dashboard | Settings | March 19th 2015, 00:04:06.916 to March 19th 2015, 00:05:48.9

NOC Dashboard

Top N Sources

Top 10 SourceAddress.raw	Count
24.25.15.94	1493
24.25.11.36	1002
24.16.206.244	405
24.25.11.26	368
24.16.205.187	334
24.71.82.57	162
24.25.205.132	138
24.171.180.4	134
24.16.206.246	116
24.25.11.42	112

Top N Destinations

Top 10 DestinationAddress.raw	Count
24.198.58.41	1492
24.16.206.126	430
24.129.122.21	406
24.8.8.8	400
24.16.206.100	394
24.129.122.43	233
24.25.11.112	196
24.25.11.147	162
24.129.122.20	161
24.16.216.120	158

Traffic Types

Throughput

Sum of KBXferred: 600k, 400k, 200k, 0

Charlotte_Log_Profile, SARPA001_LF_Profile, PARPA001_LF_Profile, Sarasota_Test FWD Profile

Top 5 LogAction.raw

Source Address Locations

Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA

1 – 827
827 – 1653
1653 – 2478
2478 – 3304
3304 – 4130

Traffic Over Time

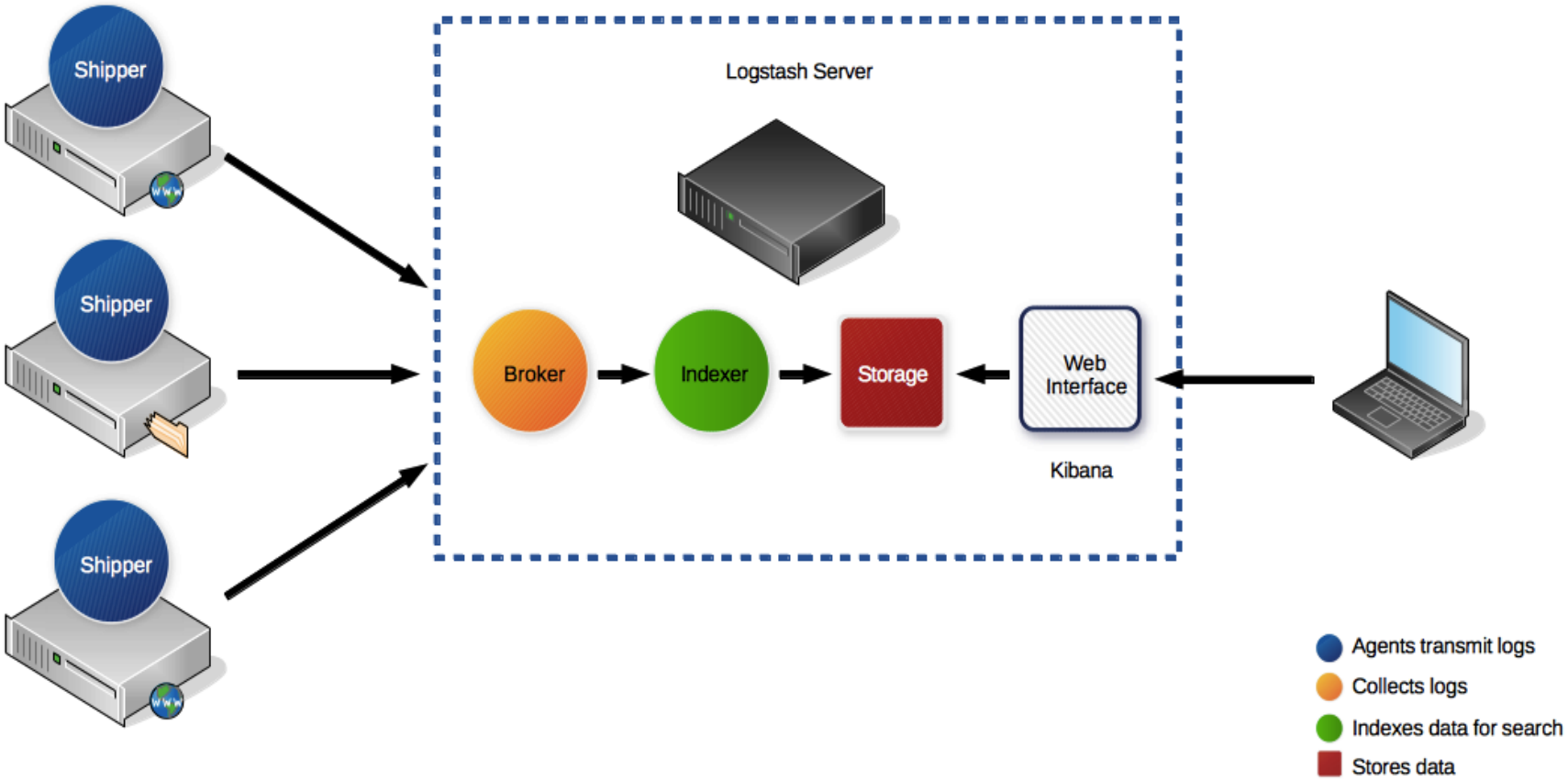
Count: 700, 600, 500, 400, 300, 200, 100, 0

00:04:15, 00:04:30, 00:04:45, 00:05:00, 00:05:15, 00:05:30, 00:05:45

Destination Address Locations

1 – 536
536 – 1072
1072 – 1607
1607 – 2143
2143 – 2678

ELK stack


Shipper
Shipper
Shipper
Logstash Server
Broker
Indexer
Storage
Web Interface
Kibana
Agents transmit logs
Collects logs
Indexes data for search
Stores data

Logstash

- Processing data from various sources
- Parse, Collect, Modify, Transport data
- Running and hungry for new input

```
input{

    file {
        path => "/var/log/wlan/*.json"
          type => "wifi"
    }

}

filter{

    if [type] == "wifi" {
        json {
            source => message
        }

        if [wlan_type] == "CL" {
            mutate {
                rename => ["ProbedESSIDs", "ProbedESSIDsArray"]
                  add_field => ["ProbedESSIDs","%{ProbedESSIDsArray}"]
                  split => ["ProbedESSIDsArray", ","]

            }
        }
    }

}

output {
    elasticsearch {
        template_name => "wifi"
          hosts => ["localhost:9200"]
          index => "wifi-%{+dd.MM.YYYY}"
    }
    stdout { codec => rubydebug }
}
```

#/viris[# *]

Logstash forwarder

> Agent for forwarding logs

> Prebuilt for some platforms

> Lack of support for some

> Can be done with some other solutions (Win – nxlog-ce, Beaver, syslog)

Elasticsearch

- Elasticsearch is a search server based on **Lucene.** It provides a distributed, multitenant-capable **full-text search** engine with a HTTP web interface and schema-free JSON documents ~ Wikipedia
- Elasticsearch is a **distributed,** scalable, real-time search and **analytics engine** ~ elastic.co
- **Document oriented** (stores entire objects or documents)
- **JSON** was picked as serialization format for documents
- Talking to Elasticsearch
  - **RESTful API** with JSON over HTTP
  - Various client APIs.

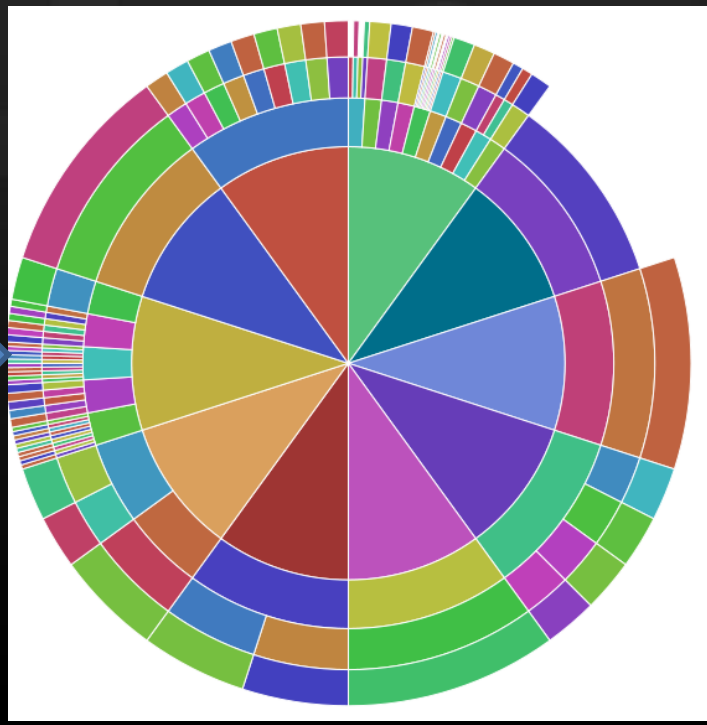
Kibana

> Graphical presentation

> The power of visualization

```
POST /elasticsearch/_msearch?timeout=0&ignore_unavailable=true&preference=1434391152506 HTTP/1.1
Host: 192.168.81.128
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:22.0) Gecko/20100101 Firefox/22.0 Iceweasel/22.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
Referer: http://192.168.81.128/
Content-Length: 786
Authorization: Basic ZWxrYWRtaW46UzBuY24wR2VzbDA=
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

{"index":"logstash-*","search_type":"count","ignore_unavailable":true}
{"query":{"filtered":{"query":{"query_string":{"query":"wlan_type:\"CL\"","analyze_wildcard":true}},"
filter":{"bool":{"must":[{"range":{"@timestamp":{"gte":1420066800000,"lte":1451602799999}}}],"must_no
t":[]}}}},"size":0,"aggs":{"2":{"terms":{"field":"ESSID.raw","size":10,"order":{"1":"desc"}},"aggs":{
"1":{"cardinality":{"field":"ESSID.raw"}},"3":{"terms":{"field":"BSSID.raw","size":10,"order":{"1":"d
esc"}},"aggs":{"1":{"cardinality":{"field":"ESSID.raw"}},"4":{"terms":{"field":"StationMAC.raw","size
":10,"order":{"1":"desc"}},"aggs":{"1":{"cardinality":{"field":"ESSID.raw"}},"5":{"terms":{"field":"M
anufacturer.raw","size":10,"order":{"1":"desc"}},"aggs":{"1":{"cardinality":{"field":"ESSID.raw"}}}}}
}}}}}}}
```



Google

setup elk

Milan

Web Images Videos Shopping News More Search tools

About 657,000 results (0.72 seconds)

How To Install Elasticsearch, Logstash, and Kibana (ELK ...
https://www.digitalocean.com/.../how-to-install-elasticsearch-logstash-and...
Mar 10, 2015 - The goal of the tutorial is to **set up** Logstash to gather syslogs of multiple ... to use CentOS instead, check out this tutorial: How To Install **ELK** on ...
Adding Logstash Filters To ... - (ELK Stack) on CentOS 7 - Mitchell Anicas

Setting up a single ELK node in 20 minutes | White snow ...
christophe.vandeplas.com/.../setting-up-single-node-**elk**-in-20-minutes.ht...
Jun 1, 2014 - This is a first article of a series to show the power of Elasticsearch, Kibana and Logstash (**ELK**) in the domain of Incident Handling and forensics ...

Elasticsearch - Logstash - Kibana 4 (ELK Stack) Setup Tutorial

https://www.youtube.com/watch?v=ge8uHdmtb1M
Mar 15, 2015 - Uploaded by AWS Tutorial Series
AWS Tutorial Series. ... This tutorial is setting up Elasticsearch in cluster mode with Logstash ...

How to Install the ELK Stack on AWS - Logz.io
logz.io/blog/install-**elk**-stack-amazon-aws/
Oct 13, 2015 - **ELK** is a great open-source stack for log aggregation and analytics. ... You can **set up** your own **ELK** stack using this guide or try out our simple ...

Howto Configure Elasticsearch, Logstash & Kibana on ...
linoxide.com/tools/configure-elasticsearch-logstash-kibana-ubuntu-15-04/
Jun 10, 2015 - We will guide you with the **setup** of **ELK** installations to configure with

SIDE EFFECT

Shodan says

SHODAN | country:at elasticsearch | Explore | Contact Us | Blog | Enterprise Access

Exploits | Maps | Download Results | Create Report

TOP COUNTRIES

Showing results 11 - 16 of 16

151.236.6.238

EDIS GmbH

HTTP/1.1 200 OK

Top 20 treatment.title	Count
min	9
osteopathi	9
triggerpunktbehandlung	7
60	6
elektrotherapi	6
manull	6
therapi	6
massag	5
bewegungstherapi	4
taping	4

„Issues“ with ELK

> No security ($$$ for auth)

> Alerts

> Constant development

> Big changes (3 or 4)

> Lack of some functionalities

Aircrack-ng

> JSON what?

> Tested a lot of things

> Source code change was winner

> Contributing to main branch?

Aircrack-ng facelift

```
#define REFRESH_RATE 100000  /* default delay in us between updates */
#define DEFAULT_HOPFREQ 250  /* default delay in ms between channel hopp
#define DEFAULT_CWIDTH  20 /* 20 MHz channels by default */

#define NB_PWR  5        /* size of signal power ring buffer */
#define NB_PRB 100        /* size of probed ESSID ring buffer */

#define MAX_CARDS 8      /* maximum number of cards to capture from */
```

```
int dump_write_json( void )
{
    int i, n, probes_written;
    struct tm *ltime;
    struct AP_info *ap_cur;
    struct ST_info *st_cur;
    char * temp;
    //printf("DUMP JSON\n");
    if (! G.record_data || !G.output_format_json)
        return 0;

    fseek( G.f_json, 0, SEEK_END );


    ap_cur = G.ap_1st;
```

Result


```
{"BSSID":"2C:5D:93:25:AF:A8", "FirstTimeSeen":"2015-11-19 08:43:38", "LastTimeSeen":"2015-11-19 08:43:38", "channel":11, "max
speed":" 54","Privacy":"OPN","Cipher":"" , "Authentication":"", "Power":-70, "#beacons":       1,"#IV":       0, "LANIP":"  0
  0.  0.  0", "ID-length": 17, "ESSID":"Renaissance_GUEST", "Manufacturer":"Ruckus Wireless", "wlan_type":"AP","timestamp":"1
47919023"}
{"BSSID":"6C:AA:B3:23:6D:78", "FirstTimeSeen":"2015-11-19 08:43:38", "LastTimeSeen":"2015-11-19 08:43:38", "channel":11, "max
speed":" 54","Privacy":"OPN","Cipher":"" , "Authentication":"", "Power":-74, "#beacons":       0,"#IV":       0, "LANIP":"  0
  0.  0.  0", "ID-length": 17, "ESSID":"Renaissance_GUEST", "Manufacturer":"Ruckus Wireless", "wlan_type":"AP","timestamp":"1
47919023"}
{"BSSID":"6C:AA:B3:1F:96:28", "FirstTimeSeen":"2015-11-19 08:43:39", "LastTimeSeen":"2015-11-19 08:43:42", "channel": 1, "max
speed":" 54","Privacy":"OPN","Cipher":"" , "Authentication":"", "Power":-75, "#beacons":       5,"#IV":       0, "LANIP":"  0
  0.  0.  0", "ID-length": 17, "ESSID":"Renaissance_GUEST", "Manufacturer":"Ruckus Wireless", "wlan_type":"AP","timestamp":"1
47919023"}
{"BSSID":"6C:AA:B3:1F:BA:08", "FirstTimeSeen":"2015-11-19 08:43:39", "LastTimeSeen":"2015-11-19 08:43:42", "channel": 1, "max
speed":" 54","Privacy":"OPN","Cipher":"" , "Authentication":"", "Power":-83, "#beacons":       5,"#IV":       0, "LANIP":"  0
  0.  0.  0", "ID-length": 17, "ESSID":"Renaissance_GUEST", "Manufacturer":"Ruckus Wireless", "wlan_type":"AP","timestamp":"1
47919023"}
{"BSSID":"6C:AA:B3:01:8B:08", "FirstTimeSeen":"2015-11-19 08:43:39", "LastTimeSeen":"2015-11-19 08:43:42", "channel": 1, "max
speed":" 54","Privacy":"OPN","Cipher":"" , "Authentication":"", "Power":-81, "#beacons":       4,"#IV":       0, "LANIP":"  0
  0.  0.  0", "ID-length": 17, "ESSID":"Renaissance_GUEST", "Manufacturer":"Ruckus Wireless", "wlan_type":"AP","timestamp":"1
47919023"}
{"BSSID":"6C:AA:B3:01:A1:78", "FirstTimeSeen":"2015-11-19 08:43:39", "LastTimeSeen":"2015-11-19 08:43:42", "channel": 1, "max
speed":" 54","Privacy":"OPN","Cipher":"" , "Authentication":"", "Power":-59, "#beacons":       6,"#IV":       2, "LANIP":"172
 20. 13. 99", "ID-length": 17, "ESSID":"Renaissance_GUEST", "Manufacturer":"Ruckus Wireless", "wlan_type":"AP","timestamp":"1
47919023"}
{"BSSID":"6C:AA:B3:1F:AA:C8", "FirstTimeSeen":"2015-11-19 08:43:40", "LastTimeSeen":"2015-11-19 08:43:40", "channel": 6, "max
speed":" 54","Privacy":"OPN","Cipher":"" , "Authentication":"", "Power":-84, "#beacons":       1,"#IV":       0, "LANIP":"  0
  0.  0.  0", "ID-length": 17, "ESSID":"Renaissance_GUEST", "Manufacturer":"Ruckus Wireless", "wlan_type":"AP","timestamp":"1
47919023"}
{"BSSID":"2C:5D:93:26:16:08", "FirstTimeSeen":"2015-11-19 08:43:40", "LastTimeSeen":"2015-11-19 08:43:40", "channel": 6, "max
speed":" 54","Privacy":"OPN","Cipher":"" , "Authentication":"", "Power":-72, "#beacons":       1,"#IV":       0, "LANIP":"  0
  0.  0.  0", "ID-length": 17, "ESSID":"Renaissance_GUEST", "Manufacturer":"Ruckus Wireless", "wlan_type":"AP","timestamp":"1
47919023"}
{"StationMAC":"8C:70:5A:12:E2:20", "FirstTimeSeen":"2015-11-19 08:43:39", "LastTimeSeen":"2015-11-19 08:43:39", "Power":-68,
```

Do not give up, the beginning is
always the hardest.

DEMO TIME

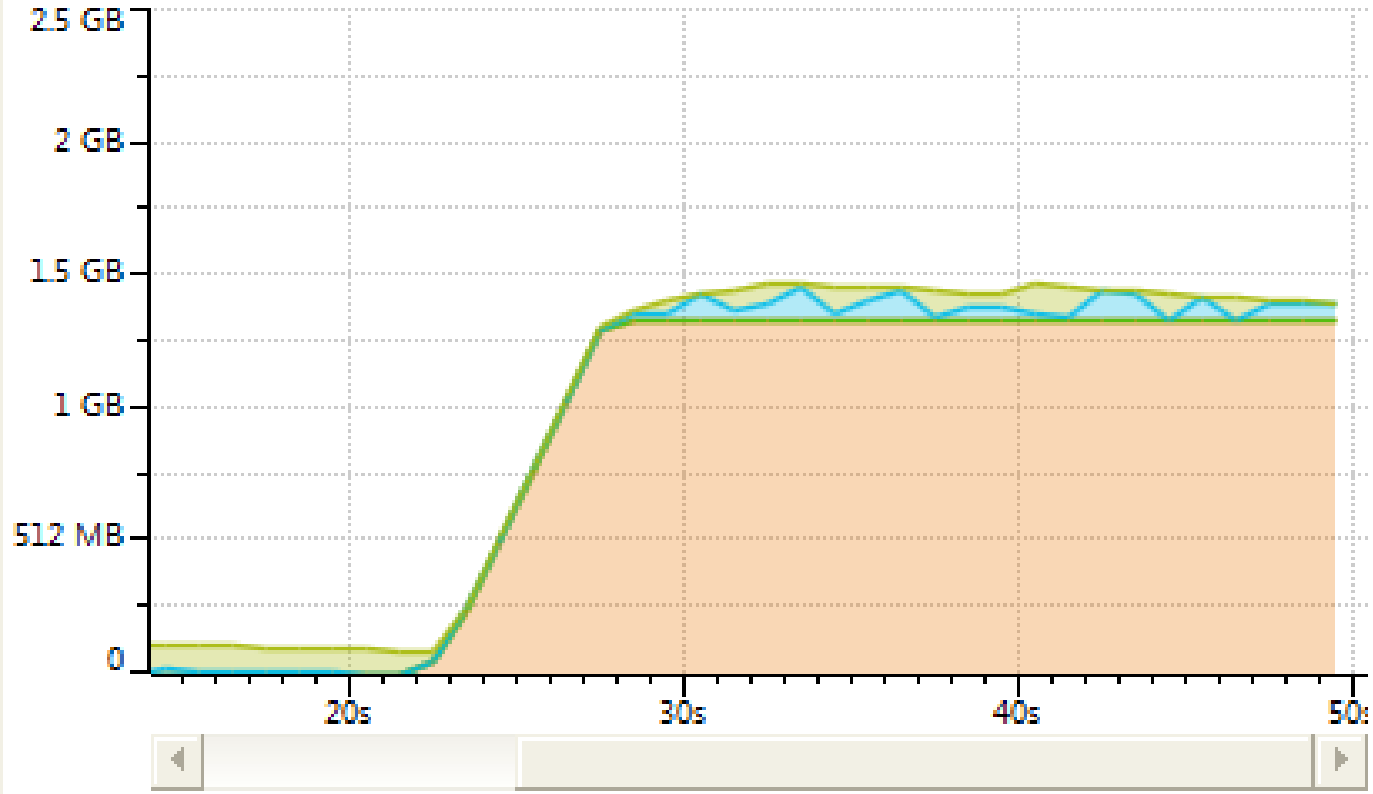
Problems

CPU | Threads | Deadlocks | **Memory** | Garbage Collection | Monito

Heap Memory

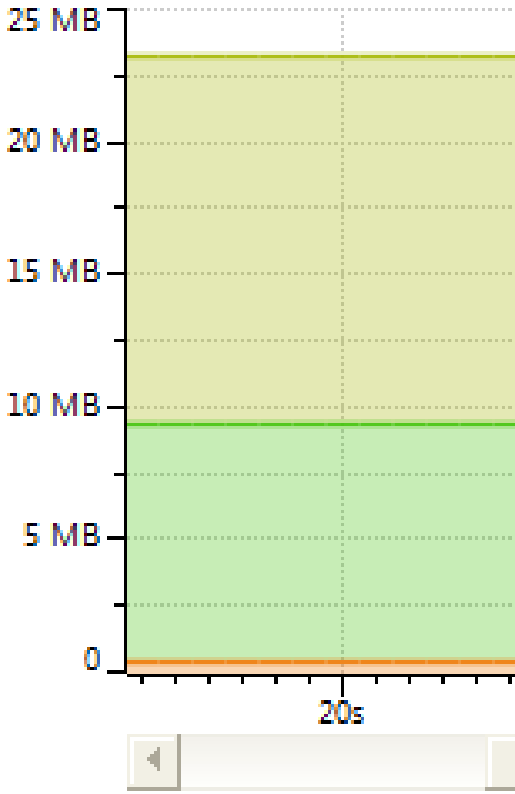
Memory Pool: All Pools

Allocated: 1.4 GB Used: 1.4 GB Limit: 1.8 GB



Memory Pool:

Allocated: 23 M



Class List | Allocations | Stack Traces | CPU Usage Estimation

```
#/viris[ # * ]
```

KEEP

CALM

it's

NOT

TRUE

Some ideas to play with

- Visualization (Penetration Testing, Security Audits)
- SIEM for Wi-Fi
- EVIL Intelligence Gathering
- Warstalking
- Tracking down stolen phones
- Adding traffic records of open networks

TRUST
YOUR
CRAZY
IDEAS

viris/wifi · GitHub

GitHub, Inc. [US] https://github.com/viris/wifi

GitHub | This repository | Search | Explore | Features | Enterprise | Pricing | Sign up | Sign in

viris / wifi

Watch 1 | Star 0 | Fork 0

4 commits | 1 branch | 0 releases | 2 contributors

Branch: master | wifi / +

viris Small changes — Latest commit 8a62925 3 days ago

README.md	Small changes	3 days ago
aircrack-ng-json.patch	Aircrack JSON patch	3 days ago

README.md

wifi

Apply patch

1. download aircrack-ng source (aircrack-ng-1.2-rc2.tar.gz)
2. download aircrack-ng-json.patch from https://github.com/viris/wifi

Code
Issues 0
Pull requests 0
Pulse
Graphs

HTTPS clone URL
https://github.com

You can clone with HTTPS or Subversion.

Clone in Desktop
Download ZIP

WE ARE
HIRING!

@MilanGabor

#/viris[# *]

Don’t be afraid to bug me! I don’t bite! ;)