WORKSHOP GARR 2018

Panel
“Monitoring, logging, log-retention”

Roma – 29/05/2018

- **Andrea Barontini**
  Network Engineer
  @Università di Parma
- **Davide Brunato**
  ICT system administrator
  @SISSA
- **Pasquale Mandato**
  System Engineer
  @GARR
- **Damiano Verzulli**
  SysNetAdmin
  APM GARR @UniCH
  APM GARR @ICRANet

Perchè questo Panel...

- Forte convinzione che moltissimi Atenei stiano gestendo o debbano gestire problemi “simili”;
- Il tema del “logging” è centrale, quando osservato da svariati punti di vista;
- Il rifiuto di accettare la logica dell’assoluto individualismo (“faccio tutto da me, da solo”);
- L’assoluta certezza che nella grande famiglia “GARR-connected” ci siano persone con competenze di eccellenza, da ~~sfrutt~~valorizzare

Andrea, Davide, Pasquale:
GRAZIE per il vostro contributo!

Di cosa parleremo...

I messaggi di LOG contengono informazioni di vario genere (data/ora; sistemi generanti; dettagli applicativi; riferimenti utente; etc.)

I LOG risultano di interesse per diverse categorie di utenza

Categorie di utenza diverse sono interessate a dettagli diversi dello stesso messaggio di LOG

Di cosa parleremo...

Il Panel sarà focalizzato su questo "poveraccio"!!!

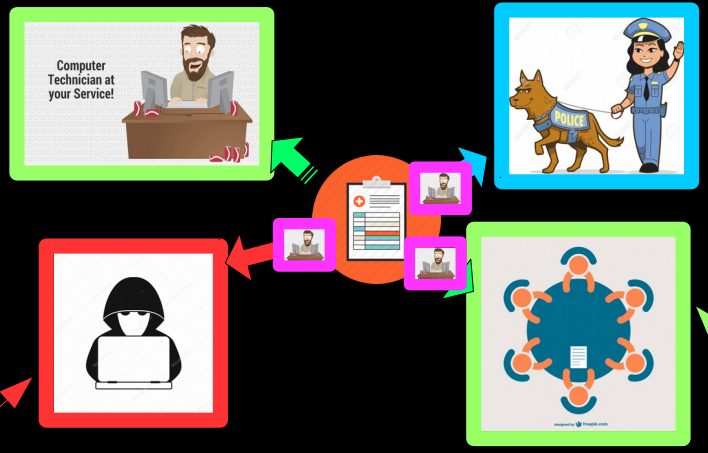
...soprattutto perchè, purtroppo, è anche "l'interfaccia" di tutti gli altri!

Di cosa parleremo...

- È ~~impor~~ **FONDAMENTALE** che “il poveraccio” sia consapevole del problema determinato dalla coppia:

“informazione trattata”, “cappello indossato”

In una LAN viaggiano frame Ethernet. Per garantire SLA in ambito L2, servono i MAC (e non gli username [che stanno a L7])



I procedimenti penali si fanno a carico di “persone” (e non di username o, peggio, MAC)

Servono “dati” (da “vendere”), “sistemi” (da usare), “utenze” (da usare per l’accesso ai sistemi)

Serve anticipare necessità di spesa e supportare la strategia dell’Ente ***(username? MAC? Che roba è?)***

Chiaramente sono solo esempi....

Di cosa parleremo…

- È proprio per AIUTARE questo “poveraccio” a fare il suo mestiere (**quello VERDE**) che….. ho chiesto ad altri tre ~~pover~~ “**amici di DISCUSSIONE**” di venire qui, a raccontare (brevissimamente) la loro situazione:

- **Andrea**: cosa c’era e dove si pensa di andare
- **Davide**: una soluzione “classica” e la necessità di “scalare”;
- **Pasquale**: il bleeding-edge del monitoring di EDUROAM
- **Damiano**: qualche spunto di riflessione

UNIVERSITÀ DI PARMA
il mondo che ti aspetta

Andrea Barontini

Network Engineer

@Università di Parma

Scuola Internazionale Superiore
di Studi Avanzati

Davide Brunato

ICT system administrator

@SISSA

Pasquale Mandato

System Engineer

@GARR

ICRANet
International Center for Relativistic Astrophysics Network

Ud'A
Università degli Studi "G. d'Annunzio"

Damiano Verzulli

System & Network Admin

APM GARR

LOG retention/analysis: perché?

- Raccolta LOG e relativa analisi, per un duplice obiettivo

Troubleshooting

- **Il più “real-time” possibile**
- **Il più “efficace” possibile**

(+) Bassa retention
(-) Ricca (necessariamente) di metadati
(-) Privacy dangerous!

“Incident response”

“Security”

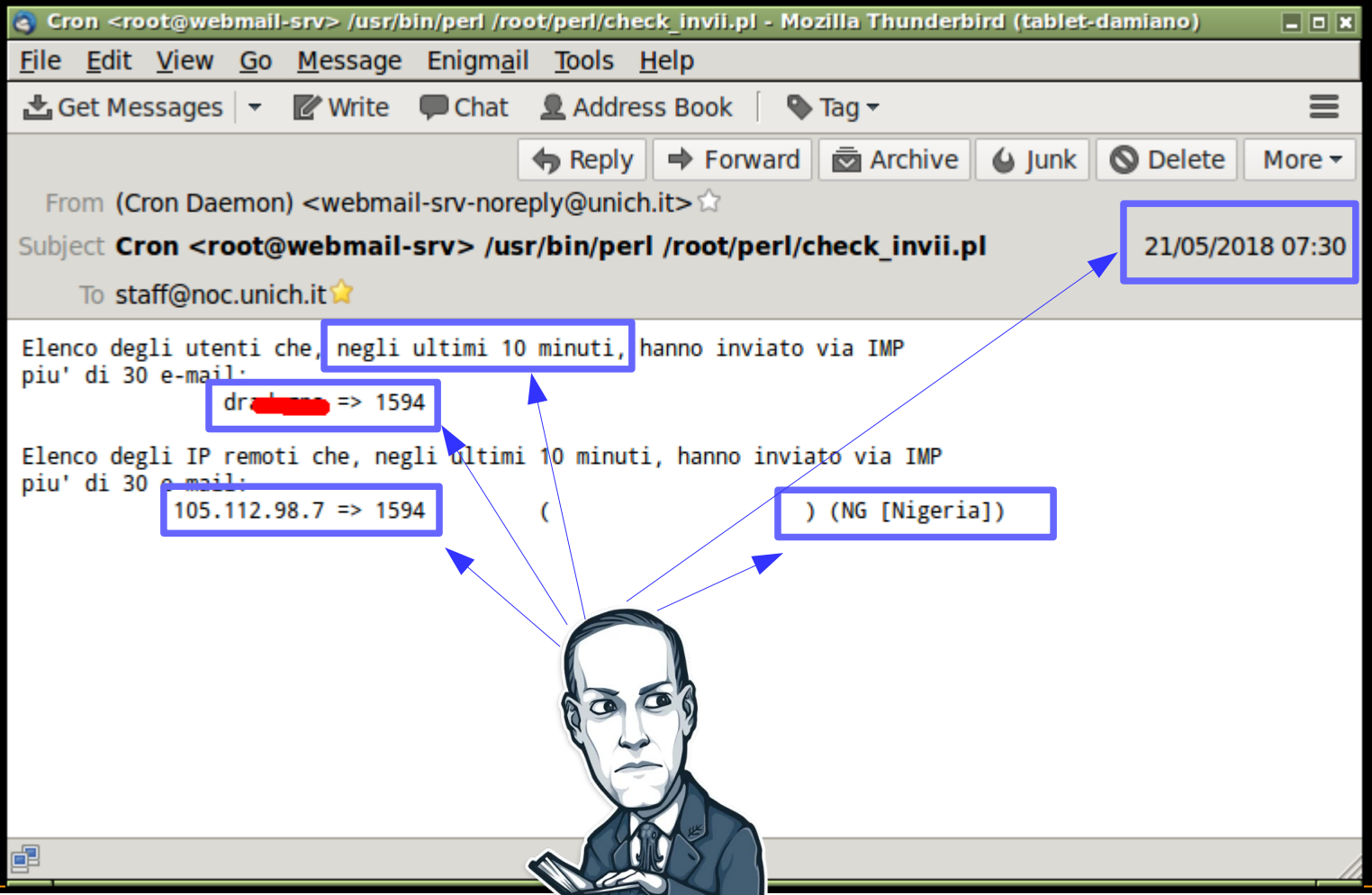
“Big picture” & “Trend analysis”

- **Comodamente “batch”**
- **Disinteressata ai dettagli**

(-) Alta/Altissima retention
(+) Privacy “friendly”

Qualche esperienza “sul campo”

- I LOG servono? Lo “username” in un LOG serve? Se ne può fare a meno? Per quanto tempo?



Qualche esperienza “sul campo”

[UNICH-LogMon]Event detected - WARNING : Autentic...erena.damiani - Mozilla Thunderbird (tablet-damiano)

File Edit View Go Message Enigmail Tools Help

Get Messages | Write | Chat | Address Book | Tag

Reply | Forward | Archive | Junk | Delete | More

From log-monitor@noc.unich.it

Subject **[UNICH-LogMon]Event detected - WARNING : Autenticazione SASL fallita per User name: Ve[redacted]ni** 21/05/2018 21:21

To staff@noc.unich.it

```
Numero degli eventi rilevati: 1
Finestra temporale di rilevazione: 0.5 min.
AS number: 12876
AS name: ONLINE S.A.S.
Country code: FR
Country name: France
Region name: Ile-de-France

2018-05-21T21:21:25+02:00 noc3 postfwd2/policy[10938]: [RULES] rule=6, id=SASL-BAD-USER,
client=unknown[163.172.204.77], user=Ve[redacted]ni, sender=<pa33ola.cetera@unibas.it>, recipient=
<rob849219@gmail.com>, helo=<[10.200.4.158]>, proto=ESMTP, state=RCPT, delay=0.08s, hits=SASL-BAD-USER,
action=REJECT SASL_FORBIDDEN - Ve[redacted] is not an authorized SASL user
```

Due casi in cui lo “username” serve….
ma a BASSA retention

Retention in ambito e-mail

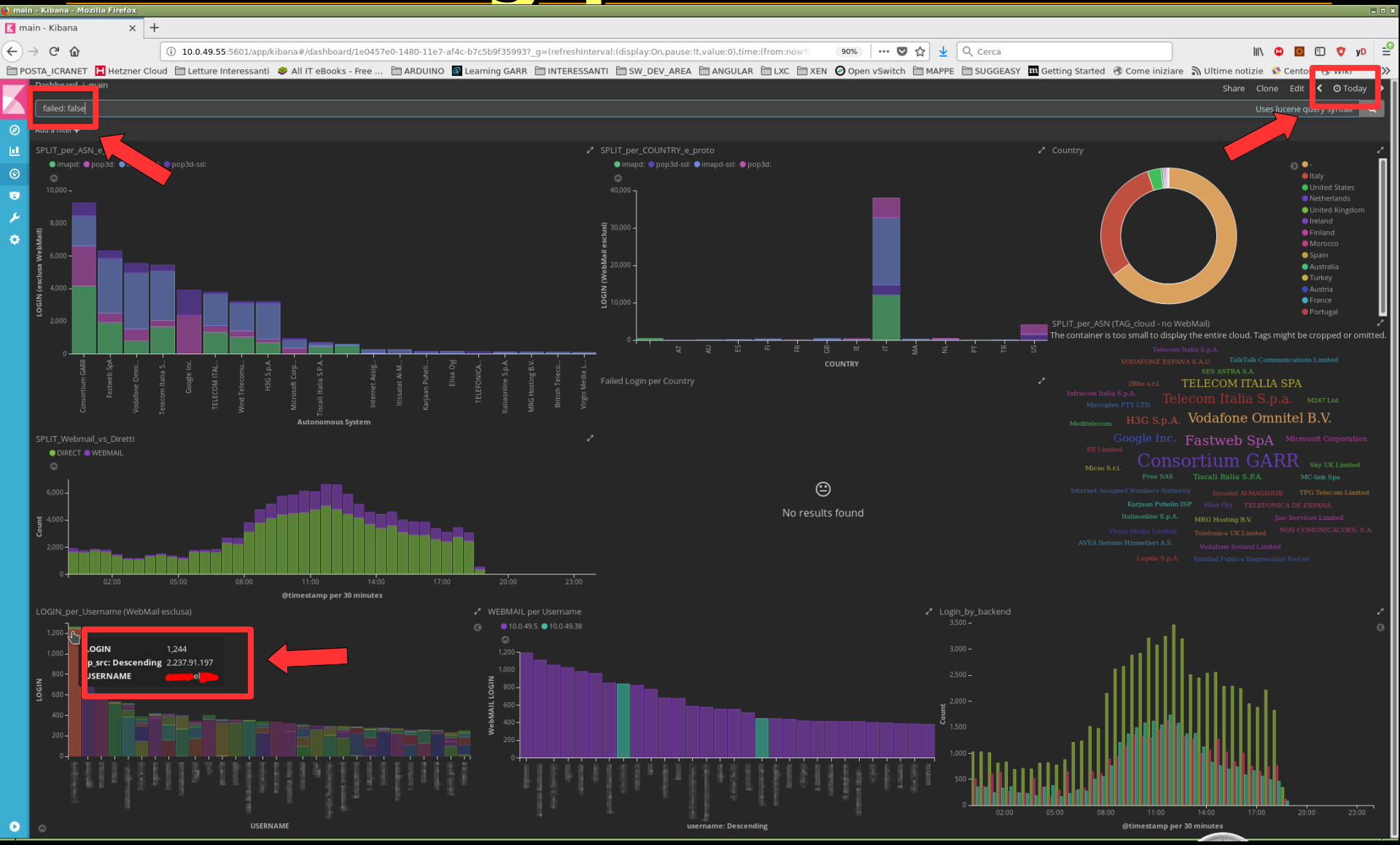
- Un “upper bound” alla retention di informazioni personali legati alla Posta Elettronica la possiamo derivare direttamente dal Garante:

“...Costituiscono parte integrante di questi strumenti anche i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore (ad esempio: ***sistemi di logging per il corretto esercizio del servizio di posta elettronica****, con conservazione dei soli dati esteriori, contenuti nella cosiddetta "envelope" del messaggio,* ***per una breve durata non superiore comunque ai sette giorni****;...)...”*

Fonte: Provvedimento n. 303 del 13 luglio 2016 - doc. web n. 5408460 “Trattamento di dati personali dei dipendenti mediante posta elettronica e altri strumenti di lavoro” - Capoverso 4.3

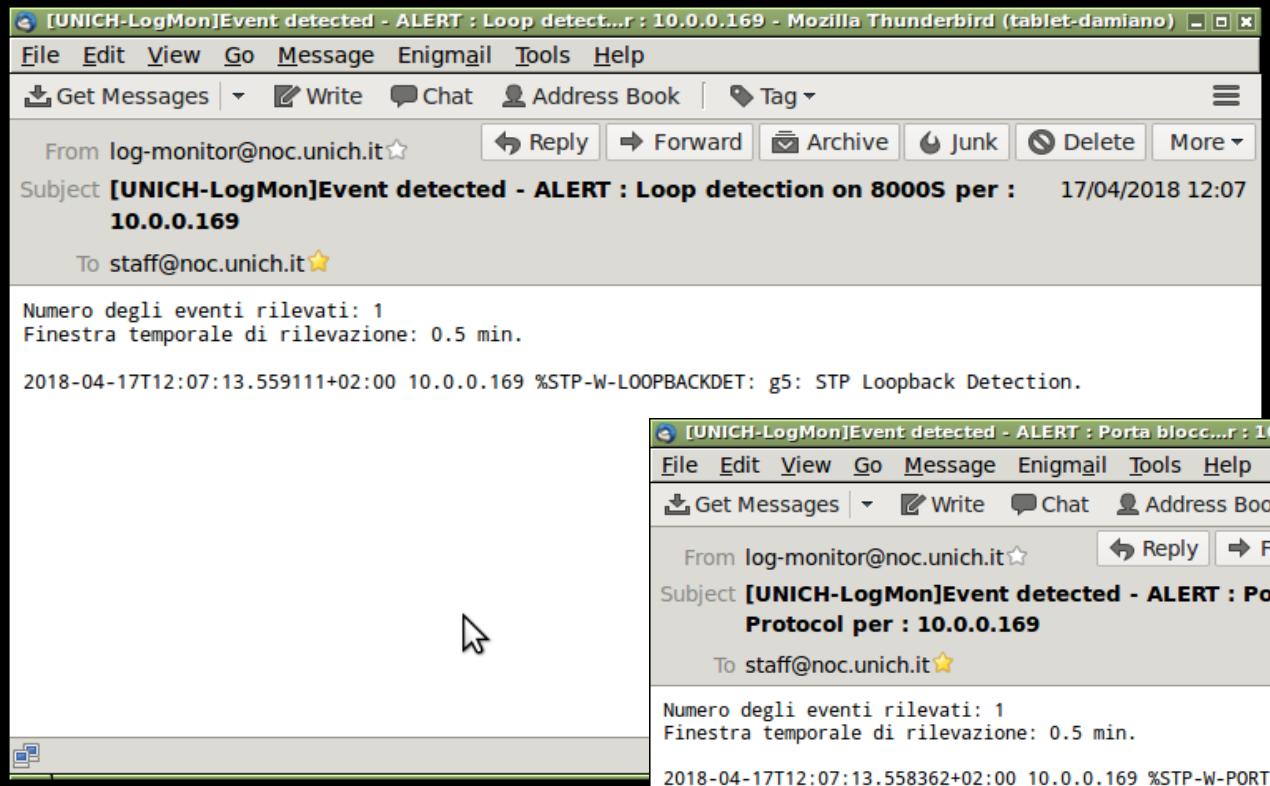
Cosa fare dopo 7 giorni?
rm? encrypt? anonymize? altro?

Email: big-picture 1

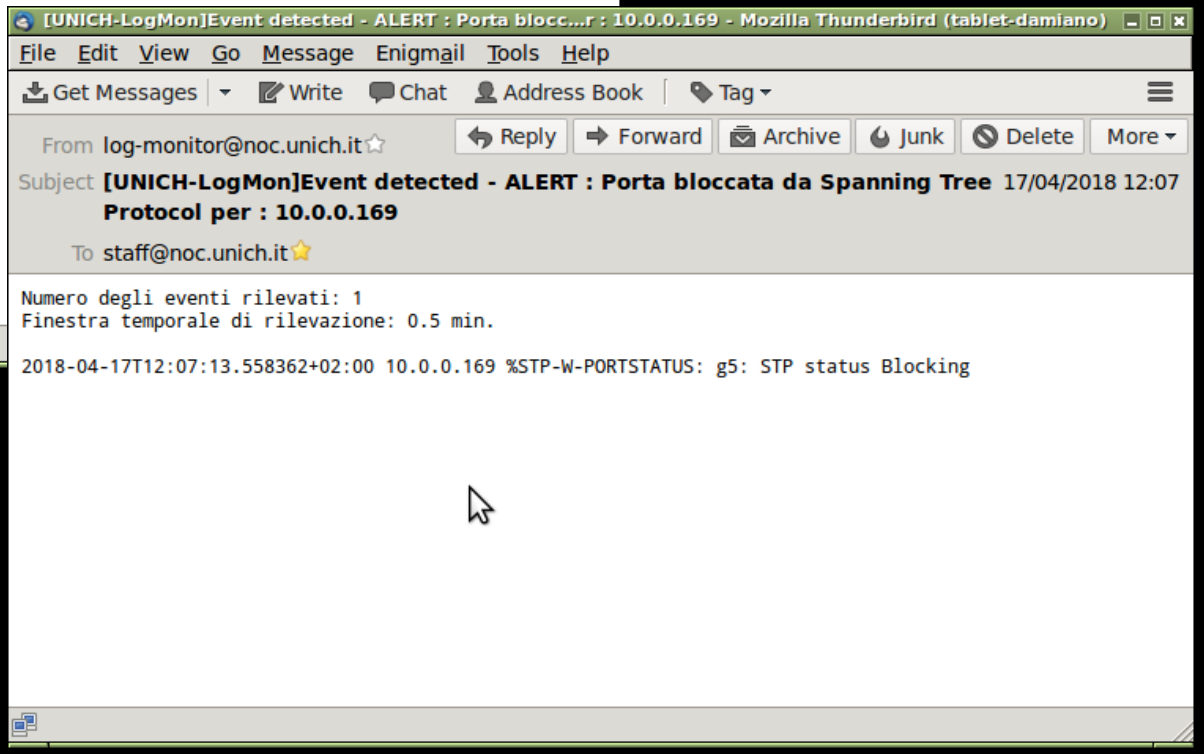


Email: big-picture 2

Network monitoring 1



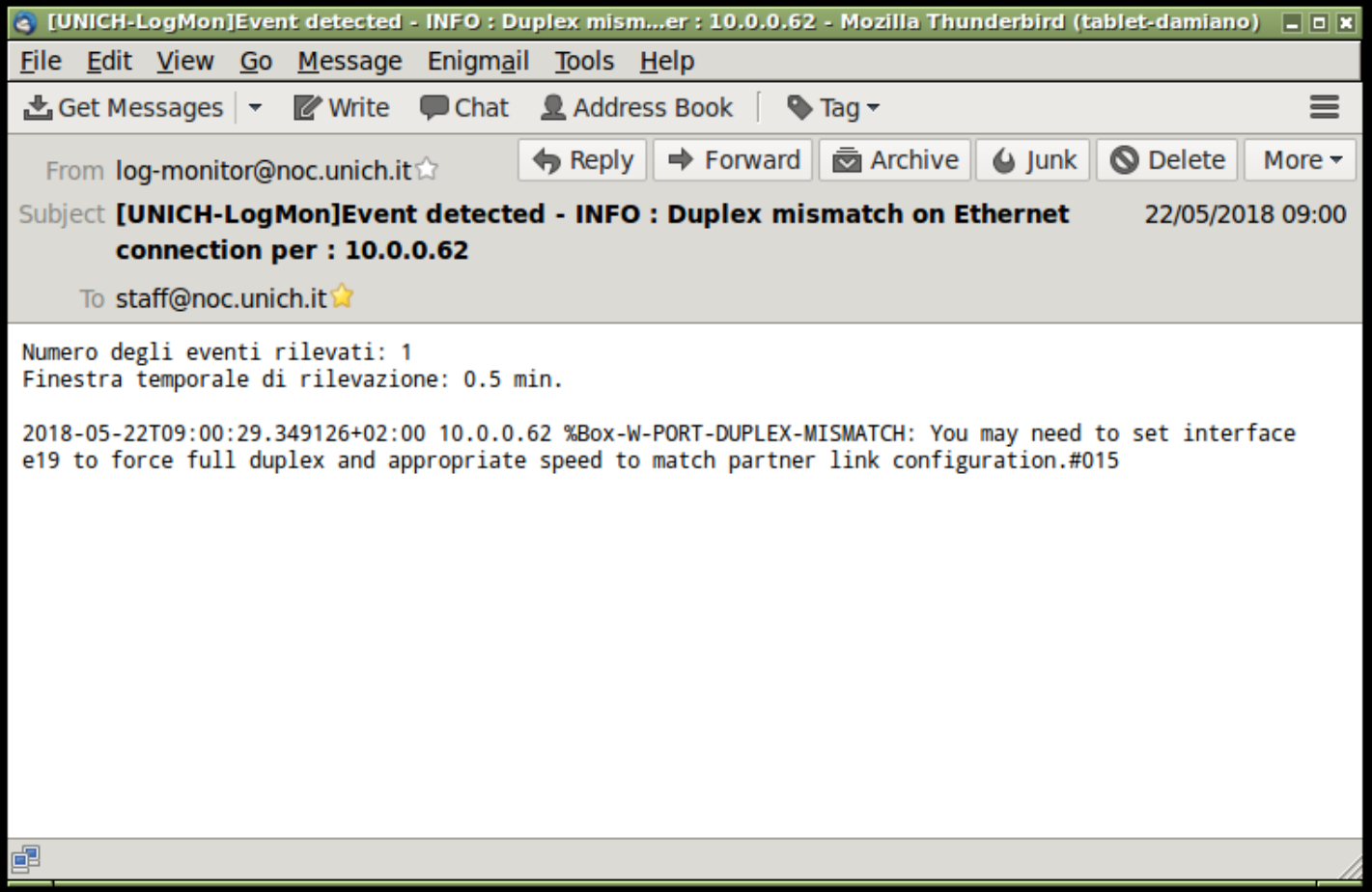
Il troubleshooting di segmenti L2 **richiede** (sempre?) soltanto riferimenti agli apparati ed alle porte. Al più, ai MAC. MAI all'utente.



Apparati diversi possono fornire messaggi diversi.
Ma comunque l'utente (username) resta un (inutile) "optional"

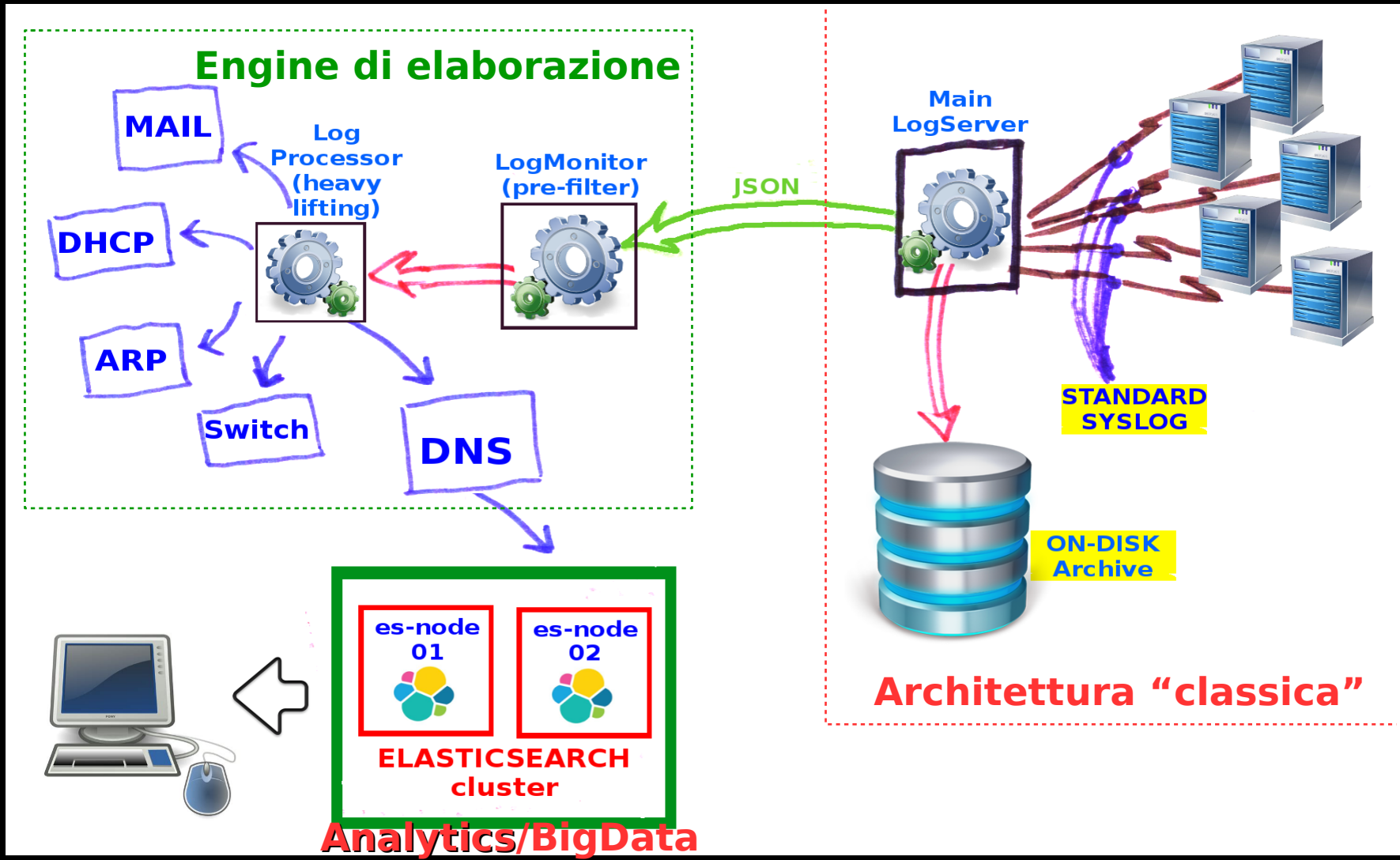
Network monitoring 2

- Con infrastrutture adeguate, si possono intercettare anche le anomalie (quasi) insignificanti:

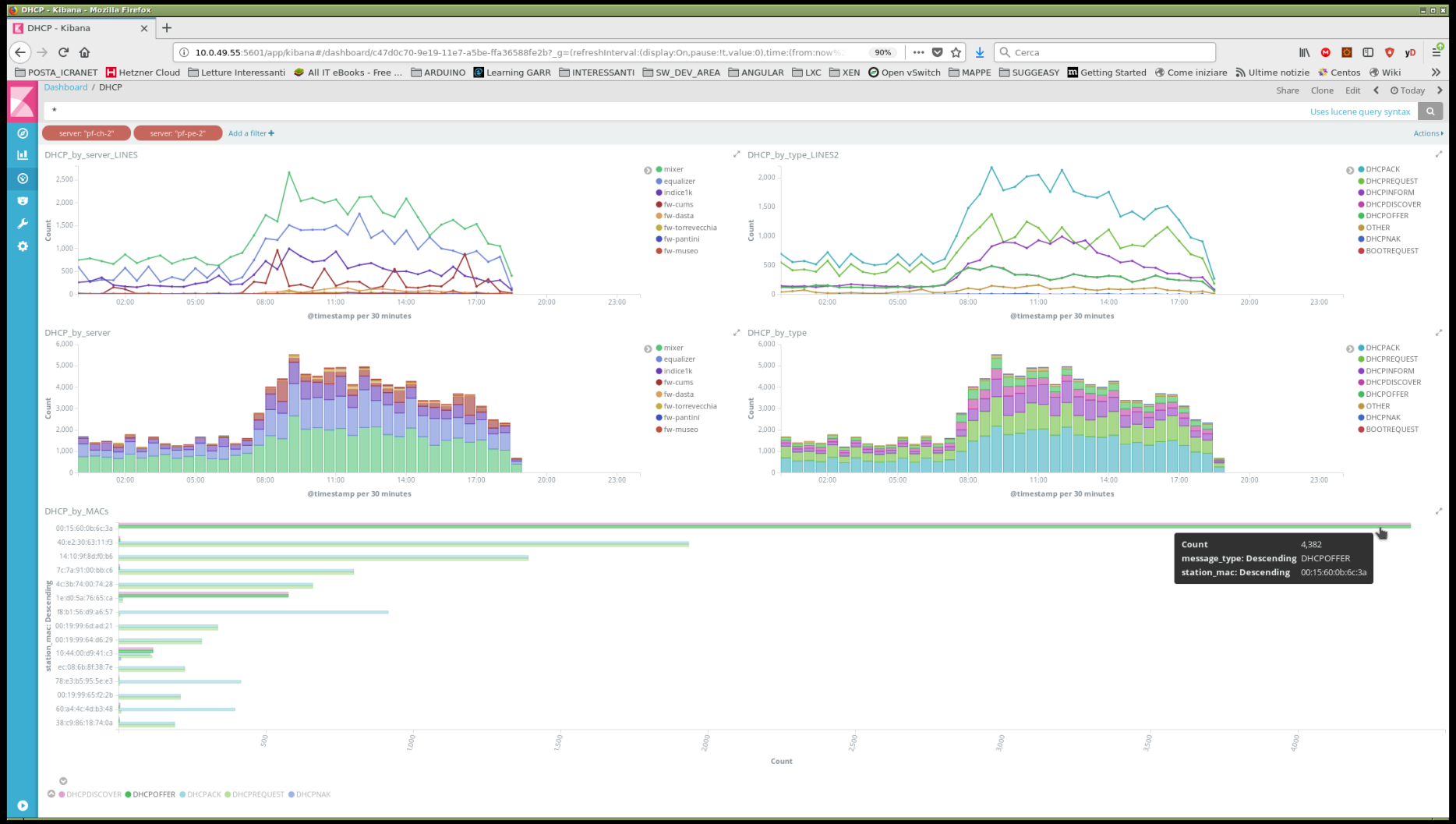


“duplex-mismatch”: esagerato? Si? No? Parliamone....

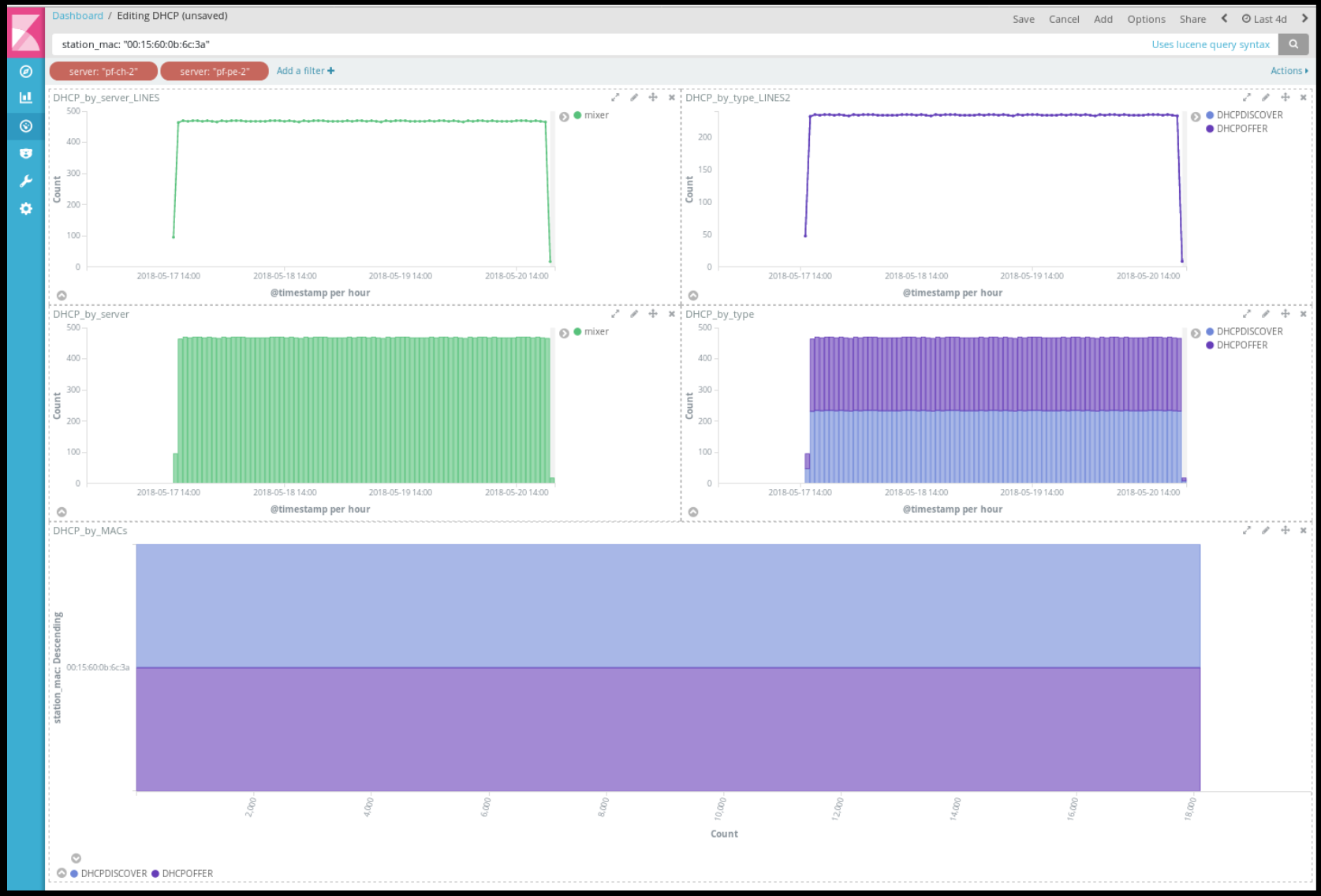
Log-Monitor: architettura



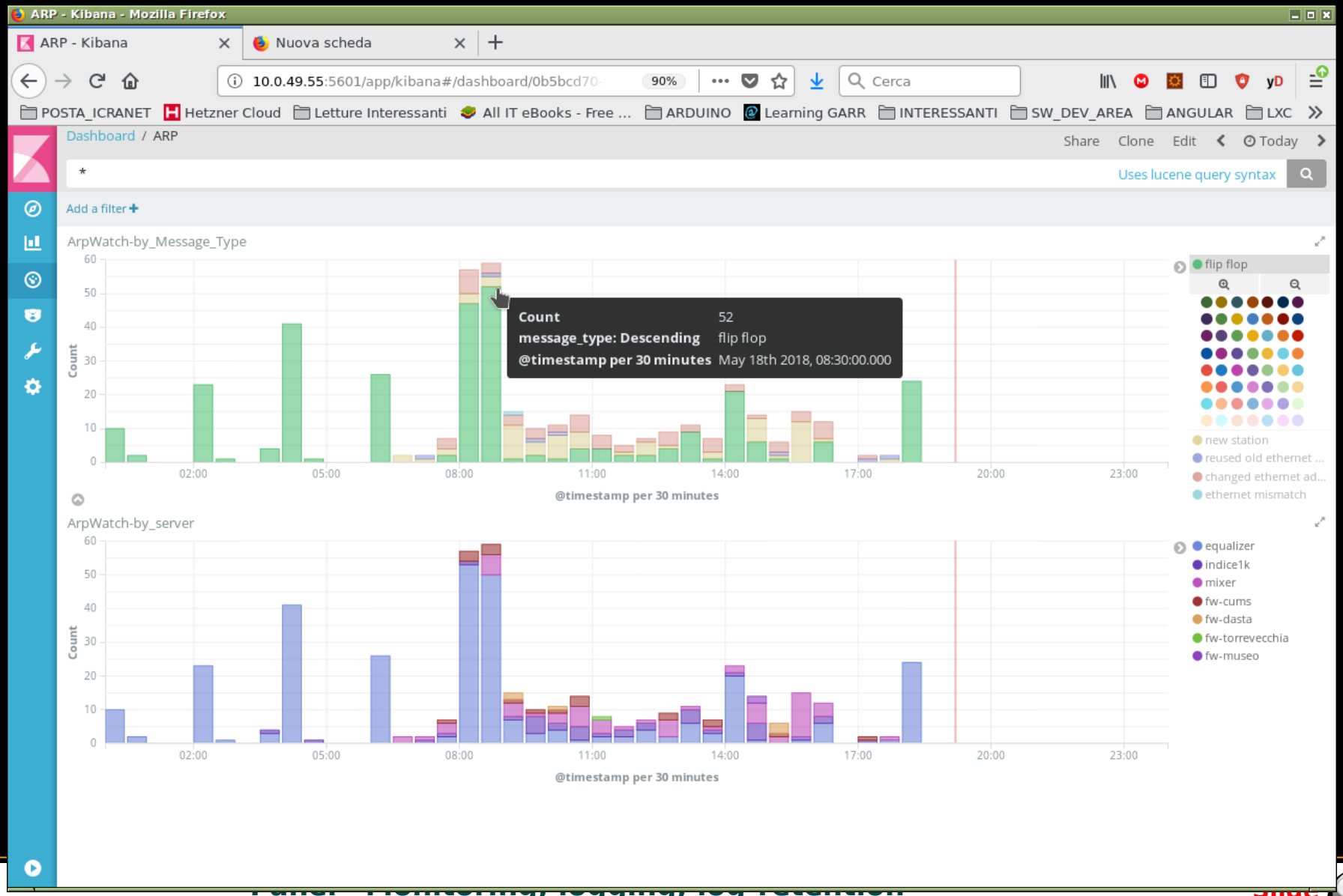
DHCP 1a


DHCP - Kibana - Mozilla Firefox
DHCP - Kibana
10.0.49.55:5601/app/kibana#/dashboard/c47d0c70-9e19-11e7-a5be-ffa36588fe2b?_g=(refreshInterval:(display:On,pause:!t,value:0),time:(from:now%
Dashboard / DHCP
Share
Clone
Edit
Today
Uses lucene query syntax
server: "pf-ch-2"
server: "pf-pe-2"
Add a filter
Actions
DHCP_by_server_LINES
DHCP_by_type_LINES2
DHCP_by_server
DHCP_by_type
DHCP_by_MACs
mixer
equalizer
indice1k
fw-cums
fw-dasta
fw-torrevecchia
fw-pantini
fw-museo
DHCPACK
DHCPREQUEST
DHCPINFORM
DHCPDISCOVER
DHCPOFFER
OTHER
DHCPNAK
BOOTREQUEST
Count
@timestamp per 30 minutes
station_mac: Descending
Count 4,382
message_type: Descending DHCPOFFER
station_mac: Descending 00:15:60:0b:6c:3a

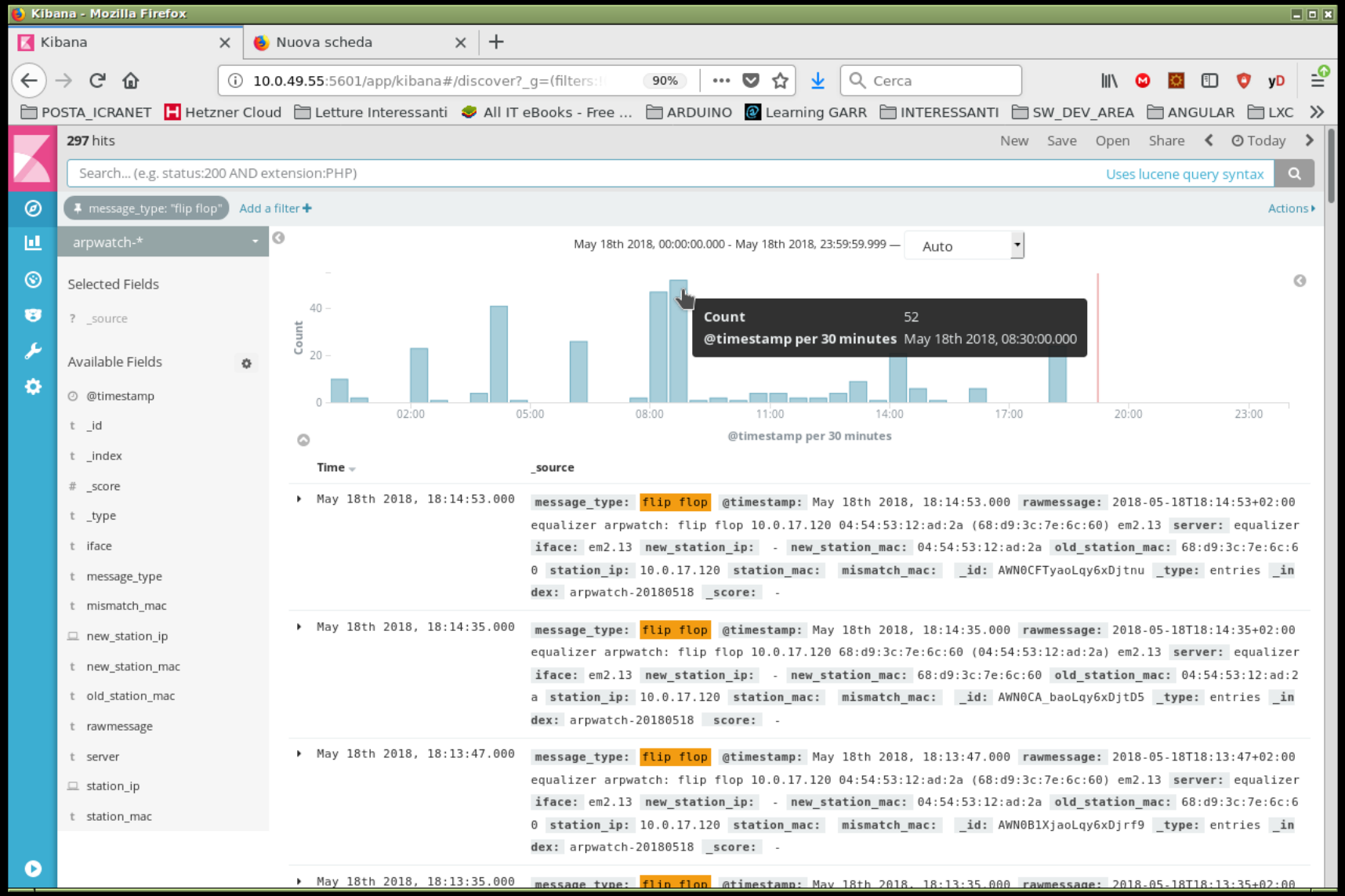
DHCP 1b


Dashboard / Editing DHCP (unsaved)
Save
Cancel
Add
Options
Share
Last 4d
station_mac: "00:15:60:0b:6c:3a"
Uses lucene query syntax
server: "pf-ch-2"
server: "pf-pe-2"
Add a filter +
Actions
DHCP_by_server_LINES
mixer
Count
@timestamp per hour
DHCP_by_type_LINES2
DHCPDISCOVER
DHCPOFFER
DHCP_by_server
DHCP_by_type
DHCP_by_MACs
station_mac: Descending
00:15:60:0b:6c:3a
Count

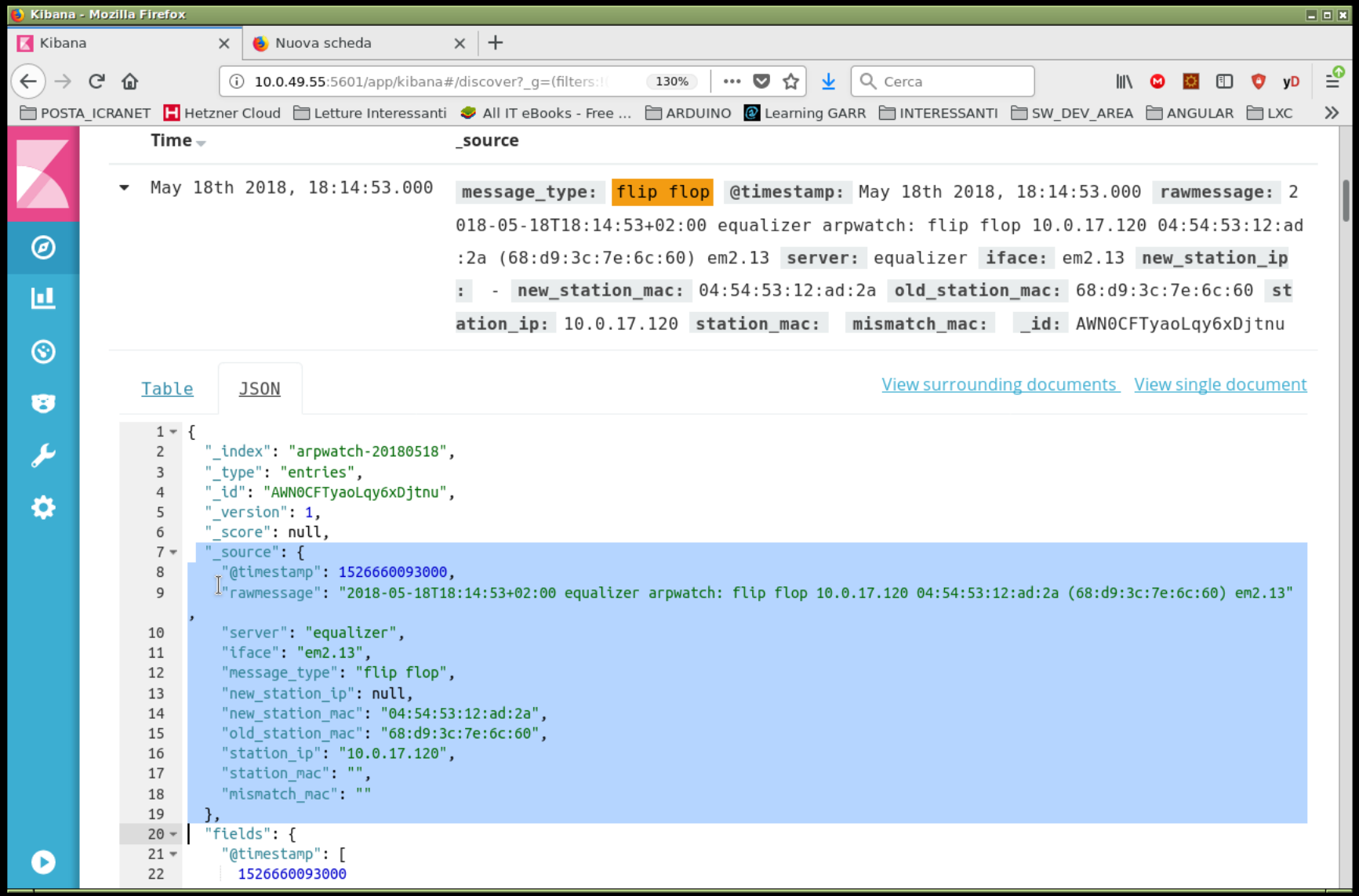
ARP / Flip-Flop 1



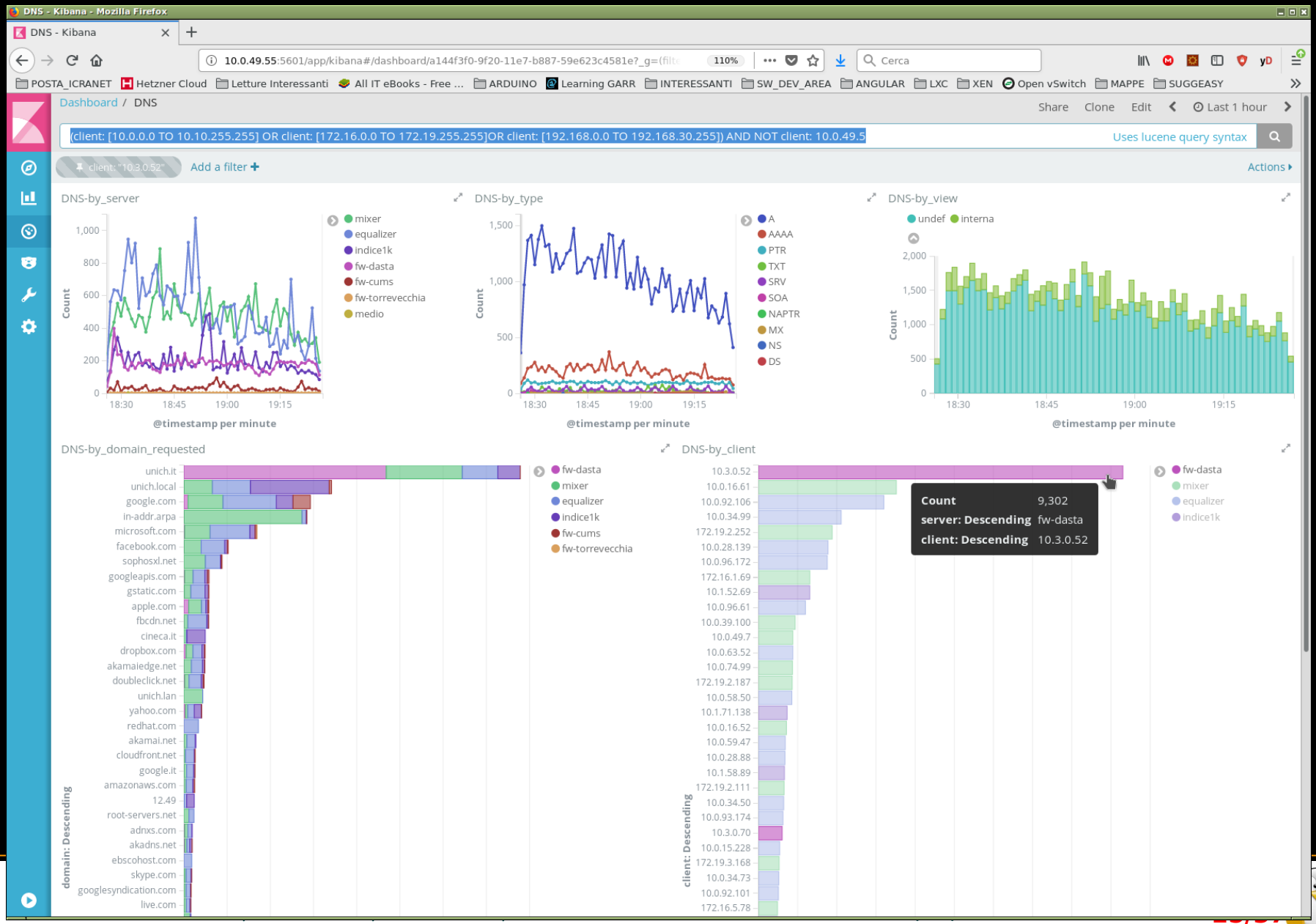
ARP / Flip-Flop 2



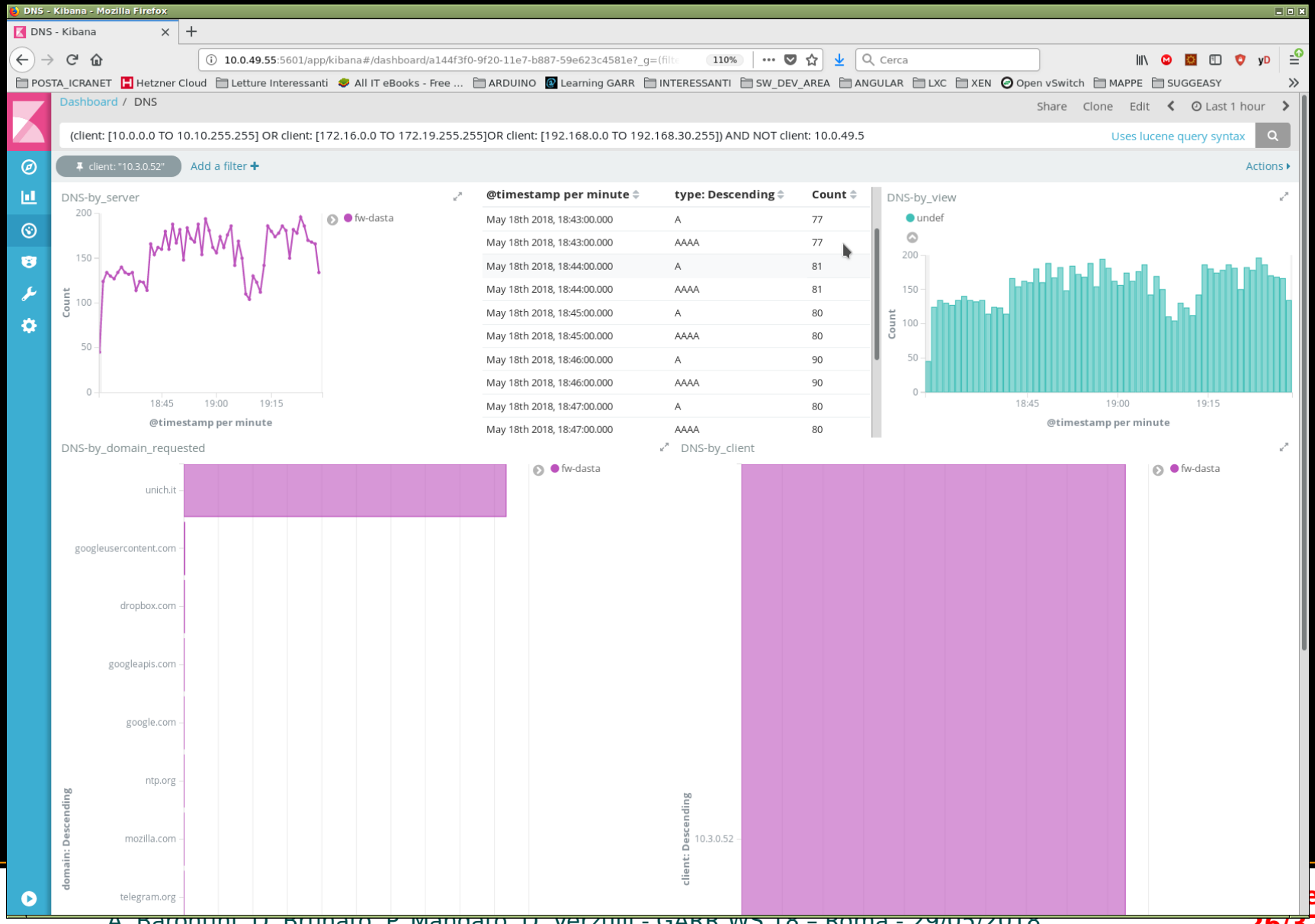
ARP / Flip-Flop 3



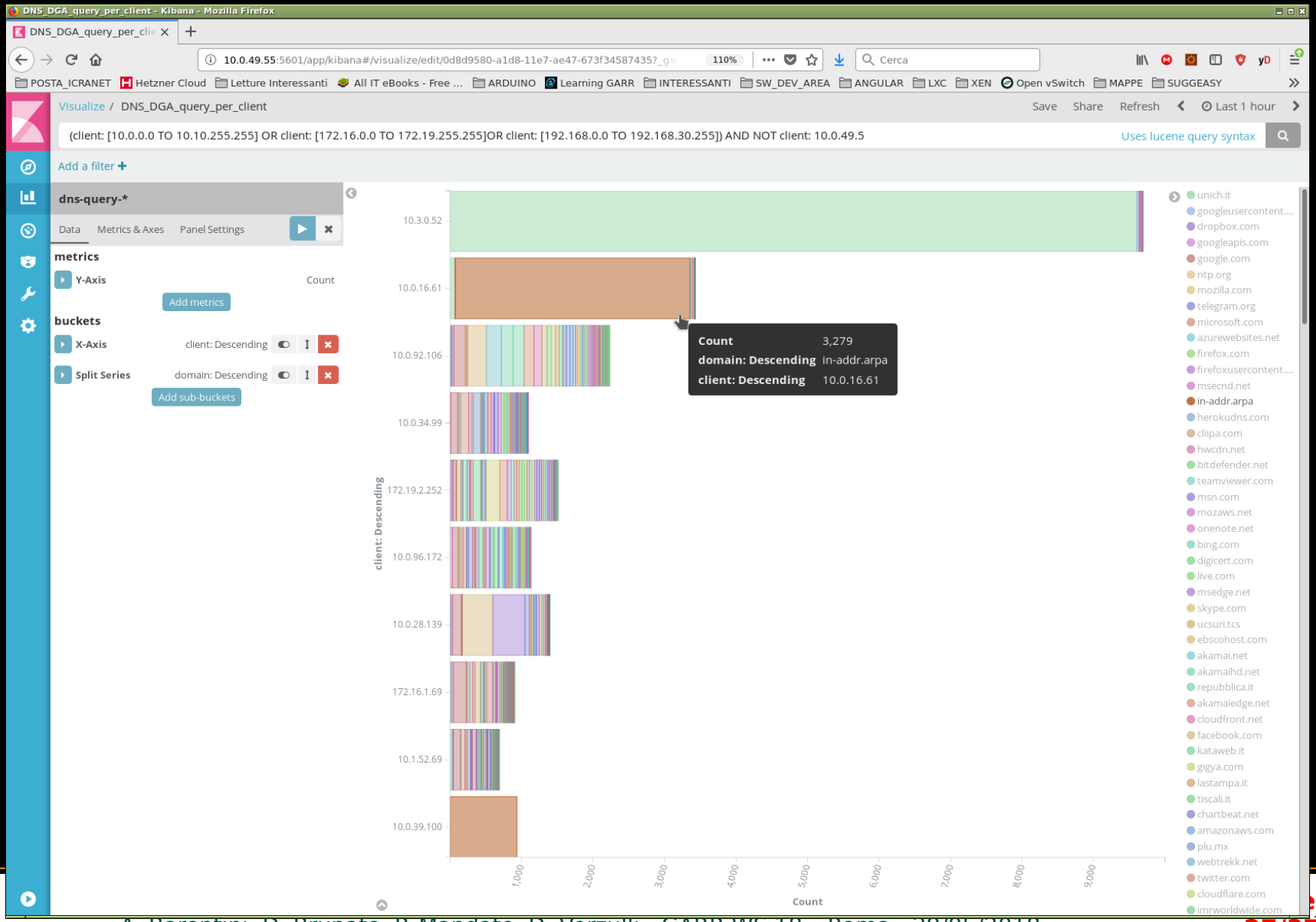
DNS 1


DNS - Kibana - Mozilla Firefox
DNS - Kibana
10.0.49.55:5601/app/kibana#/dashboard/a144f3f0-9f20-11e7-b887-59e623c4581e?_g=(filt
110%
Cerca
POSTA_ICRANET
Hetzner Cloud
Letture Interessanti
All IT eBooks - Free ...
ARDUINO
Learning GARR
INTERESSANTI
SW_DEV_AREA
ANGULAR
LXC
XEN
Open vSwitch
MAPPE
SUGGEASY
Dashboard / DNS
Share
Clone
Edit
Last 1 hour
(client: [10.0.0.0 TO 10.10.255.255] OR client: [172.16.0.0 TO 172.19.255.255]OR client: [192.168.0.0 TO 192.168.30.255]) AND NOT client: 10.0.49.5
Uses lucene query syntax
client: "10.3.0.52"
Add a filter +
Actions
DNS-by_server
mixer
equalizer
indice1k
fw-dasta
fw-cums
fw-torrevecchia
medio
Count
@timestamp per minute
DNS-by_type
A
AAAA
PTR
TXT
SRV
SOA
NAPTR
MX
NS
DS
DNS-by_view
undef
interna
DNS-by_domain_requested
unich.it
unich.local
google.com
in-addr.arpa
microsoft.com
facebook.com
sophosxl.net
googleapis.com
gstatic.com
apple.com
fbcdn.net
cineca.it
dropbox.com
akamaiedge.net
doubleclick.net
unich.lan
yahoo.com
redhat.com
akamai.net
cloudfront.net
google.it
amazonaws.com
12.49
root-servers.net
adnxs.com
akadns.net
ebscohost.com
skype.com
googlesyndication.com
live.com
domain: Descending
DNS-by_client
10.3.0.52
10.0.16.61
10.0.92.106
10.0.34.99
172.19.2.252
10.0.28.139
10.0.96.172
172.16.1.69
10.1.52.69
10.0.96.61
10.0.39.100
10.0.49.7
10.0.63.52
10.0.74.99
172.19.2.187
10.0.58.50
10.1.71.138
10.0.16.52
10.0.59.47
10.0.28.88
10.1.58.89
172.19.2.111
10.0.34.50
10.0.93.174
10.3.0.70
10.0.15.228
172.19.3.168
10.0.34.73
10.0.92.101
172.16.5.78
client: Descending
Count 9,302
server: Descending fw-dasta
client: Descending 10.3.0.52

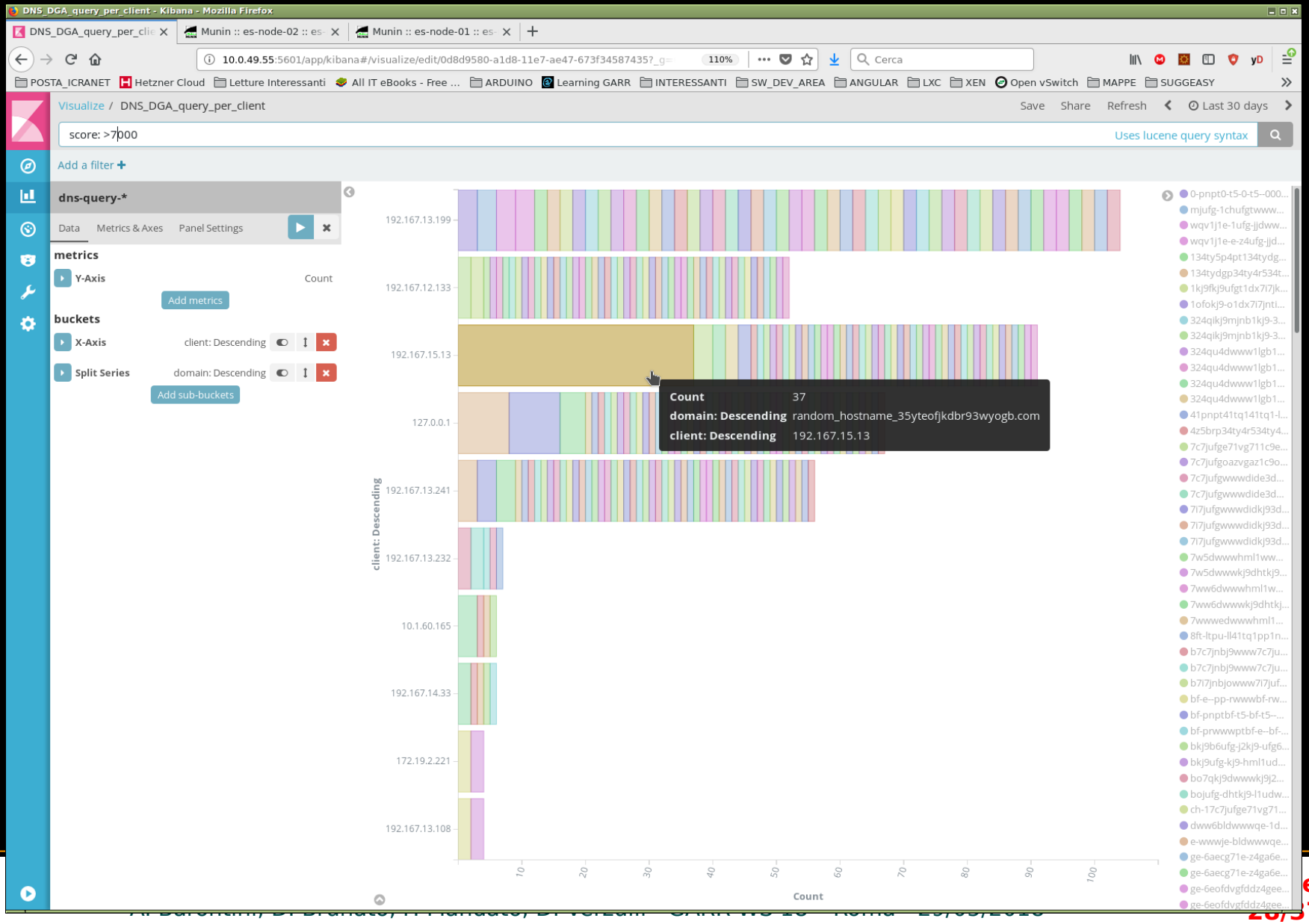
DNS 2


DNS - Kibana - Mozilla Firefox
DNS - Kibana
10.0.49.55:5601/app/kibana#/dashboard/a144f3f0-9f20-11e7-b887-59e623c4581e?_g=(filt
110%
Cerca
POSTA_ICRANET
Hetzner Cloud
Letture Interessanti
All IT eBooks - Free ...
ARDUINO
Learning GARR
INTERESSANTI
SW_DEV_AREA
ANGULAR
LXC
XEN
Open vSwitch
MAPPE
SUGGEASY
Dashboard / DNS
Share
Clone
Edit
Last 1 hour
(client: [10.0.0.0 TO 10.10.255.255] OR client: [172.16.0.0 TO 172.19.255.255]OR client: [192.168.0.0 TO 192.168.30.255]) AND NOT client: 10.0.49.5
Uses lucene query syntax
client: "10.3.0.52"
Add a filter +
Actions
DNS-by_server
fw-dasta
Count
@timestamp per minute
@timestamp per minute
type: Descending
Count
May 18th 2018, 18:43:00.000 A 77
May 18th 2018, 18:43:00.000 AAAA 77
May 18th 2018, 18:44:00.000 A 81
May 18th 2018, 18:44:00.000 AAAA 81
May 18th 2018, 18:45:00.000 A 80
May 18th 2018, 18:45:00.000 AAAA 80
May 18th 2018, 18:46:00.000 A 90
May 18th 2018, 18:46:00.000 AAAA 90
May 18th 2018, 18:47:00.000 A 80
May 18th 2018, 18:47:00.000 AAAA 80
DNS-by_view
undef
Count
@timestamp per minute
DNS-by_domain_requested
fw-dasta
unich.it
googleusercontent.com
dropbox.com
googleapis.com
google.com
ntp.org
mozilla.com
telegram.org
domain: Descending
DNS-by_client
fw-dasta
client: Descending
10.3.0.52

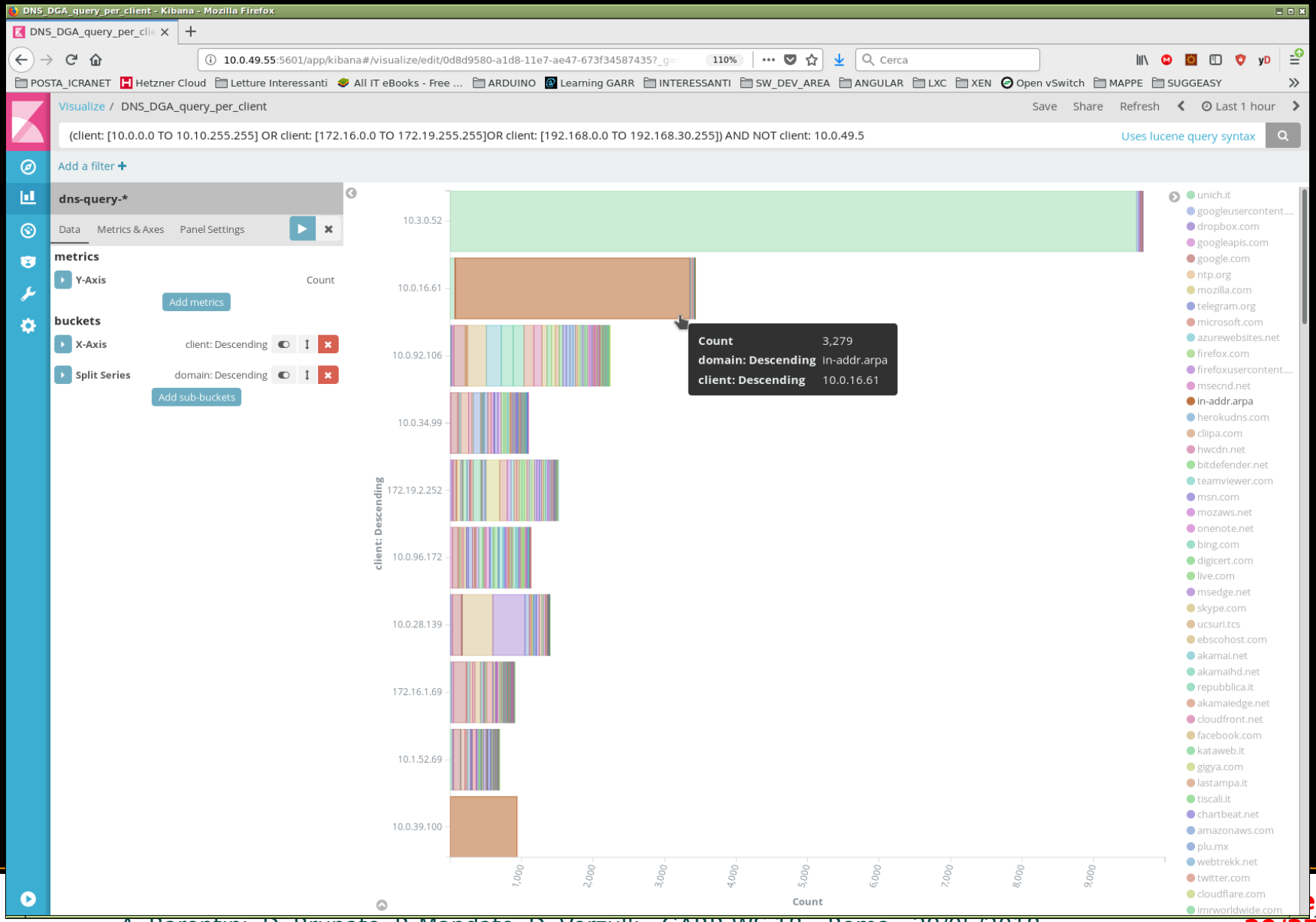
DNS 3


DNS_DGA_query_per_client - Kibana - Mozilla Firefox
10.0.49.55:5601/app/kibana#/visualize/edit/0d8d9580-a1d8-11e7-ae47-673f34587435?_g=
Visualize / DNS_DGA_query_per_client
Save
Share
Refresh
Last 1 hour
(client: [10.0.0.0 TO 10.10.255.255] OR client: [172.16.0.0 TO 172.19.255.255]OR client: [192.168.0.0 TO 192.168.30.255]) AND NOT client: 10.0.49.5
Uses lucene query syntax
Add a filter
dns-query-*
Data
Metrics & Axes
Panel Settings
metrics
Y-Axis
Count
Add metrics
buckets
X-Axis
client: Descending
Split Series
domain: Descending
Add sub-buckets
10.3.0.52
10.0.16.61
10.0.92.106
10.0.34.99
172.19.2.252
10.0.96.172
10.0.28.139
172.16.1.69
10.1.52.69
10.0.39.100
client: Descending
Count
3,279
domain: Descending
in-addr.arpa
client: Descending
10.0.16.61
1,000
2,000
3,000
4,000
5,000
6,000
7,000
8,000
9,000
Count
unich.it
googleusercontent....
dropbox.com
googleapis.com
google.com
ntp.org
mozilla.com
telegram.org
microsoft.com
azurewebsites.net
firefox.com
firefoxusercontent....
msecnd.net
in-addr.arpa
herokudns.com
cliipa.com
hwcdn.net
bitdefender.net
teamviewer.com
msn.com
mozaws.net
onenote.net
bing.com
digicert.com
live.com
msedge.net
skype.com
ucsuri.tcs
ebscohost.com
akamai.net
akamaihd.net
repubblica.it
akamaiedge.net
cloudfront.net
facebook.com
kataweb.it
gigya.com
lastampa.it
tiscali.it
chartbeat.net
amazonaws.com
plu.mx
webtrekk.net
twitter.com
cloudflare.com
imrworldwide.com

DNS 4

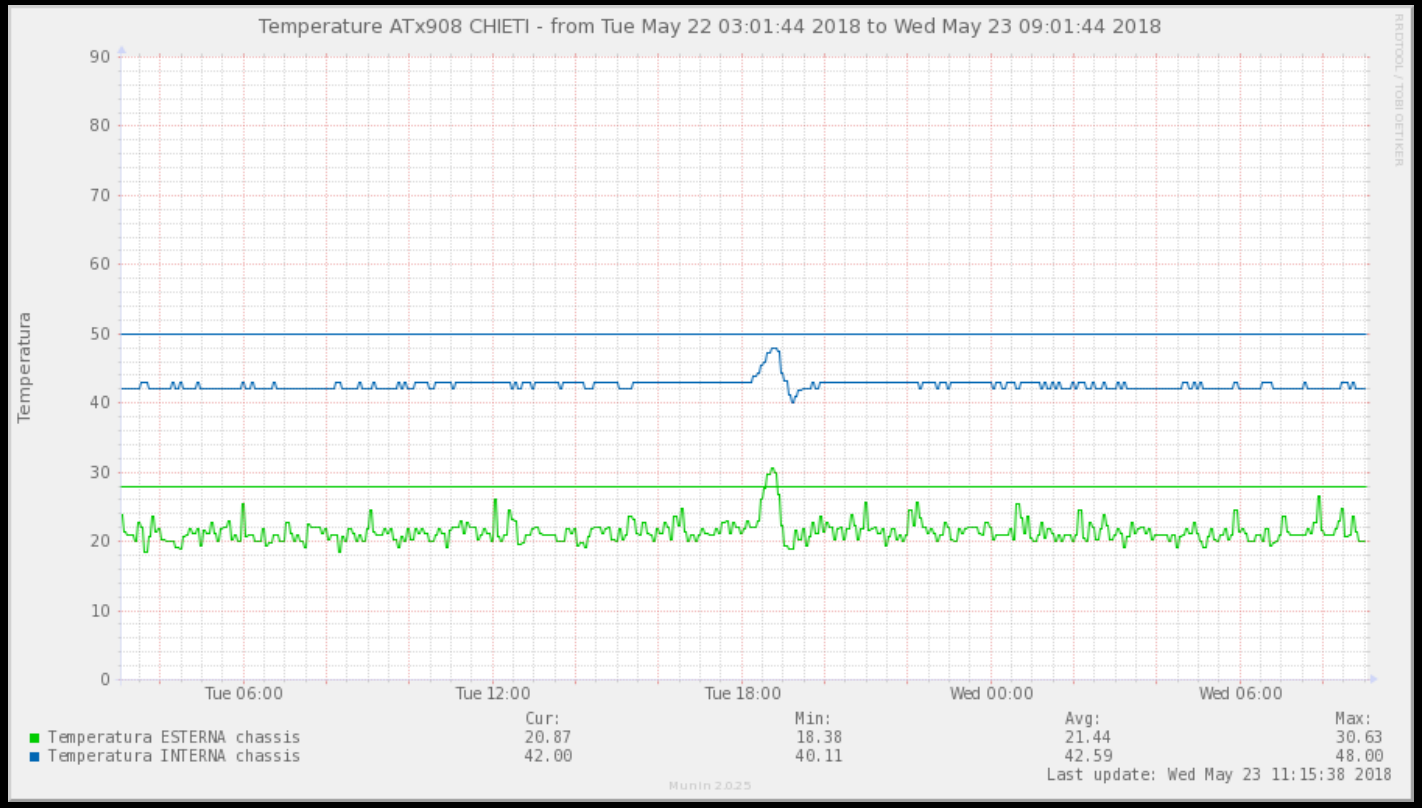

DNS_DGA_query_per_client - Kibana - Mozilla Firefox
Visualize / DNS_DGA_query_per_client
Save
Share
Refresh
Last 30 days
score: >7000
Uses lucene query syntax
Add a filter +
dns-query-*
Data
Metrics & Axes
Panel Settings
metrics
Y-Axis
Count
Add metrics
buckets
X-Axis
client: Descending
Split Series
domain: Descending
Add sub-buckets
192.167.13.199
192.167.12.133
192.167.15.13
127.0.0.1
192.167.13.241
192.167.13.232
10.1.60.165
192.167.14.33
172.19.2.221
192.167.13.108
client: Descending
Count
Count 37
domain: Descending random_hostname_35yteofjkdbr93wyogb.com
client: Descending 192.167.15.13
10
20
30
40
50
60
70
80
90
100
Count

DNS 3


DNS_DGA_query_per_client - Kibana - Mozilla Firefox
10.0.49.55:5601/app/kibana#/visualize/edit/0d8d9580-a1d8-11e7-ae47-673f34587435?_g=
Visualize / DNS_DGA_query_per_client
Save
Share
Refresh
Last 1 hour
(client: [10.0.0.0 TO 10.10.255.255] OR client: [172.16.0.0 TO 172.19.255.255]OR client: [192.168.0.0 TO 192.168.30.255]) AND NOT client: 10.0.49.5
Uses lucene query syntax
Add a filter
dns-query-*
Data
Metrics & Axes
Panel Settings
metrics
Y-Axis
Count
Add metrics
buckets
X-Axis
client: Descending
Split Series
domain: Descending
Add sub-buckets
10.3.0.52
10.0.16.61
10.0.92.106
10.0.34.99
172.19.2.252
10.0.96.172
10.0.28.139
172.16.1.69
10.1.52.69
10.0.39.100
client: Descending
Count
Count 3,279
domain: Descending in-addr.arpa
client: Descending 10.0.16.61
1,000
2,000
3,000
4,000
5,000
6,000
7,000
8,000
9,000
unich.it
googleusercontent....
dropbox.com
googleapis.com
google.com
ntp.org
mozilla.com
telegram.org
microsoft.com
azurewebsites.net
firefox.com
firefoxusercontent....
msecnd.net
in-addr.arpa
herokudns.com
cliipa.com
hwcdn.net
bitdefender.net
teamviewer.com
msn.com
mozaws.net
onenote.net
bing.com
digicert.com
live.com
msedge.net
skype.com
ucsuri.tcs
ebscohost.com
akamai.net
akamaihd.net
repubblica.it
akamaiedge.net
cloudfront.net
facebook.com
kataweb.it
gigya.com
lastampa.it
tiscali.it
chartbeat.net
amazonaws.com
plu.mx
webtrekk.net
twitter.com
cloudflare.com
imrworldwide.com

“Altri” tipi di monitoraggio

- A volte, strumenti di monitoraggio pensati per uno scopo, possono produrre “informazioni” di altro genere

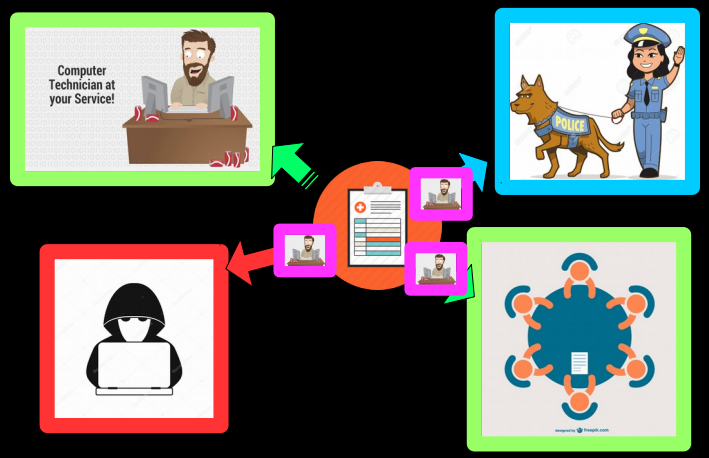


Utile? Inutile? Parliamone...

A proposito di MAC....

- Ripartendo da questo precedente passaggio

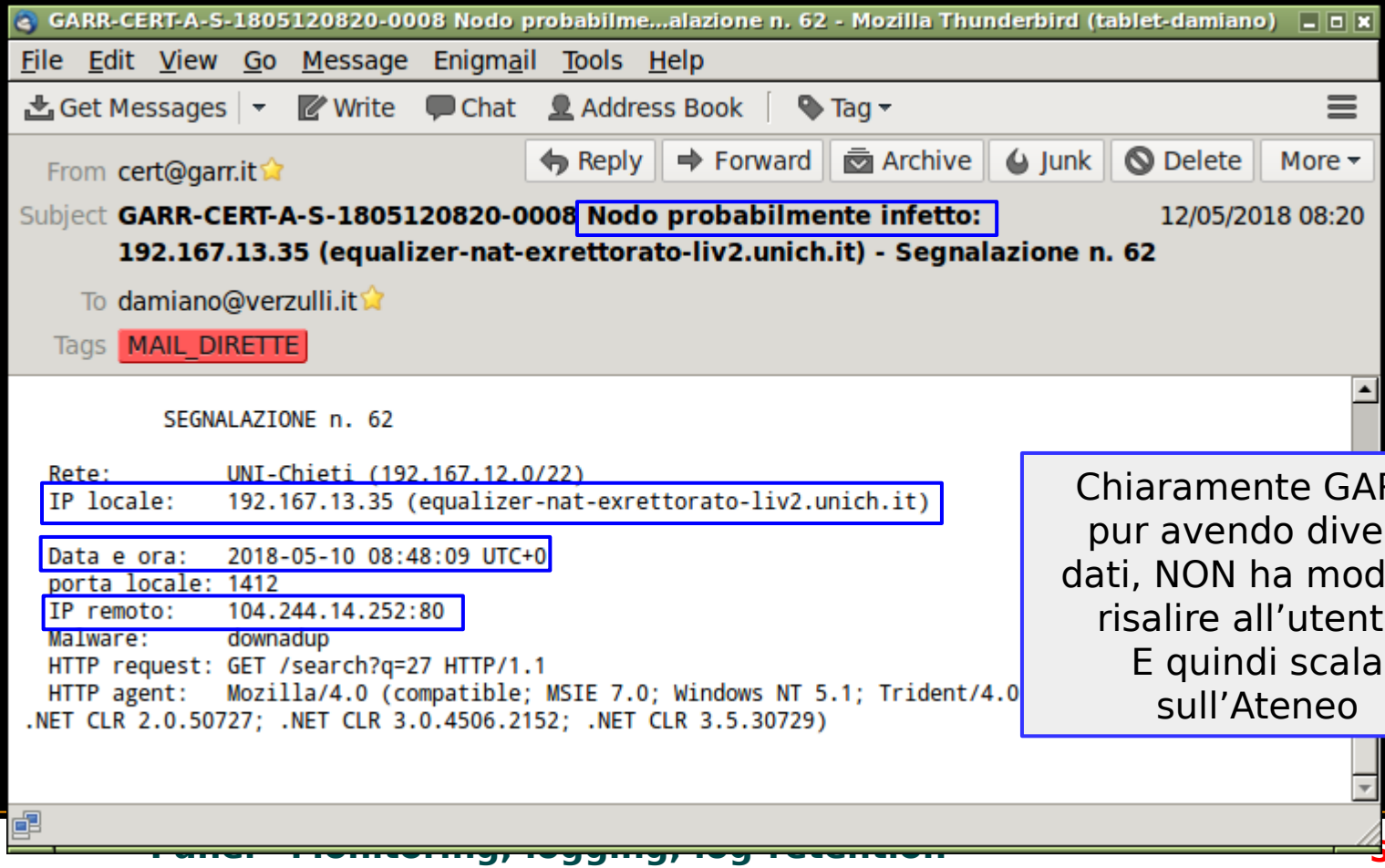
In una LAN viaggiano frame Ethernet. Per garantire SLA in ambito L2, servono i MAC (e non gli username [che stanno a L7])



...e focalizzati unicamente sugli aspetti di “gestione” dell’infrastruttura LAN, proviamo a capire se sia realmente possibile “monitorare” la rete, senza tirare in ballo “username”

NetMon/L2-Flows: 1

- Supponiamo che GARR-CERT invii una segnalazione relativa ad attività “malevole” generata da una postazione INTERNA



Chiaramente GARR, pur avendo diversi dati, NON ha modo di risalire all’utente. E quindi scala sull’Ateneo

NetMon/L2-Flows: 2

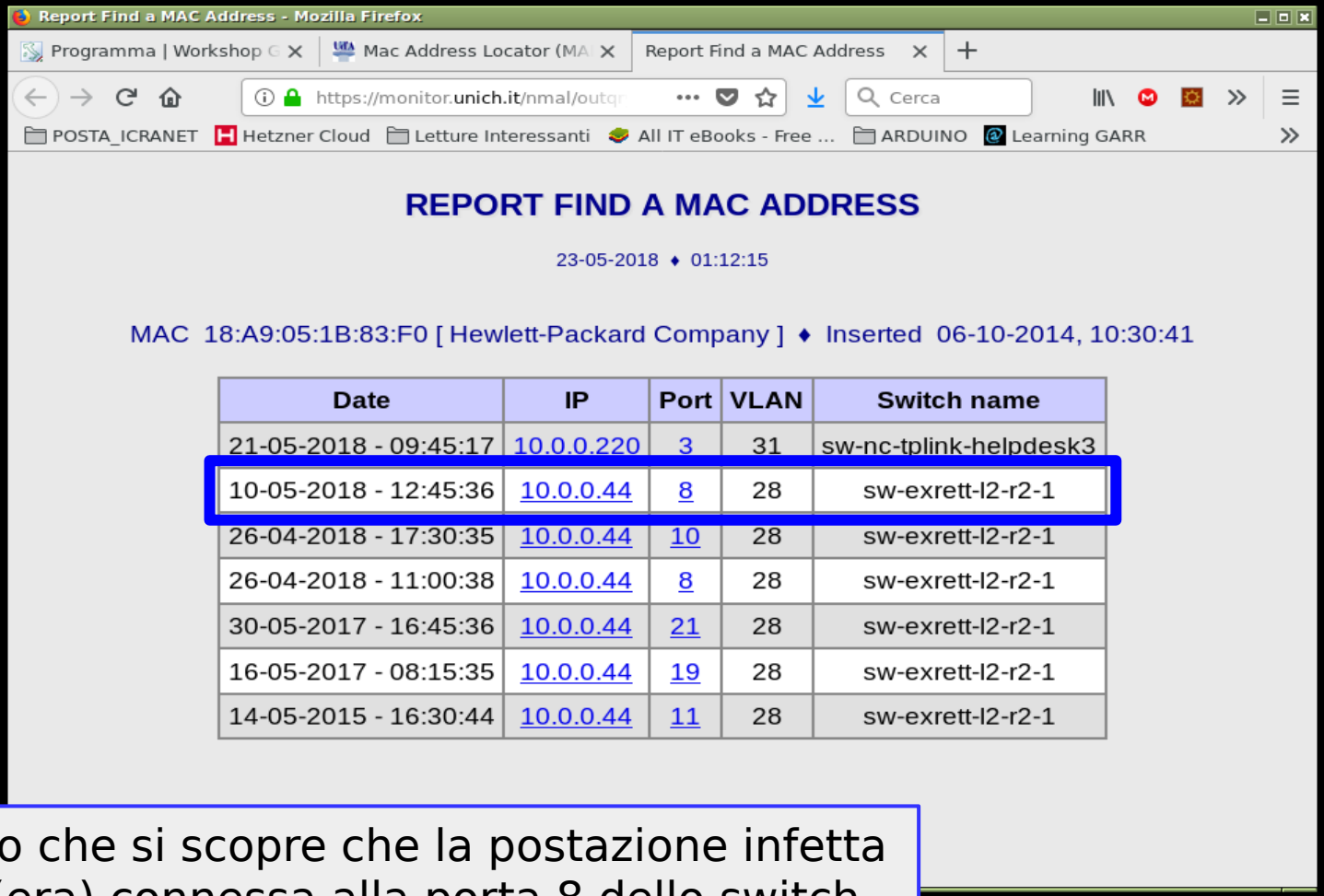
- Supponiamo che l'Ateneo tenga traccia del traffico LAN, a livello 2 e 3 (src_mac, dst_mac, src_ip, dst_ip, src_port, dst_port, proto)

```
[root@logsrv em2.28]# pwd
/var/log/2018/05/10/pmacct/equalizer/em2.28
[root@logsrv em2.28]# zgrep 104.244.14.252 *gz | sort -k 2
pmacct.201805101048.gz:b0:83:fe:cf:ce:81  18:a9:05:1b:83:f0  104.244.14.252  10.0.28.177      80    1401    4 192
pmacct.201805101048.gz:b0:83:fe:cf:ce:81  18:a9:05:1b:83:f0  104.244.14.252  10.0.28.177      80    1407    4 192
pmacct.201805101049.gz:b0:83:fe:cf:ce:81  18:a9:05:1b:83:f0  104.244.14.252  10.0.28.177      80    1411    4 188
pmacct.201805101049.gz:b0:83:fe:cf:ce:81  18:a9:05:1b:83:f0  104.244.14.252  10.0.28.177      80    1412    4 188
pmacct.201805101049.gz:b0:83:fe:cf:ce:81  18:a9:05:1b:83:f0  104.244.14.252  10.0.28.177      80    1422    4 192
pmacct.201805101050.gz:b0:83:fe:cf:ce:81  18:a9:05:1b:83:f0  104.244.14.252  10.0.28.177      80    1428    4 192
pmacct.201805101050.gz:b0:83:fe:cf:ce:81  18:a9:05:1b:83:f0  104.244.14.252  10.0.28.177      80    1431    4 192
pmacct.201805101050.gz:b0:83:fe:cf:ce:81  18:a9:05:1b:83:f0  104.244.14.252  10.0.28.177      80    1435    4 192
pmacct.201805101050.gz:b0:83:fe:cf:ce:81  18:a9:05:1b:83:f0  104.244.14.252  10.0.28.177      80    1436    4 192
pmacct.201805101051.gz:b0:83:fe:cf:ce:81  18:a9:05:1b:83:f0  104.244.14.252  10.0.28.177      80    1443    4 192
pmacct.201805101051.gz:b0:83:fe:cf:ce:81  18:a9:05:1b:83:f0  104.244.14.252  10.0.28.177      80    1444    4 192
pmacct.201805101052.gz:b0:83:fe:cf:ce:81  18:a9:05:1b:83:f0  104.244.14.252  10.0.28.177      80    1448    4 192
pmacct.201805101048.gz:18:a9:05:1b:83:f0  b0:83:fe:cf:ce:81  10.0.28.177     104.244.14.252   1401  80      3 364
pmacct.201805101048.gz:18:a9:05:1b:83:f0  b0:83:fe:cf:ce:81  10.0.28.177     104.244.14.252   1407  80      3 364
pmacct.201805101049.gz:18:a9:05:1b:83:f0  b0:83:fe:cf:ce:81  10.0.28.177     104.244.14.252   1411  80      3 364
pmacct.201805101049.gz:18:a9:05:1b:83:f0  b0:83:fe:cf:ce:81  10.0.28.177     104.244.14.252   1412  80      3 364
pmacct.201805101049.gz:18:a9:05:1b:83:f0  b0:83:fe:cf:ce:81  10.0.28.177     104.244.14.252   1422  80      3 364
pmacct.201805101050.gz:18:a9:05:1b:83:f0  b0:83:fe:cf:ce:81  10.0.28.177     104.244.14.252   1428  80      3 364
pmacct.201805101050.gz:18:a9:05:1b:83:f0  b0:83:fe:cf:ce:81  10.0.28.177     104.244.14.252   1431  80      3 364
pmacct.201805101050.gz:18:a9:05:1b:83:f0  b0:83:fe:cf:ce:81  10.0.28.177     104.244.14.252   1435  80      3 364
pmacct.201805101050.gz:18:a9:05:1b:83:f0  b0:83:fe:cf:ce:81  10.0.28.177     104.244.14.252   1436  80      3 364
pmacct.201805101051.gz:18:a9:05:1b:83:f0  b0:83:fe:cf:ce:81  10.0.28.177     104.244.14.252   1443  80      3 364
pmacct.201805101051.gz:18:a9:05:1b:83:f0  b0:83:fe:cf:ce:81  10.0.28.177     104.244.14.252   1444  80      3 364
pmacct.201805101052.gz:18:a9:05:1b:83:f0  b0:83:fe:cf:ce:81  10.0.28.177     104.244.14.252   1448  80      3 364
```

I dati di traffico consentono subito l'individuazione dell'**HOST** che ha originato il traffico malevolo.
Nello specifico: **18:a9:05:1b:83:f0**

NetMon/L2-Flows: 3

- Supponiamo che l'Ateneo tenga traccia dell'associazione MAC<=>Switch/Porta



Date	IP	Port	VLAN	Switch name
21-05-2018 - 09:45:17	10.0.0.220	3	31	sw-nc-tplink-helpdesk3
10-05-2018 - 12:45:36	10.0.0.44	8	28	sw-exrett-l2-r2-1
26-04-2018 - 17:30:35	10.0.0.44	10	28	sw-exrett-l2-r2-1
26-04-2018 - 11:00:38	10.0.0.44	8	28	sw-exrett-l2-r2-1
30-05-2017 - 16:45:36	10.0.0.44	21	28	sw-exrett-l2-r2-1
16-05-2017 - 08:15:35	10.0.0.44	19	28	sw-exrett-l2-r2-1
14-05-2015 - 16:30:44	10.0.0.44	11	28	sw-exrett-l2-r2-1

Ecco che si scopre che la postazione infetta è (era) connessa alla porta 8 dello switch 10.0.0.44.

NetMon/L2-Flows: 4

- E ora che conosciamo il MAC? Che facciamo?

SHUTDOWN della porta!!!!

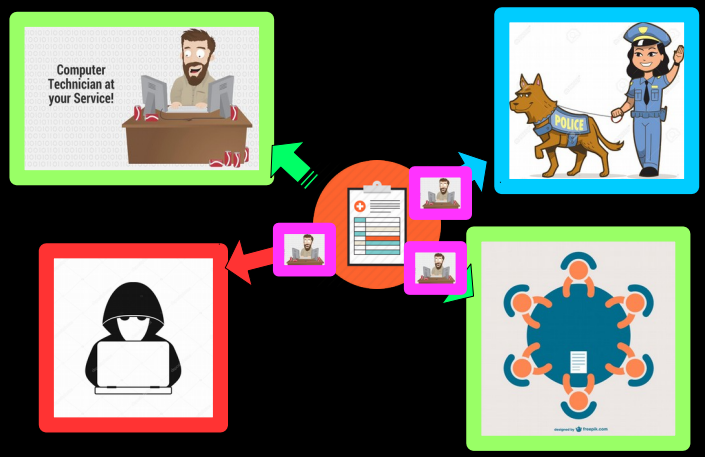
Questo “signore”:

- DEVE assicurare il corretto funzionamento del network. Quindi DEVE isolare gli oggetti originanti traffico “anomalo” (L2 & L3);
- NON è un funzionario di PG, quindi a lui NON interessano le persone!
- NON è il responsabile dell’ufficio “performance”, quindi a lui NON interessa cosa si faccia con i PC;
- Così come un medico soccorre un passante senza chiedergli chi sia, allo stesso modo lui assicura l’instradamento di frame ethernet e pacchetti IP senza conoscere l’identità (umana/reale/virtuale) di chi quel pacchetto l’abbia generato

Strano? ...eppure FUNZIONA!

Conclusioni

- "LOG" è un termine molto generco (f(osservatore, dataset, ...))
- La produzione di (molti) messaggi di LOG è (poco) democratica
- la "delicatezza" di un messaggio di LOG:
  - è funzione di ALCUNI elementi del dataset
  - è funzione della "correlabilità" con altri LOG



- l' "utilità" di un messaggio di LOG:
  - è funzione dell'intero dataset
  - è funzione della "correlabilità" con altri LOG
- Le tecnologie attuali (HW e SW) rendono possibile l'impossibile
- Il livello di competenze necessarie per "muoversi", è importante. Quindi:
  - da soli, non si va da nessuna parte
  - è necessario fare sistama (in alternativa: bandiera bianca)

(P.S.: almeno noi "tecnici", DISCUTIAMONE!)

È tutto....

Grazie!