

Relazione progetto

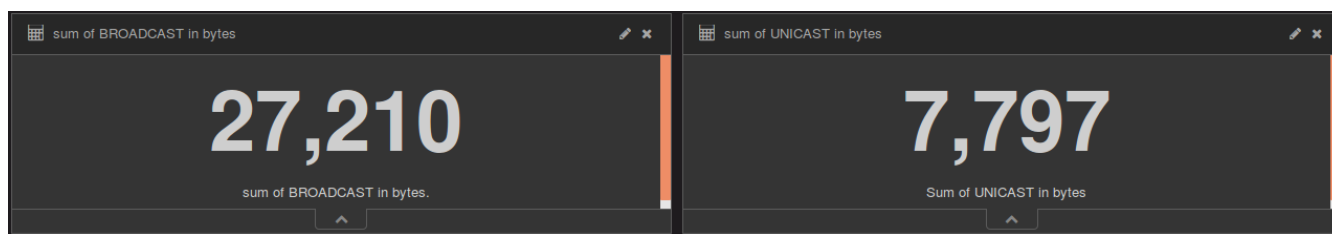
la dashboard realizzata si divide in due colonne. Nella prima, quella di sinistra, sono visualizzati i dati che la macchina riesce a raccogliere riguardo al traffico di tipo broadcast, ovvero il numero di bytes in ingresso nel tempo e gli indirizzi degli host che appaiono in più flussi.

Nella colonna di destra invece sono concentrati i grafici riguardanti i dettagli sul traffico unicast della macchina su cui sta girando lo sniffer.

Si è cercato di dare un'idea precisa del tipo di traffico generato dall'utente della macchina e di poter risalire a come l'utente stia impiegando la sua banda a disposizione, attraverso l'analisi dei protocolli, gli host raggiunti e le richieste inoltrate al server DNS.

Lo scopo della dashboard è, quindi, quello di concentrarsi sull'analisi del computer locale, inserendo però quest'analisi nel contesto della rete in cui si trova.

Doppio contatore



Come primo elemento della dashboard è presente un doppio contatore che tiene traccia dei bytes in ingresso generati dal traffico broadcast e unicast, rispettivamente.

È stato inserito in alto e prende tutto lo spazio in larghezza perché aiuta a comprendere meglio la divisione sottostante.

Entrambi sono grafici di tipo *metric*, in cui si aggrega per *Sum* specificando nel campo *Field* la voce *IN_BYTES*.

È necessario specificare due diversi filtri per diversificare il traffico che si intende catturare, nella barra di ricerca in alto

- per il traffico broadcast:

```
NOT (IPV4_SRC_ADDR: 192.168.2.101) AND NOT (IPV4_DST_ADDR: 192.168.2.101)
```

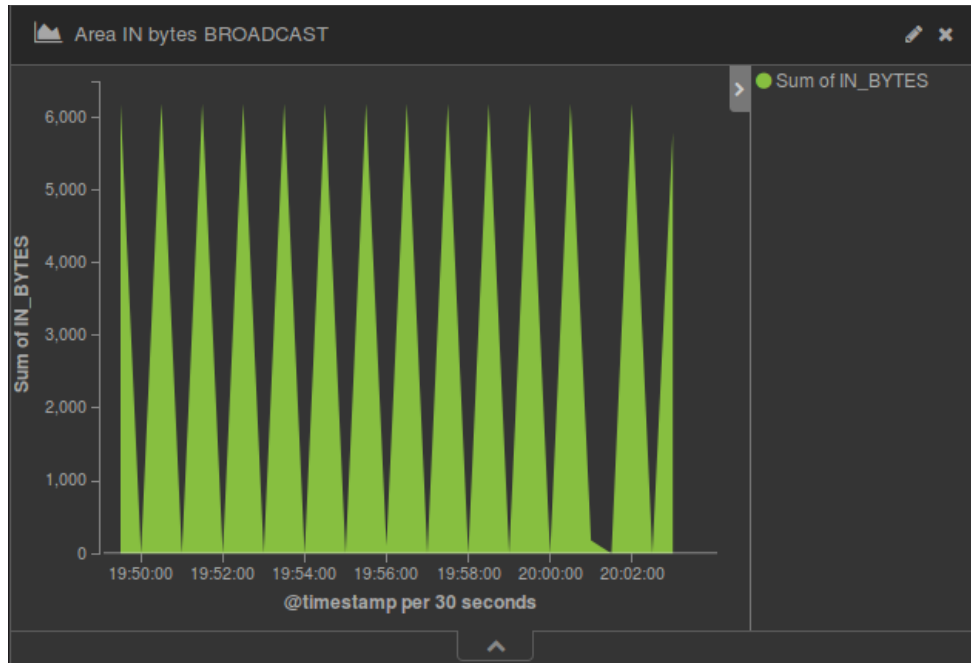
- per il traffico unicast:

```
IPV4_SRC_ADDR: 192.168.2.101 OR IPV4_DST_ADDR: 192.168.2.101
```

in cui 192.168.2.101 nel mio caso è l'indirizzo della scheda di rete con cui sto catturando il traffico

COLONNA SINISTRA – BROADCAST

Area IN bytes



parametri:

Metrics

Aggregation: Sum

Field: IN_BYTES

Buckets

Aggregation: Date Histogram

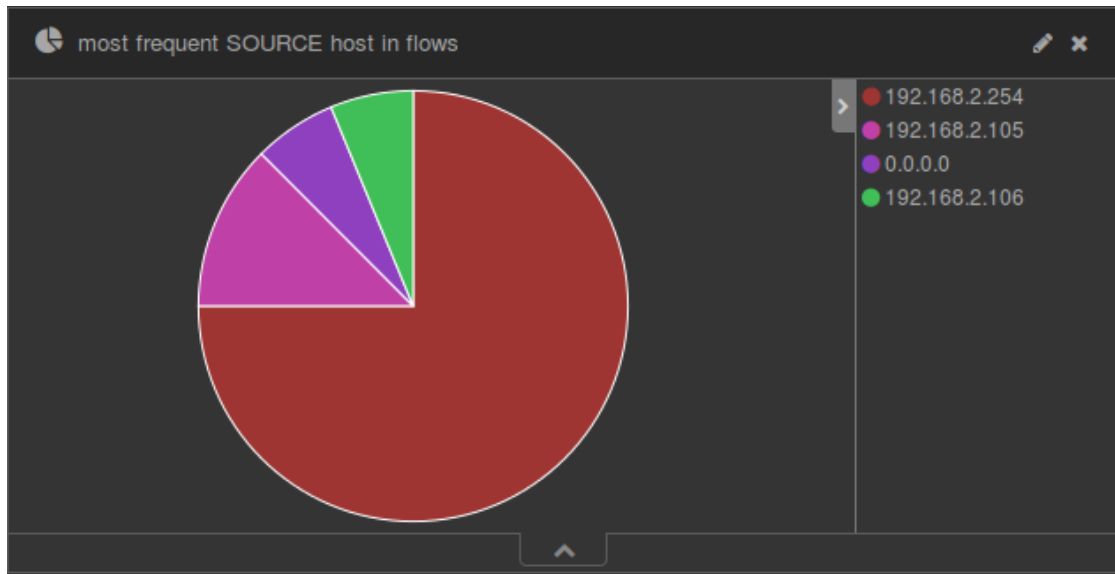
Field: @timestamp

Interval: auto

Attraverso un grafico di tipo *Area Chart* si monitora il traffico in ingresso di tipo broadcast che l'host riesce a catturare. Viene utilizzato il filtro visto in precedenza per escludere i pacchetti destinati alla macchina su cui gira lo sniffer

```
NOT (IPV4_SRC_ADDR: 192.168.2.101) AND NOT (IPV4_DST_ADDR:  
192.168.2.101)
```

Most frequent source hosts



parametri:

Metrics

Aggregation: Count

Buckets

Aggregation: Terms

Field: IPV4_SRC_ADDR

anche in questo caso viene utilizzato il filtro di broadcast per evitare di visualizzare anche i dati relativi all'host locale, lasciando spazio agli altri host presenti sulla stessa rete e nello stesso broadcast domain.

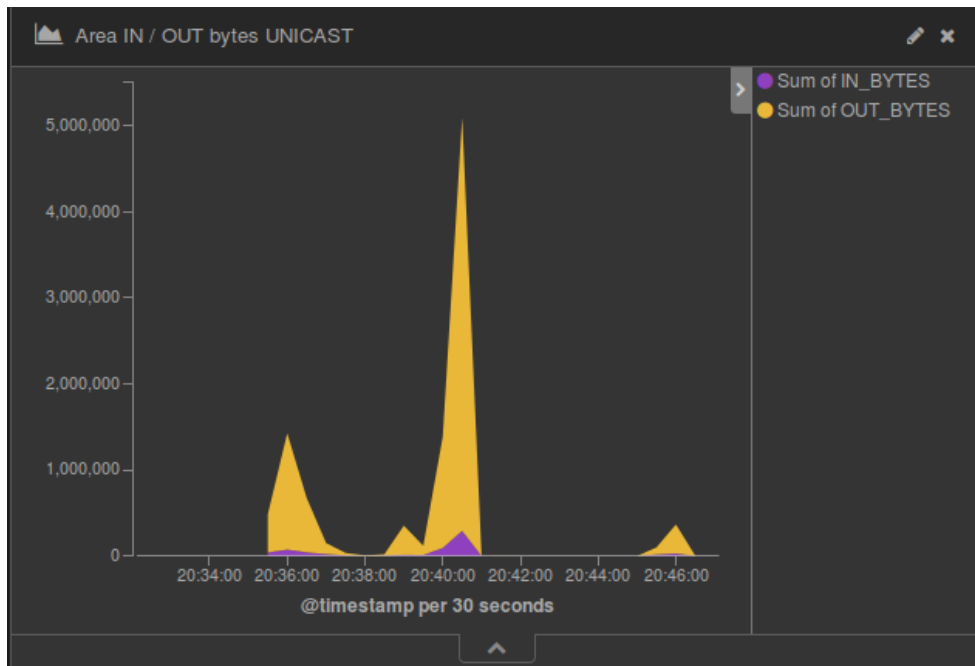
Invece di considerare gli host in base a quanto traffico generano, in questo caso si è data più importanza al numero di flussi in cui appaiono come indirizzo di sorgente o destinazione.

COLONNA DESTRA – UNICAST

in tutti i grafici di questa sezione viene applicato lo stesso filtro per selezionare il solo traffico unicast:

IPV4_SRC_ADDR: 192.168.2.101 OR IPV4_DST_ADDR: 192.168.2.101

In / out bytes



parametri:

Y-axis

Aggregation: sum
Field: IN_BYTES

Aggregation: sum
Field: OUT_BYTES

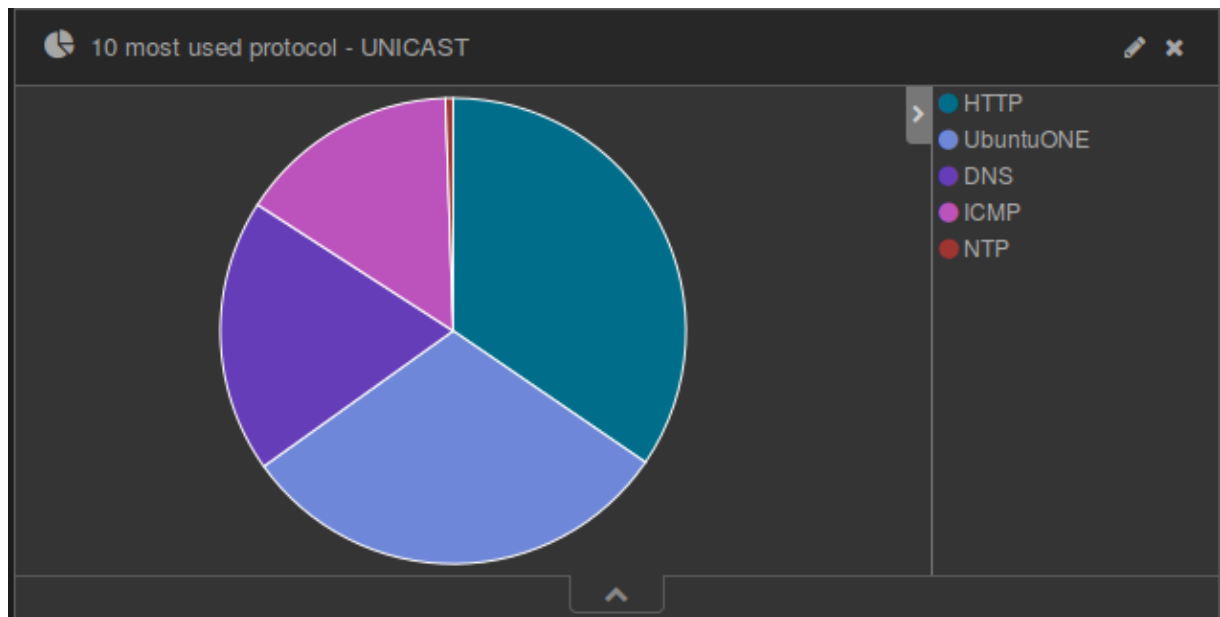
X-axis

Aggregation: Date Histogram
Field: @timestamp
Interval: auto

Questo grafico misura il traffico in ingresso e uscita che genera il nostro PC. Ci consente di rilevare possibili anomalie nel sistema semplicemente osservando i picchi dei valori presenti in istanti di tempo inaspettati, e cioè quando l'utente non stava consapevolmente usando la connessione di rete.

Attraverso i grafici successivi è possibile risalire al tipo di protocollo utilizzato e indirizzo IP del server in caso di traffico anomalo.

Most used protocols



parametri:

Metrics

Aggregation: Sum

Field: IN_BYTES

Buckets

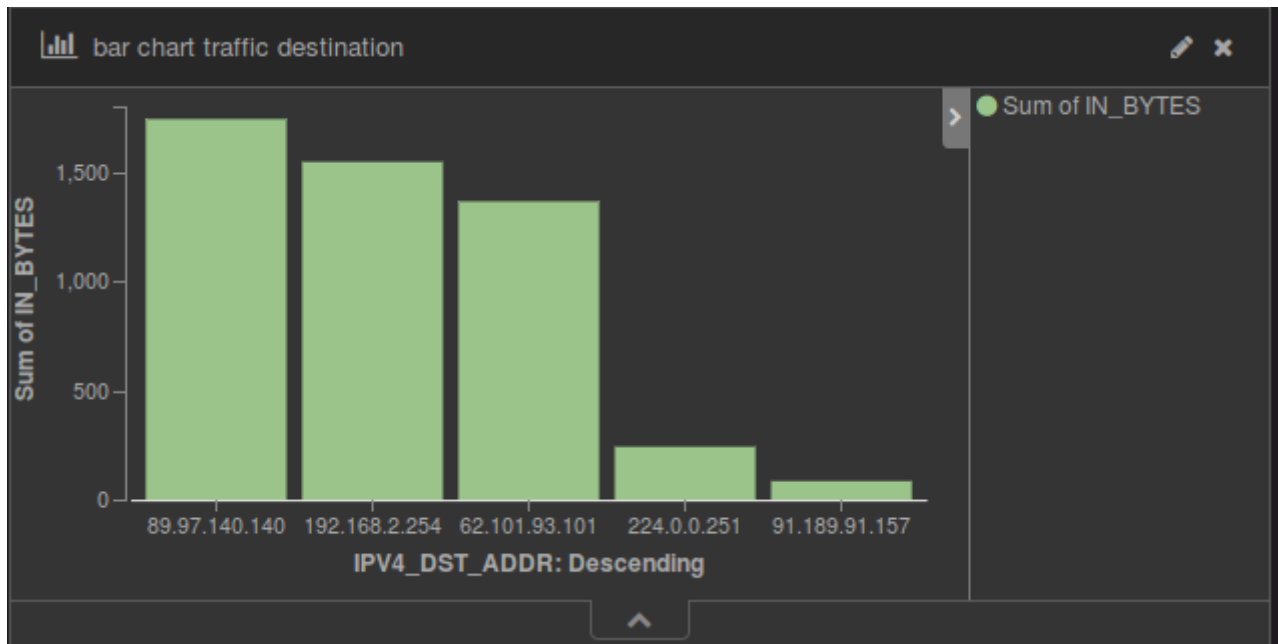
Split Slices

Aggregation: Terms

Field: L7_PROTO_NAME.raw

L'areogramma ci fornisce a colpo d'occhio i protocolli più utilizzati nella finestra temporale di riferimento. Utile per rendersi conto di possibili applicazioni che girano in background e utilizzano uno specifico protocollo proprietario.
É dedicata maggiore area ai protocolli che generano più traffico in ingresso

Most reached destinations



parametri:

Metrics

Y-Axis

Aggregation: Sum

Field: IN_BYTES

Buckets

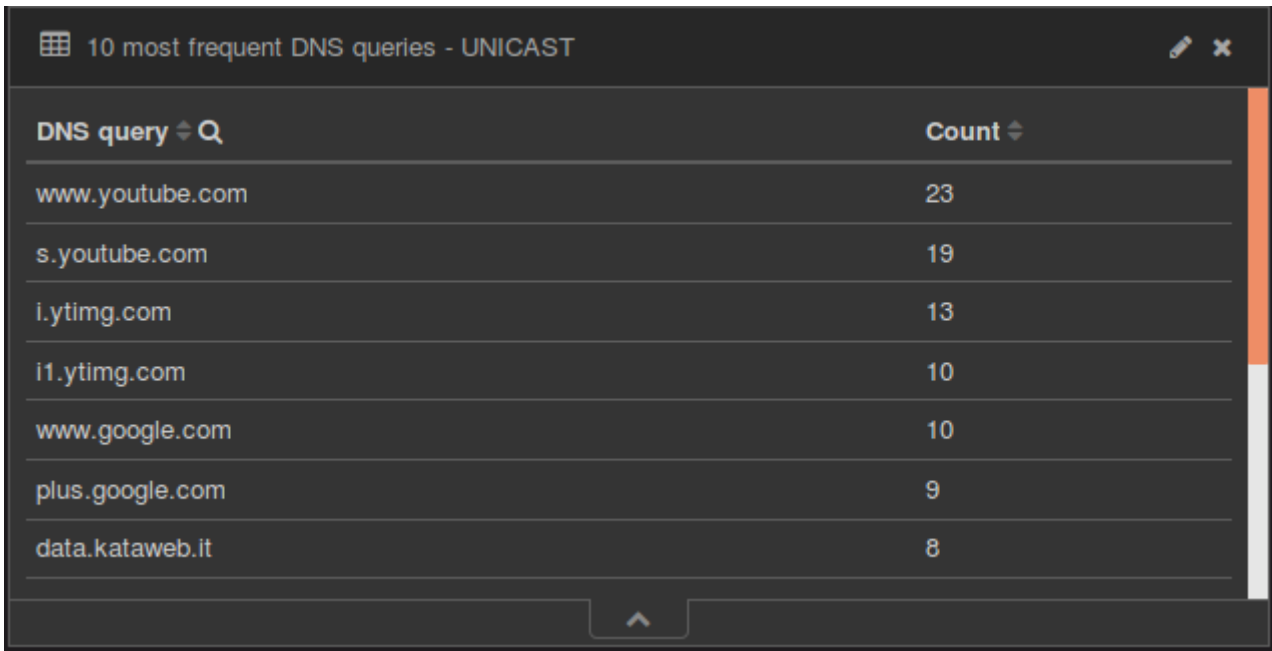
X-Axis

Aggregation: Terms

Field: IPV4_DST_ADDR

Il grafico tiene traccia dei server da cui scarichiamo più dati, ovviamente è utile controllare gli indirizzi che generano più traffico per capire se sono destinazioni che ci si aspettava o meno.

Most frequent DNS queries



The screenshot shows a Kibana dashboard window titled "10 most frequent DNS queries - UNICAST". It contains a table with two columns: "DNS query" and "Count". The table lists the following data:

| DNS query | Count |
|-----------------|-------|
| www.youtube.com | 23 |
| s.youtube.com | 19 |
| i.ytimg.com | 13 |
| i1.ytimg.com | 10 |
| www.google.com | 10 |
| plus.google.com | 9 |
| data.kataweb.it | 8 |

parametri:

Metrics

Aggregation: Count

Buckets

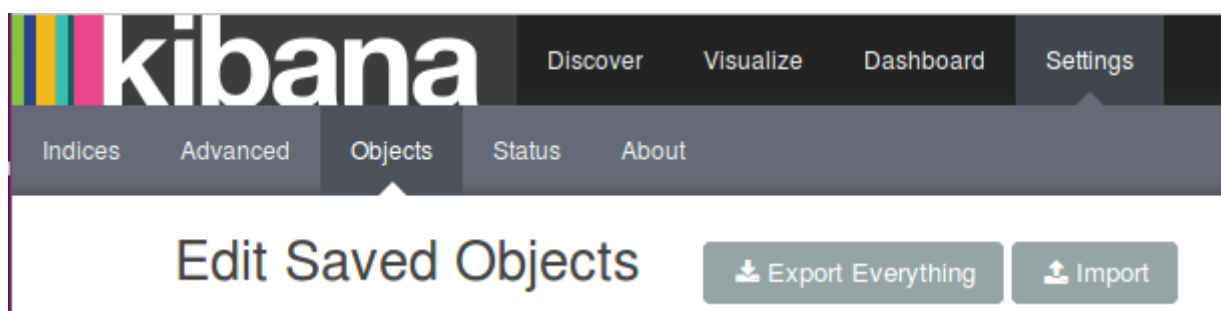
Aggregation: Terms

Field: DNS_QUERY.raw

la tabella mostra le richieste inoltrate al server DNS che partono dal computer in uso. Sono aggregate per flussi invece che per traffico in ingresso generato.

Esportazione e Importazione della dashboard – Json

Kibana permette di esportare la propria dashboard creata nel formato json. Per farlo è sufficiente selezionare, dalla barra in alto, *Settings*, e successivamente *Objects*.



Da questa pagina è possibile esportare tutti i grafici, le dashboard e le ricerche insieme, attraverso il pulsante *Export Everything*, o selezionare ed esportare solo gli oggetti di nostro interesse.

Dallo stesso menù è inoltre possibile importare materiale precedentemente salvato tramite la funzione *Import* che aprirà una finestra di file manager consentendoci di navigare fino al file in formato json desiderato.

Considerazioni finali

ho trovato il software molto intuitivo, vi si prende confidenza con facilità, nonostante contenga molte funzionalità nascoste e attivabili tramite scripting. Il fatto che questi due tipi di esperienza utente rimangono separati aiuta l'utilizzatore a non perdersi nell'esplorazione di troppe opzioni e configurazioni, permettendo che si concentri su ciò che viene offerto di default, che comunque non è poco.