

# Rappresentazione dei flussi tramite Kibana

Progetto di Gestione di Rete – Anno Accademico 2014/2015

Casini Alice - Matricola 505292

Campinotti Sara - Matricola 503987

Fornesi Erica - Matricola 505528

Pierotti Arrigo - Matricola 464247

## 0. Uso di ntopng con ElasticSearch/Kibana

### 0.1 Prerequisiti:

1. Avere installato ntopng (scaricabile da [qui](#)) seguendo le istruzioni contenute nel file readme.ntopng eseguendo anche il comando 'make geoip' per includere i dati per la geolocalizzazione degli indirizzi IP.
2. Avere installato ElasticSearch e Kibana.

### 0.2 Avvio cattura traffico tramite ntopng

1. Aprire il terminale e navigare verso la cartella dove è stato installato ntopng.
2. Eseguire il comando, in super utente,

```
# sudo ./ntopng -F "es;flows;[index];[hostES]:9200/_bulk" -i [interface]
```

[index] | il nome dell'indice dei record da utilizzare per l'inserimento nel database ElasticSearch (es. ntopng-%Y.%m.%d)

[hostES] | indirizzo IP del database ElasticSearch installato ed accessibile dalla porta 9200 (es. <http://localhost>)

[interface] | l'interfaccia di rete su cui si vuole catturare il traffico (es. eth0)

Nel caso all'esecuzione del comando precedente venga restituito l'errore

```
ERROR: ntopng requires redis server to be up and running
```

eseguire il comando

```
# redis-server
```

per avviare Redis Server e poi eseguire nuovamente il comando di avvio di ntopng.

1. Da questo momento ntopng sta catturando tutto il traffico in transito sull'interfaccia selezionata e lo esporta come flussi verso il database ElasticSearch.

### 0.3 Primo accesso a Kibana

1. Aprire un browser internet e andare all'indirizzo

[http://\[hostK\]:5601](http://[hostK]:5601)


[hostK] | indirizzo IP di Kibana (es. localhost)

1. Spuntare *Index contains time-based events* nella pagina di prima configurazione di Kibana.
2. All'interno della casella di testo *Index name or pattern* inserire solo la parte fissa dell'index specificato nel comando di avvio di ntopng con l'aggiunta al suo termine del carattere '\*' (es. ntopng-\*).
3. Cliccare su *Create* per creare l'indice da utilizzare per estrarre, in modo automatico con Kibana, i flussi salvati da ntopng all'interno del database Elasticsearch.
4. La schermata passerà automaticamente alla scheda *Discover* dove è possibile vedere tutti i flussi, con tutti i rispettivi campi creati da ntopng, estratti da Elasticsearch.
5. E' possibile modificare l'intervallo temporale su cui stiamo lavorando cliccando su *Last 15 minutes* nell'angolo in alto a destra dell'interfaccia di Kibana e scegliendo tra quelli proposti nelle schede *Quick*, *Relative* e *Absolute*.



Inoltre è possibile abilitare il refresh automatico dalla scheda *Refresh Interval* e selezionando un intervallo tra quelli possibili.

### 0.4 Creazione di un grafico


1. Selezionare la scheda *Visualize* nella parte alta dell'interfaccia grafica di Kibana.
2. Scegliere il tipo di grafico desiderato.
3. Selezionare *From a new search* per visualizzare tutti i dati, altrimenti *From a saved search* per una visualizzazione dei dati relativi ad una query effettuata e salvata nella scheda *Discover*.
4. Nel caso siano stati inseriti in Kibana più di un index, verrà mostrato un menù a tendina da cui scegliere l'index da utilizzare.
5. Ciascun grafico presenta una propria interfaccia per scegliere i dati da visualizzare (relativi ai campi dei flussi) e per come mostrarli, oltre a personalizzare alcuni semplici aspetti grafici (presenza di legenda, eventuali modifiche alla rappresentazione grafica, ...).

6. Una volta soddisfatti del grafico realizzato, può essere salvato cliccando sul tasto *Save Visualization*, rappresentato dall'icona , fornendo poi un nome per il salvataggio.

## 0.5 Creazione di una dashboard

1. Selezionare la scheda *Dashboard* nella parte alta dell'interfaccia di Kibana
2. Cliccare sull'icona  per aprire il menù di selezione contenente i grafici precedentemente creati e salvati.
3. Selezionare il grafico da inserire.
4. E' possibile modificare le dimensioni del grafico inserito nella dashboard portando il puntatore nell'angolo in basso a destra per poi tenere premuto e muovere il mouse fino a che non si raggiunge la dimensione voluta.
5. E' possibile modificare la posizione del grafico trascinandolo dalla sua barra del titolo
6. Inserire, se desiderati, altri grafici eseguendo di nuovo i passi appena descritti.
7. Una volta soddisfatti della dashboard realizzata, può essere salvata cliccando sul tasto *Save Dashboard*, rappresentato dall'icona , fornendo poi un nome per il salvataggio.

## 0.6 Esportazione/importazione di una dashboard

1. Cliccare sull'icona  per ottenere il link diretto alla dashboard, inseribile nella barra degli indirizzi di un qualunque browser, e il codice HTML in tag `<iframe>`, inseribile all'interno del sorgente di una qualunque pagina HTML.  
! Attenzione: se si esporta il tag HTML i client devono poter accedere a Kibana, modificando eventualmente l'indirizzo.

## 1. Introduzione

Analizzare il traffico di rete generato da una macchina è utile per localizzare problemi nella connettività in uno specifico intervallo di tempo sia nello storico che in tempo reale, così da identificarne la possibile sorgente. Kibana permette di rappresentare i flussi del traffico attraverso un'interfaccia grafica realizzabile dall'utente o importata da sorgenti esterne e di applicarvi filtri per avere una visione ristretta sui campi interessati.

## 2. Architettura del sistema

La cattura dei pacchetti del traffico avviene tramite il collezionatore ntopng che li "aggrega" in flussi (insieme di pacchetti con caratteristiche simili) contententi i campi più significativi per identificarlo tra tutti gli altri come il protocollo, gli indirizzi IP di sorgente e destinatario, il numero di pacchetti, il timestamp ed altri eventualmente con l'aggiunta di plugin.

Questi flussi sono inseriti all'interno del database ElasticSearch secondo un indice, stabilito all'avvio di ntopng, che ne permette una gestione più efficiente grazie al timestamp aggiunto.

Kibana quindi estrae da ElasticSearch soltanto i flussi dell'indice selezionato, fornendone una prima e grezza rappresentazione, nella vista "Discover", in un intervallo di tempo impostabile dall'utente con la possibilità di filtrarne il contenuto secondo i valori dei campi e di effettuarci delle semplici query.



## 3. Creazione di un grafico su Kibana



### 1. Grafici realizzabili su Kibana

Su Kibana è possibile realizzare diversi tipi di grafici per avere una visione più personalizzabile e pratica dei flussi; una volta selezionato il grafico desiderato, l'interfaccia di Kibana consente di scegliere i campi del flusso da rappresentare con eventuali aggregazioni (conteggio, somma, media, ...). Una volta terminata la creazione, il grafico può essere salvato con un nome in modo da essere utilizzato all'interno di una Dashboard.

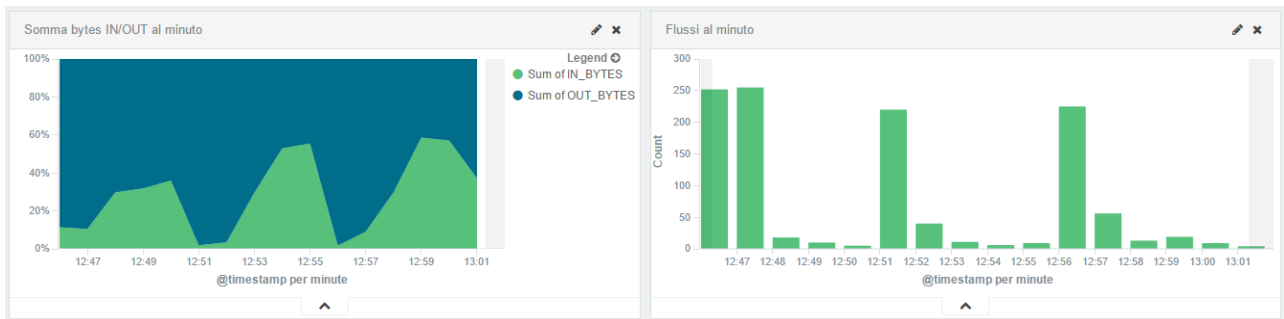
## 4. Funzionamento della dashboard di Kibana

La view "Dashboard" di Kibana consente di mostrare più grafici in una unica schermata in modo da avere una visione globale di tutti i dati che sono stati ritenuti importanti per l'analisi del traffico. La potenza della dashboard sta nella sua interattività: selezionando una parte di grafico (es. un protocollo) tutti gli altri modificano i propri contenuti per mostrare solo i dati relativi alla selezione effettuata (es. IN/OUT bytes del protocollo selezionato) se questa ha corrispondenze nel particolare grafico.

## 5. Dashboard realizzata

La dashboard realizzata è rivolta al controllo del traffico (attuale e passato) di una singola macchina dove ciascun grafico ne analizza un aspetto particolare.

### 5.1 Somma IN/OUT bytes al minuto - Flussi al minuto

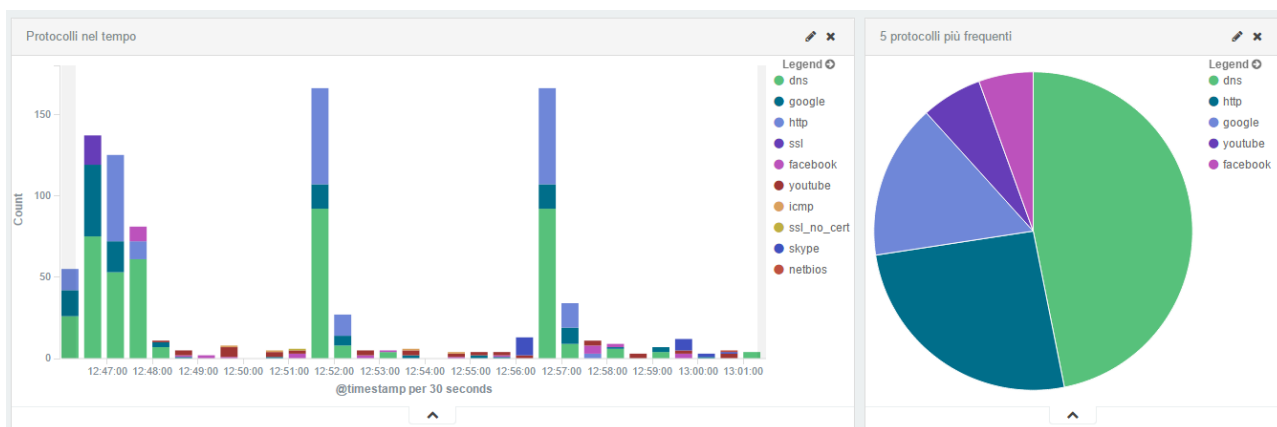


Il primo grafico mostra la suddivisione in percentuale dei bytes dei flussi di input/output raggruppati per minuto, così da poter riscontrare se ci sono delle variazioni anomale del traffico. Il secondo invece mostra quanti flussi, sia in entrata che in uscita, sono stati collezionati in ogni minuto in modo da poter vedere quando la macchina è stata più o meno attiva nel generare traffico.

I campi del primo grafico sono da interpretarsi come:

%IN\_BYTES Incoming flow bytes (src->dst)  
%OUT\_BYTES Outgoing flow bytes (dst->src)

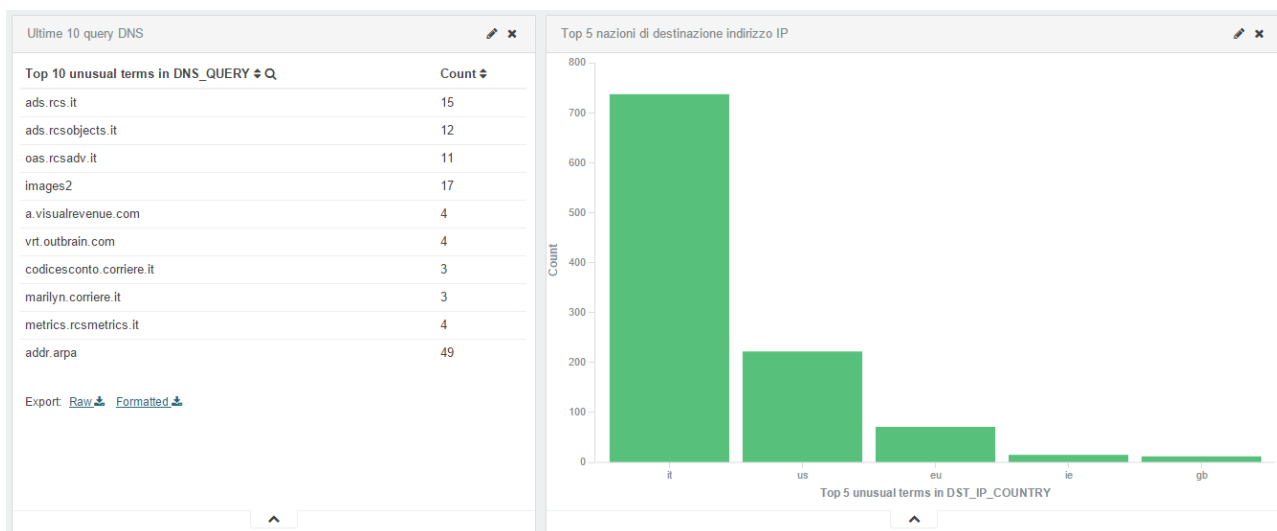
### 5.2 Protocolli



Questi due grafici raggruppano, in modo diverso, i protocolli che sono stati riscontrati all'interno dei flussi catturati: nel primo sono visibili i tre protocolli più frequenti in ogni minuto, mentre nel secondo i cinque protocolli più utilizzati nella finestra temporale selezionata. Selezionando un protocollo in questi grafici ne otteniamo una visualizzazione specifica.

Con questi due grafici siamo in grado di vedere quanti e quali protocolli sono utilizzati dalle applicazioni eseguite sulla macchina così da avere una visione storica dell'uso che ne fa l'utente.

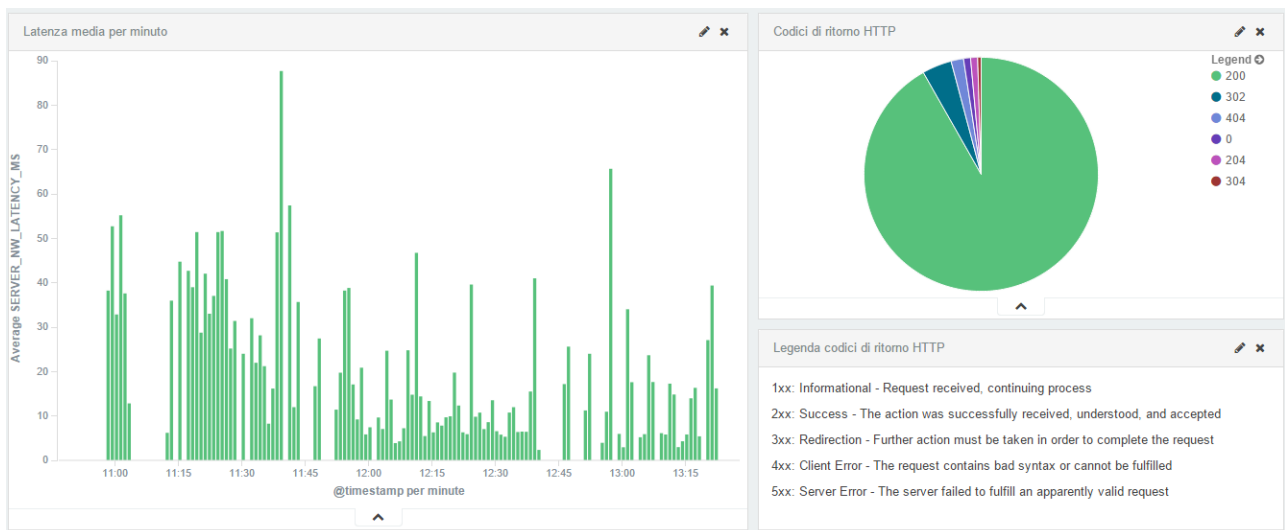
### 5.3 Query DNS - Origini indirizzi IP



La tabella mostra le ultime 10 Query DNS, raggruppate per frequenza, che sono state eseguite utilizzando il protocollo DNS, così da vedere che cosa richiedono maggiormente le applicazioni. La presenza preponderante delle query di "addr.arpa" e "in" è causata dalla risoluzione DNS inversa che permette di risalire al nome dell'host connesso ad internet conoscendone l'indirizzo IP.

Il grafico consente invece di conoscere le cinque nazioni/regioni dove sono maggiormente localizzati gli indirizzi IP che vengono contattati dalle applicazioni.

### 5.4 Latenza - Codici di stato HTTP



Nel primo grafico è possibile vedere la latenza media (in ogni minuto) tra l'invio di un pacchetto e la ricezione della sua risposta per tutti i protocolli che consentono questa misurazione, in modo da identificare possibili rallentamenti nel traffico e quale protocollo specifico lo abbia causato.

Nel grafico a torta sono visualizzati i codici di stato HTTP per la normale navigazione verso siti web, con una semplice legenda sotto, consentendo di stabilire se il problema nella navigazione è causato dal server o dal client.

## 6. Link e codice della dashboard

La dashboard è importabile in una istanza funzionante di Kibana semplicemente inserendo il link sottostante in un qualunque browser web :

```
http://localhost:5601/#/dashboard/Dashboard-progetto-definitiva?_a=(filters:!( ),panels:!( (col:1,id:Protocolli-nel-tempo,row:4,size_x:8,size_y:4,type:visualization), (col:1,id:Somma-bytes-IN-slash-OUT-al-minuto,row:1,size_x:6,size_y:3,type:visualization), (col:7,id:Flussi-al-minuto,row:1,size_x:6,size_y:3,type:visualization), (col:9,id:'5-protocolli-pi%C3%B9-frequenti',row:4,size_x:4,size_y:4,type:visualization), (col:1,id:Ultime-10-query-DNS,row:8,size_x:5,size_y:5,type:visualization), (col:6,id:Top-5-nazioni-di-destinazione-indirizzo-IP,row:8,size_x:7,size_y:5,type:visualization), (col:8,id:Codici-di-ritorno-HTTP,row:13,size_x:5,size_y:3,type:visualization), (col:8,id:Legenda-codici-di-ritorno-HTTP,row:16,size_x:5,size_y:2,type:visualization), (col:1,id:Latenza-media-per-minuto,row:13,size_x:7,size_y:5,type:visualization)),query:(query_string:(analyze_wildcard:!t,query:'*')),title:'Dashboard%20progetto%20definitiva')&_g=(refreshInterval:(display:Off,section:0,value:0),time:(from:'2015-05-21T08:46:42.233Z',mode:absolute,to:'2015-05-21T11:27:54.348Z'))
```

Oppure è importabile in una qualunque pagina web aggiungendo il tag HTML `<iframe>` sottostante al suo sorgente:

```
<iframe
src="http://localhost:5601/#/dashboard/Dashboard-progetto-definitiva?embed&_a=(filters:!( ),panels:!( (col:1,id:Protocolli-nel-tempo,row:4,size_x:8,size_y:4,type:visualization), (col:1,id:Somma-bytes-IN-slash-OUT-al-minuto,row:1,size_x:6,size_y:3,type:visualization), (col:7,id:Flussi-al-minuto,row:1,size_x:6,size_y:3,type:visualization), (col:9,id:'5-protocolli-pi%C3%B9-frequenti',row:4,size_x:4,size_y:4,type:visualization), (col:1,id:Ultime-10-query-DNS,row:8,size_x:5,size_y:5,type:visualization), (col:6,id:Top-5-nazioni-di-destinazione-indirizzo-IP,row:8,size_x:7,size_y:5,type:visualization), (col:8,id:Codici-di-ritorno-HTTP,row:13,size_x:5,size_y:3,type:visualization), (col:8,id:Legenda-codici-di-ritorno-HTTP,row:16,size_x:5,size_y:2,type:visualization), (col:1,id:Latenza-media-per-minuto,row:13,size_x:7,size_y:5,type:visualization)),query:(query_string:(analyze_wildcard:!t,query:'*')),title:'Dashboard%20progetto%20definitiva')&_g=(refreshInterval:(display:Off,section:0,value:0),time:(from:'2015-05-21T08:46:42.233Z',mode:absolute,to:'2015-05-21T11:27:54.348Z'))" height="600" width="800"></iframe>
```

Importante è modificare la parte sottolineata nei due link soprastanti con l'indirizzo di rete della macchina che ospita Kibana. Non è invece necessario modificare la porta relativa all'indirizzo.