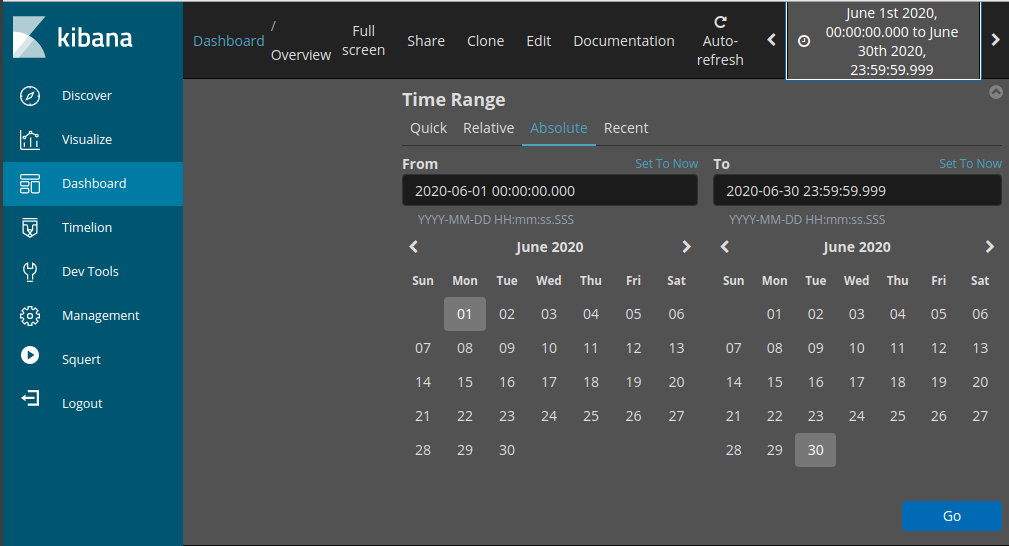
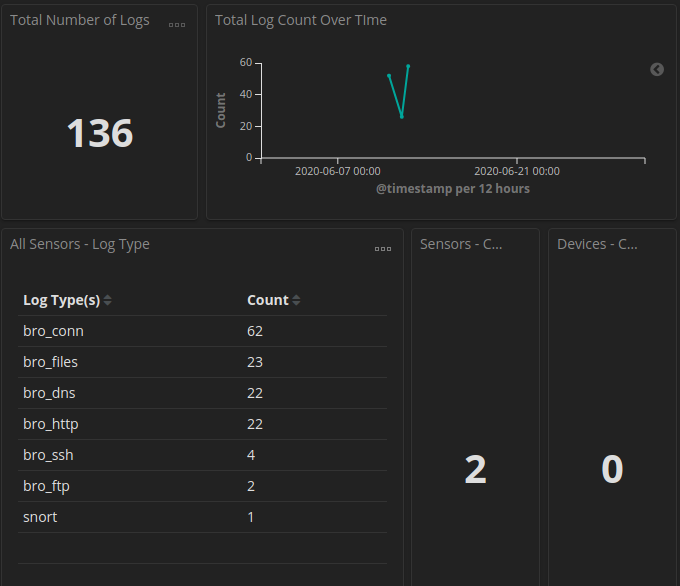
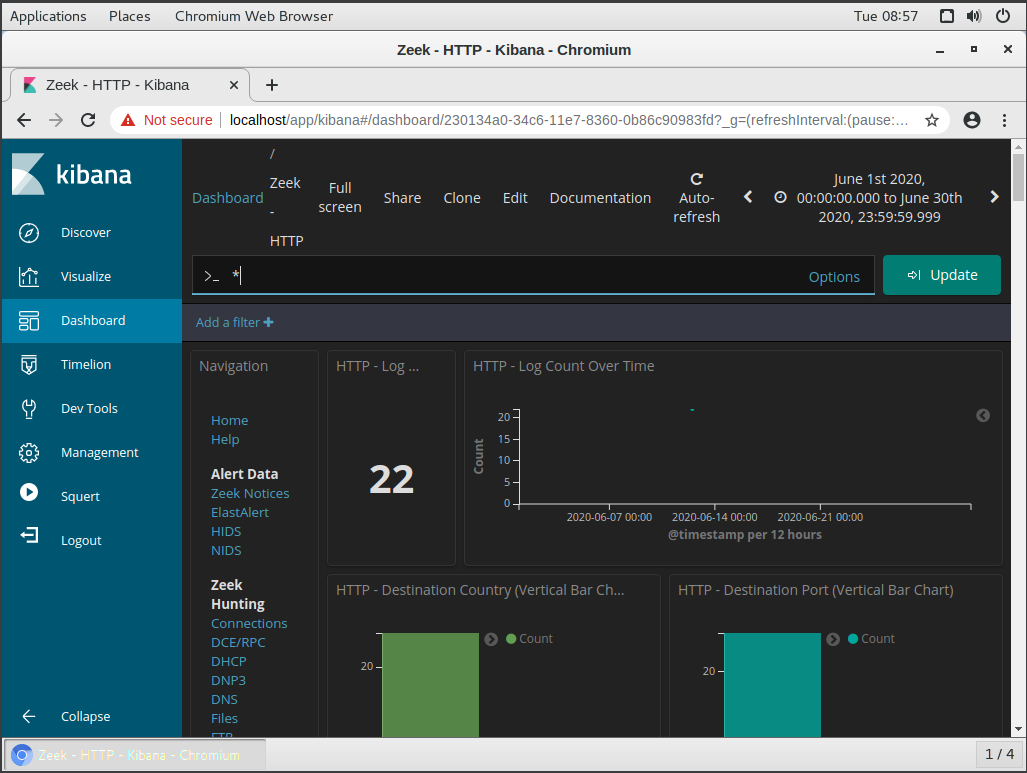
**Interpretare i dati HTTP e DNS per isolare l'attore malevolo**

Dopo aver effettuato l’accesso a kibana con username **analyst** e password **cyberops** bisogna inserire un range orario dal 2020-06-01 al 2020-06-30.

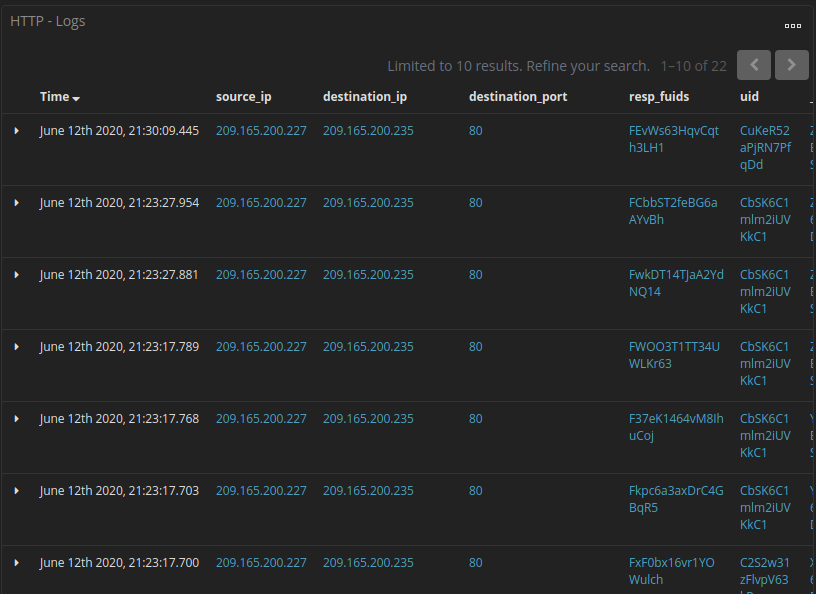


Noteremo subito un numero di 136 log totali di quel mese

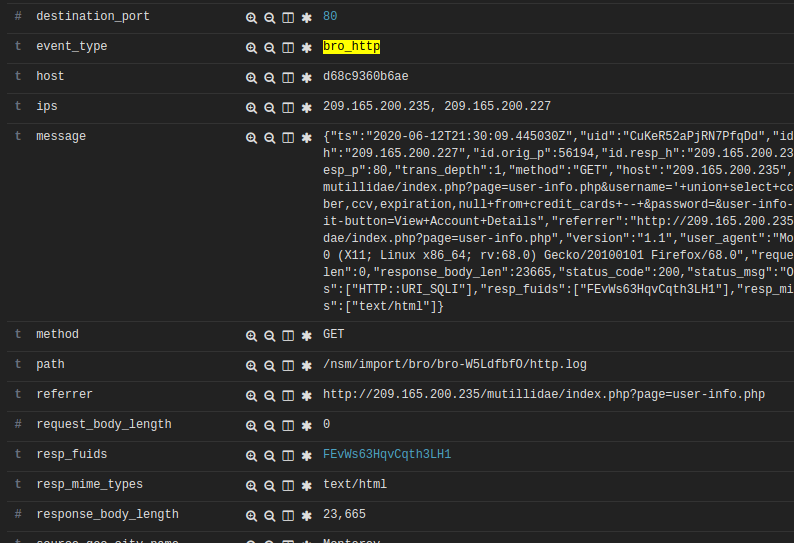
Utilizzando uno dei filtri già presenti andremo a filtrare per log di http



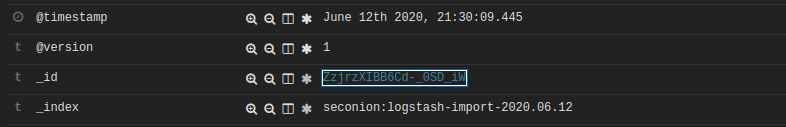
Scorrendo tra i risultati notiamo l’ip sorgente e di destinazione e la porta.



Espandendo i log noteremo varie informazioni tra cui anche l’event\_type e message.

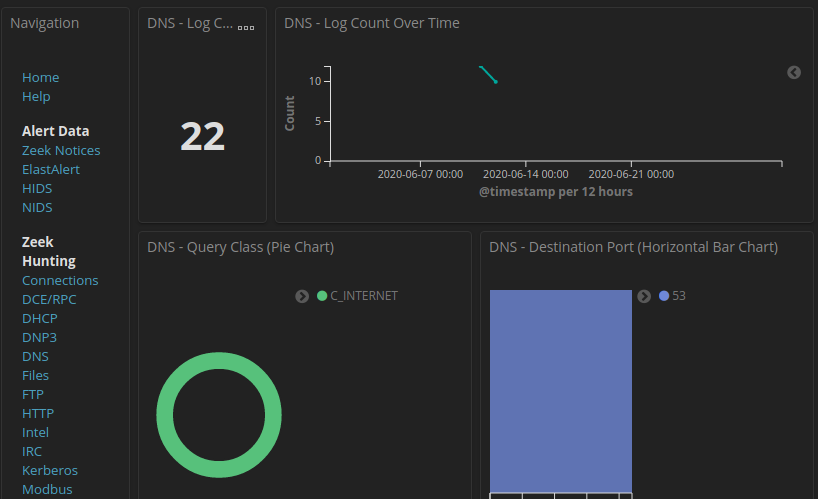


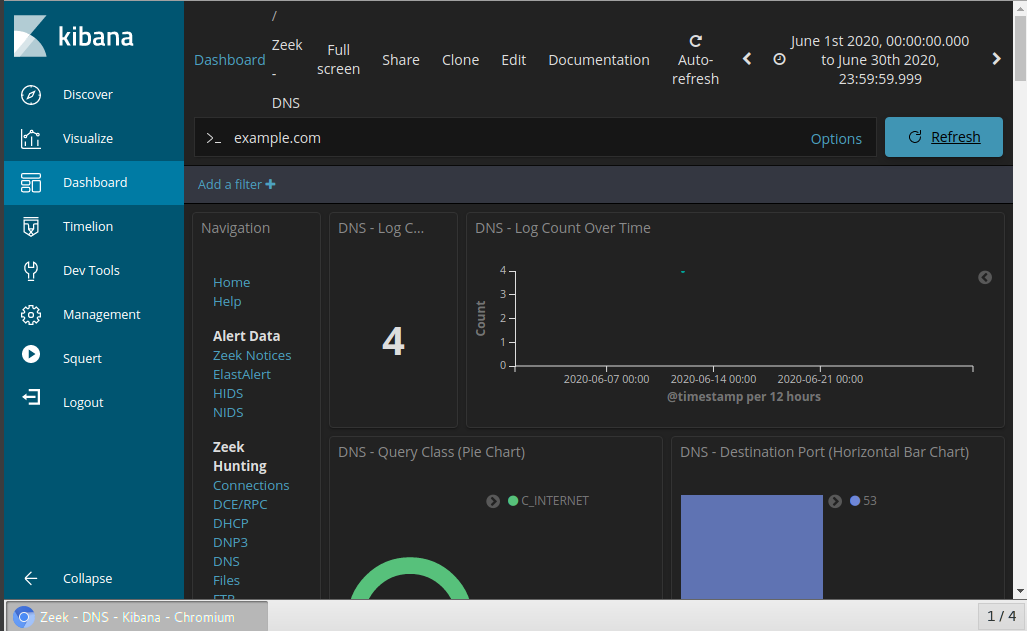
Da come si può verificare all’interno del campo message si può dedurre una SQLi per recuperare informazioni di carte di credito.

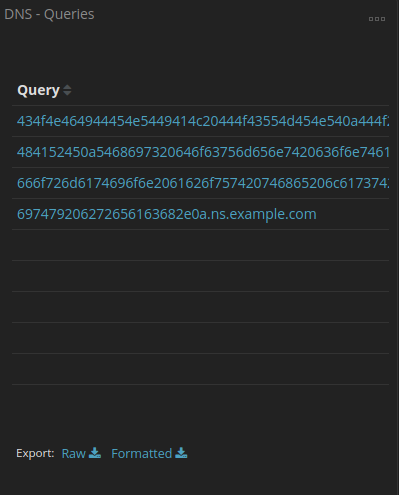
Successivamente è possibile entrare più nel dettaglio del log grazie al campo \_id   
Il quale apre la seguente schermata che, filtrando per username, troviamo le informazioni estratte 

PARTE 2

Un amministratore di rete ha notato sospette attività per quanto riguarda interrogazioni al DNS, quindi modificando il filtro su DNS possiamo iniziare ad analizzare i log.



Per effettuare una ricerca più dettagliata aggiungiamo un ulteriore filtro **example.com** ****

Dopo aver estratto premendo **EXPORT:RAW** in formato CSV le informazioni sospette   


Eseguiamo un xxd per decodificare il CSV e rinominarlo in secret.txt e utilizziamo il cat per avere un output del file e noteremo questo risultato

