127.0.0.1 - admin [14/May/2019:08:52:48.582 +0530] "GET /en-US/splunkd/\_\_raw/services/server/health/splunkd?output\_mode=json&\_=1557803955854 HTTP/1.1" 200 832 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36" - e9da568639cd530993f3893d4d73493e 1ms

Pink – hour

Green – file

Yellow – http\_status

Red – web\_browser

Ash – Web\_Server

Cyan – Transaction\_ID

You have to extract all above listed patterns using rex one by one. Also you have to extract all these field using one rex command.

You can see this data by accessing below query –

Ex.- index=\_internal sourcetype=splunkd\_ui\_access