TEAM-20

Network Monitoring

TEAM MEMBERS :

BL.EN.U4AIE20031 - KUNISETTY JASWANTH

BL.EN.U4AIE20051 - PRANAV RAMACHANDRULA

BL.EN.U4AIE20055 - S SRUTHI

Contents

Introduction

Real time data analysis :

Real time data analysis refers to the process of preparing and measuring data as soon as it enters the database

In our project we have taken real time data using Wireshark and performed preprocessing. Once the preprocessing of the data is done, we find the network which have consumed higher amount of data.

Wireshark:

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection

Network monitoring using IP address

While monitoring the overall network, the network packets are captured and exported such that all the required fields are present into a .csv file.

The .csv file is sent to Kafka to the topic IP one row at a time

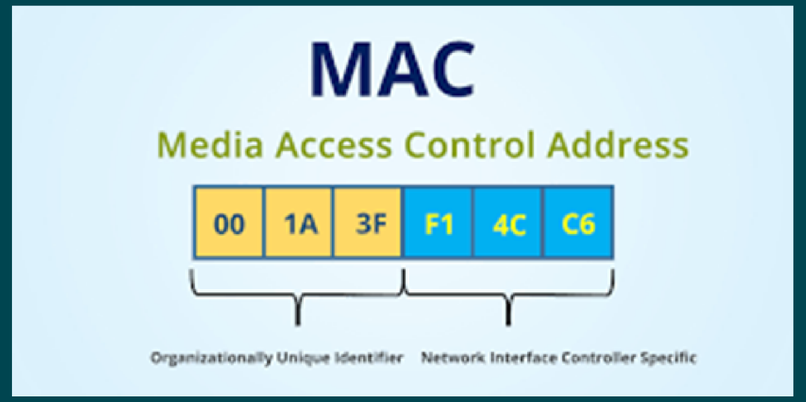
the data from Kafka is received and preprocessed to store in MongoDB to the **network_ip** database.

Network monitoring using MAC address

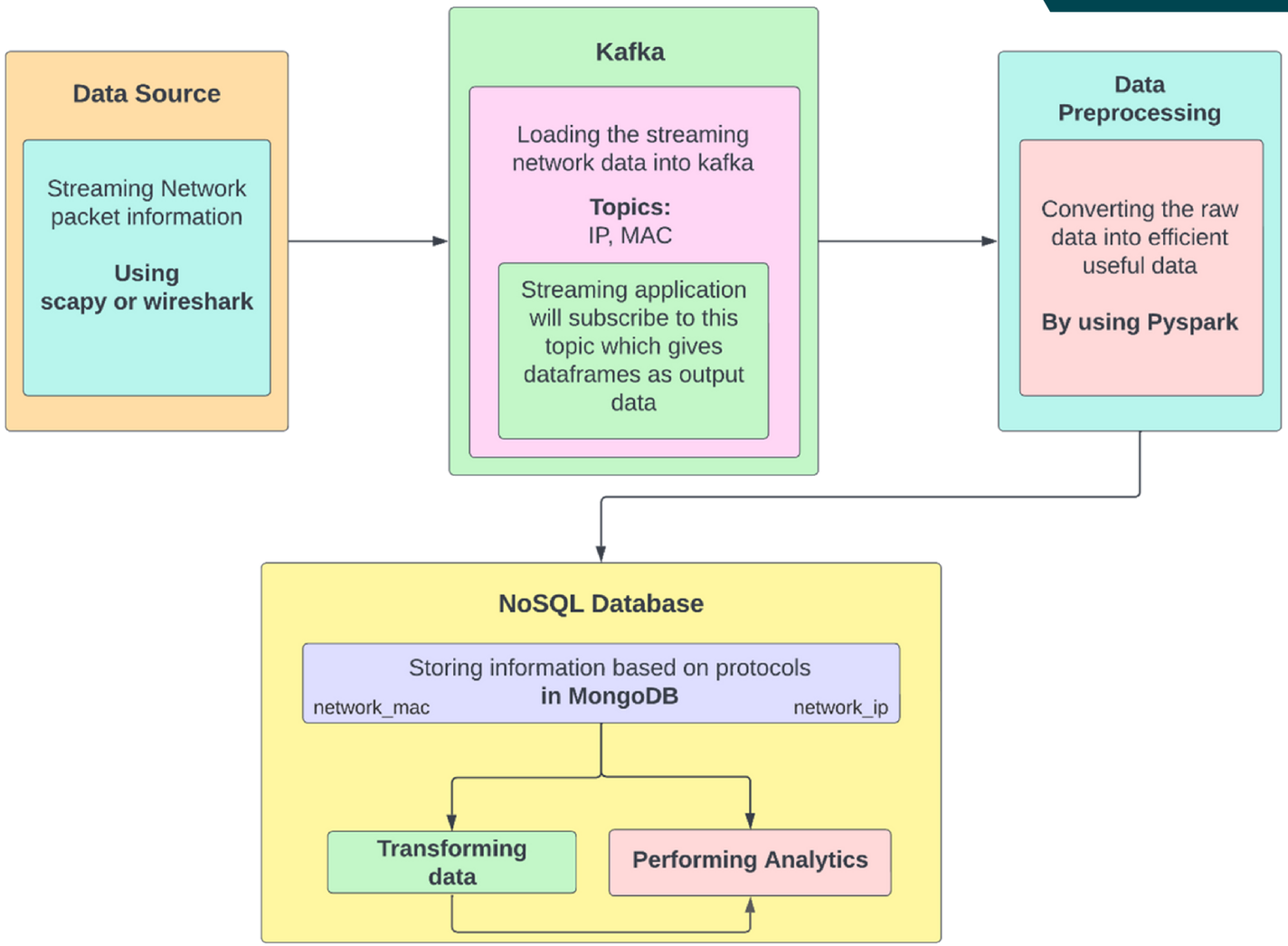
While monitoring each individual device the network packets are captured by configuring the external Wi-Fi module into monitor mode and exported to the .csv file

The .csv file is sent to Kafka to the topic MAC one row at a time

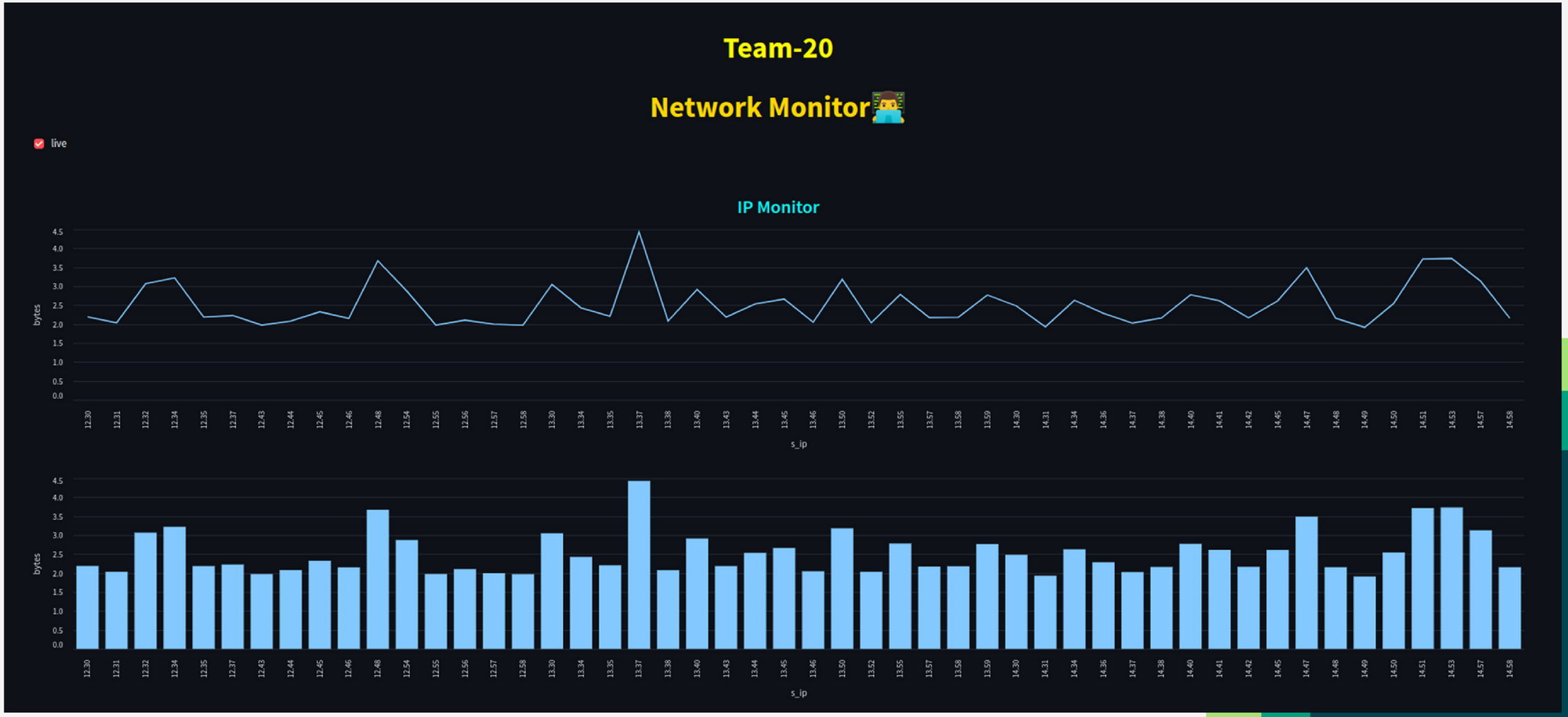
the data from Kafka is received and preprocessed to store in MongoDB to the **network_mac** database.



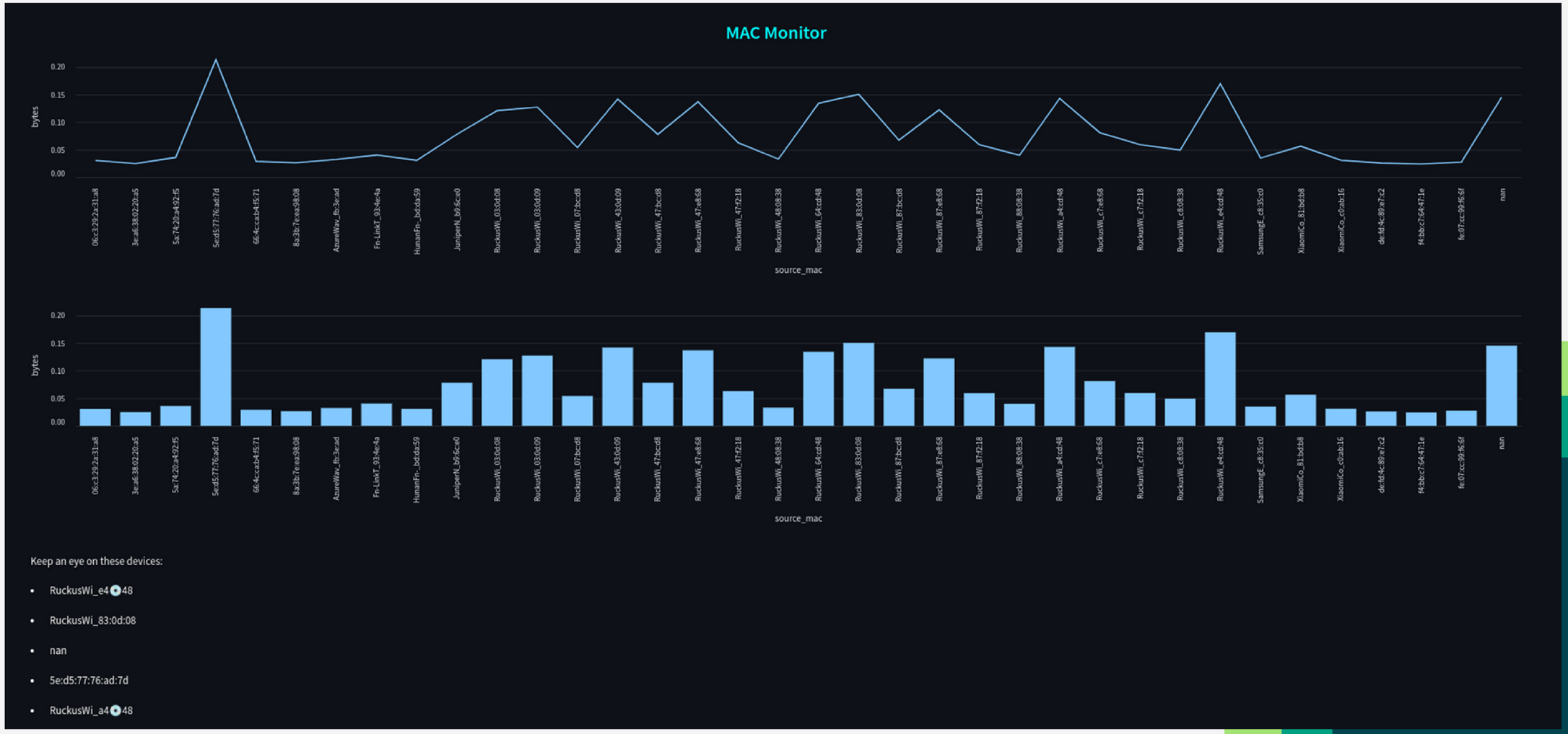
Data Pipeline



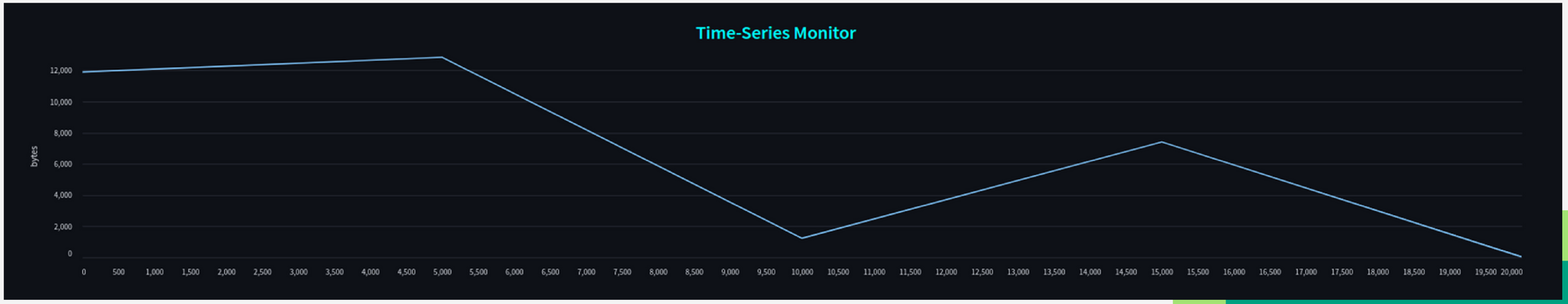
Results



Results


MAC Monitor
bytes
0.20
0.15
0.10
0.05
0.00
06:c3:29:2a:31:a8
3e:a6:38:02:20:a5
5a:74:20:a4:92:f5
5e:d5:77:76:ad:7d
66:4c:ca:b4:f5:71
8a:3b:7e:ea:98:08
AzureWav_fb:3e:ad
Fn-LinkT_93:4e:4a
HunanFn__bd:da:59
JuniperN_b9:6c:e0
RuckusWi_03:0d:08
RuckusWi_03:0d:09
RuckusWi_07:bc:d8
RuckusWi_43:0d:09
RuckusWi_47:bc:d8
RuckusWi_47:e8:58
RuckusWi_47:f2:18
RuckusWi_48:08:38
RuckusWi_64:cd:48
RuckusWi_83:0d:08
RuckusWi_87:bc:d8
RuckusWi_87:e8:58
RuckusWi_87:f2:18
RuckusWi_88:08:38
RuckusWi_a4:cd:48
RuckusWi_c7:e8:58
RuckusWi_c7:f2:18
RuckusWi_c8:08:38
RuckusWi_e4:cd:48
SamsungE_c8:35:c0
XiaomiCo_81:bd:b8
XiaomiCo_c0:ab:16
de:fd:4c:89:e7:c2
f4:bb:c7:64:47:1e
fe:07:cc:99:f6:6f
nan
source_mac
Keep an eye on these devices:
RuckusWi_e4:cd:48
RuckusWi_83:0d:08
nan
5e:d5:77:76:ad:7d
RuckusWi_a4:cd:48

Results



Time series Monitor:
A collection of data points that describes the time-varying values of a metric

Thank you..!!