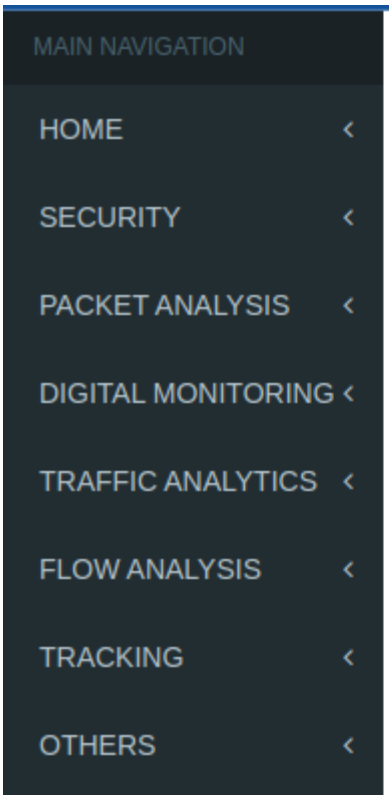
MILESTONE 3

INTERFACE:

Front interface of our Website looks like



The front interface contains following sections

- ➢ Home
- ➢ security
- ➢ Packet Analysis,
- ➢ Digital Monitoring
- ➢ Traffic Analytics
- ➢ Flow Analysis
- ➢ Tracking
- ➢ Others

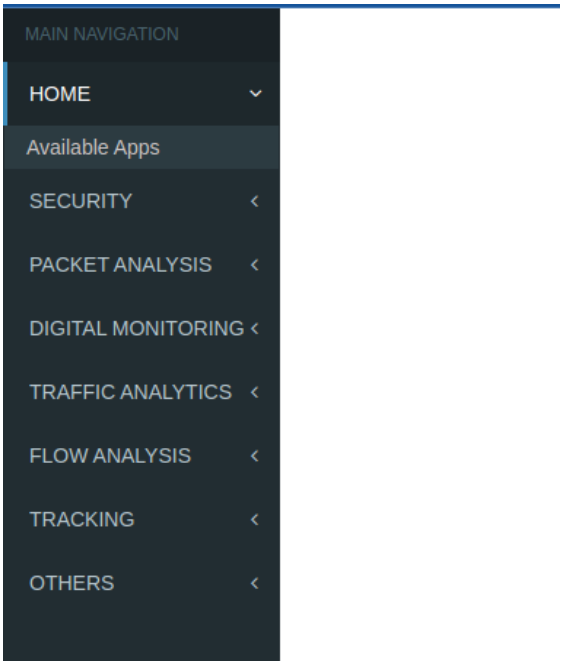
➔ If we click on each section, we can find sub-sections under each section which are the applications of our database.

If you click on home you can see the following subsections:

Home

- Available apps

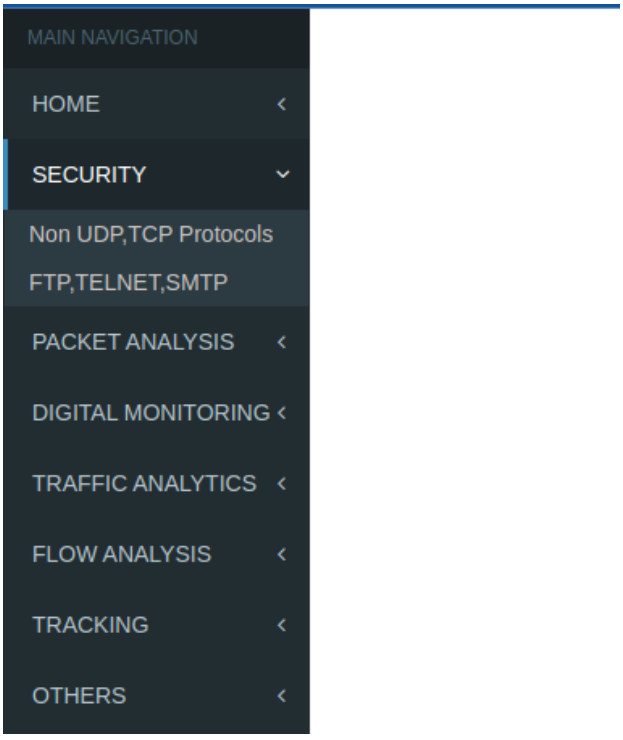
MILESTONE 3



If you click on the security, you can see the following subsections

Security

- Non UDP,TCP protocols
- FTP,TELNET,SMTP

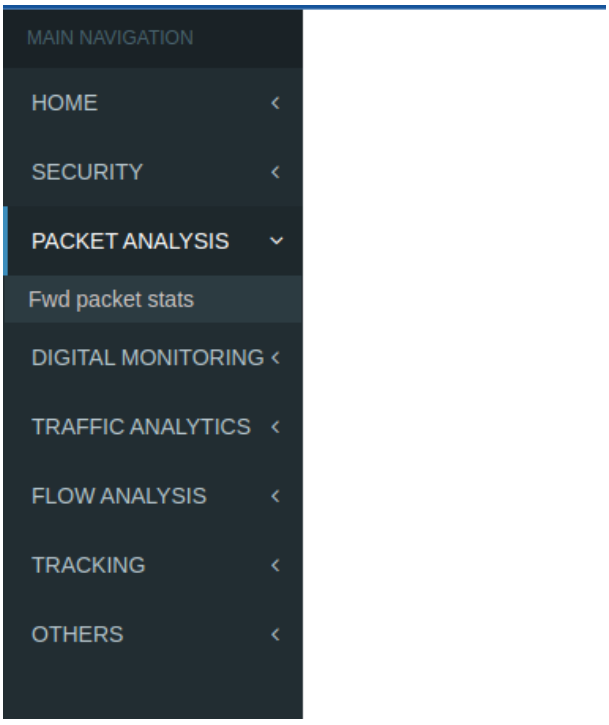


MILESTONE 3

If you click on the packet analysis you can see the following subsections

Packet Analysis

- fwd packets stats

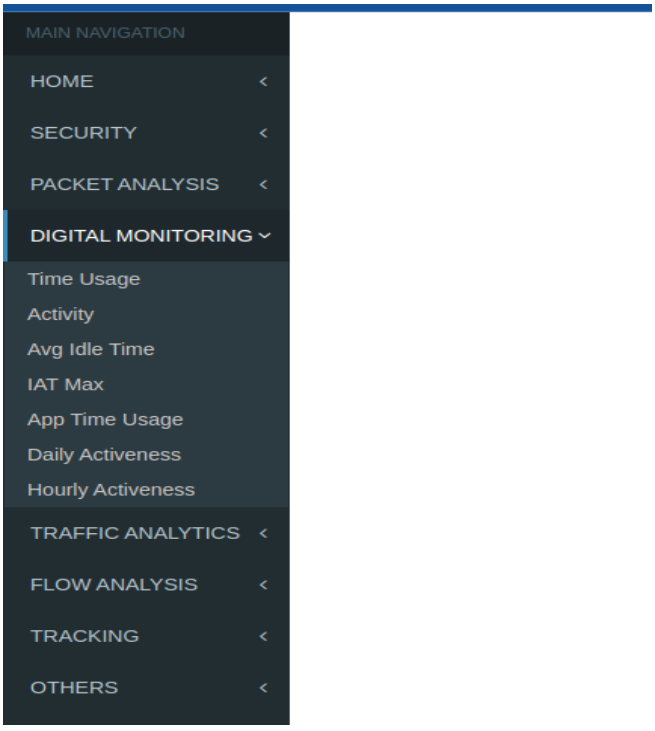


If you click on the Digital Monitoring you can see the following subsections

Digital Monitoring

- Time usage
- Activity
- Avg Idle Time
- IAT Max
- App Time Usage
- Daily Activeness
- Hourly Activeness

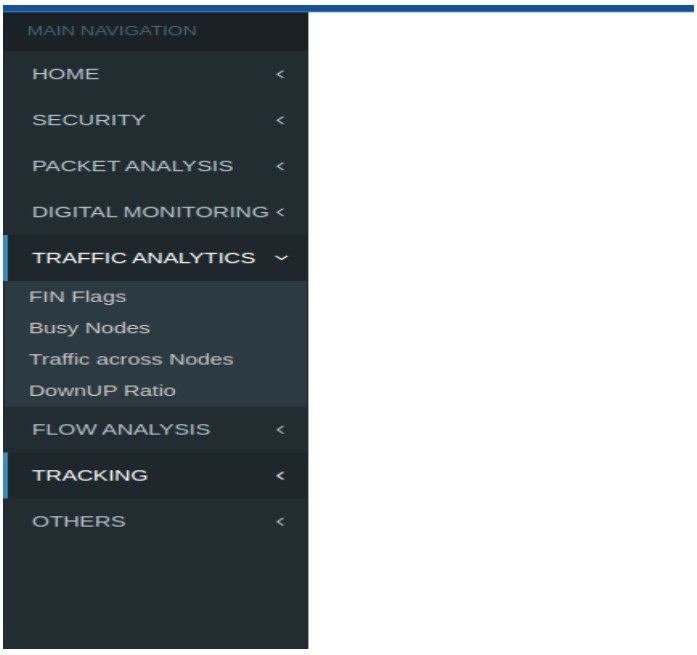
MILESTONE 3



If you click on the Traffic Analytics you can see the following subsections

Traffic Analytics

- FIN Flags
- Busy Nodes
- Traffic across Nodes
- DownUp Ratio

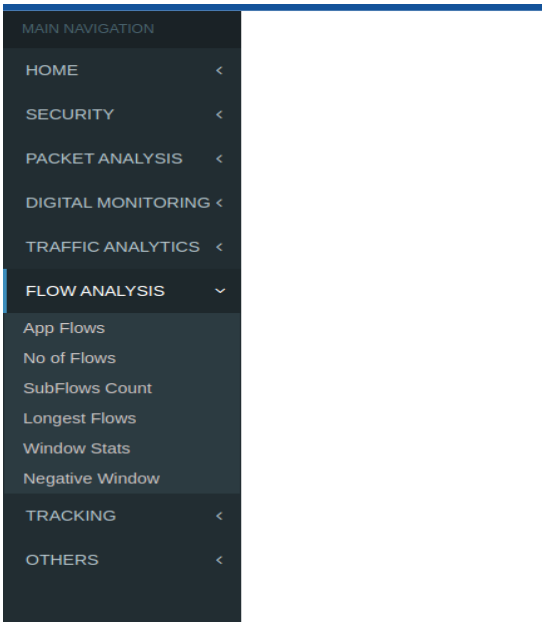


MILESTONE 3

If you click on the Flow Analysis you can see the following subsections

Flow Analysis

- App Flows
- No of Flows
- SubFlows Count
- Longest Flows
- Window Stats
- Negative Window

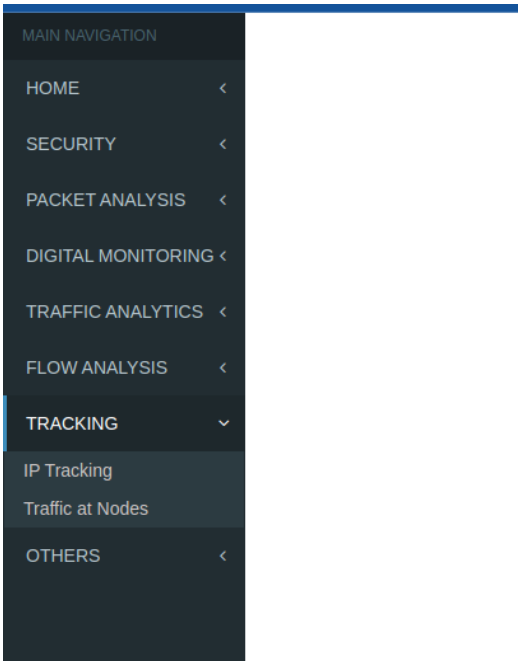


If you click on the Tracking you can see the following subsections

Tracking

- IP Tracking
- Traffic at nodes

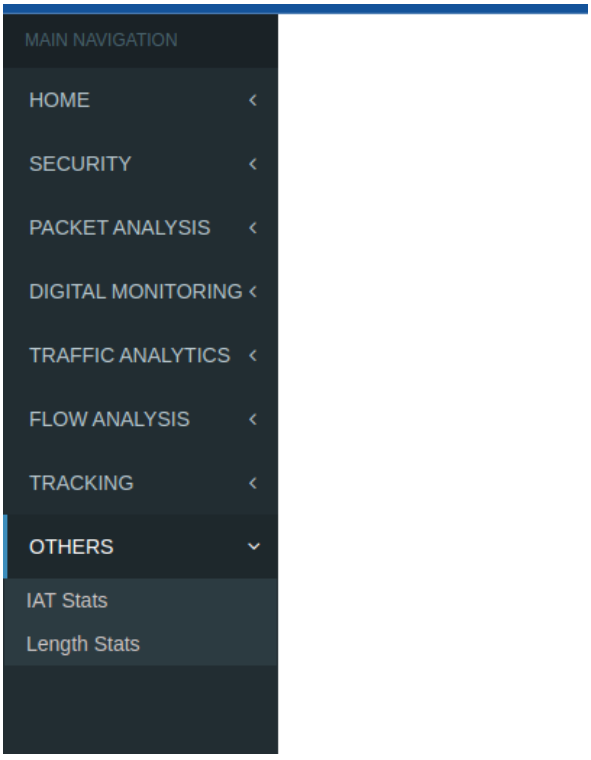
MILESTONE 3



If you click on the others you can see the following subsections

Others

- IAT stats
- Length Stats



MILESTONE 3

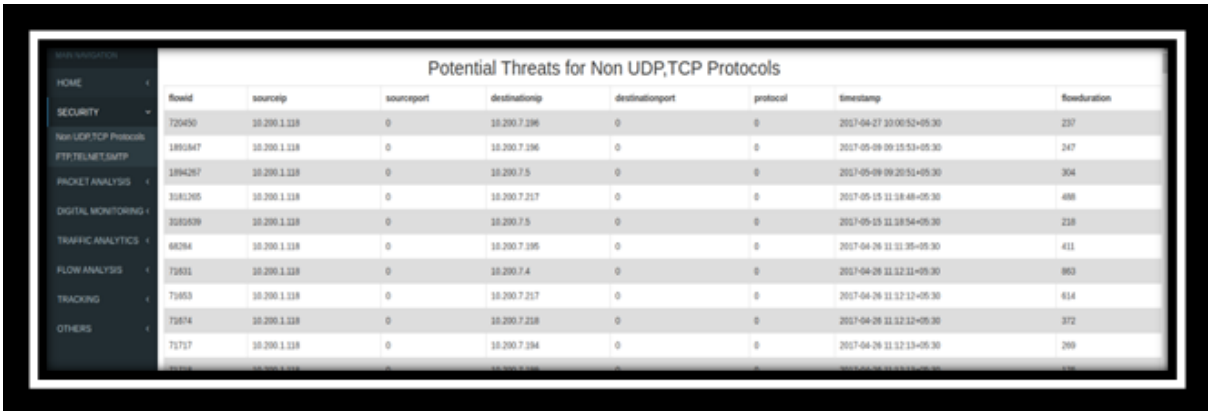
APPLICATIONS & RESULTS:

- **Available Apps**

If you click on this it gives all the apps for which data is available

- **Non UDP,TCP protocols**

If you click on this it gives the Potential Threats for Non UDP,TCP Protocols



flowid	sourceip	sourceport	destinationip	destinationport	protocol	timestamp	flowduration
720450	10.200.1.118	0	10.200.7.196	0	0	2017-04-27 10:00:52+05:30	237
1891847	10.200.1.118	0	10.200.7.196	0	0	2017-05-09 09:15:53+05:30	247
1894267	10.200.1.118	0	10.200.7.5	0	0	2017-05-09 09:20:51+05:30	304
3181265	10.200.1.118	0	10.200.7.217	0	0	2017-05-15 11:18:48+05:30	488
3181639	10.200.1.118	0	10.200.7.5	0	0	2017-05-15 11:18:54+05:30	218
68284	10.200.1.118	0	10.200.7.195	0	0	2017-04-26 11:11:35+05:30	411
71631	10.200.1.118	0	10.200.7.4	0	0	2017-04-26 11:12:11+05:30	863
71653	10.200.1.118	0	10.200.7.217	0	0	2017-04-26 11:12:12+05:30	614
71674	10.200.1.118	0	10.200.7.218	0	0	2017-04-26 11:12:12+05:30	372
71717	10.200.1.118	0	10.200.7.194	0	0	2017-04-26 11:12:13+05:30	269

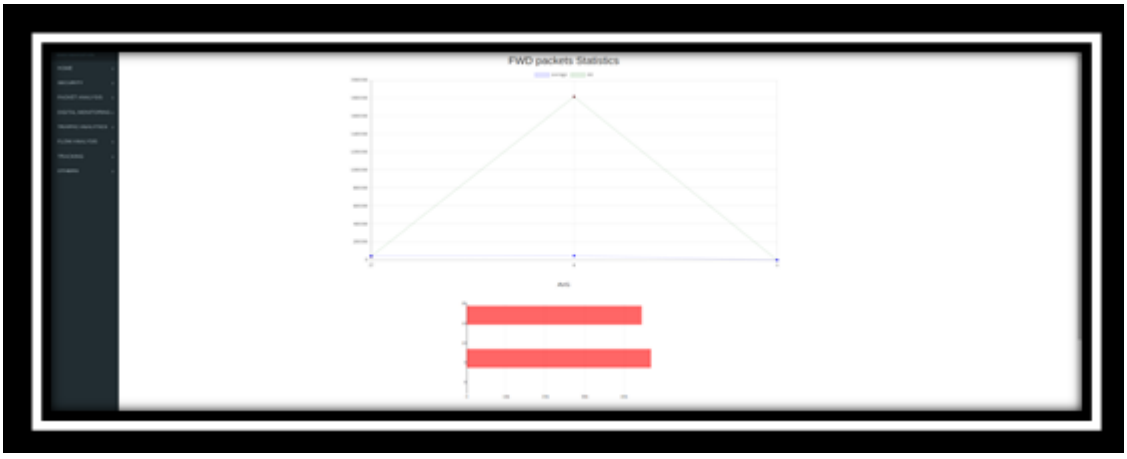
MILESTONE 3

- **FTP,TELNET,SMTP**

If you click on this it gives the Potential Threats which are FTP , Telnet , SNMP

- **fwd packets stats**

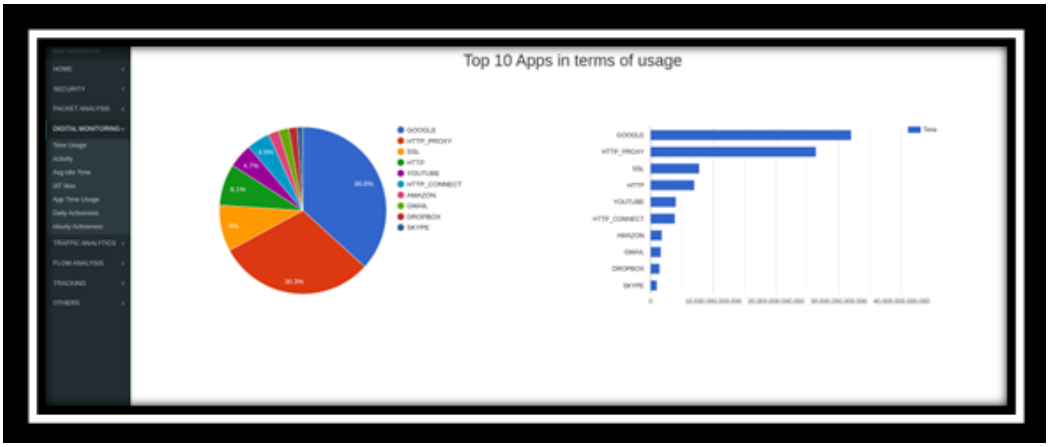
If you click on this it gives the average and standard deviation of the total length of forward packets for each protocol.



- **Time usage**

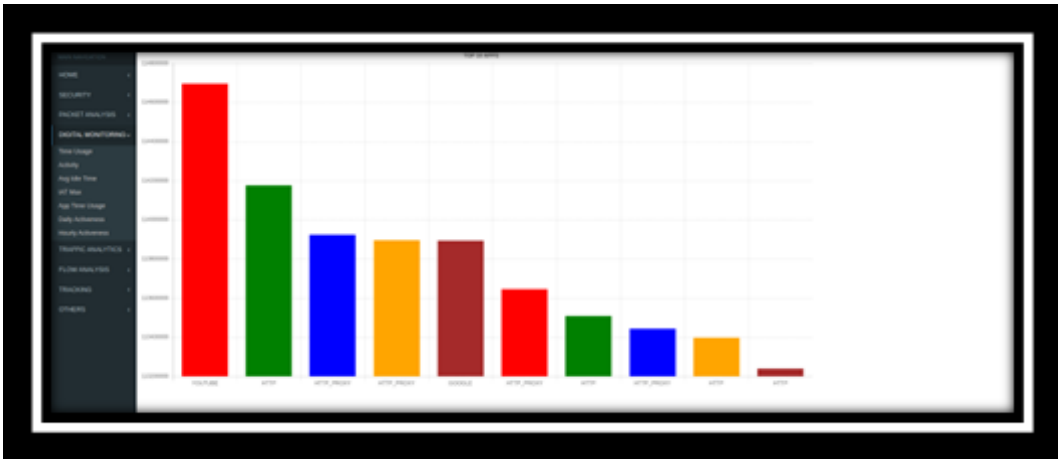
If you click on this it gives top10 apps in terms of maximum usage time

MILESTONE 3



- **Activity**

If you click on this it gives the top 10 active apps in terms of maximum active time.

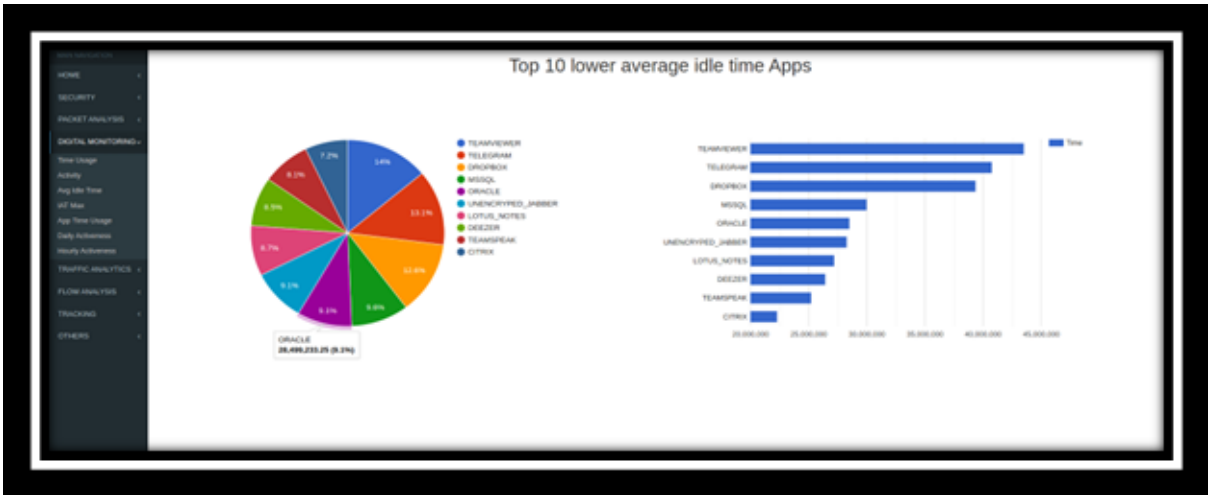


- **Avg Idle Time**

If you click on this it gives the top 10 apps in terms of maximum avg idle time used.

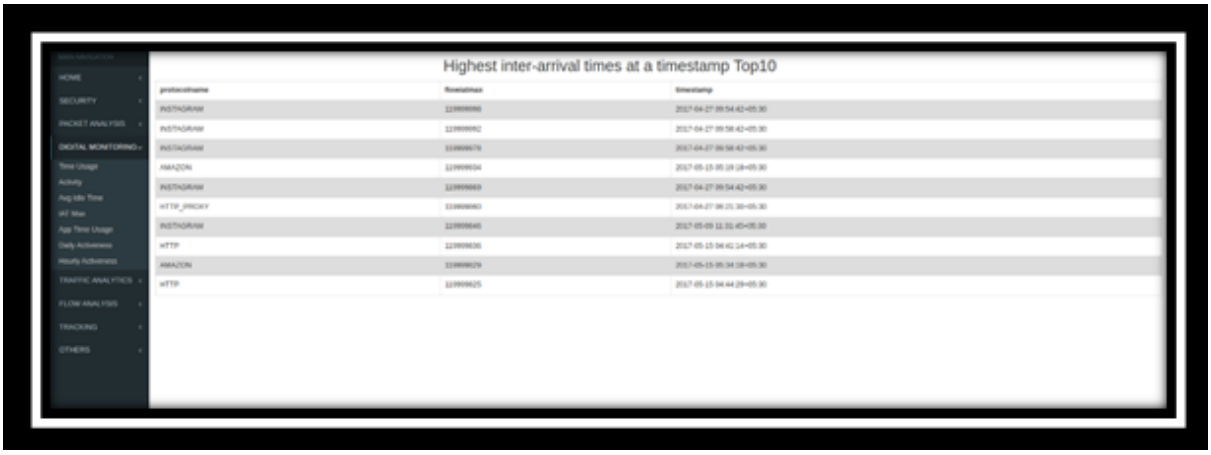
A lower average idle time could indicate a more active network flow, while a higher average idle time could suggest a less active or stalled flow.

MILESTONE 3



- **IAT Max**

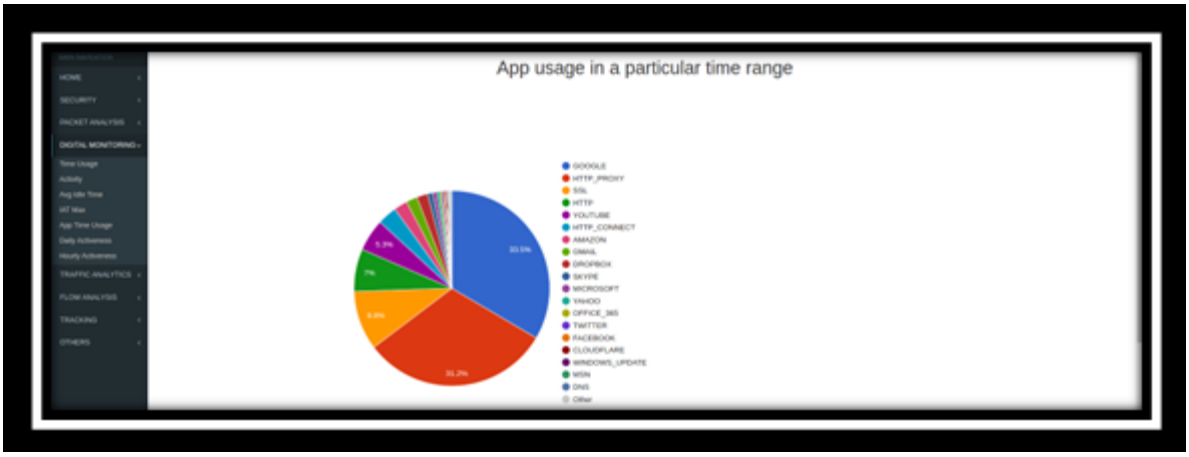
If you click on this it gives the top10 apps with highest inter arrival times
This query can be used to identify flows that have unusually long inter-arrival times between packets, which could be indicative of certain types of applications or activities.



MILESTONE 3

- **App Time Usage**

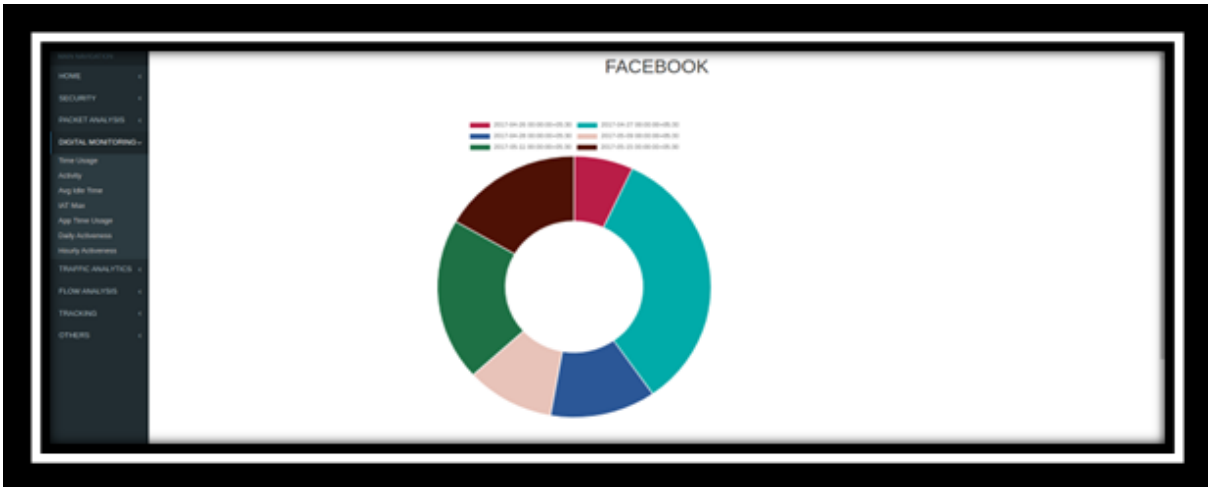
If you click on this first it asks the starttime and endtime later if you submit it gives which apps uses how much time for that time range .



MILESTONE 3

- **Daily Activeness**

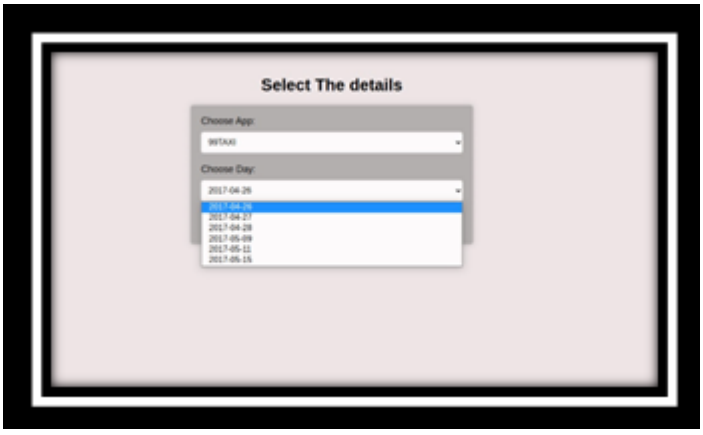
If you click on this first it asks the app you need to examine/know about, later it gives the daily activeness of the selected app in 6 days

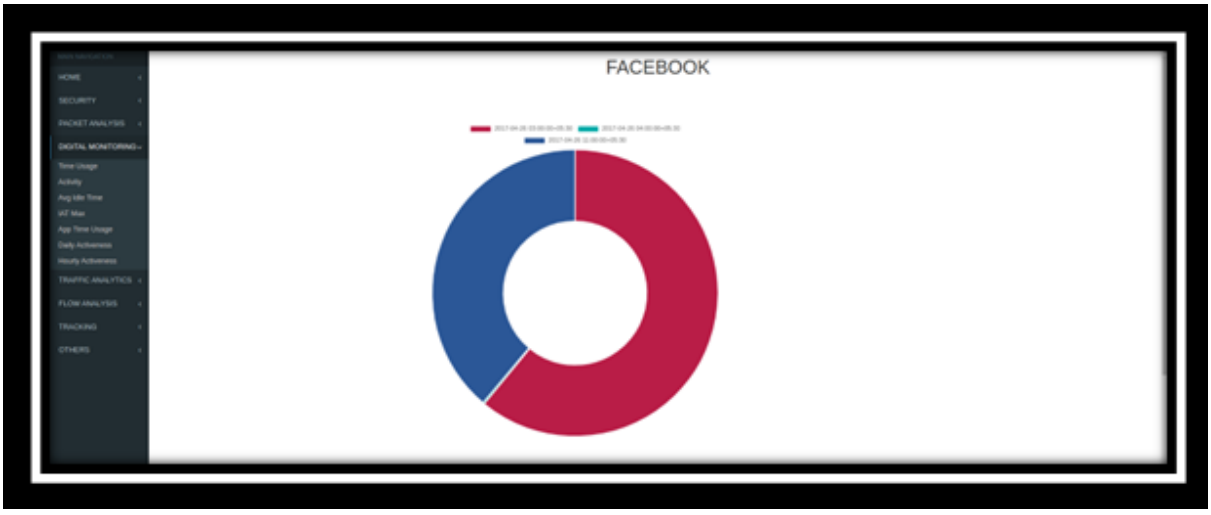


MILESTONE 3

- **Hourly Activeness**

If you click on this first it asks app name and the date of the day on which you what the hourly activeness of the app,later it gives the hourly activeness of the selected app in a given day

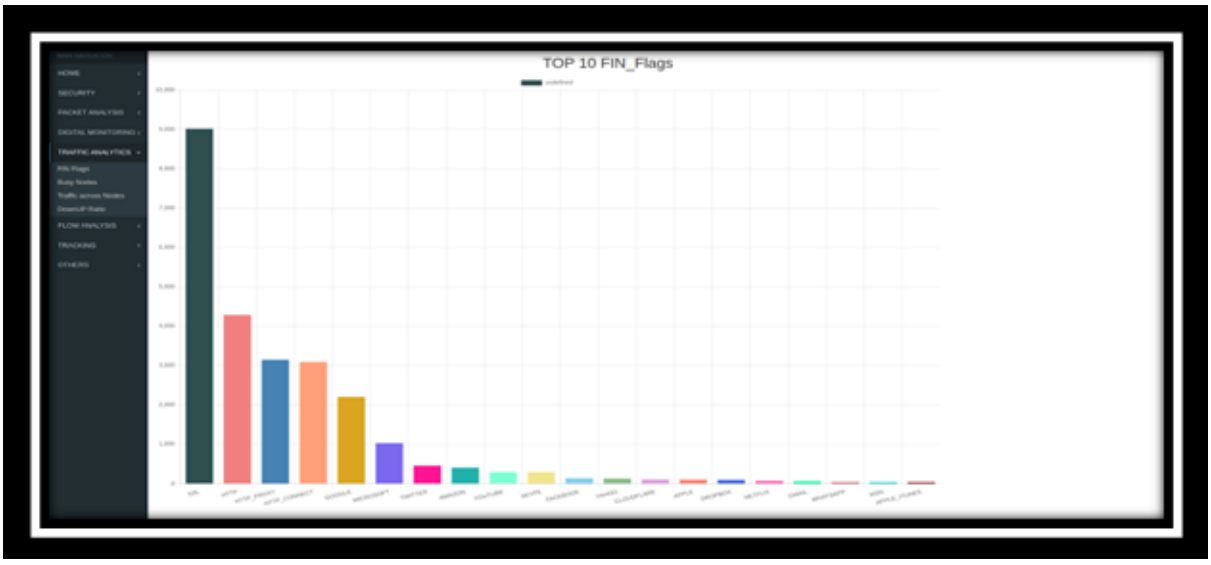




MILESTONE 3

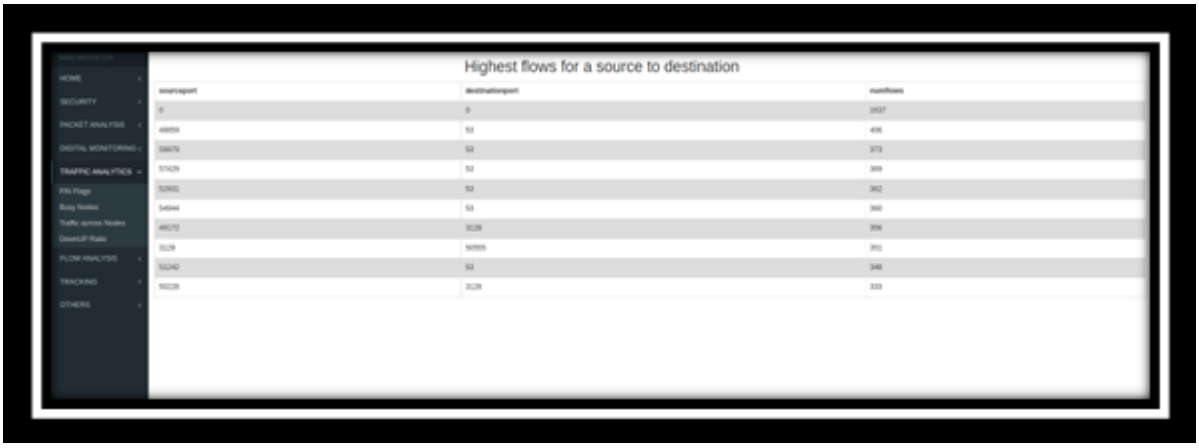
- **FIN Flags**

If you click on this it gives top 20 apps with a high number of FIN flags



- **Busy Nodes**

If you click on this it gives the top10 nodes with highest number of flows
To optimize resource allocation, we could analyze network usage and identify areas where resources can be reallocated to improve performance and reduce costs.

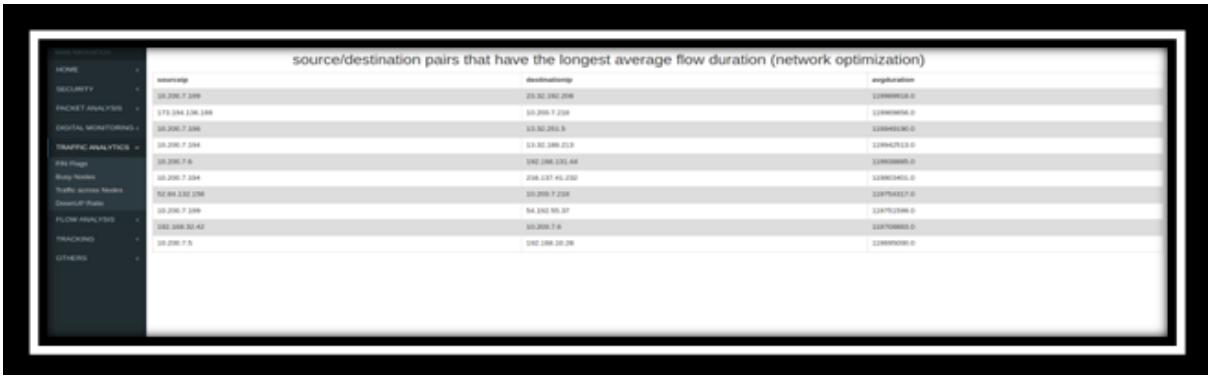


MILESTONE 3

- **Traffic across nodes**

If you click on this it gives the Top 10 source/destination pairs having the longest avg flow duration.

Application to find the source/destination pairs that have the longest average flow duration (network optimization)



- **DownUp Ratio**

If you click on this it gives the apps which have high Down/Up Ratio
This table can be useful for analyzing network traffic patterns and identifying potential network congestion or bandwidth issues.

For example, a high down/up ratio for a particular flow could indicate that the flow is consuming more downlink bandwidth than uplink bandwidth, which could lead to network congestion or other performance issues. Network administrators can use this information to identify and resolve such issues

MILESTONE 3

- **App Flows**

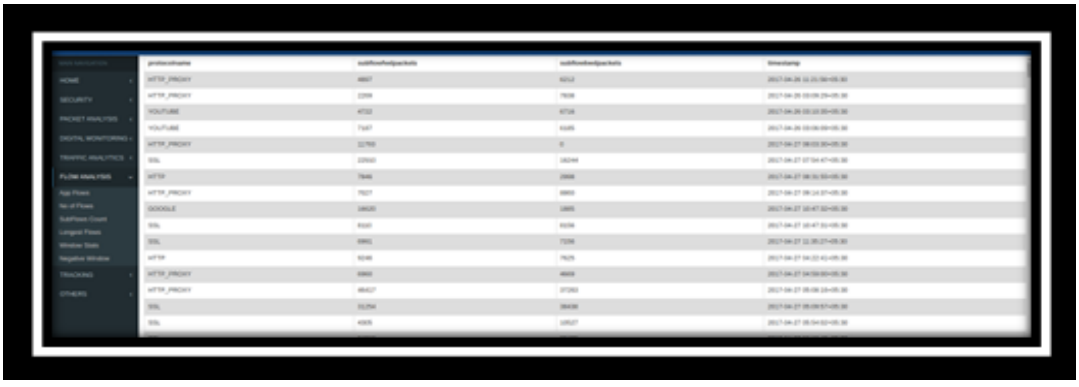
If you click on this it gives apps that are using longest flows in flowDuration at a given timestamp

- **No of Flows**

If you click on this it gives the count of flows for each protocol

- **SubFlows count**

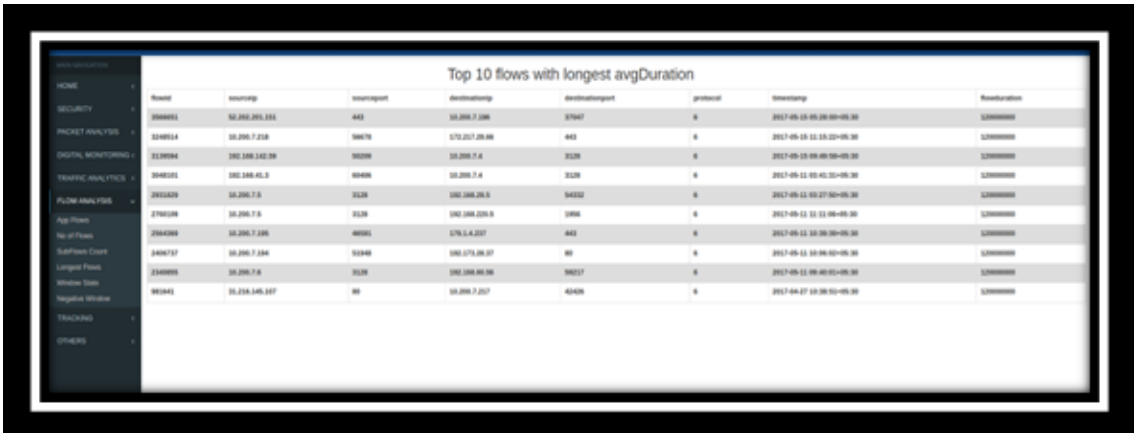
If you click on this it gives all Apps having flows with a high number of subflows at a given timestamp



MILESTONE 3

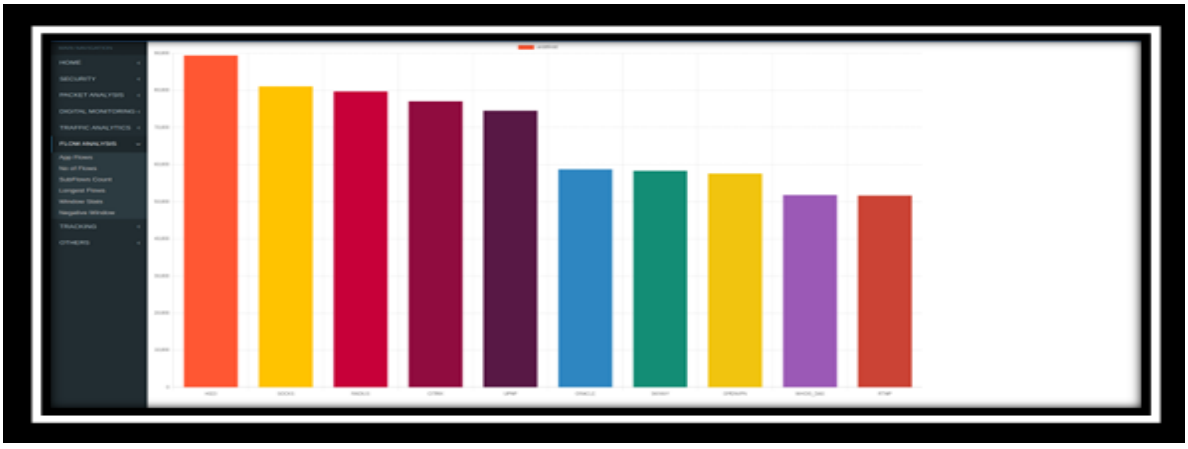
- **longest flows**

If you click on this it gives the top 10 flows with longest avgDuration



- **Window stats**

If you click on this it gives the protocols having avg(initial window) in desc



MILESTONE 3

- **Negative window**

If you click on this it gives protocols having avg(initial window) negative

- **IP Tracking**

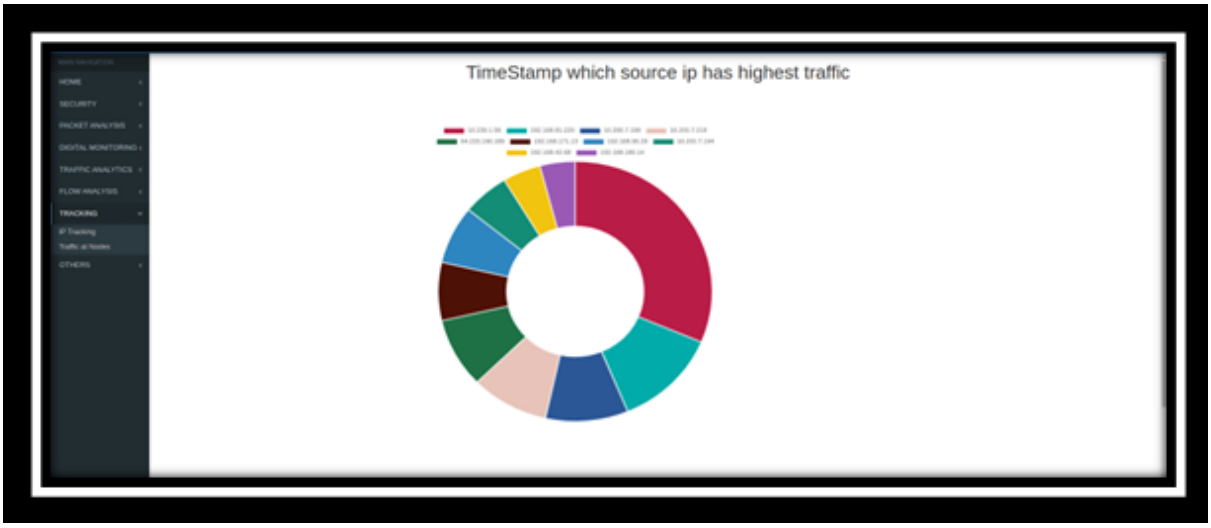
If you click on this it gives the reachable ip address from the given ip address in a given Timestamp

---

MILESTONE 3

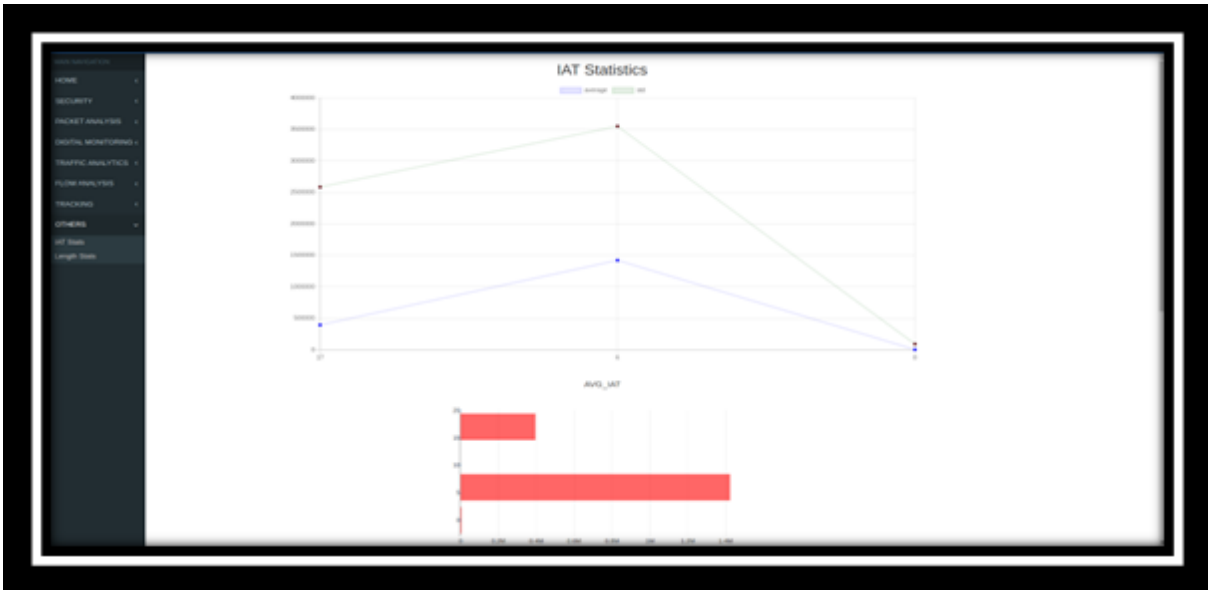
- **Traffic at nodes**

If you click on this it gives the source IP with highest traffic in a given Timestamp.



- **IAT Stats**

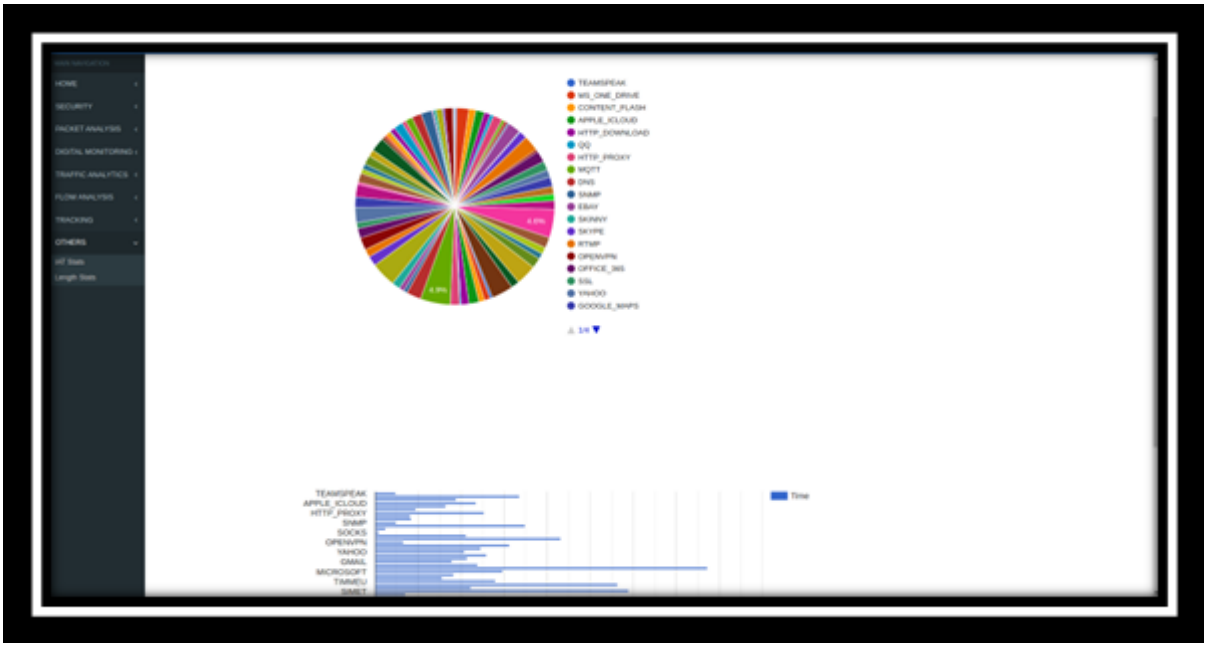
If you click on this it gives the average and standard deviation of the flow inter-arrival time for each protocol



MILESTONE 3

- **Length Stats**

If you click on this it gives average packet length for each protocol



SUBMISSION LINK: https://github.com/Lozsku/Alpha