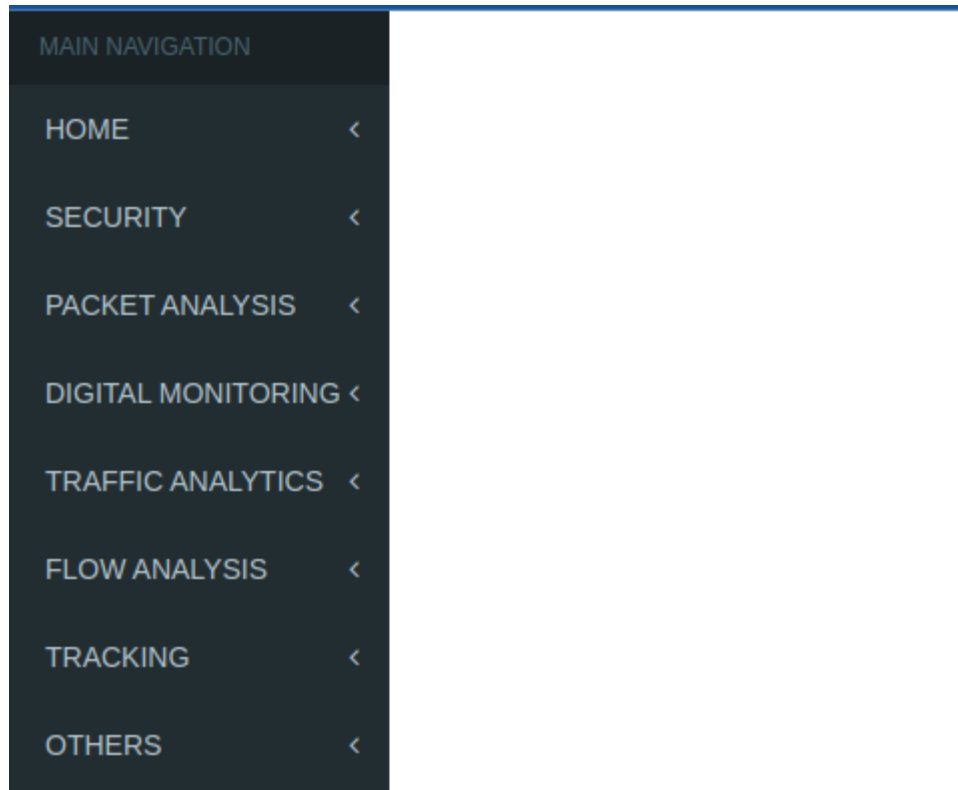


MILESTONE 3

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

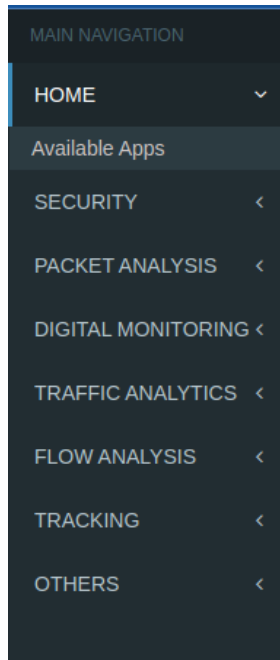
➔ If we click on each section, we can find sub-sections under each section which are the applications of our database.

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

Home

- Available apps

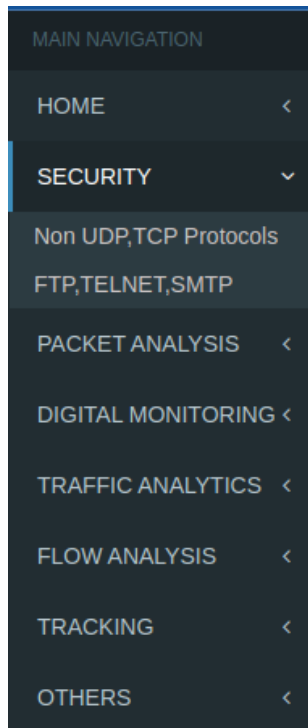
MILESTONE 3



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

Security

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

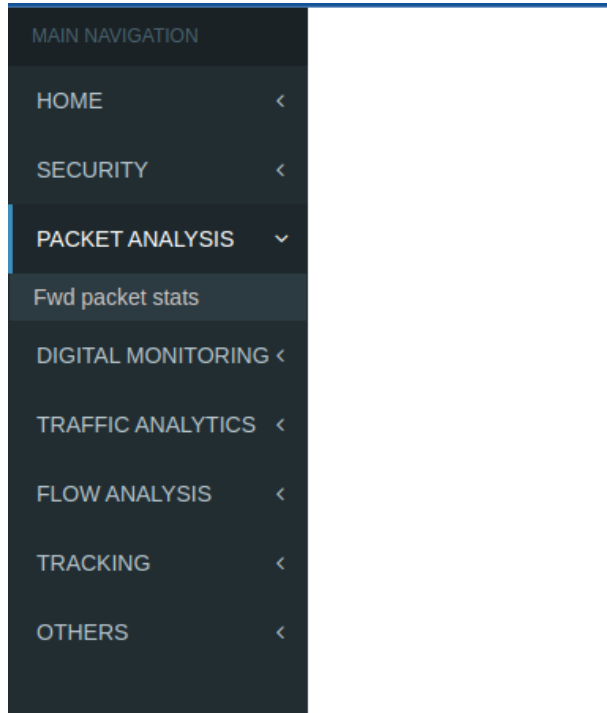


MILESTONE 3

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

Packet Analysis

- fwd packets stats

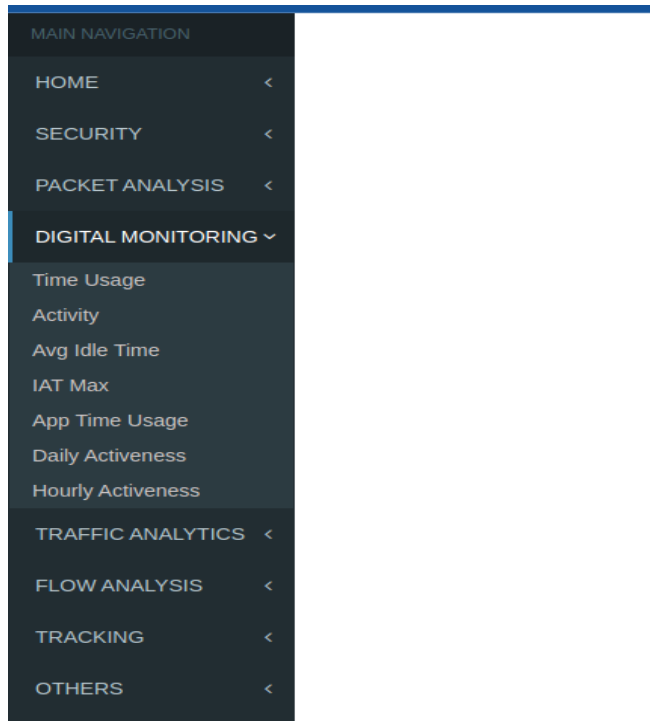


If you click on the Digital Monitoring you can see the following subsections

Digital Monitoring

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

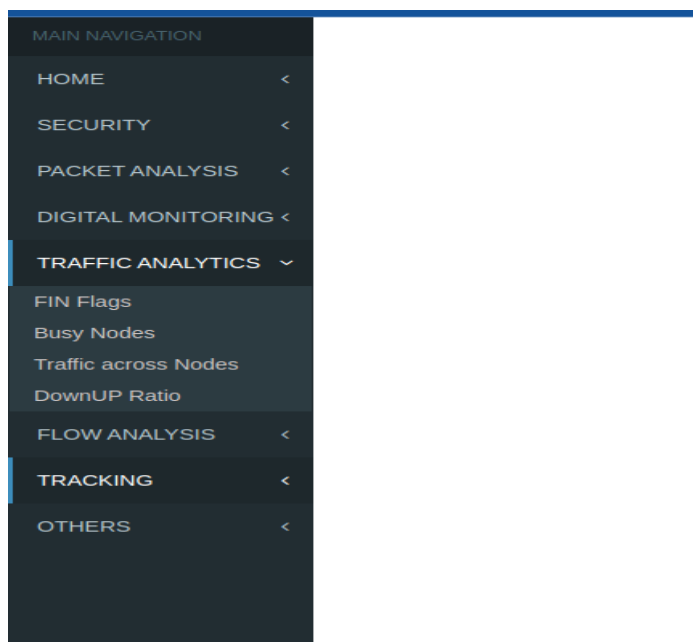
MILESTONE 3



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

Traffic Analytics

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

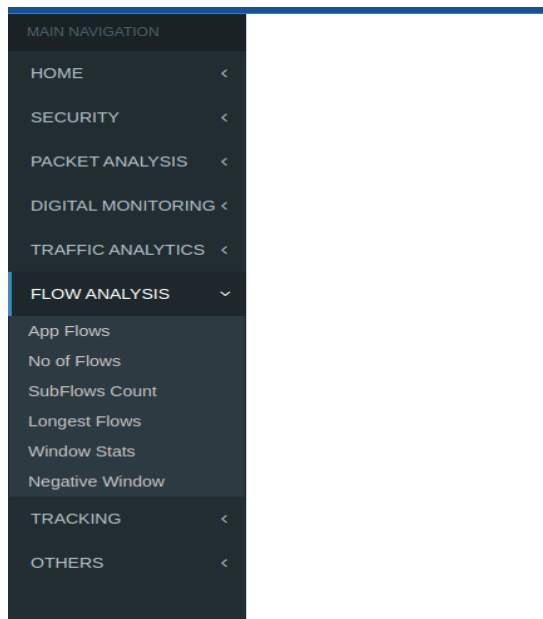


MILESTONE 3

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

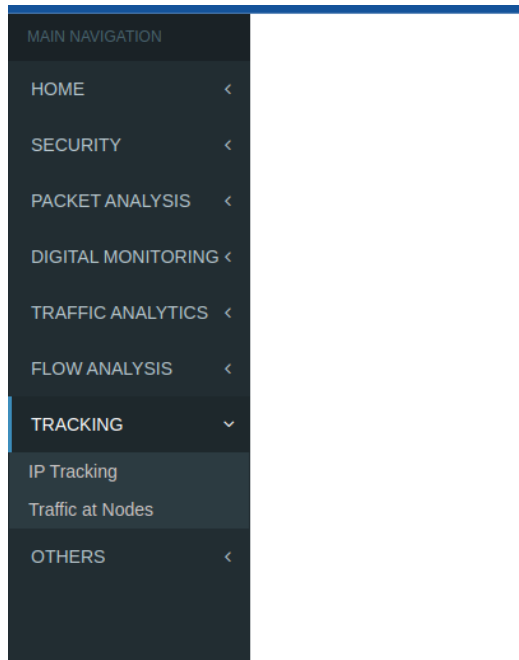


If you click on the Tracking you can see the following subsections

Tracking

- IP Tracking
- Traffic at nodes

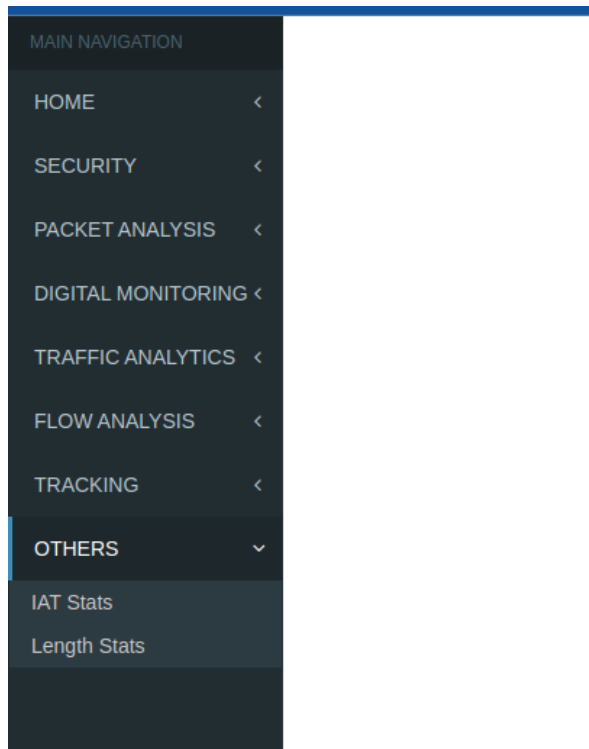
MILESTONE 3



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

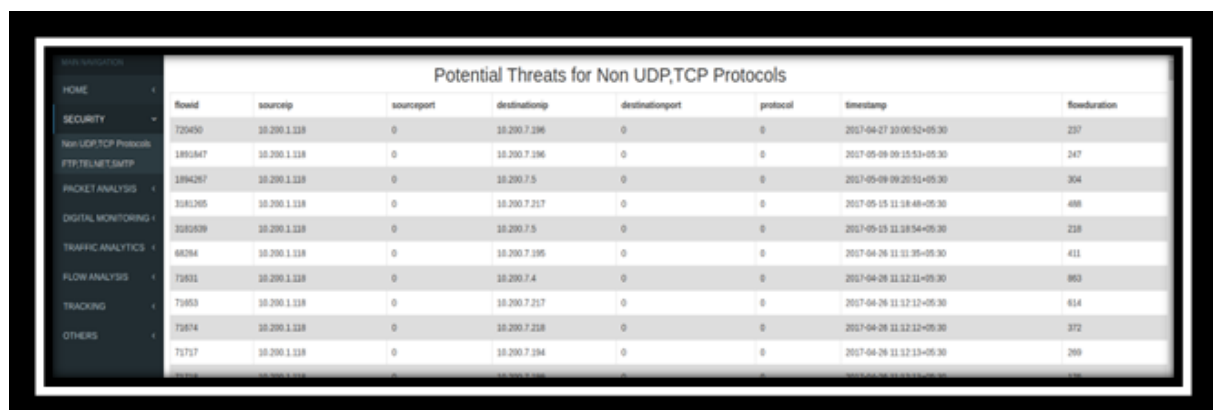


The screenshot shows a web application interface with a sidebar on the left containing navigation links: HOME, Available Apps, SECURITY, PACKET ANALYSIS, DIGITAL MONITORING, TRAFFIC ANALYTICS, FLOW ANALYSIS, TRACKING, and OTHERS. The main content area is titled 'ALL APPS' and displays a list of applications: WIFIAX, AMAZON, APPLE, APPLE_CLOUD, APPLE_IUNES, BGP, BITTORRENT, CITRIX, CITRIX_ONLINE, CLOUDFLARE, CNN, CONTENT_FLASH, DEEZER, and DNS.

ALL APPS	
WIFIAX	
AMAZON	
APPLE	
APPLE_CLOUD	
APPLE_IUNES	
BGP	
BITTORRENT	
CITRIX	
CITRIX_ONLINE	
CLOUDFLARE	
CNN	
CONTENT_FLASH	
DEEZER	
DNS	

- **Non UDP,TCP protocols**

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



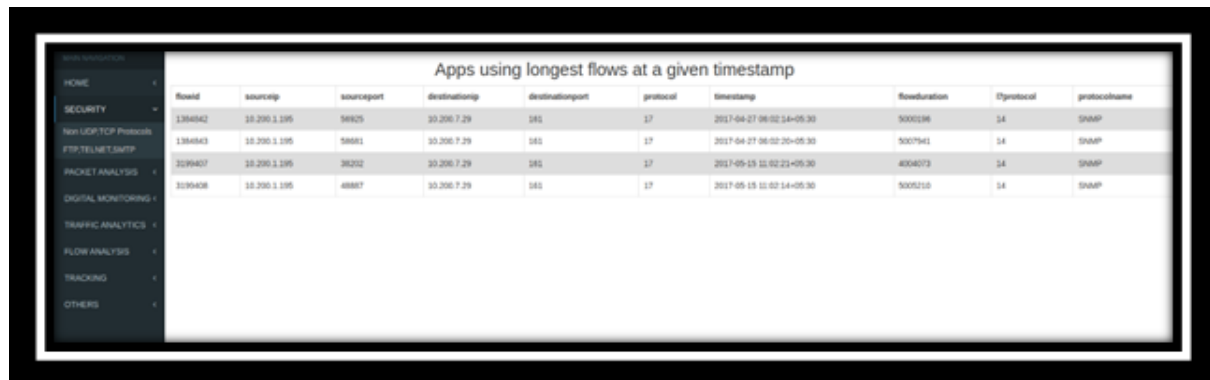
The screenshot shows a web application interface with a sidebar on the left containing navigation links: HOME, SECURITY, Non UDP,TCP Protocols, FTP,TELNET,SMTP, PACKET ANALYSIS, DIGITAL MONITORING, TRAFFIC ANALYTICS, FLOW ANALYSIS, TRACKING, and OTHERS. The main content area is titled 'Potential Threats for Non UDP,TCP Protocols' and displays a table with the following columns: RowId, sourceip, sourceport, destinationip, destinationport, protocol, timestamp, and Rowduration.

RowId	sourceip	sourceport	destinationip	destinationport	protocol	timestamp	Rowduration
720430	10.200.1.118	0	10.200.7.196	0	0	2017-04-27 10:00:52+05:30	237
1893847	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	408
3285639	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	10.200.7.196	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
71853	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
1894268	10.200.1.118	0	10.200.7.196	0	0	2017-05-09 09:20:52+05:30	1126

MILESTONE 3

- **FTP,TELNET,SMTP**

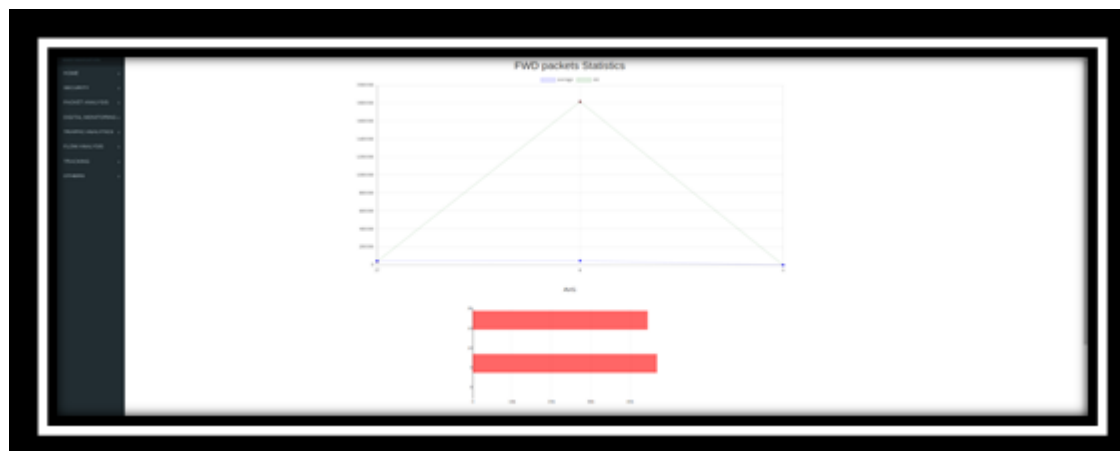
If you click on this it gives the Potential Threats which are FTP , Telnet , SNMP



flowid	sourceip	sourceport	destinationip	destinationport	protocol	timestamp	flowduration	protocol	protocolname
1384042	10.200.1.195	56925	10.200.7.29	143	17	2017-04-27 06:02:14+05:30	5000136	14	SNMP
1384043	10.200.1.195	56981	10.200.7.29	143	17	2017-04-27 06:02:20+05:30	5007941	14	SNMP
1099407	10.200.1.195	36232	10.200.7.29	143	17	2017-05-15 11:02:21+05:30	4004073	14	SNMP
1099408	10.200.1.195	48887	10.200.7.29	143	17	2017-05-15 11:02:14+05:30	5005210	14	SNMP

- **fwd packets stats**

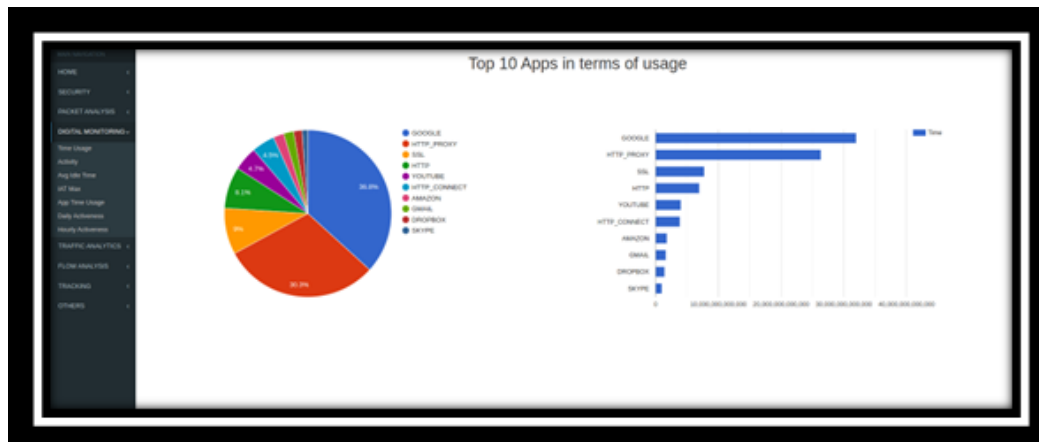
If you click on this it gives the average and standard deviation of the total length of forward packets for each protocol.



- **Time usage**

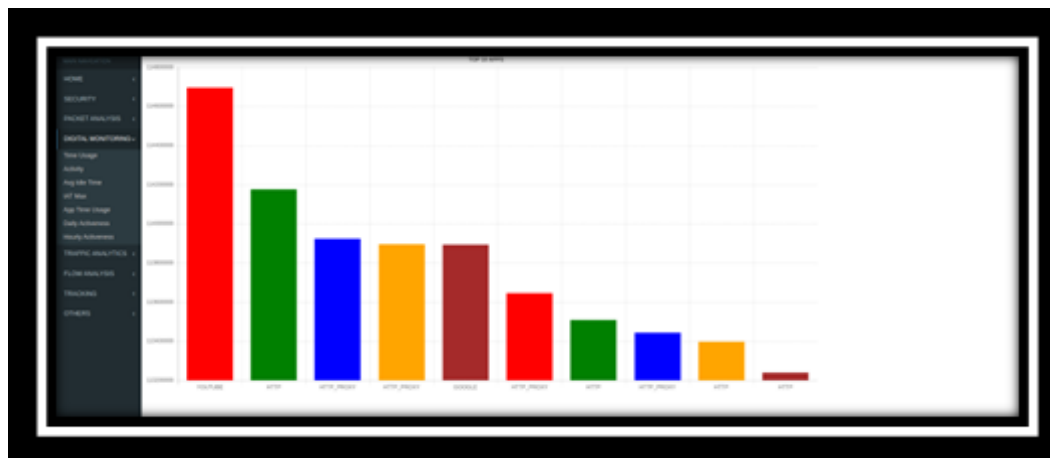
If you click on this it gives top10 apps in terms of maximum usage time

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.

Top 10 lower average idle time Apps

Pie Chart Data (Average Idle Time):

Application	Percentage
TELEVIEWER	1.4%
TELEGRAM	13.1%
SPROBOK	12.2%
MISQI	9.9%
ORACLE	9.6%
UNENCRYPTED_JABBER	9.1%
LOPUS_NOTES	8.7%
DEEZER	8.6%
TEAMSPEAK	7.2%
CITRIX	5.2%

Horizontal Bar Chart Data (Total Idle Time):

Application	Total Idle Time (Approximate)
TELEVIEWER	43,000,000
TELEGRAM	41,000,000
SPROBOK	39,000,000
MISQI	31,000,000
ORACLE	29,000,000
UNENCRYPTED_JABBER	27,000,000
LOPUS_NOTES	26,000,000
DEEZER	25,000,000
TEAMSPEAK	24,000,000
CITRIX	21,000,000

Oracle Detail:
 ORACLE
 28,495,233.25 (9.3%)

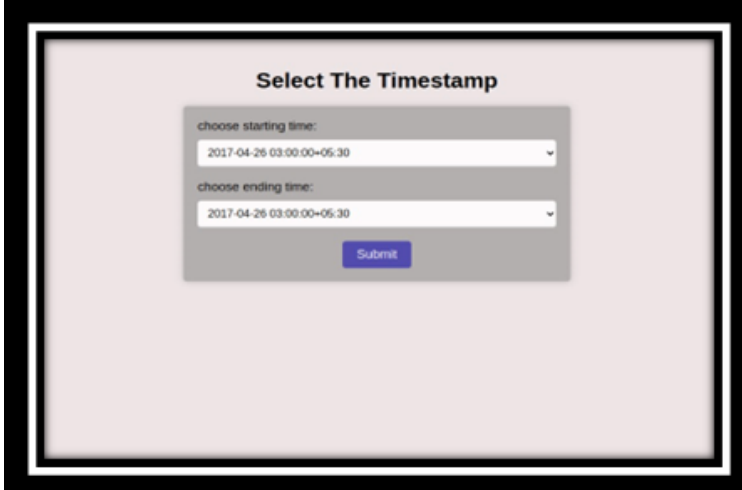
If you click on this it gives the top10 apps with highest inter arrival times
This query can be used to identify flows that have unusually long inter-arrival times between packets, which could be indicative of certain types of applications or activities.

Highest inter-arrival times at a timestamp Top10		
protocolname	Rownumax	Timestamp
INSTAGRAM	127000000	2017-04-27 00:54:42+00:00
INSTAGRAM	127000002	2017-04-27 00:50:42+00:00
INSTAGRAM	127000076	2017-04-27 00:50:42+00:00
AMAZON	127000004	2017-05-15 05:10:18+00:00
INSTAGRAM	127000008	2017-04-27 00:54:42+00:00
HTTP_PROXY	127000000	2017-04-27 00:25:30+00:00
INSTAGRAM	127000040	2017-05-09 11:21:45+00:00
HTTP	127000030	2017-05-15 04:42:14+00:00
AMAZON	127000076	2017-05-15 05:10:18+00:00
HTTP	127000025	2017-05-15 04:44:20+00:00

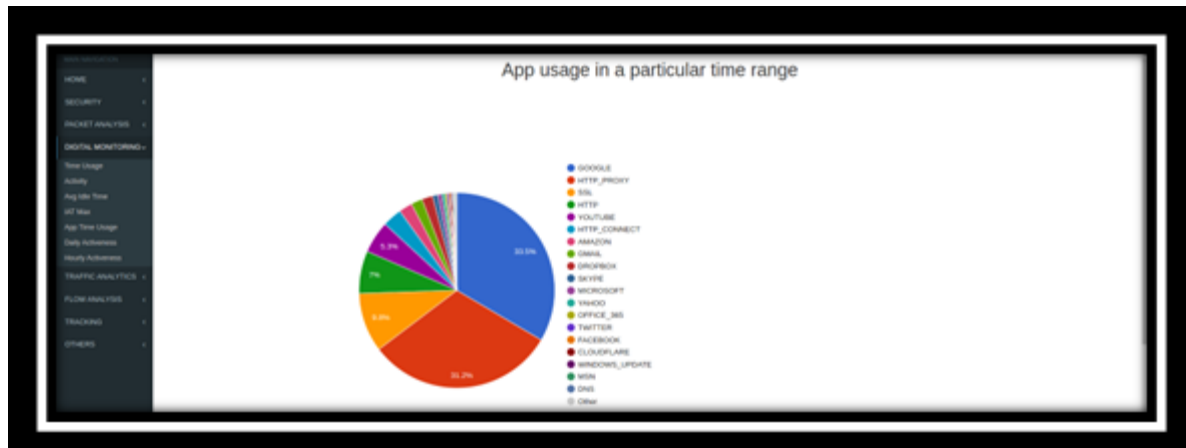
MILESTONE 3

- **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 .



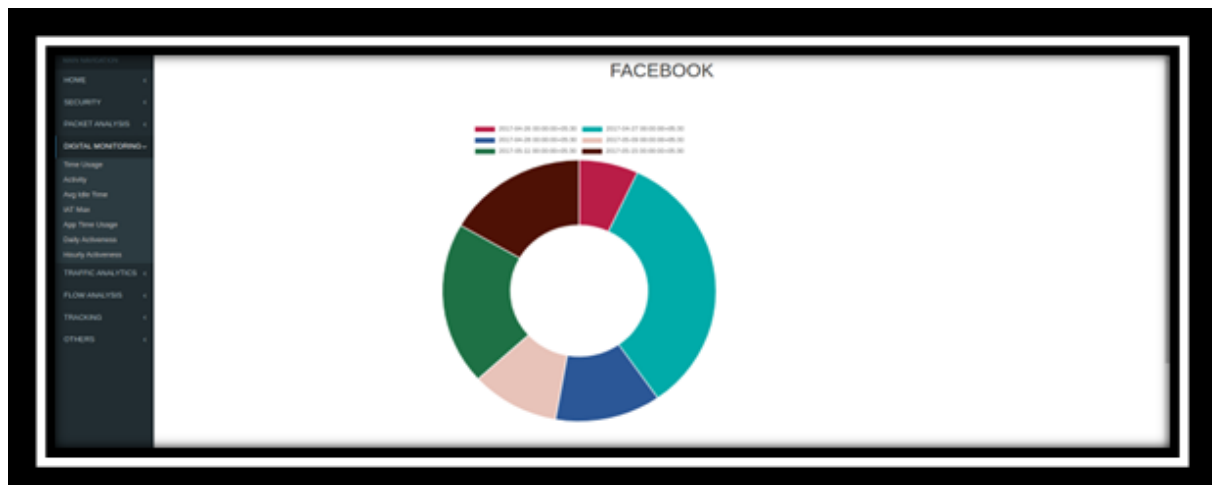
The screenshot shows a web form titled "Select The Timestamp". It contains two dropdown menus for selecting a starting and ending time, both currently set to "2017-04-26 03:00:00-05:30". A blue "Submit" button is located below the dropdowns.



MILESTONE 3

- **Daily Activeness**

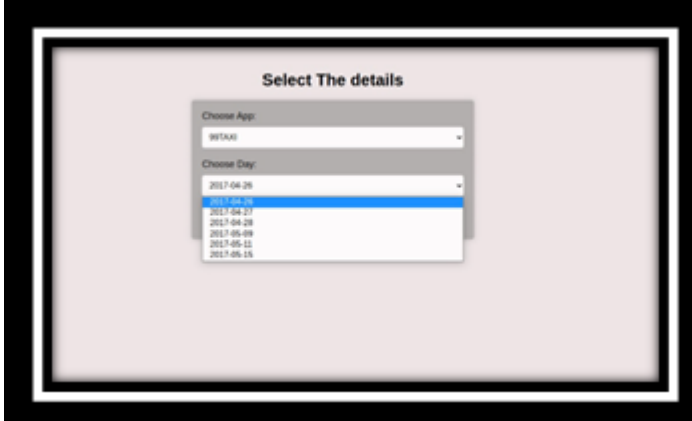
If you click on this first it asks the app you need to examine/know about, later it gives the daily activeness of the selected app in 6 days



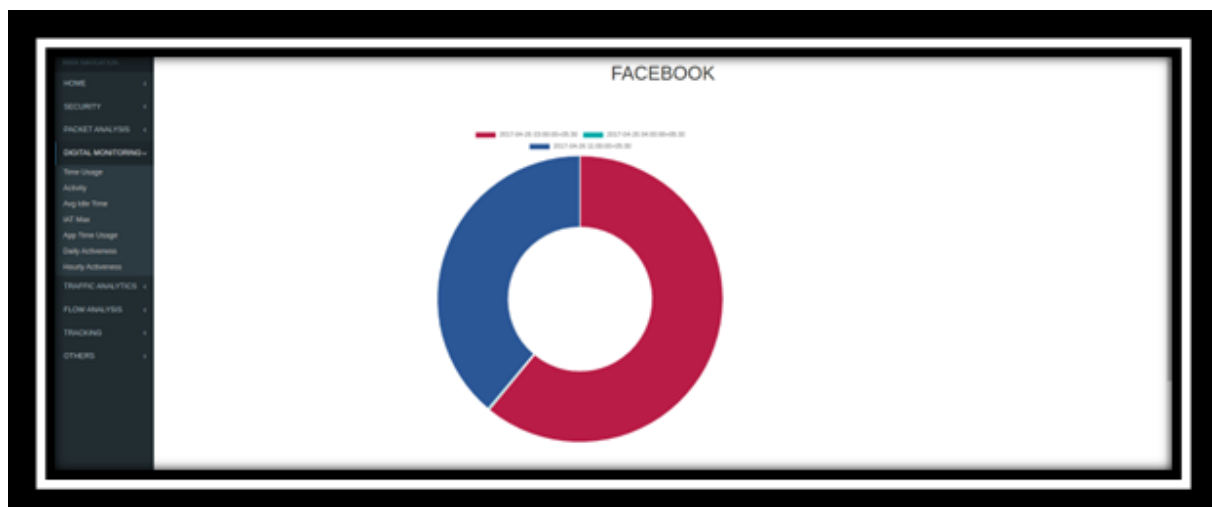
MILESTONE 3

- **Hourly Activeness**

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



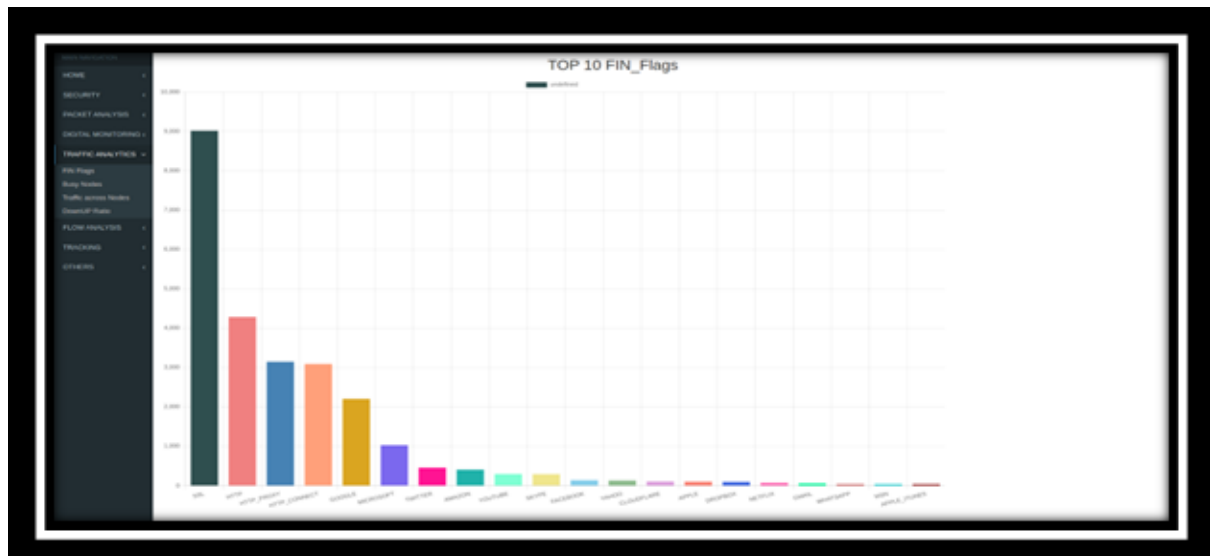
The screenshot shows a web interface with a title "Select The details". Below the title are two dropdown menus. The first dropdown is labeled "Choose App" and has "WhatsApp" selected. The second dropdown is labeled "Choose Day" and has a date selected from a list of dates ranging from 2017-04-26 to 2017-05-15.



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.

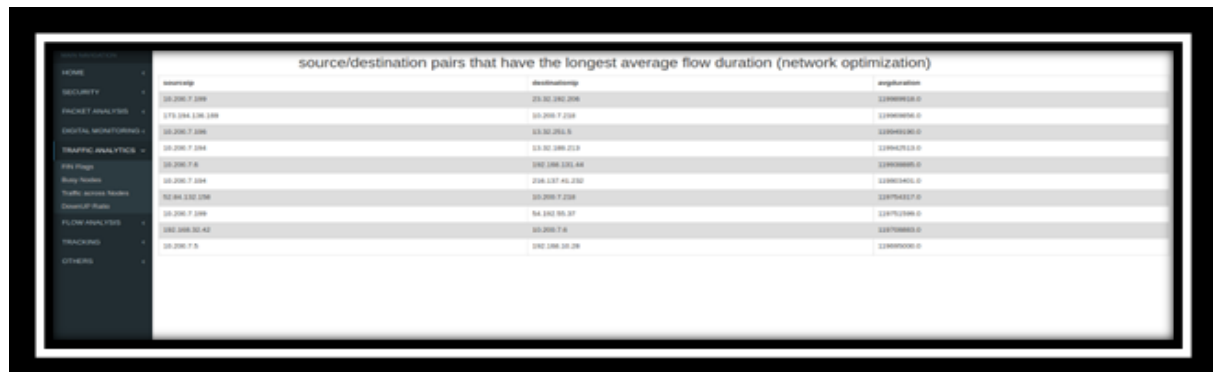
sourceip	destinationip	numflows
10.10.10.1	10.10.10.1	10000
10.10.10.2	10.10.10.2	10000
10.10.10.3	10.10.10.3	10000
10.10.10.4	10.10.10.4	10000
10.10.10.5	10.10.10.5	10000
10.10.10.6	10.10.10.6	10000
10.10.10.7	10.10.10.7	10000
10.10.10.8	10.10.10.8	10000
10.10.10.9	10.10.10.9	10000
10.10.10.10	10.10.10.10	10000

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)



The screenshot shows a web application interface with a sidebar on the left containing menu items: HOME, SECURITY, PACKET ANALYSIS, DIGITAL MONITORING, TRAFFIC ANALYTICS, and OTHERS. The main content area displays a table titled "source/destination pairs that have the longest average flow duration (network optimization)". The table has three columns: "sourceip", "destinationip", and "avgduration". It lists 10 rows of data representing different IP pairs and their average flow durations.

sourceip	destinationip	avgduration
10.200.7.100	25.101.100.100	1.00000000.0
173.104.136.100	10.200.7.100	1.00000000.0
10.200.7.100	10.200.7.100	1.00000000.0
10.200.7.100	10.200.7.100	1.00000000.0
10.200.7.100	10.200.7.100	1.00000000.0
10.200.7.100	10.200.7.100	1.00000000.0
10.200.7.100	10.200.7.100	1.00000000.0
10.200.7.100	10.200.7.100	1.00000000.0
10.200.7.100	10.200.7.100	1.00000000.0
10.200.7.100	10.200.7.100	1.00000000.0

- **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



The screenshot shows a web application interface with a sidebar on the left containing menu items: HOME, SECURITY, PACKET ANALYSIS, DIGITAL MONITORING, TRAFFIC ANALYTICS, and OTHERS. The main content area displays a table titled "Apps having Down/Up more ratio(For congestion checking)". The table has three columns: "protocolname", "timeinterval", and "downupratio". It lists 2 rows of data representing different protocols and their down/up ratios.

protocolname	timeinterval	downupratio
HTTP_PROXY	2017-08-08 08:24:00-08:30	200
DROPPED	2017-08-08 08:24:00-08:30	200

MILESTONE 3

- **App Flows**

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

Apps using longest flows at a given timestamp			
TIME	hostname	Reputation	timestamp
SECURITY	AMAZON	120000000	2017-05-18 05:20:00+05:30
PACKET ANALYSIS	GOOGLE	120000000	2017-05-18 11:19:22+05:30
DIGITAL MONITORING	HTTP_PROXY	120000000	2017-05-18 06:40:58+05:30
TELEMETRY ANALYTICS	HTTP_PROXY	120000000	2017-05-12 03:43:30+05:30
FLOW ANALYSIS	HTTP_PROXY	120000000	2017-05-12 03:27:30+05:30
App Flows	HTTP_PROXY	120000000	2017-05-01 01:04:00+05:30
Net of Flows	SSL	120000000	2017-05-12 20:39:39+05:30
SubFlows Count	HTTP	120000000	2017-05-12 20:08:02+05:30
Longest Flows	HTTP_PROXY	120000000	2017-05-11 06:40:02+05:30
Window Size			
Negative Windows	HTTP	120000000	2017-04-27 20:30:52+05:30
TRACKING			
OTHERS			

- **No of Flows**

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

Count number of flows for each protocol

protocol	count
TCP	2860
HTTP	282075
SSH	2827

- **SubFlows count**


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

Asset Categories	assetcategory	assetcategoryname	assetcategoryname	assetcategoryname	assetcategoryname
HOME	HTTP_PROXY	8081	8081	8081	2017-04-26 22:25:04-05:30
SECURITY	HTTP_PROXY	8080	8080	8080	2017-04-26 22:25:04-05:30
PROJECT ANALYTICS	VOLUME	8732	8732	8732	2017-04-26 22:25:04-05:30
PROJECT ANALYTICS	VOLUME	1587	1587	1587	2017-04-26 22:25:04-05:30
PROJECT ANALYTICS	HTTP_PROXY	8730	8730	8730	2017-04-27 00:03:29-05:30
PROJECT ANALYTICS	SQL	12903	12903	12903	2017-04-27 07:04:47-05:30
PROJECT ANALYTICS	HTTP	7645	7645	7645	2017-04-27 08:56:53-05:30
Project Files	HTTP_PROXY	7027	7027	7027	2017-04-27 09:24:37-05:30
SQL of Files	GOOGLE	12605	12605	12605	2017-04-27 10:47:32-05:30
Project Files	SQL	8329	8329	8329	2017-04-27 10:47:32-05:30
Project Files	SQL	8981	8981	8981	2017-04-27 12:28:27-05:30
Project Files	HTTP	7026	7026	7026	2017-04-27 14:22:43-05:30
PROJECT FILES	HTTP_PROXY	8980	8980	8980	2017-04-27 14:59:49-05:30
PROJECT FILES	HTTP_PROXY	8607	8607	87260	2017-04-27 15:00:23-05:30
PROJECT FILES	SQL	12594	12594	89408	2017-04-27 15:00:31-05:30
PROJECT FILES	SQL	4024	4024	12027	2017-04-27 15:04:52-05:30

MILESTONE 3

- **longest flows**

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

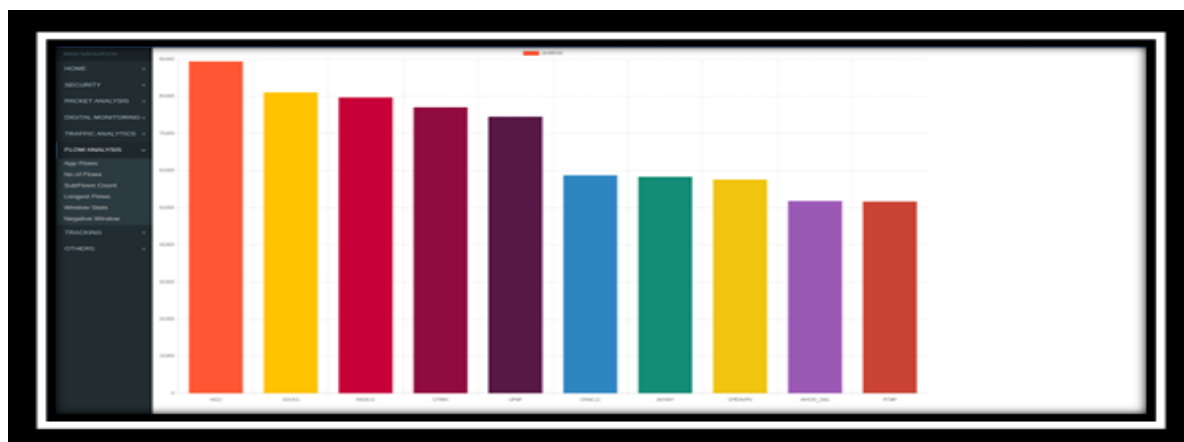


The screenshot shows a dashboard with a sidebar on the left containing menu items: HOME, SECURITY, PACKET ANALYSIS, DIGITAL MONITORING, TRAFFIC ANALYSIS, FLOW ANALYSIS, App Flows, Top of Flows, SubFlow Count, Longest Flows, Window Stats, Negative Window, TRACINGS, and OTHERS. The main area displays a table titled 'Top 10 flows with longest avgDuration'.

FlowID	sourceip	sourceport	destinationip	destinationport	protocol	timeRange	FlowDuration
3049551	52.202.261.155	443	10.200.7.100	37647	6	2017-09-15 09:20:00-09:30	1.00000000
3140514	10.200.7.210	90070	170.217.20.86	443	6	2017-09-15 11:15:00-09:30	1.00000000
3139594	100.100.142.90	50000	10.200.7.4	3120	6	2017-09-15 09:00:00-09:30	1.00000000
3040101	100.100.41.3	40400	10.200.7.4	3120	6	2017-09-11 03:41:30-09:30	1.00000000
3031429	10.200.7.5	3120	100.100.20.5	54232	6	2017-09-11 03:27:00-09:30	1.00000000
3740109	10.200.7.5	3120	100.100.20.5	1000	6	2017-09-11 11:11:00-09:30	1.00000000
3044500	10.200.7.100	40000	170.217.20.86	443	6	2017-09-11 10:30:00-09:30	1.00000000
3404757	10.200.7.100	51940	100.170.20.17	80	6	2017-09-11 10:00:00-09:30	1.00000000
3140005	10.200.7.5	3120	100.100.80.10	50017	6	2017-09-11 09:00:00-09:30	1.00000000
001041	10.210.140.107	80	10.200.7.217	42420	6	2017-04-27 10:30:00-09:30	1.00000000

- **Window stats**

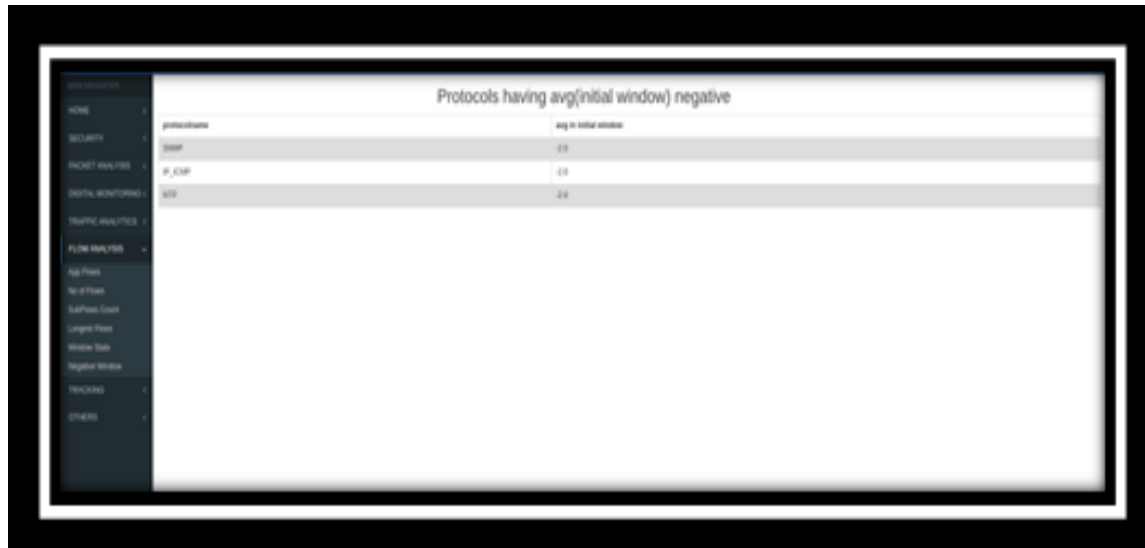
If you click on this it gives the protocols having avg(initial window) in desc



MILESTONE 3

- **Negative window**

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



The screenshot shows a web application interface with a sidebar on the left containing navigation links: HOME, SECURITY, PACKET ANALYSIS, DIGITAL MONITORING, TRAFFIC ANALYTICS, FLOW ANALYSIS, TRACKING, and OTHERS. The main content area is titled "Protocols having avg(initial window) negative". It contains a table with two columns: "protocolName" and "avg in initial window".

protocolName	avg in initial window
TCP	-25
IP_TCP	-24
UDP	-24

- **IP Tracking**

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



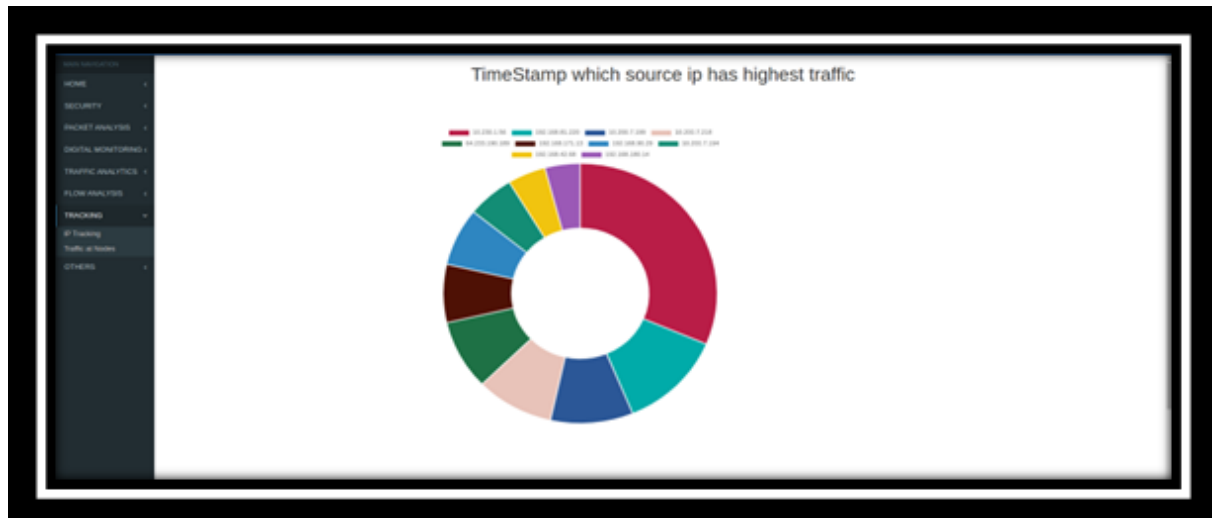
The screenshot shows the same web application interface. The main content area is titled "Reachable ip from the given ip address in a given time TimeStamp". It contains a table with two columns: "timestamp" and "reachable_nodes".

timestamp	reachable_nodes
2017-04-26 12:12:09-05:30	10.200.7.9 192.168.180.27 192.168.32.49 192.168.42.98

MILESTONE 3

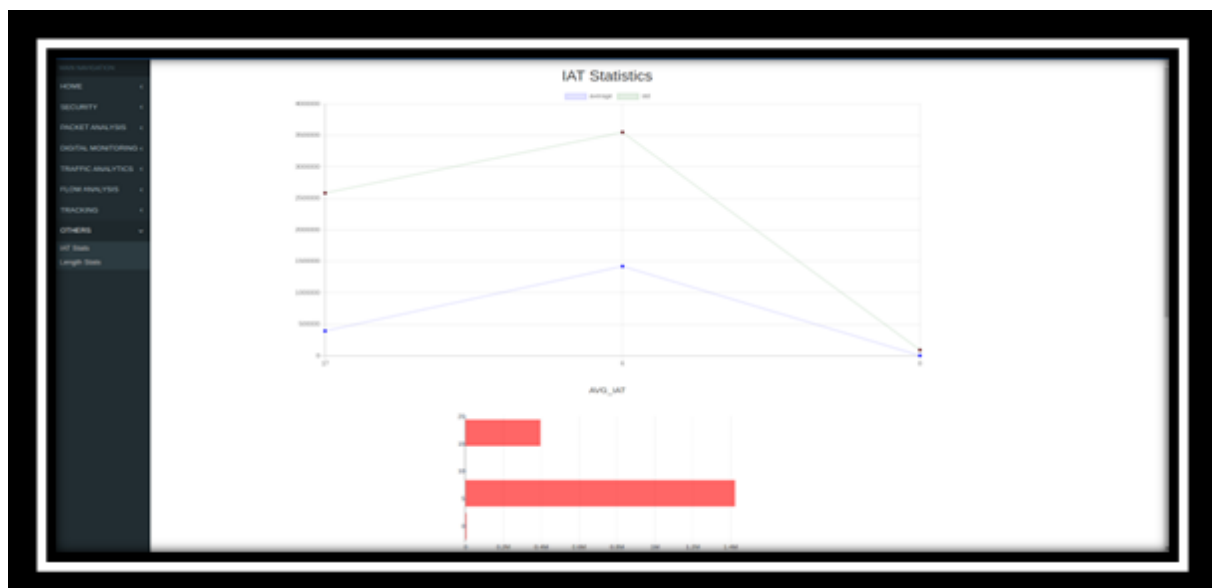
- Traffic at nodes**

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



- IAT Stats**

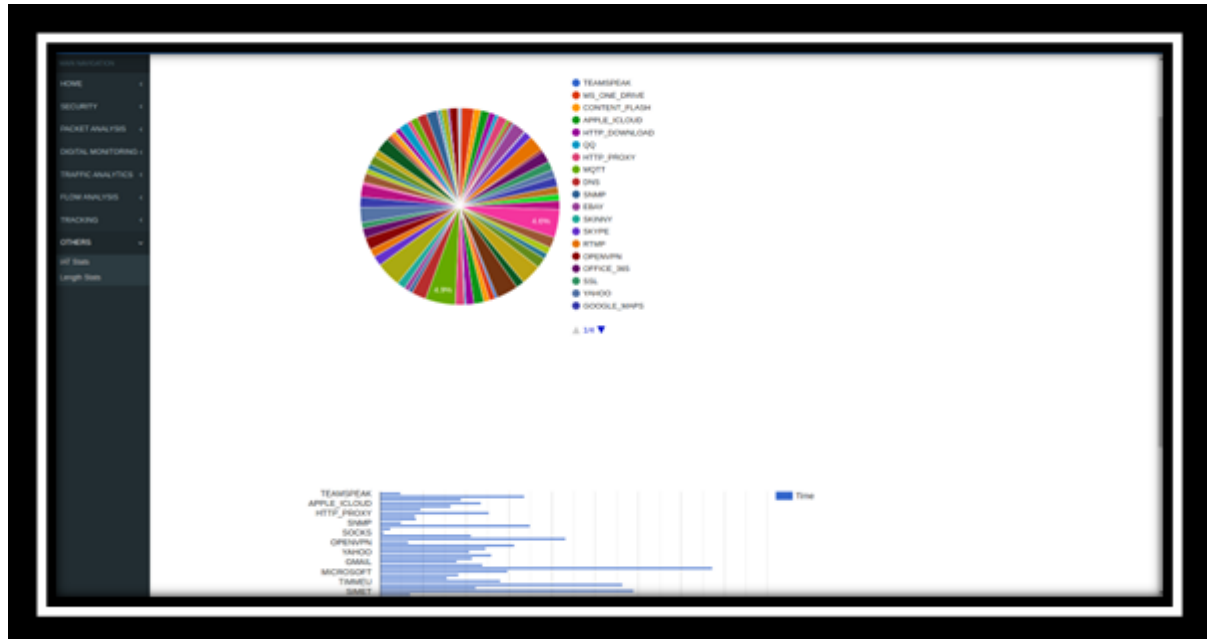
If you click on this it gives the average and standard deviation of the flow inter-arrival time for each protocol



MILESTONE 3

- **Length Stats**

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



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