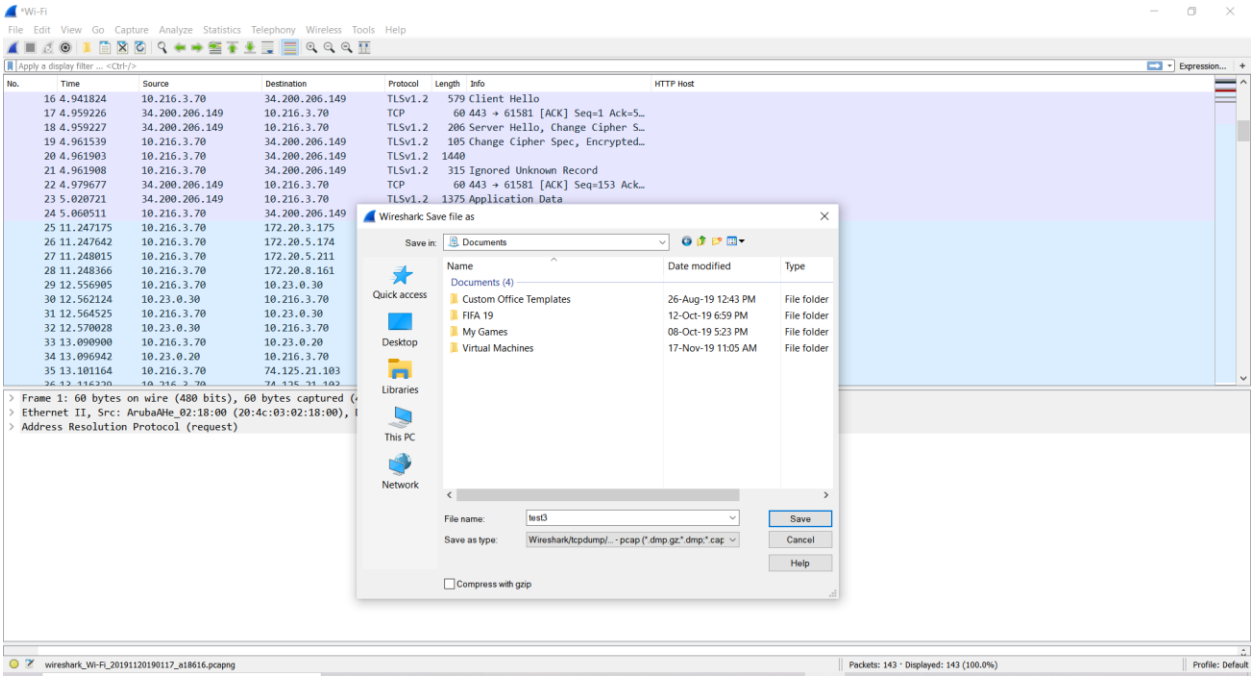
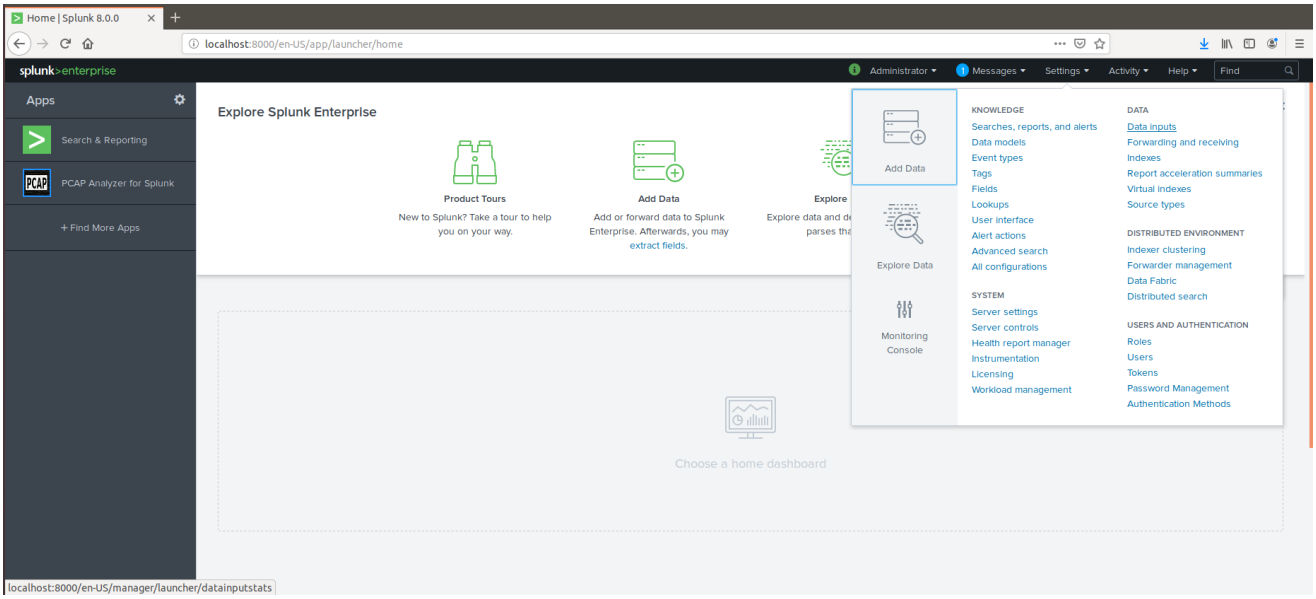
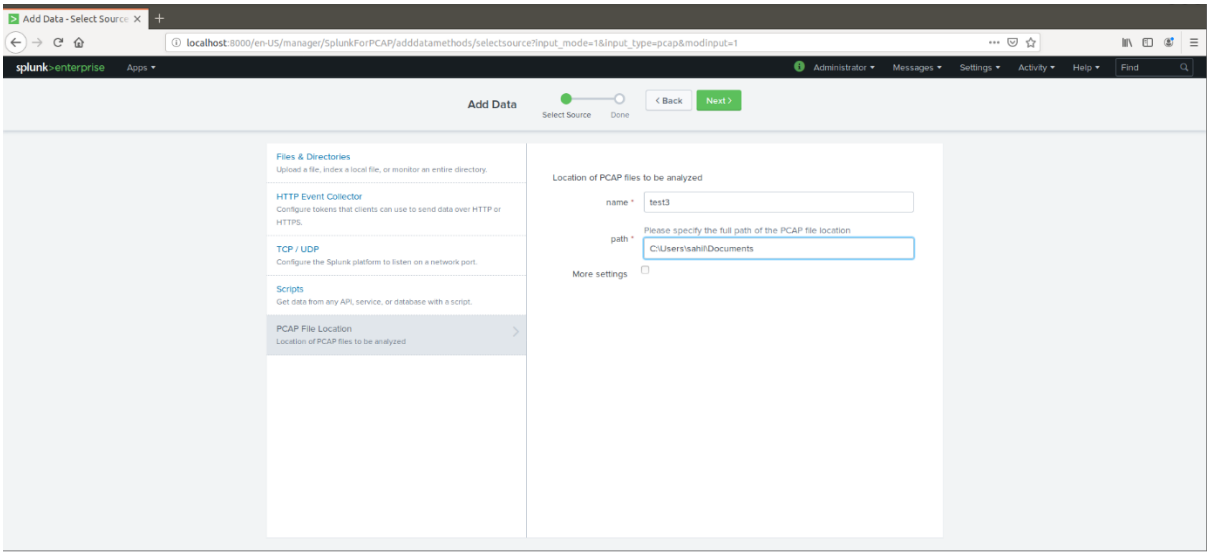
## Bonus Lab: Part 1 Report

1. Creating the pcap file.

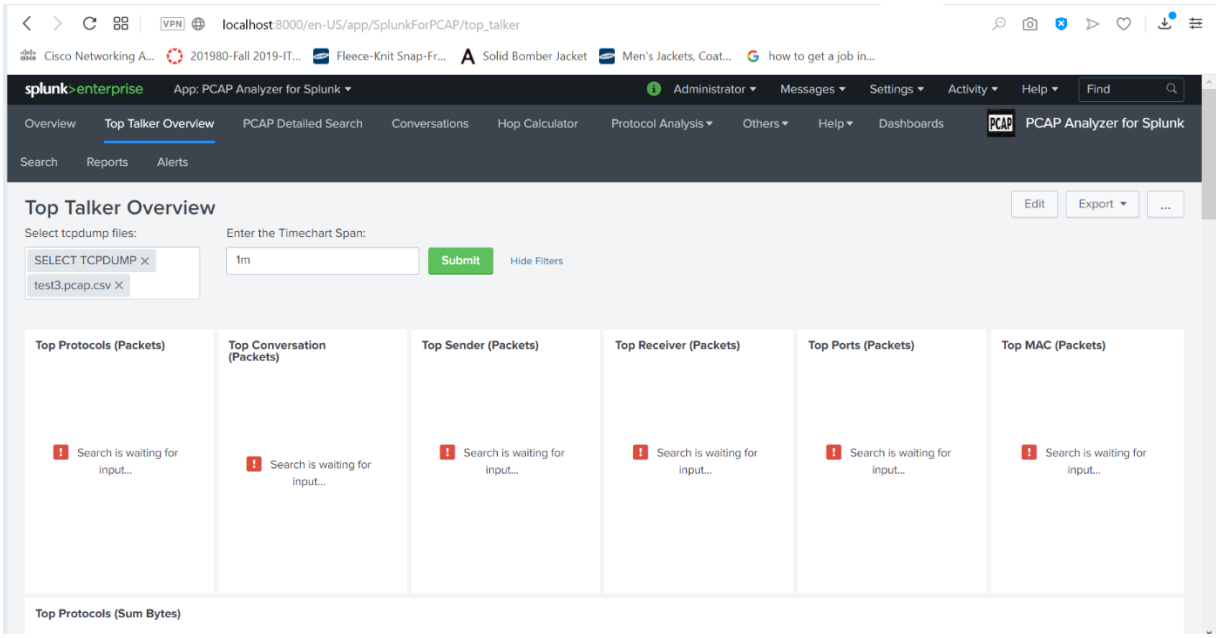


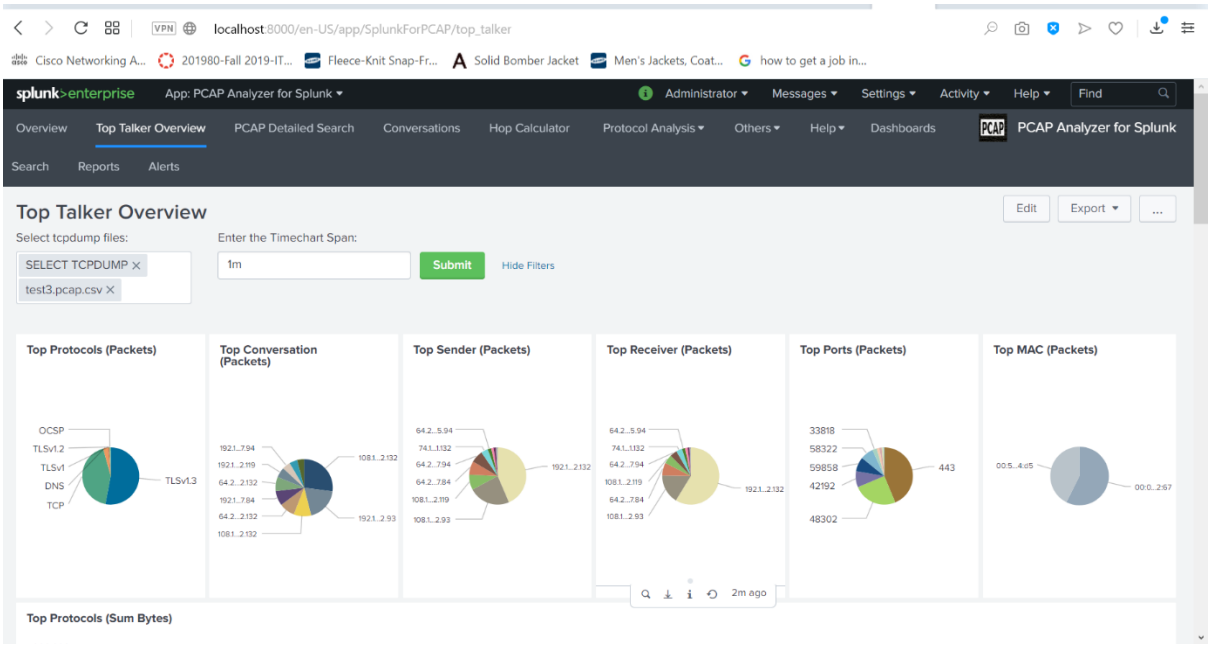

2. Inputing the pcap file which was created as a result of Step 1.

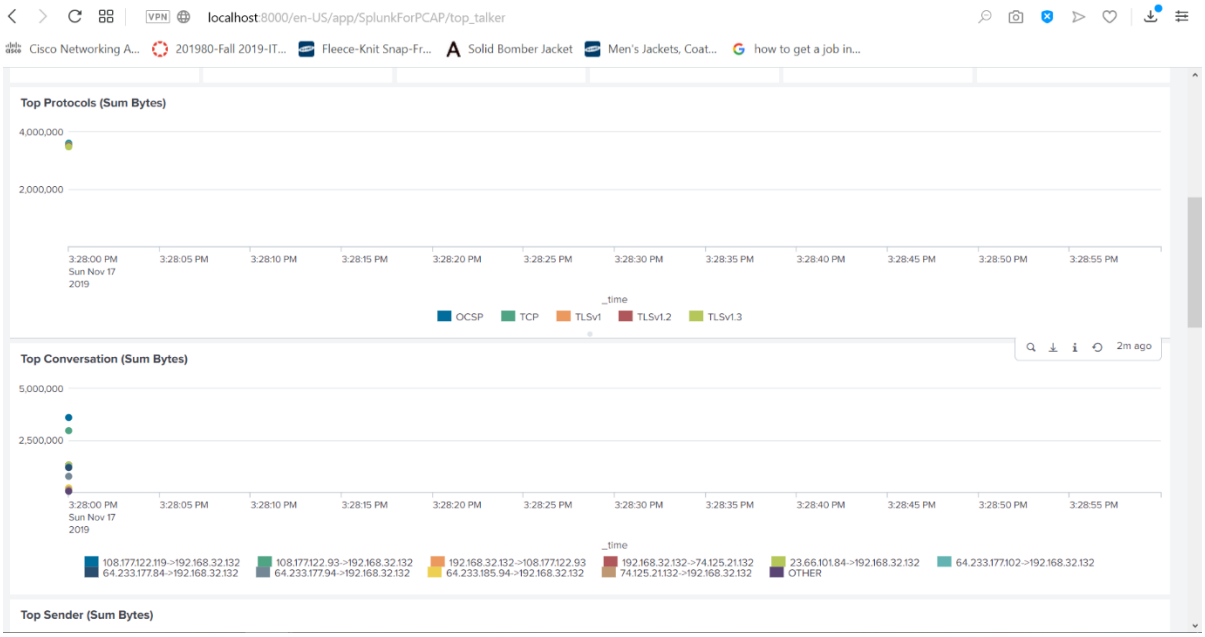


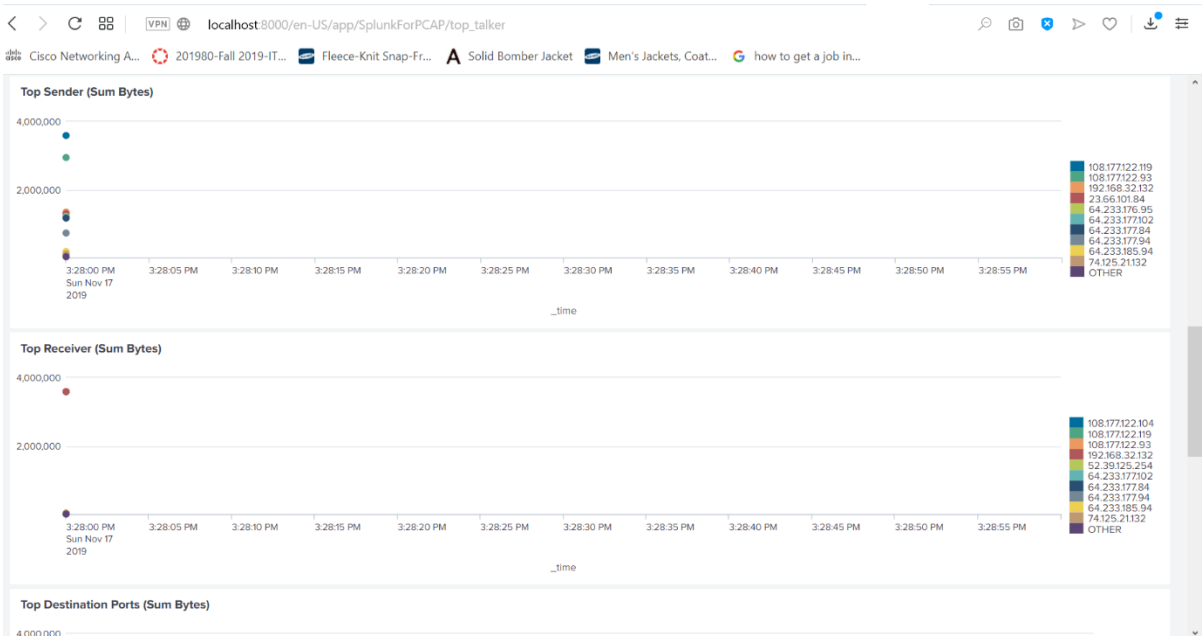


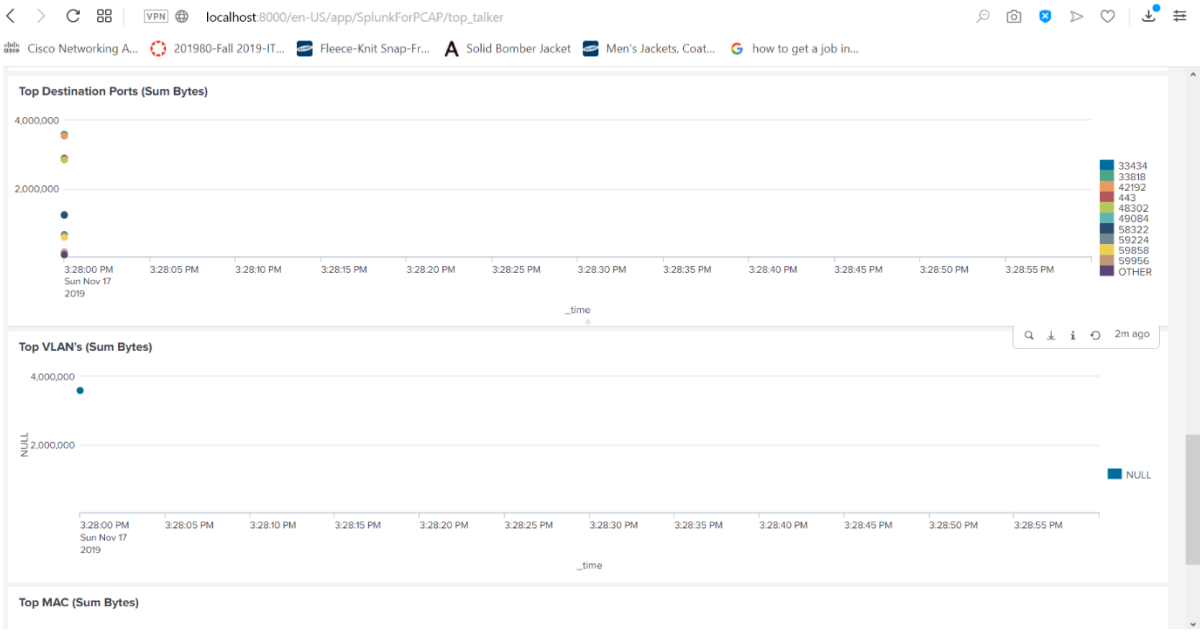

3. Selecting the pcap file for analysis of data. (The pcap file was exported as a csv file from Wireshsark).

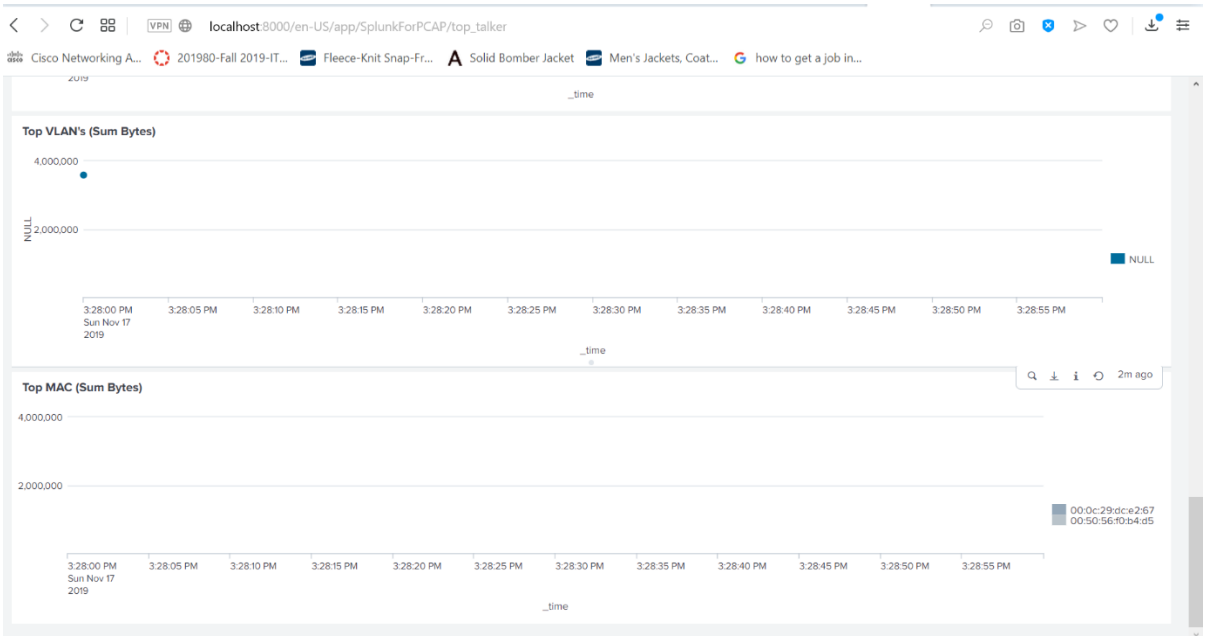



localhost:8000/en-US/app/SplunkForPCAP/top_talker
splunk>enterprise
App: PCAP Analyzer for Splunk
Administrator
Messages
Settings
Activity
Help
Find
Overview
Top Talker Overview
PCAP Detailed Search
Conversations
Hop Calculator
Protocol Analysis
Others
Help
Dashboards
PCAP Analyzer for Splunk
Search
Reports
Alerts
Top Talker Overview
Edit
Export
Select tcpdump files:
SELECT TCPDUMP
test3.pcap.csv
Enter the Timechart Span:
1m
Submit
Hide Filters
Top Protocols (Packets)
OCSP
TLSv1.2
TLSv1
DNS
TCP
TLSv1.3
Top Conversation (Packets)
Top Sender (Packets)
Top Receiver (Packets)
Top Ports (Packets)
33818
58322
59858
42192
48302
443
Top MAC (Packets)
2m ago
Top Protocols (Sum Bytes)


localhost:8000/en-US/app/SplunkForPCAP/top_talker
Top Protocols (Sum Bytes)
4,000,000
2,000,000
3:28:00 PM
Sun Nov 17
2019
3:28:05 PM
3:28:10 PM
3:28:15 PM
3:28:20 PM
3:28:25 PM
3:28:30 PM
3:28:35 PM
3:28:40 PM
3:28:45 PM
3:28:50 PM
3:28:55 PM
_time
OCSP
TCP
TLSv1
TLSv1.2
TLSv1.3
2m ago
Top Conversation (Sum Bytes)
5,000,000
2,500,000
Top Sender (Sum Bytes)


localhost:8000/en-US/app/SplunkForPCAP/top_talker
Cisco Networking A...
201980-Fall 2019-IT...
Fleece-Knit Snap-Fr...
Solid Bomber Jacket
Men's Jackets, Coat...
how to get a job in...
Top Sender (Sum Bytes)
4,000,000
2,000,000
3:28:00 PM Sun Nov 17 2019
3:28:05 PM
3:28:10 PM
3:28:15 PM
3:28:20 PM
3:28:25 PM
3:28:30 PM
3:28:35 PM
3:28:40 PM
3:28:45 PM
3:28:50 PM
3:28:55 PM
_time
108.177.122.119
108.177.122.93
192.168.32.132
23.66.101.84
64.233.176.95
64.233.177.102
64.233.177.84
64.233.177.94
64.233.185.94
74.125.21.132
OTHER
Top Receiver (Sum Bytes)
4,000,000
2,000,000
3:28:00 PM Sun Nov 17 2019
3:28:05 PM
3:28:10 PM
3:28:15 PM
3:28:20 PM
3:28:25 PM
3:28:30 PM
3:28:35 PM
3:28:40 PM
3:28:45 PM
3:28:50 PM
3:28:55 PM
_time
108.177.122.104
108.177.122.119
108.177.122.93
192.168.32.132
52.39.125.254
64.233.177.102
64.233.177.84
64.233.177.94
64.233.185.94
74.125.21.132
OTHER
Top Destination Ports (Sum Bytes)
4,000,000


localhost:8000/en-US/app/SplunkForPCAP/top_talker
Cisco Networking A...
201980-Fall 2019-IT...
Fleece-Knit Snap-Fr...
Solid Bomber Jacket
Men's Jackets, Coat...
how to get a job in...
Top Destination Ports (Sum Bytes)
4,000,000
2,000,000
3:28:00 PM Sun Nov 17 2019
3:28:05 PM
3:28:10 PM
3:28:15 PM
3:28:20 PM
3:28:25 PM
3:28:30 PM
3:28:35 PM
3:28:40 PM
3:28:45 PM
3:28:50 PM
3:28:55 PM
_time
33434
33818
42192
443
48302
49084
58322
59224
59858
59956
OTHER
2m ago
Top VLAN's (Sum Bytes)
4,000,000
2,000,000
NULL
3:28:00 PM Sun Nov 17 2019
3:28:05 PM
3:28:10 PM
3:28:15 PM
3:28:20 PM
3:28:25 PM
3:28:30 PM
3:28:35 PM
3:28:40 PM
3:28:45 PM
3:28:50 PM
3:28:55 PM
_time
NULL
Top MAC (Sum Bytes)


localhost:8000/en-US/app/SplunkForPCAP/top_talker
Cisco Networking A...
201980-Fall 2019-IT...
Fleece-Knit Snap-Fr...
Solid Bomber Jacket
Men's Jackets, Coat...
how to get a job in...
_time
Top VLAN's (Sum Bytes)
4,000,000
2,000,000
NULL
NULL
3:28:00 PM
Sun Nov 17
2019
3:28:05 PM
3:28:10 PM
3:28:15 PM
3:28:20 PM
3:28:25 PM
3:28:30 PM
3:28:35 PM
3:28:40 PM
3:28:45 PM
3:28:50 PM
3:28:55 PM
_time
2m ago
Top MAC (Sum Bytes)
4,000,000
2,000,000
00:0c:29:dc:e2:67
00:50:56:f0:b4:d5
3:28:00 PM
Sun Nov 17
2019
3:28:05 PM
3:28:10 PM
3:28:15 PM
3:28:20 PM
3:28:25 PM
3:28:30 PM
3:28:35 PM
3:28:40 PM
3:28:45 PM
3:28:50 PM
3:28:55 PM
_time