Bonus Lab Part 2

Parag Mhatre

Section II

Q1.

Part 1:

In Part 1, we performed the following tasks:

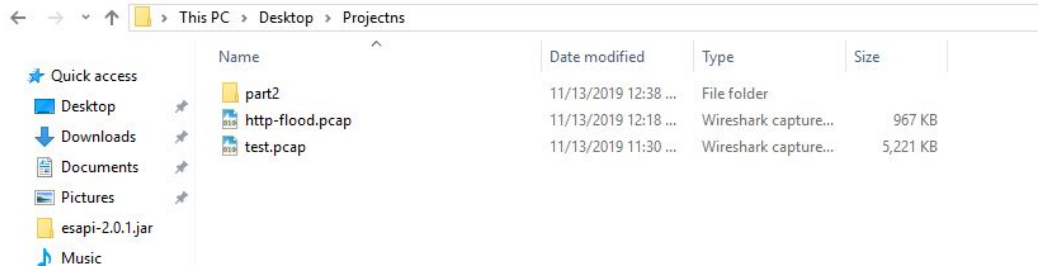
a. Download and setup Splunk.

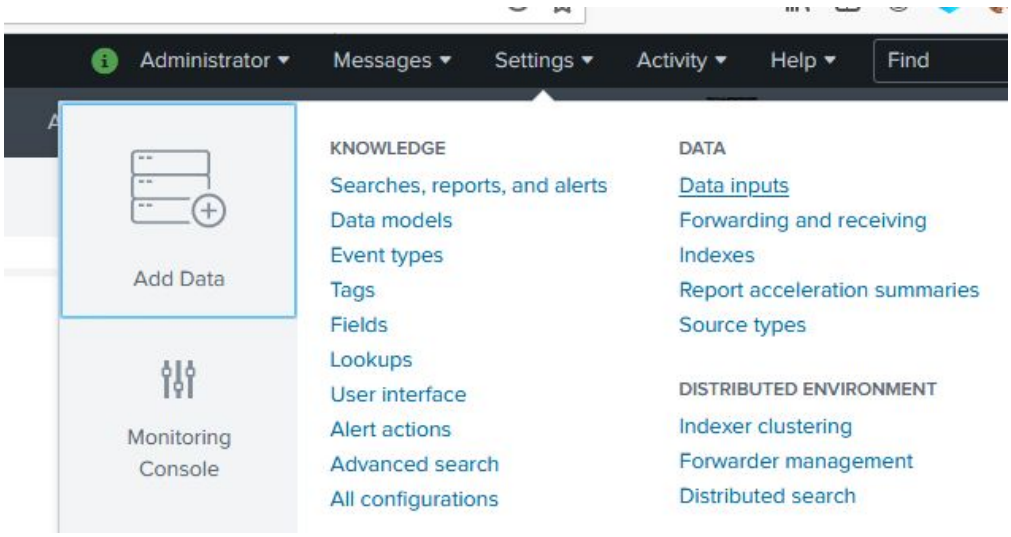
b. Capture test data from Wireshark.

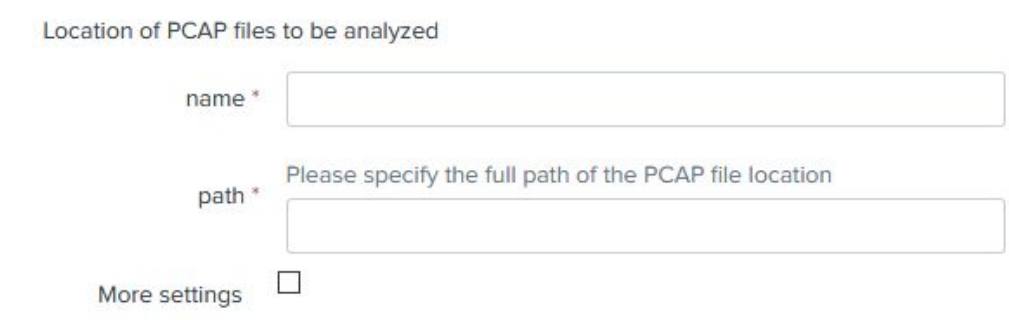
c. Add the data to Splunk in PCAP format for Splunk to convert that to CSV.

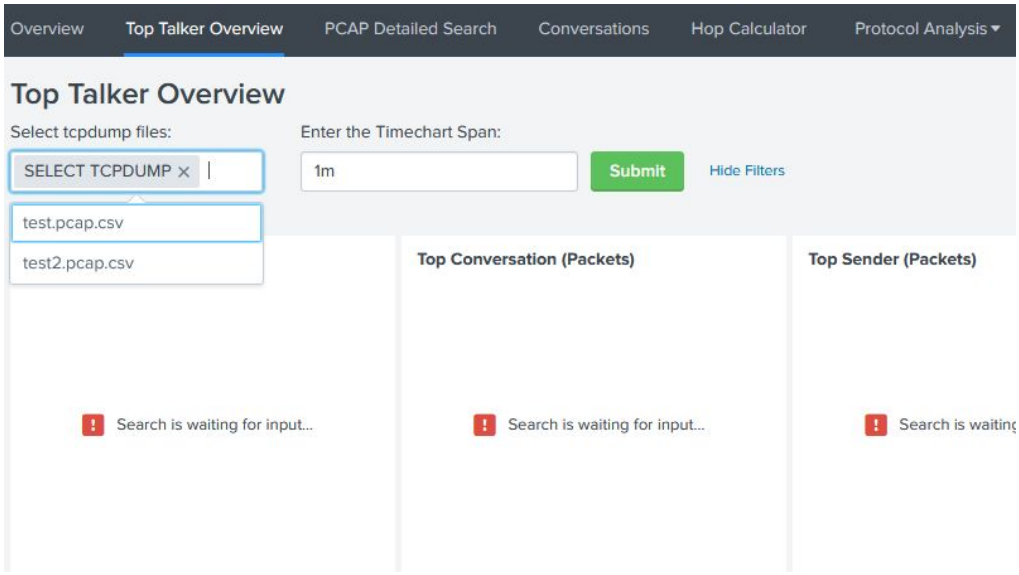
d. Visualize and examine the data in Splunk.

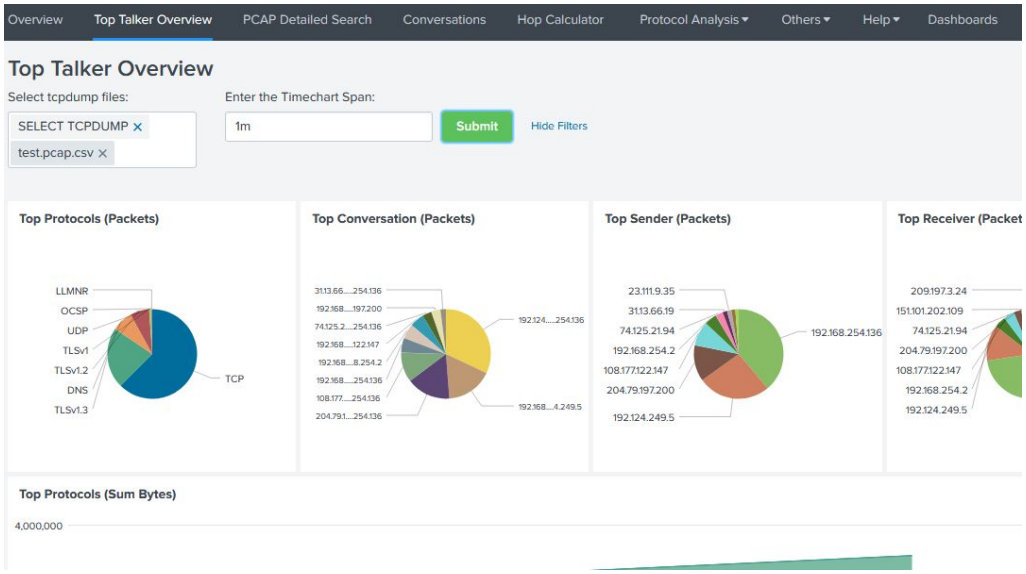
Following are the required Screenshots for Part 1:






Location of PCAP files to be analyzed
name *
path *
Please specify the full path of the PCAP file location
More settings


Overview
Top Talker Overview
PCAP Detailed Search
Conversations
Hop Calculator
Protocol Analysis
Top Talker Overview
Select tcpdump files:
SELECT TCPDUMP ×
test.pcap.csv
test2.pcap.csv
Enter the Timechart Span:
1m
Submit
Hide Filters
Top Conversation (Packets)
Top Sender (Packets)
Search is waiting for input...
Search is waiting for input...
Search is waiting


Overview
Top Talker Overview
PCAP Detailed Search
Conversations
Hop Calculator
Protocol Analysis
Others
Help
Dashboards
Top Talker Overview
Select tcpdump files:
SELECT TCPDUMP ×
test.pcap.csv ×
Enter the Timechart Span:
1m
Submit
Hide Filters
Top Protocols (Packets)
LLMNR
OCSP
UDP
TLSv1
TLSv1.2
DNS
TLSv1.3
TCP
Top Conversation (Packets)
Top Sender (Packets)
23.111.9.35
31.13.66.19
74.125.21.94
192.168.254.2
108.177.122.147
204.79.197.200
192.124.249.5
192.168.254.136
Top Receiver (Packet
209.197.3.24
151.101.202.109
74.125.21.94
204.79.197.200
108.177.122.147
192.168.254.2
192.124.249.5
Top Protocols (Sum Bytes)
4,000,000

Part 2:

In Part 2, we performed the following tasks:

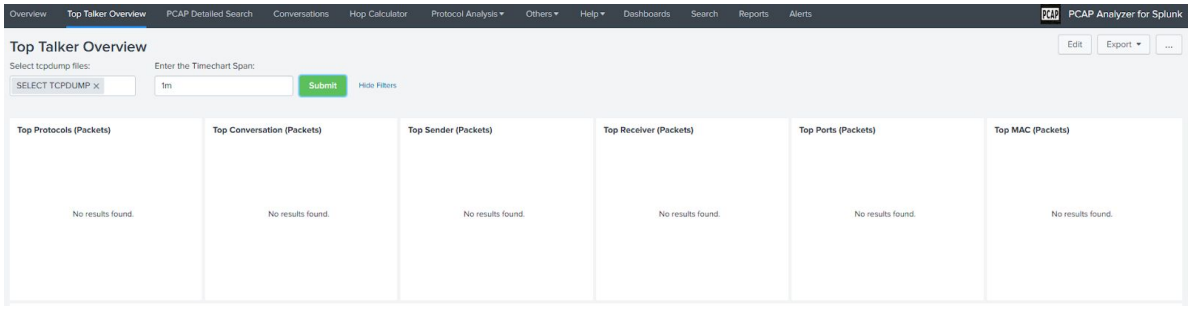
a. Download the data provided.

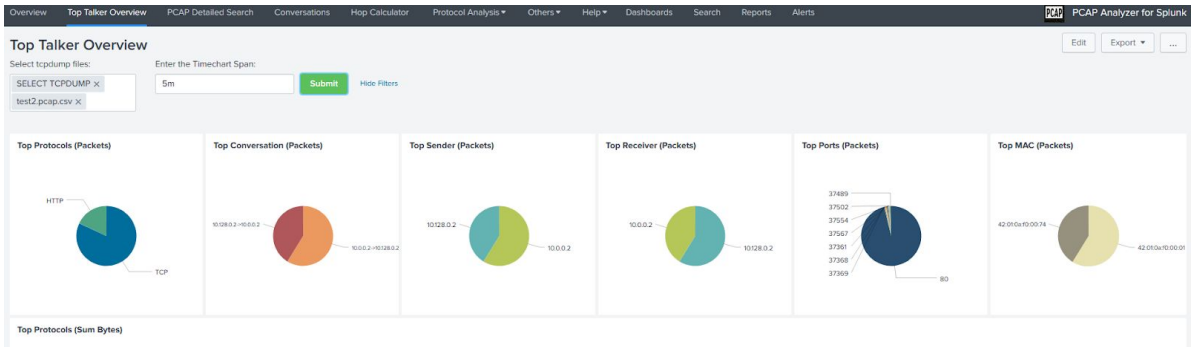
b. Add the data to Splunk.

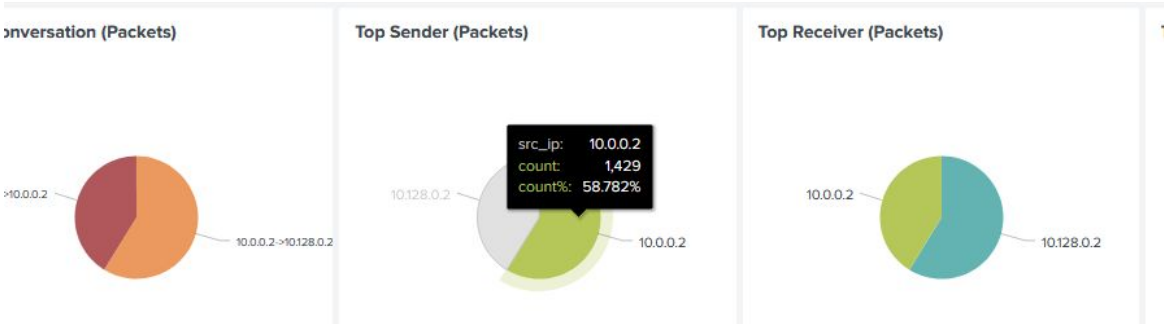
c. Visualize the data.

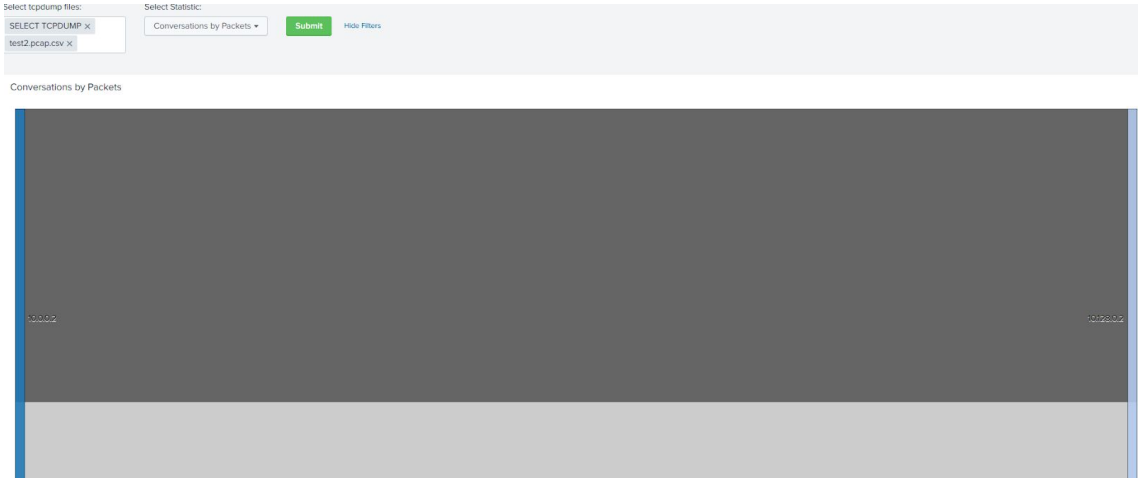
d. Explore various options and try some of them to find relevant information.

Following are the required Screenshots for Part 1:








Select tcpdump files:
SELECT TCPDUMP
test2.pcap.csv
Select Statistic:
Conversations by Packets
Submit
Hide Filters
Conversations by Packets
10.0.0.2
10.23.0.2

Q2.

a. What are the three top differences (in terms of pros and cons) between Wireshark and Splunk? Be as specific as possible.

1. Splunk shows data in Graphical format which makes it easier to analyze.
2. Wireshhark shows data packets as they are. This is highly beneficial when we want to analyze packets in their raw format or in detail.
3. Splunk can use rules to flag data and act on it automatically.

b. What are your three favorite Splunk data analysis and visualization features? Justify your answers.

1. Real-time analysis - Splunk can collect real-time data and process it.
2. Support for various Apps that allow various functionalities.
3. Has a really great and functional dashboard - This is one of the best in the market in its class. It is highly customizable and offers high functionality.

c. What are other SIEM products similar to Splunk? Name at least two. Compare their strengths and weaknesses against Splunk.

1. McAfee ESM -

a. It has a lot of reviews calling for better user interface/experience instead of Splunk which has been called really easy-to-use.
b. Does not capture, store and analyze network flow data directly.

2. Solarwinds:
    a. It offers a well integrated solution that has a simple architecture, easy licensing and robust out of the box features instead of splunk where you have to install apps.
    b. It is difficult to integrate Solarwinds with third-party security solutions due to its closed ecosystem.

d. What Splunk network security applications (other than detecting DDoS attacks) can you think of?

We can configure Splunk to detect and flag whatever criteria of network data that comes under its scan. It can range from detecting unusual dns requests to detecting malware communicating to it's command and control servers.

e. Find at least one pcap file repository on the Internet. What do you think is the purpose of the website?

www.netresec.com

Netresec is an independent and independent software vendor which has it's focus in Security, especially network security. This repository is for the purpose of study, training and research.

Sources:

a. https://wiki.splunk.com/Community:Splunk_for_Network_Security
b. https://www.edureka.co/blog/what-is-splunk/
c. https://mindmajix.com/splunk-interview-questions
d. https://www.itcentralstation.com/products/comparisons/mcafee-enterprise-security-manager-mcafee-esm_vs_splunk
e. https://answers.splunk.com/answers/607442/pros-and-cons-of-splunk-vs-solarwinds.html
f. https://www.splunk.com/pdfs/technical-briefs/advanced-threat-detection-and-response-tech-brief.pdf