UNC CHARLOTTE

College of Computing and Informatics

Department of Software and Information Systems

Network Security
ITIS 6167

BONUS LAB

SAHIL BHIRUD

Table of Contents

1.0 Introduction

1.1 Goal

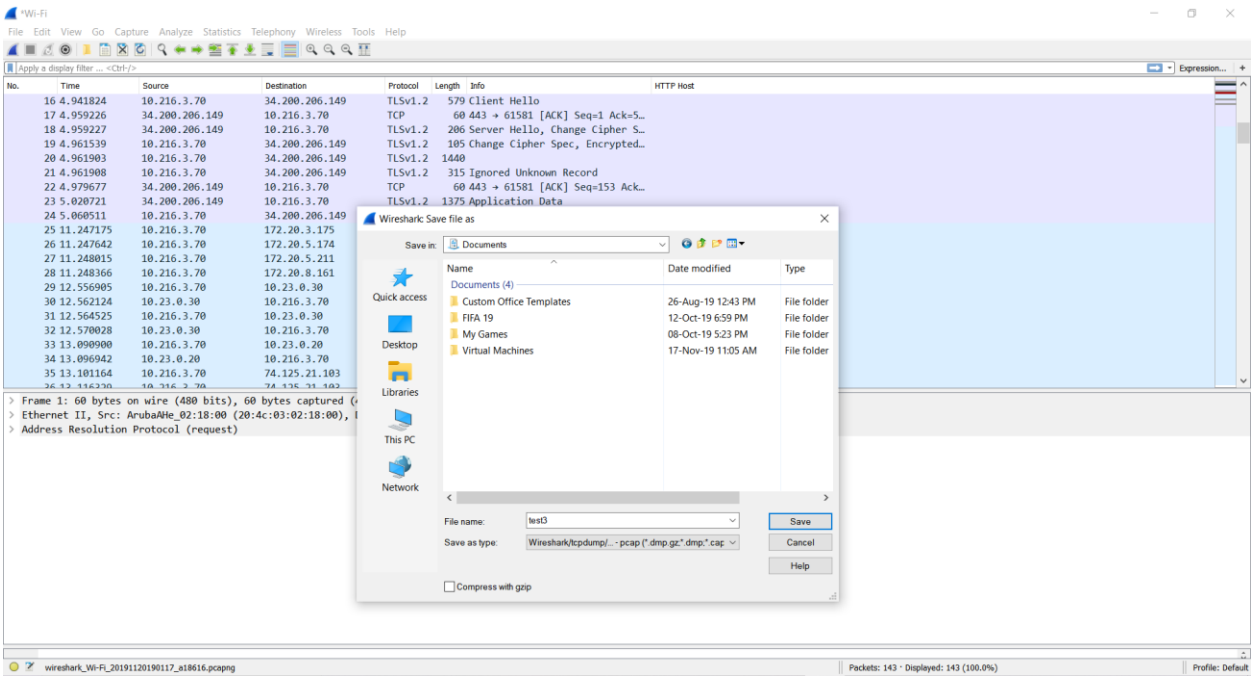
The goal of this lab is to make use of packet analyzing software, Wireshark and a SIEM tool, Splunk to perform network analysis on packets captured using Wireshark.

1.2 Motivation

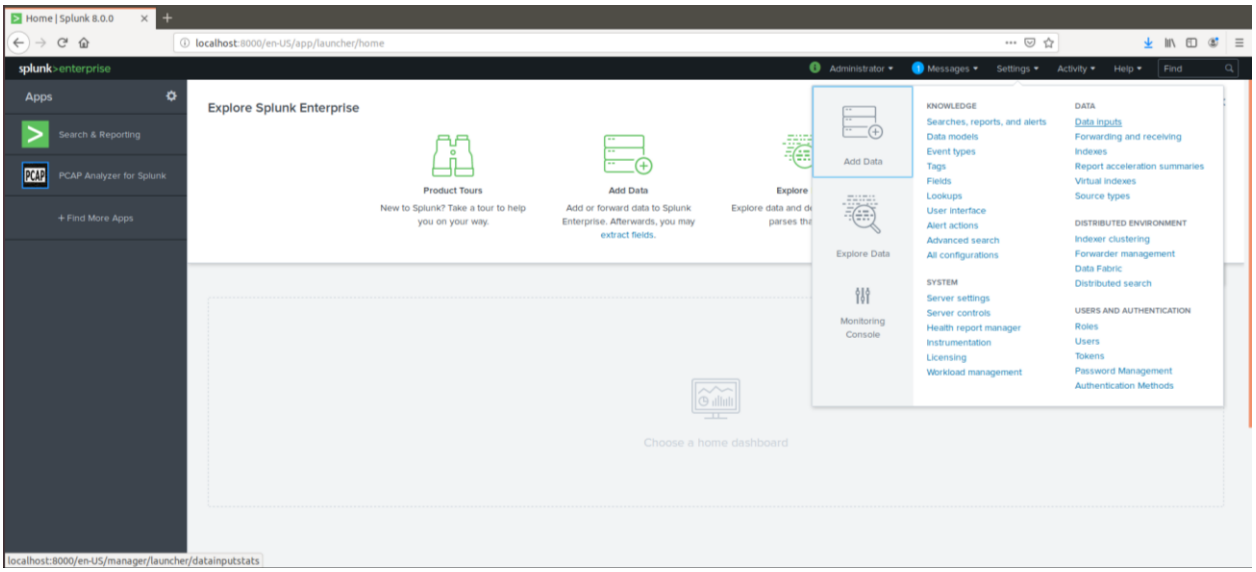
Data packets were successfully captured and analyzed using Wireshark and Splunk respectively.

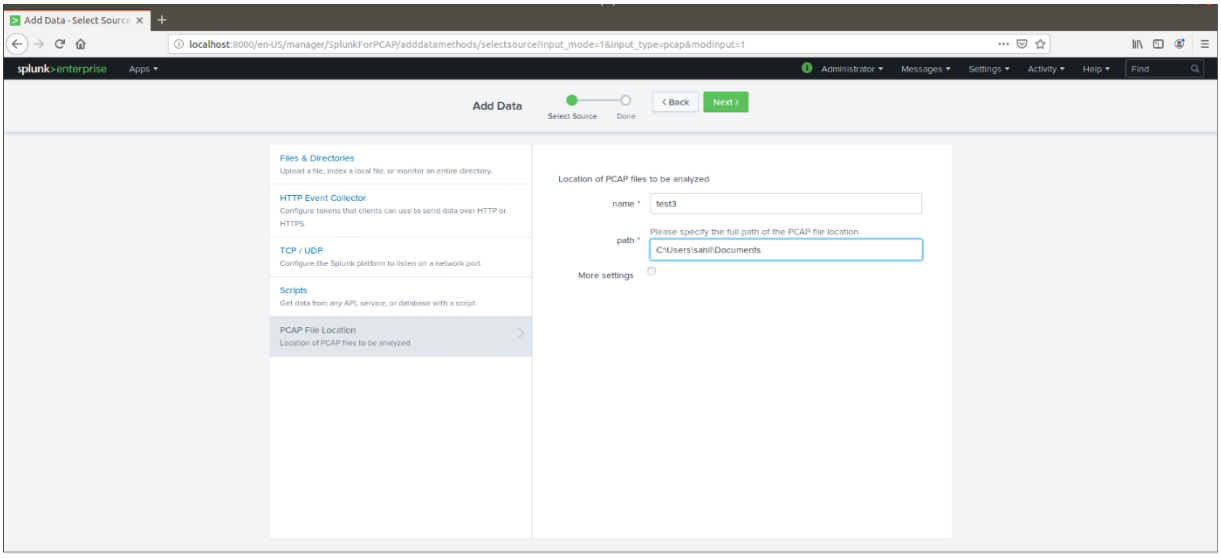
2.0 Part 1 and 2 Tasks

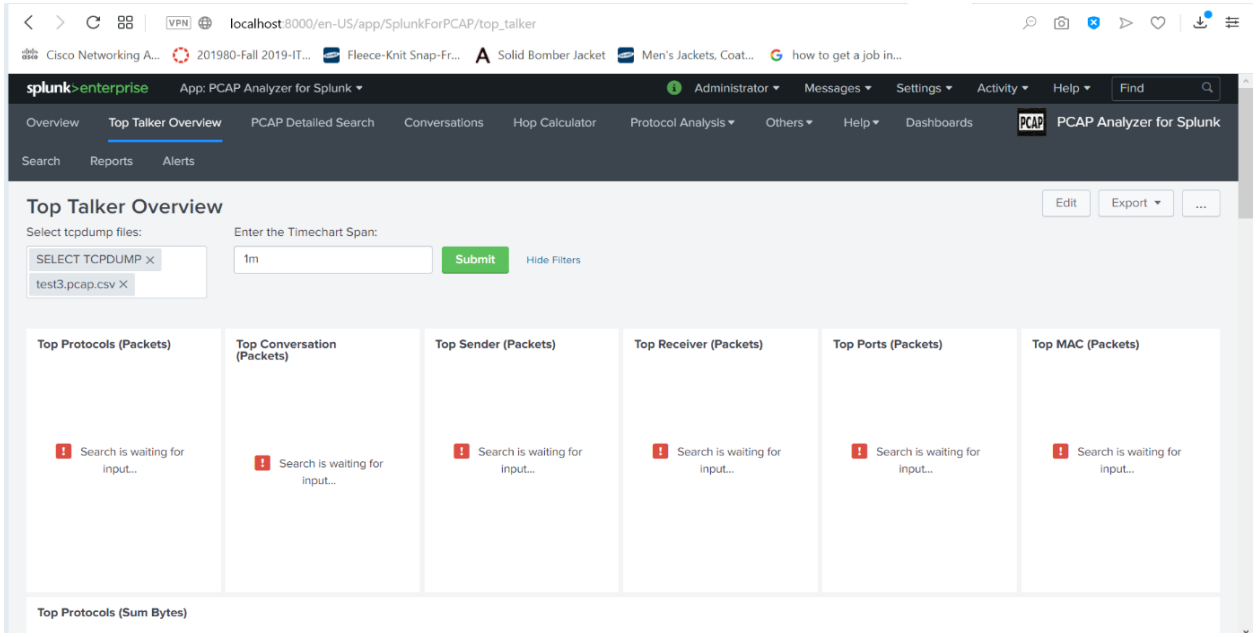
2.1 In Part 1, the following steps were performed:

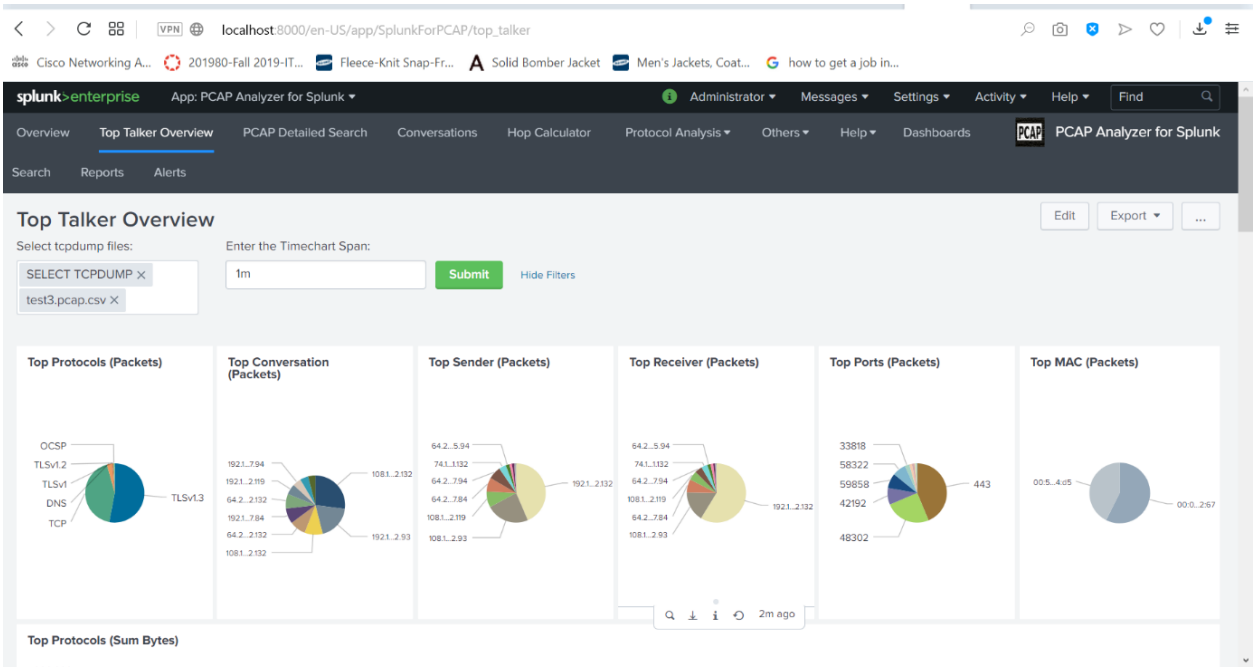


- Opened Wireshark and captured some traffic by opening a browser and visiting a URL.
- Configured PCAP Analyzer and used for importing and viewing the graphs for the saved pcap file.



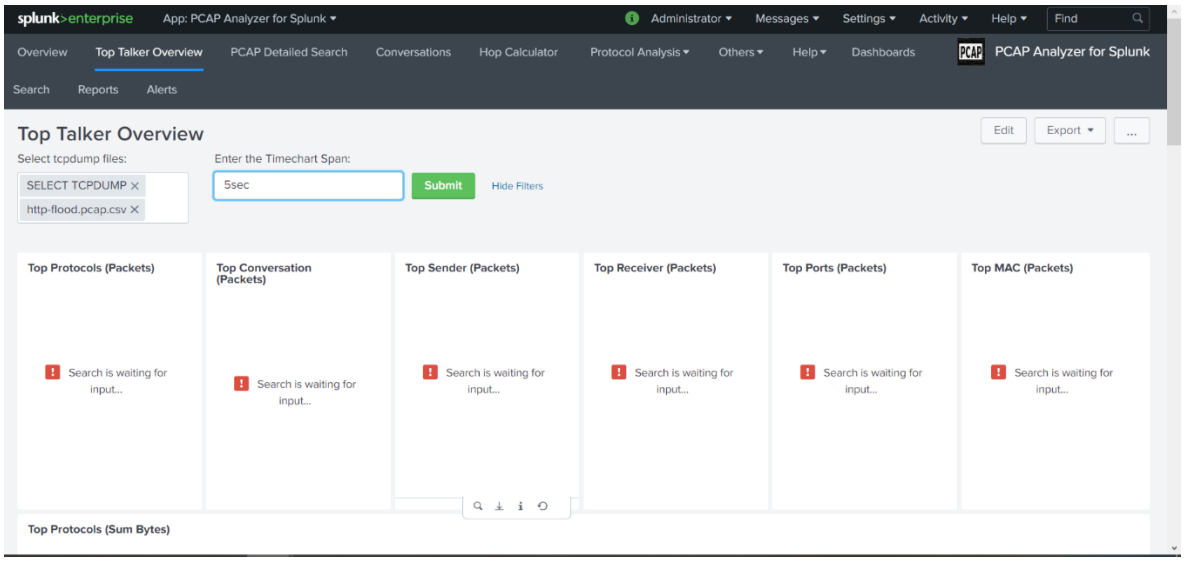


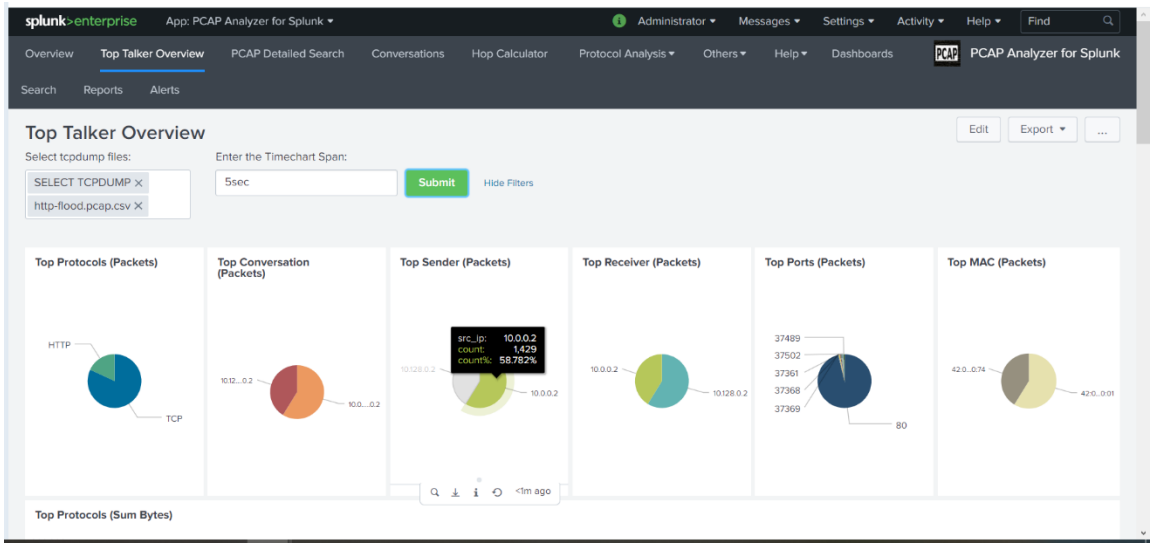

localhost:8000/en-US/app/SplunkForPCAP/top_talker
Cisco Networking A...
201980-Fall 2019-IT...
Fleece-Knit Snap-Fr...
Solid Bomber Jacket
Men's Jackets, Coat...
how to get a job in...
splunk>enterprise
App: PCAP Analyzer for Splunk
Administrator
Messages
Settings
Activity
Help
Find
Overview
Top Talker 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)
Top Conversation (Packets)
Top Sender (Packets)
Top Receiver (Packets)
Top Ports (Packets)
Top MAC (Packets)
Search is waiting for input...
Top Protocols (Sum Bytes)

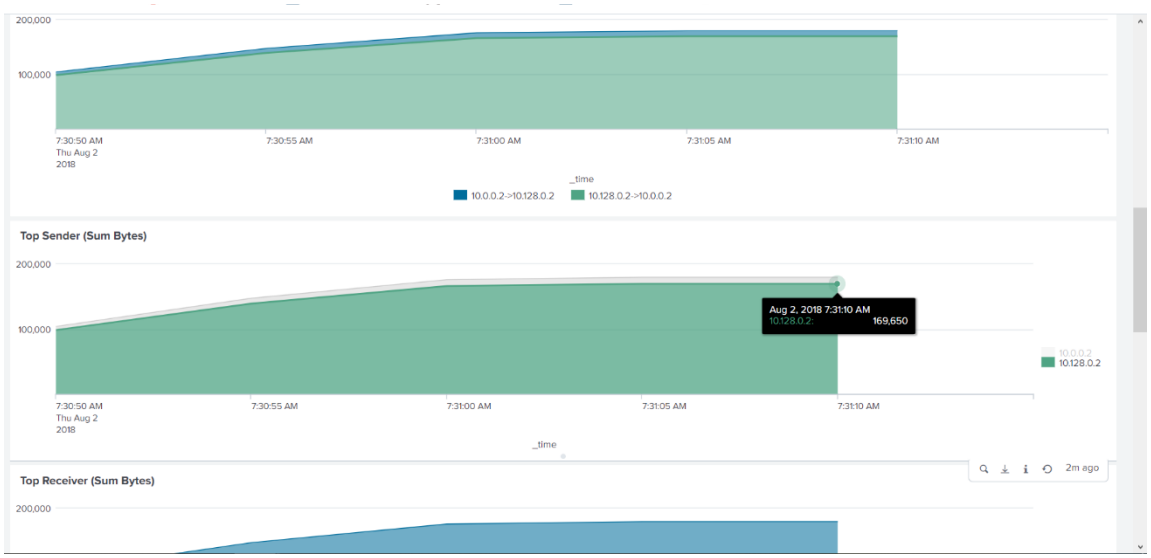

localhost:8000/en-US/app/SplunkForPCAP/top_talker
Cisco Networking A...
201980-Fall 2019-IT...
Fleece-Knit Snap-Fr...
Solid Bomber Jacket
Men's Jackets, Coat...
how to get a job in...
splunk>enterprise
App: PCAP Analyzer for Splunk
Administrator
Messages
Settings
Activity
Help
Find
Overview
Top Talker 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)

2.2 In part 2, the following steps were performed:

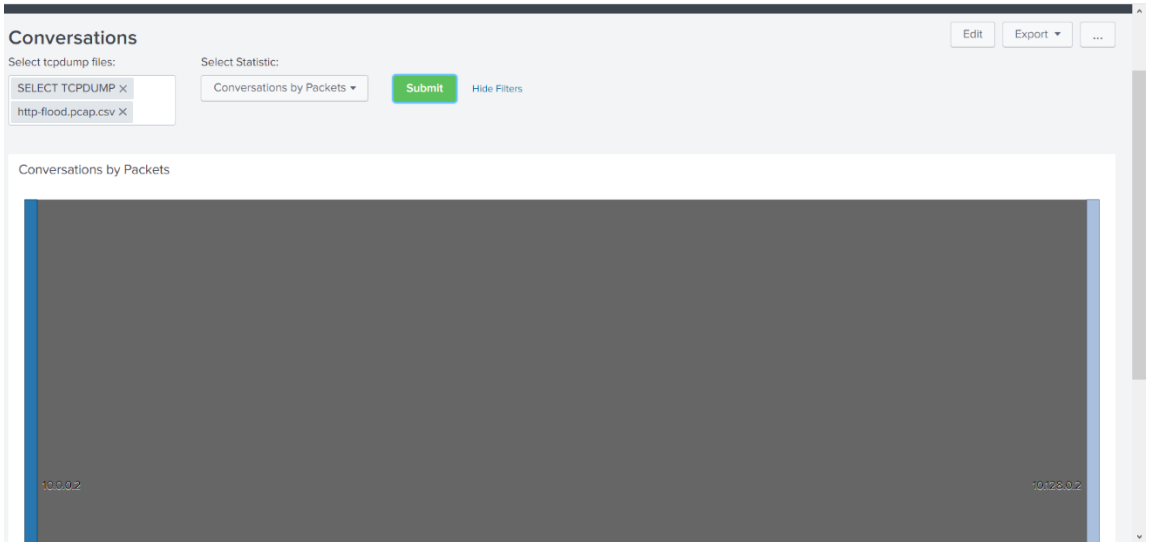
- Loaded a pre-created pcap file in Splunk and analyzed how a DDoS attack was performed.
- Using the Top Senders section in Splunk, we could see the machine which sent a lot of requests to the server and made it ineffective.







- Next, under Conversations tab we could see the sender of the DDoS attack communicating with the network's IP.



2.3 Differences between Wireshark and Splunk

1. Wireshark captures immense amount of data which can be used for tracking the source of the data packets which a user receives whereas Splunk is used to analyze the event logs of a particular session.
2. The amount of data to monitor can be sometimes overwhelming in Wireshark but Splunk provides intuitive and informative search options to analyze the data.
3. Wireshark is well integrated and does not require technical support every now and then. On the other hand, Splunk needs training to work on and also needs a lot of hands on experience to get used to it (trustradius).

2.4 Splunk Data Analysis and Visualization Features

1. **Timeline**

It shows the start, stop and duration of processes on a timeline. Liked it because we can monitor processes which run for a long time and also we will be able to monitor batch processes.

2. **Windows Event Log Analysis**

   It analyzes the entries from a Windows server via Splunk Universal Forwarder or Windows Event Log Forwarding or Remote Windows Event Log collection via WMI as Splunk input. We get a global view of all windows server and come to know which servers are generating a large number of events.

3. **Punchcard**

   It visualizes a metric based on two dimensions: hours of the day and days of the week. It helps us to visualize cyclical trends in the data captured over a network (splunk-1).

2.5 Other SIEM Products

1. **SolarWinds Security Event Manager**

   It offers threat containment and quarantine control functionality which its competitors don't offer. It hosted in a closed ecosystem which makes it challenging to integrate it with third party security solutions whereas Splunk provides multiplatform availability through the applications it provides through Splunkbase.

2. **AlienVault Unified Security Management**

It provides wide range of integrated security functionality at a lower cost than its competitors. Splunk's licensing model is a bit tedious as observed by its clients and it is also expensive as compared to its competitors (comparitech).

2.6 Splunk Network Security Applications

1. Insider Threat Detection – Using baseline and behavior analytics
2. Fraud Detection and Investigation – It gives an enterprise-wide view of the fraud.
3. Log Management – Consolidate, collect, store, search, visualize, analyze and report security relevant data to identify and resolve security issues (Splunk-2).

2.7 pcap File

https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=SkypeIRC.cap

This repository contains Skype, IRC and DNS traffic.

Skype is used for free one-to-one or group video calls or normal phone calls. It also allows its user to send instant messages and share files with other people on Skype (wiki).

REFERENCES:

1. Trustradius - https://www.trustradius.com/reviews/wireshark-2016-11-04-08-52-32
2. Trustradius - https://www.trustradius.com/products/splunk-enterprise/reviews
3. Splunk-1 - https://www.splunk.com/en_us/products/splunk-enterprise/features/visualizations.html
4. Comparitech - https://www.comparitech.com/net-admin/siem-tools/
5. Splunk-2 - https://www.splunk.com/pdfs/solution-guides/splunk-for-security.pdf
6. Wiki - https://wiki.wireshark.org/SampleCaptures#Sample_Captures