|  |
| --- |
|  |
| Network Security ITIS 6167 |
| **BONUS LAB 1 AND 2**  **LAB: ANALYSIS OF PCAP DATA FILES WITH A SIEM TOOL**  **&**  **ANALYZING A DENIAL OF SERVICE (DOS) ATTACK**  **Ruchira Pokhriyal - 801085619** |

Page **1** of **16**

**Table of Contents**

**1.0 Introduction 3-3**

**2.0 Part 2 Tasks 4-16**

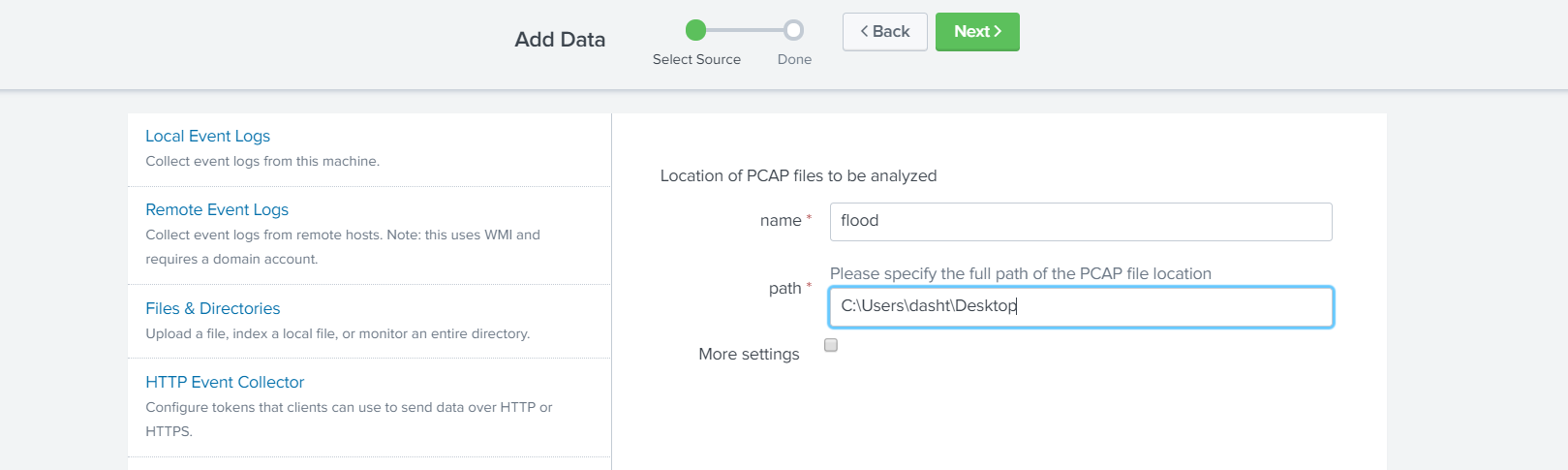
**Introduction**

**Motivation:** The motivation for this lab experiment is primarily to learn more about the functions that network monitoring tools such as Wireshark and Splunk can perform with respect to analyzing network traffic. This lab focuses on familiarizing us with the visualization features of Splunk and how using the PCAP analyzer for Splunk application, one can look into the various details of a captured PCAP file such as top protocols, top conversations, top sender, top receiver, top ports. With this lab I would achieve the necessary hands-on experience in learning how to capture live packets in the network with WireShark and uploading the capture file (PCAP file) to Splunk to visualize the various aspects of the capture file such as detecting a DDoS attack from a network traffic data set.

**Goal:** Introduction to Spunk and using it along with Wireshark to analyze a captured PCAP file is the main goal of this experiment. With the instructions in this experiment, we would achieve practical knowledge of understanding the intricate details of the traffic in a captured PCAP file and we would also perform a deep analysis of a DOS attack which is performed on Splunk using the provided PCAP file.

**2.0** Similar to the steps that we performed in bonus lab part 1, following steps were performed to achieve Part 2 of the lab:

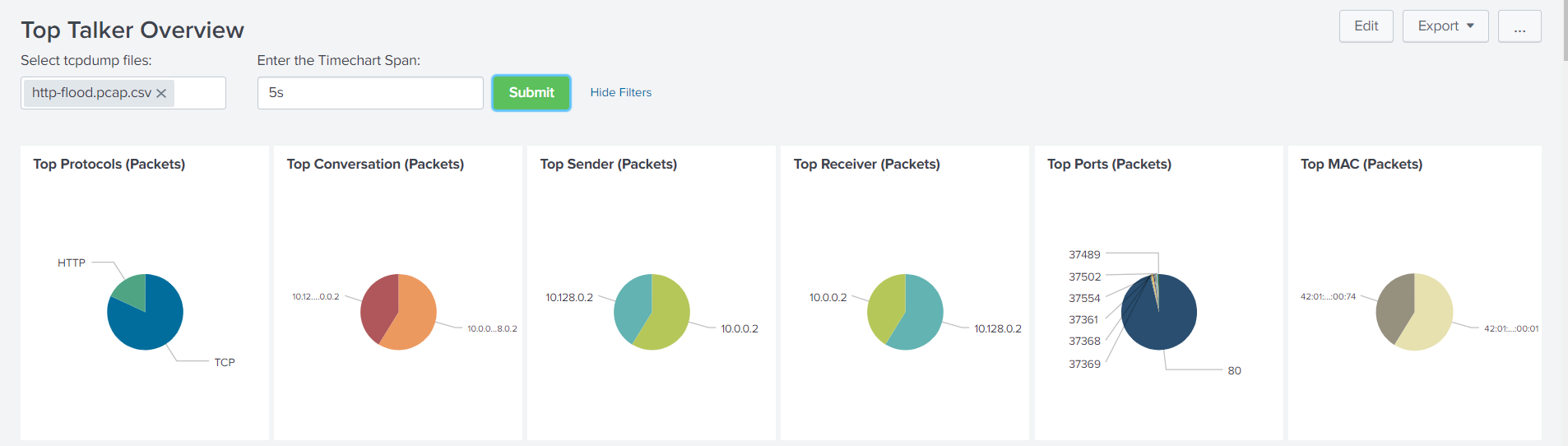
* + - 1. The http-flood.pcap file was downloaded and uploaded on Splunk’s PCAP Analyzer Application’s “Data Input” option using Settings>Data Input>PCAP File Location Tab



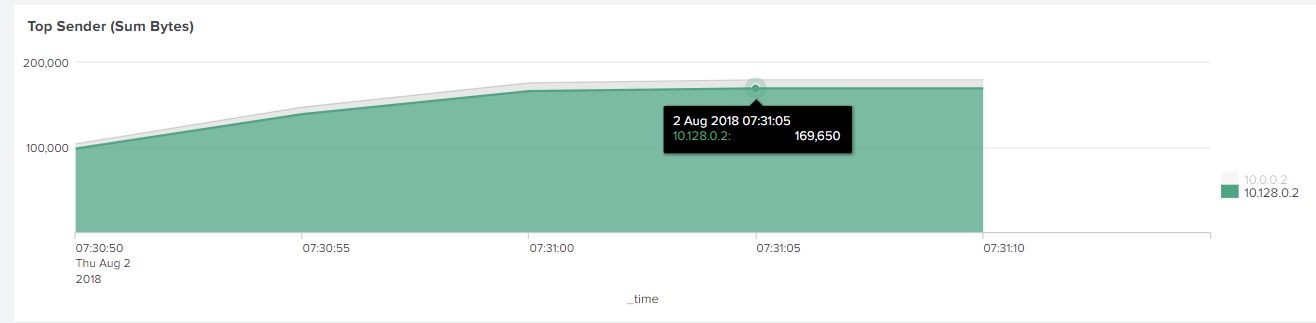
This PCAP File was then provided as an input to Top Talker Overview Dashboard.

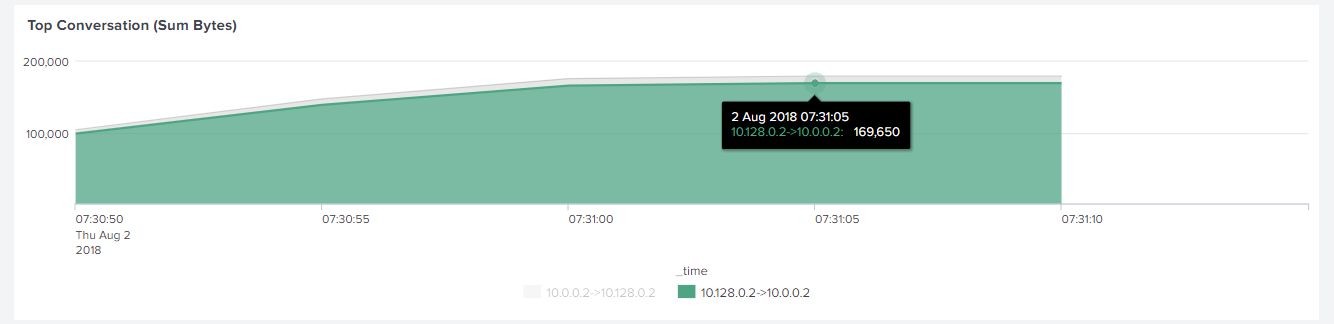
Under “Enter the Time Chart Span” I typed 5s. This number represents the period of time the graph is divided into when visualizing. We use 5 seconds here because the capture was only about 4 minutes long. Next, we Click Submit to start the visualization.

Below is the Analysis on the Top Talker Dashboard:

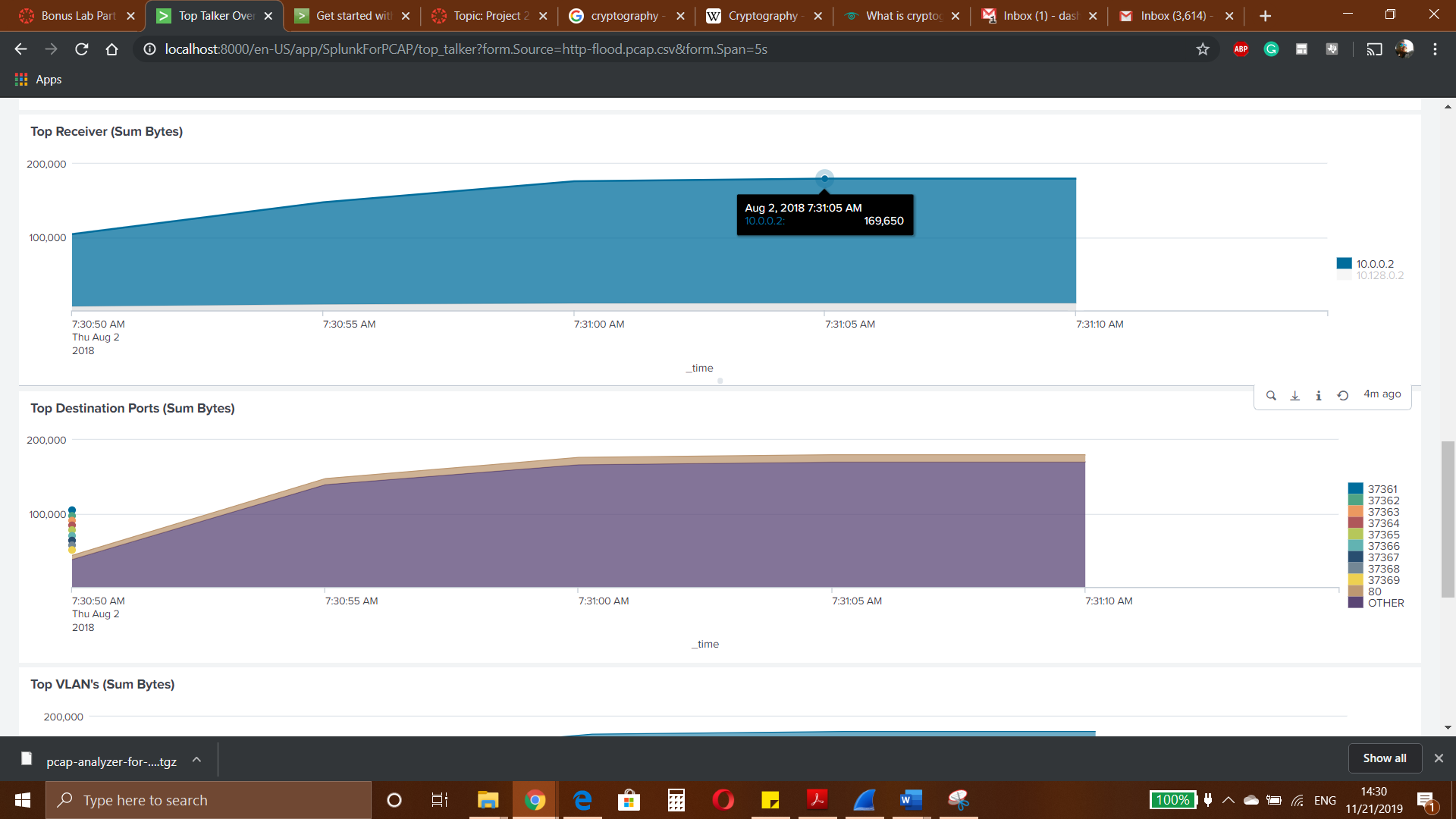


When we scroll down, we get an even detailed analysis of this PCAP file in form of graphs:

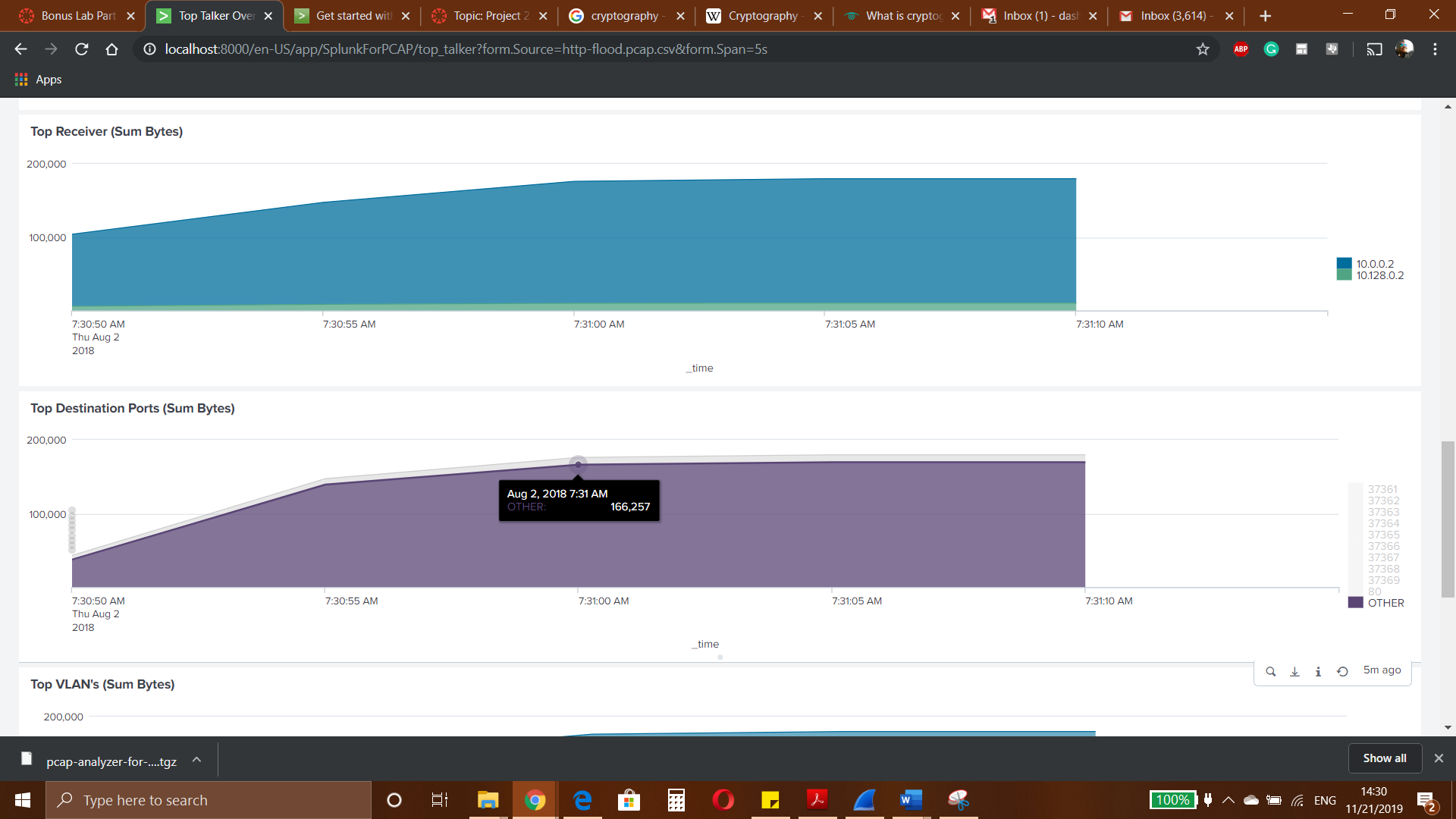
In the Top Sender Graph, following sender packets were visualized in the dashboard and an IP 10.128.0.2 was obtained by hovering the mouse:

Following screenshots displays conversation tab where the attacker is communicating with network IPS:

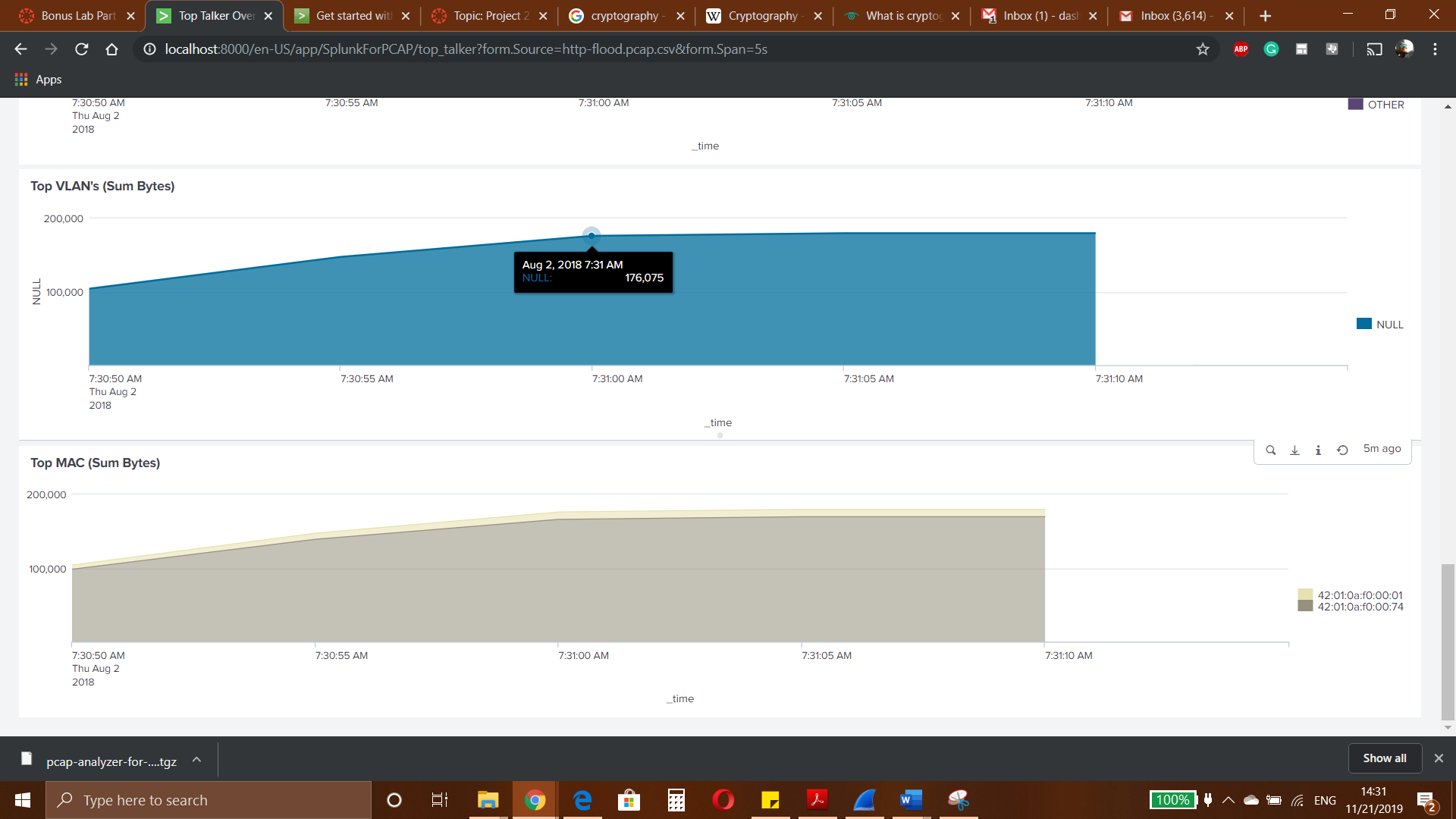
Similarly, below graph represents the Top Receiver with an IP of 10.0.0.2



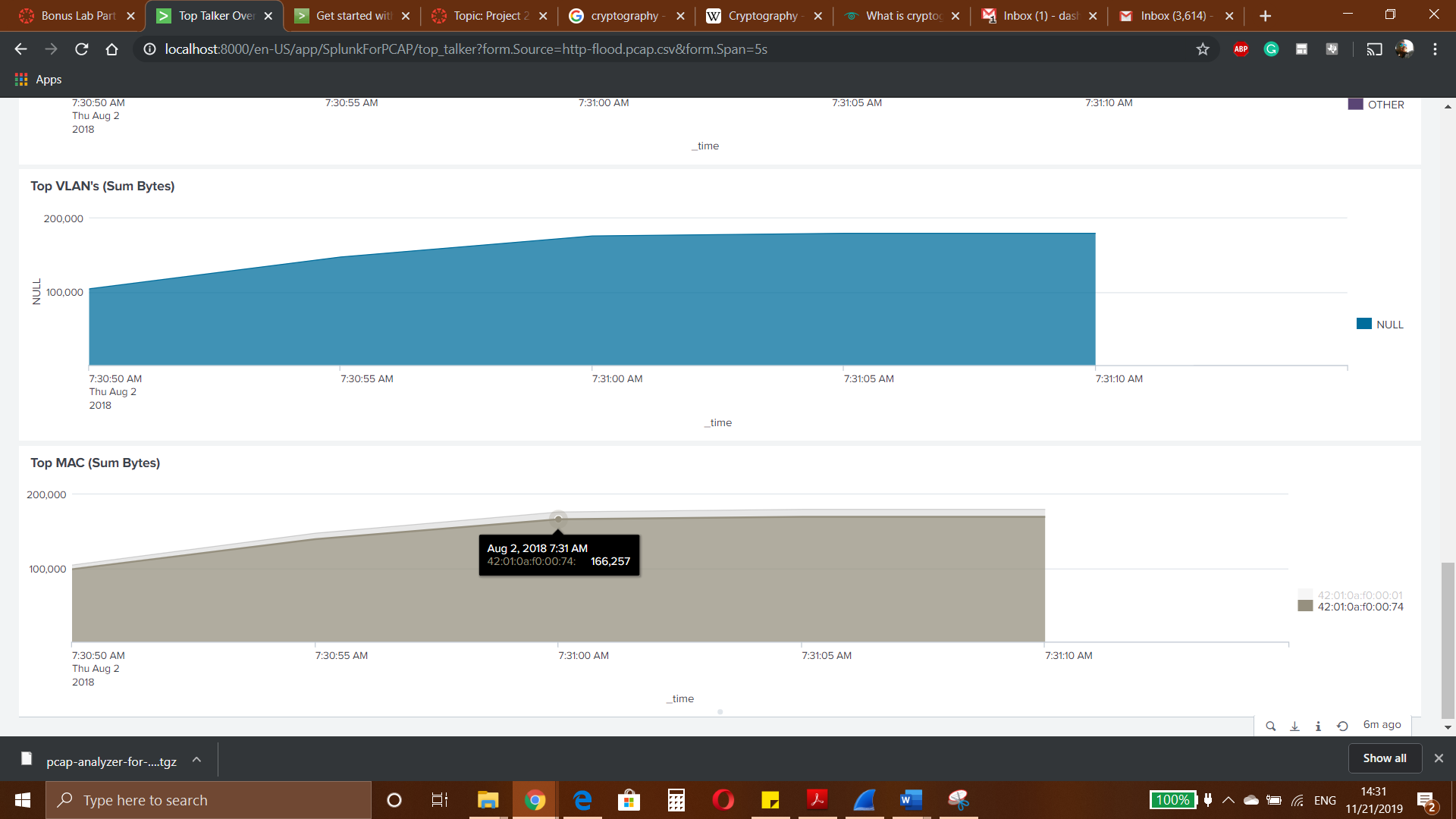
Top Destination Ports are represented by the following graph:



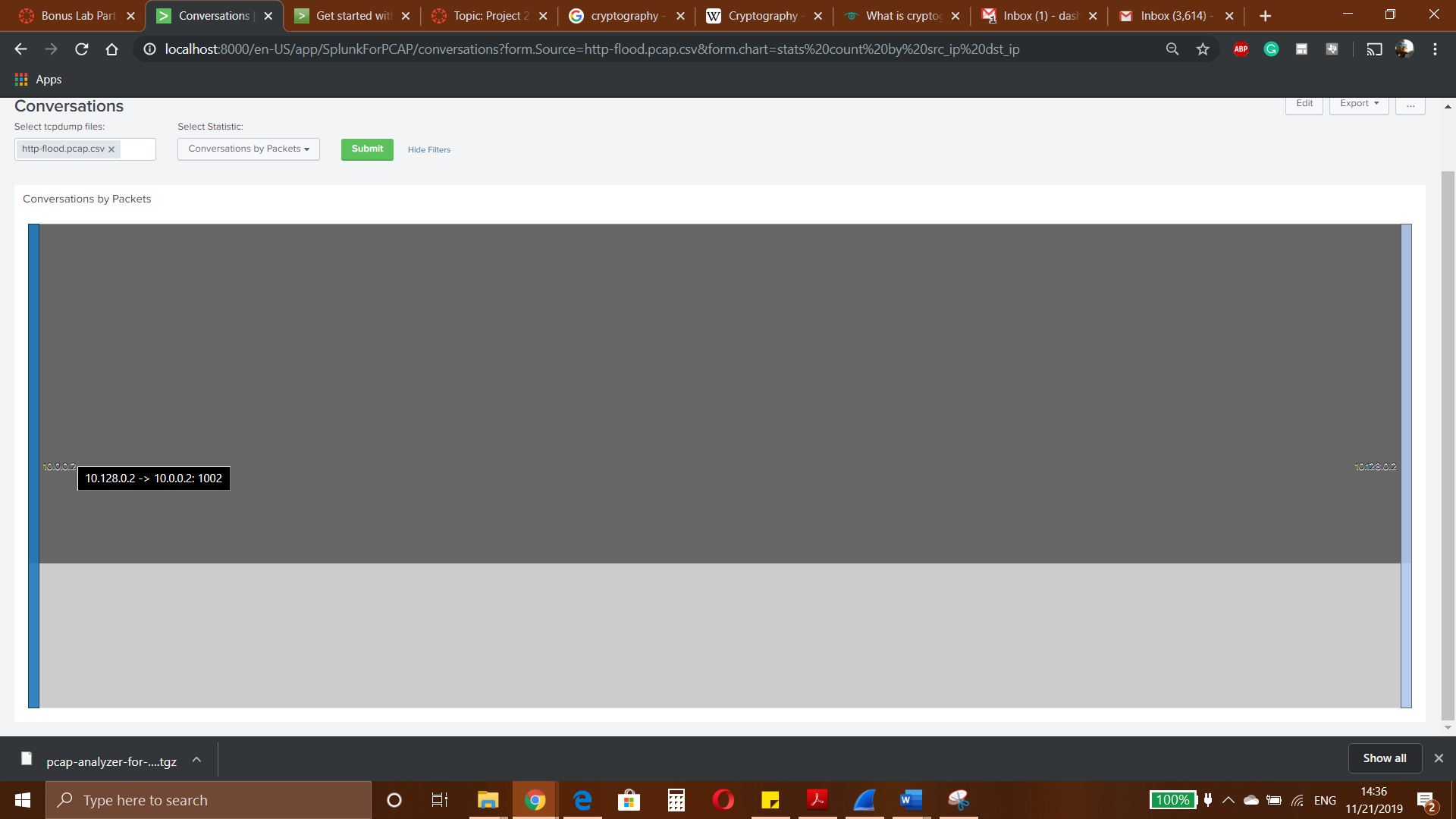
Top VLAN’s is represented by the following graph



Top MAC is represented by the following graph



And finally, when we move to the Conversations tab. In here we’ll be able to see our sender of the DDoS attack communicating with our network’s IP:



* + 1. What are the three top differences (in terms of pros and cons) between Wireshark and Splunk?

Be as specific as possible.

# Solution:

# Splunk Pros:

# 1.very well documented tool, any beginner can troubleshoot easily using the documentations.

# 2.Easy to learn and use.

# 3.very powerful tool which can deal with a large amount of data very fast.

# Splunk Cons:

# setup costs in terms of money and complexity are high

# Cloud platform is not native.

# Wireshark Pros:

# Easy to setup.

# Meets Specific requirements.

# It’s free so cost efficient.

# Wireshark Cons:

1. Not enough quality support
2. Harder to learn and understand

2.What are your three favorite Splunk data analysis and visualization features? Justify your answers.  
1. Splunk provides critical alerts in real time. Splunk's custom alert actions feature makes it simple to automatically kickoff subsequent action when an alert is triggered.

2. Splunk can automatically find useful information enclosed in data, so you don’t have to identify it yourself.

3. Splunk allows for complete utilization of metrics data to boost search performance and save in data storage costs.

**4.** Splunk creates analytical reports with interactive charts, graphs, and tables, and shares them with others which is productive for users.

1. What are other SIEM products similar to Splunk? Name at least two. Compare their strengths and weaknesses against Splunk.
2. **Loggly:** Comes with proactive monitoring of key metrics and resources to eliminate problems before it affects end-users. Helps to trace the root cause of issues with an in-depth analysis of existing logs.
3. [**LogDNA**](https://logdna.com): This was created to solve many problems existing in current log management solutions. This tool offers a high degree of flexibility to organizations when it comes to powerful powerful logging and deployment models available for cloud-based, on-premise, private cloud, and hybrid/multi-cloud,
4. **Fluentd: This is a** tool which ingests structured, unstructured, and semi-structured data sets. It acts as an intermediary between data sources and outputs, allowing it to convert and route data for a number of different platforms, services, applications, and programming languages.

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

Monitoring, breach analysis and response, alert and incident handling, Posture assessment, CSIRT, and event correlation.

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

Website: [www.netresec.com](http://www.netresec.com/)

NETRESEC AB is an independent software vendor (ISV) with focus on network security monitoring and network forensics. We develop and sell software products specially designed to capture and analyze network traffic on the wire as well as in pcap files.

References:

<https://www.quora.com/Whats-good-and-bad-about-Splunk>

<https://www.splunk.com/en_us/software/splunk-enterprise/features.html>

<https://answers.splunk.com/answers/607442/pros-and-cons-of-splunk-vs-solarwinds.html>

<https://techtalk.gfi.com/the-top-20-free-network-monitoring-and-analysis-tools-for-sys-admins/comment-page-1/>