Digital forensic: How to use DFIR (Digital Forensic Incident Respond) tools for quick analysis during an incident.

Introduction

Digital forensics is the collection and examination of digital evidence residing on electronic devices. In the rise of cyber-attacks and data breaches digital forensic plays a major role for companies and law enforcement. Digital forensics helps gather evidence and indication of compromise to help understand what happened? How did that happen? It also helps collect and preserve evidence for courts of law.

In this lab, I am going to use Splunk and PCAP Analyzer to analyze network packets and try to figure out what happened

Requirements

- PCAP Analysis for Splunk
- Data provided by Western Regional Collegiate Cyber Defense Competition in February of 2019. https://archive.wrccdc.org/pcaps/2019/qualifiers/team10/

Execution

1-boot up Splunk and login

2-First thing is to check your splunk home setting and make sure you have the right setup.

```
  GNU nano 4.8                                    /etc/environment
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin"
SPLUNK_HOME="/opt/splunk"
```

If not, you can use Nano and access the splunk environment and change it

Run this command: **sudo nano /etc/environment**

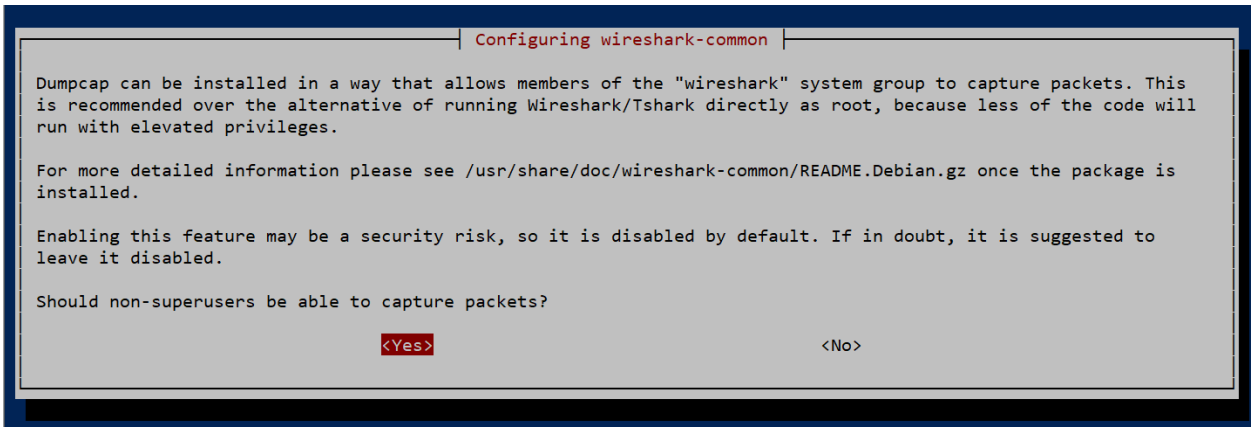
Make sure the second line of the file is **SPLUNK_HOME="/opt/splunk"**

3-Make sure your splunk appliance is update and install Tshark. Tshark is Wireshark without a graphical interface.

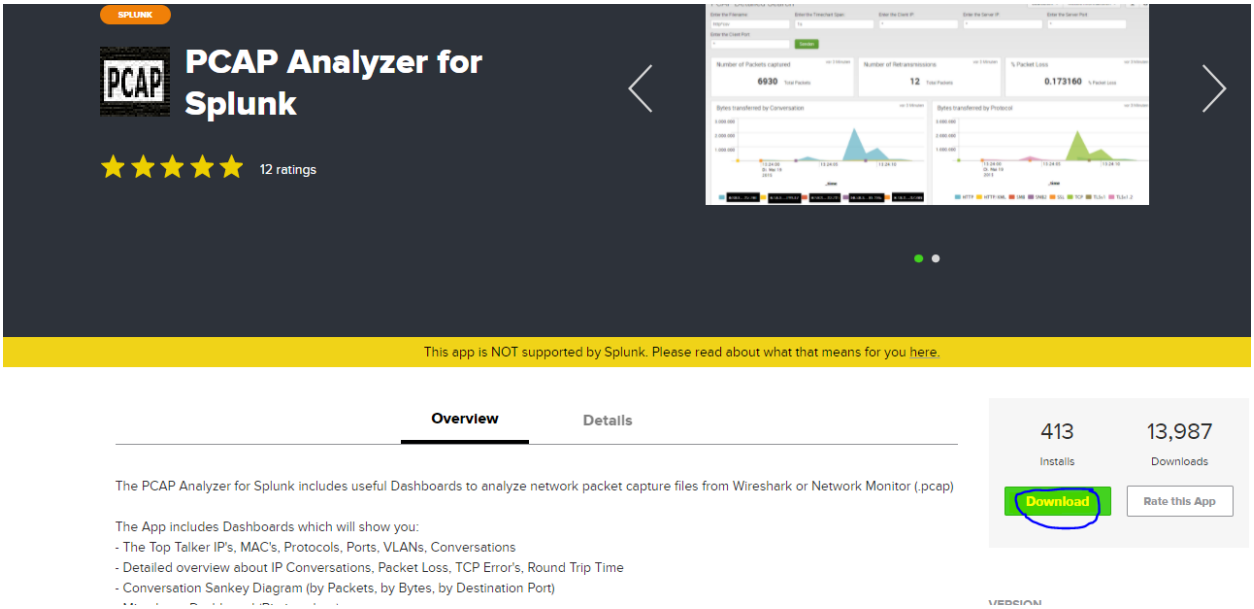
- **sudo apt-get update | sudo apt-get upgrade –y**

- **sudo apt install tshark –y**

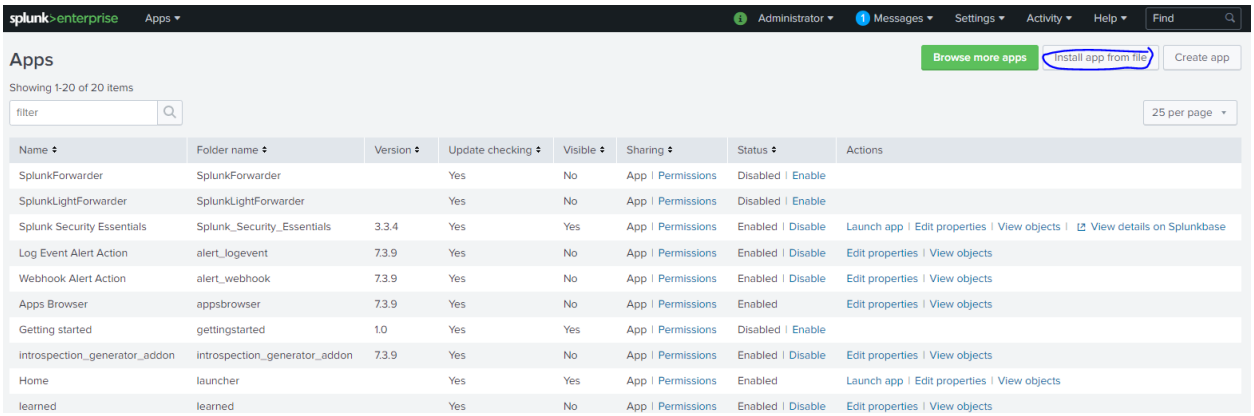
Select yes at the screen below to allow non-superusers to capture packets



4-Download PCAP Analyzer from Splunk base. You will need a Splunk account for that



5- Login in Splunk and install the PCAP Analyzer.



Click install app from file, go to the folder and select the file you just downloaded.

After clicking install you need to restart Splunk. Just click on restart now.

6- Next input this command into your terminal to set executable permission for the PCAP file.

sudo chmod -R 777 /opt/splunk/etc/apps/SplunkForPCAP/

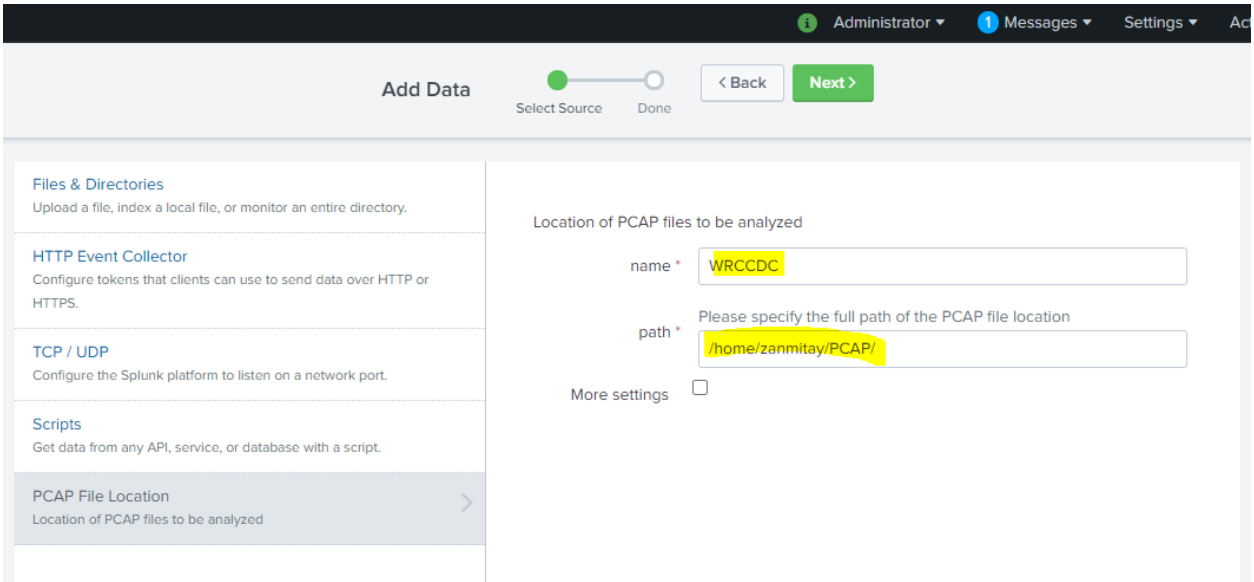
7- Now let download the example PCAP file that we are to investigate from GitHub. Save the file in your home directory.

git clone https://github.com/pat-oconnor/PCAP/

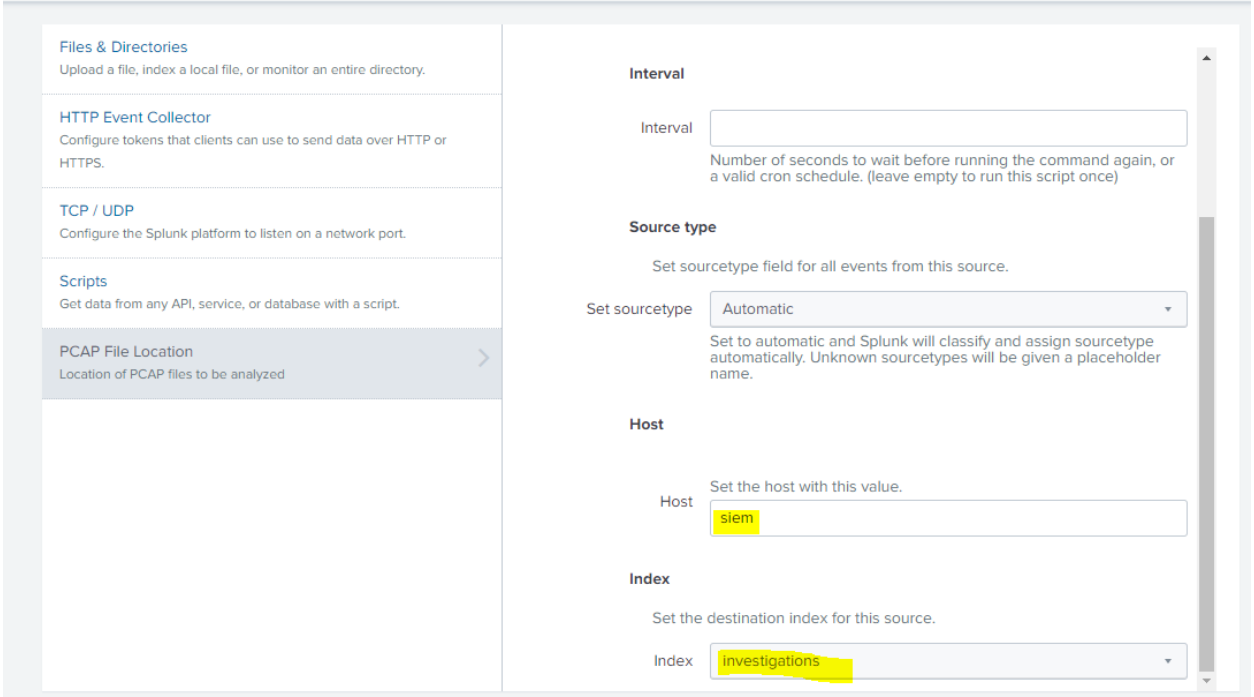
8- Create a new index in Splunk called “Investigations “. Leave the other fields set to default and click save.

9- Next go to setting – Data Input-- Monitor – PCAP file Location

- Name: WRCCDC
- Path: the directory of PCAP file downloaded from GitHub. My is **/home/zanmitay/PCAP/**

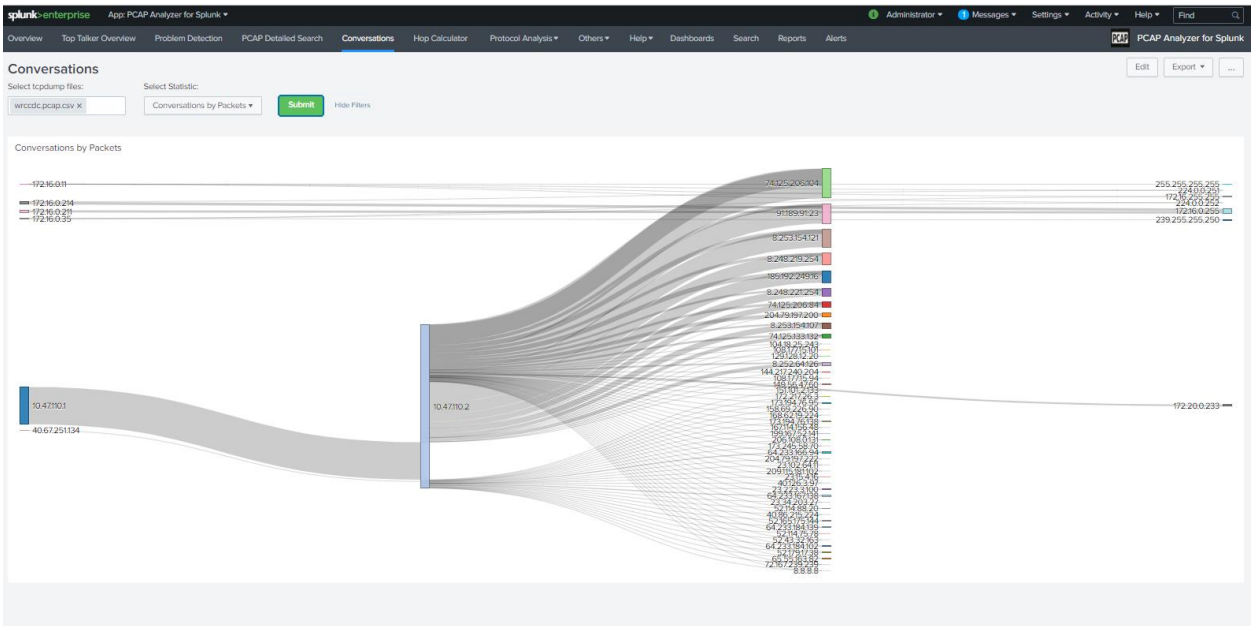


Next, click more setting and change Host to siem and index to Investigations

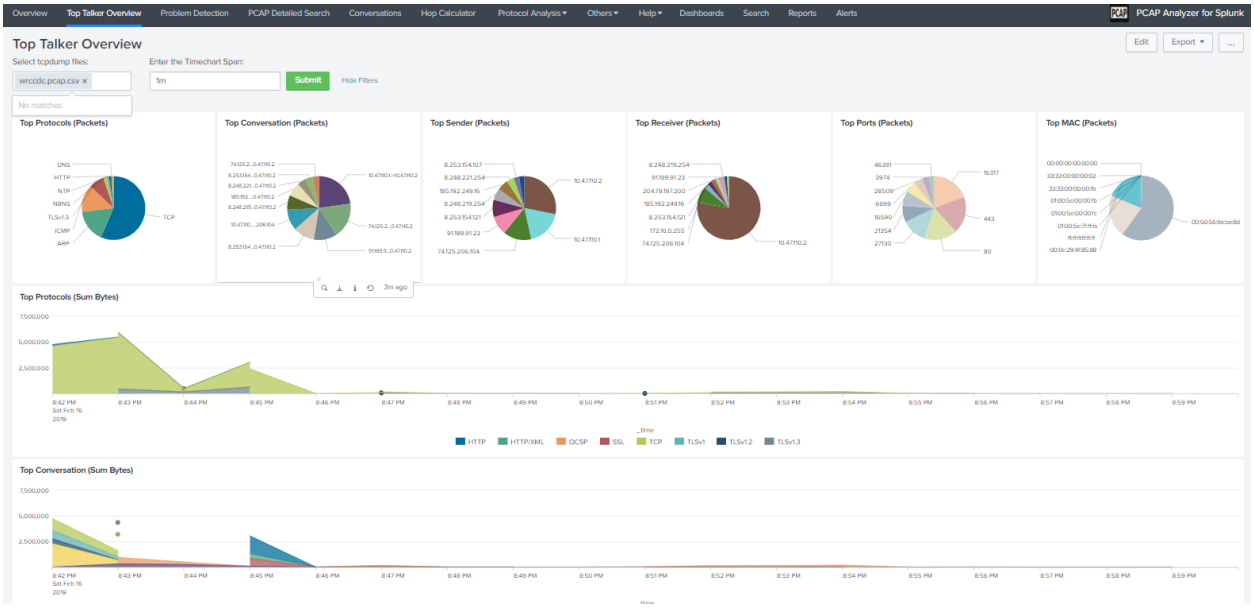


Click next

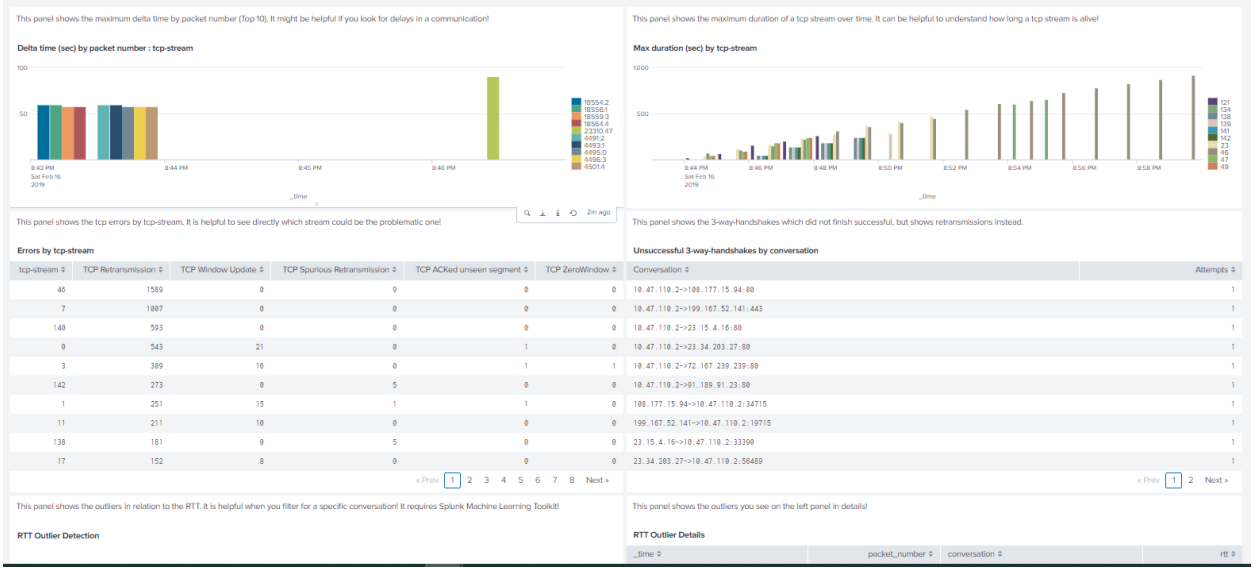
10- Wait for the data to finish indexed. After the data is done indexed, go to the PCAP Analyzer app than go to conversation. Select wrccdc.pcap.csv file and click submit. Now you can see a visual representation of the conversation that was going on during the network capture.



11-next go to Top Talker Overview. You can see a breakdown by top Protocols, top conversation, top sender, top receivers, top Ports, and top MAC



12 – Next go to Problem Detection



13- After you can take a look at the HTTP overview.