

# 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**

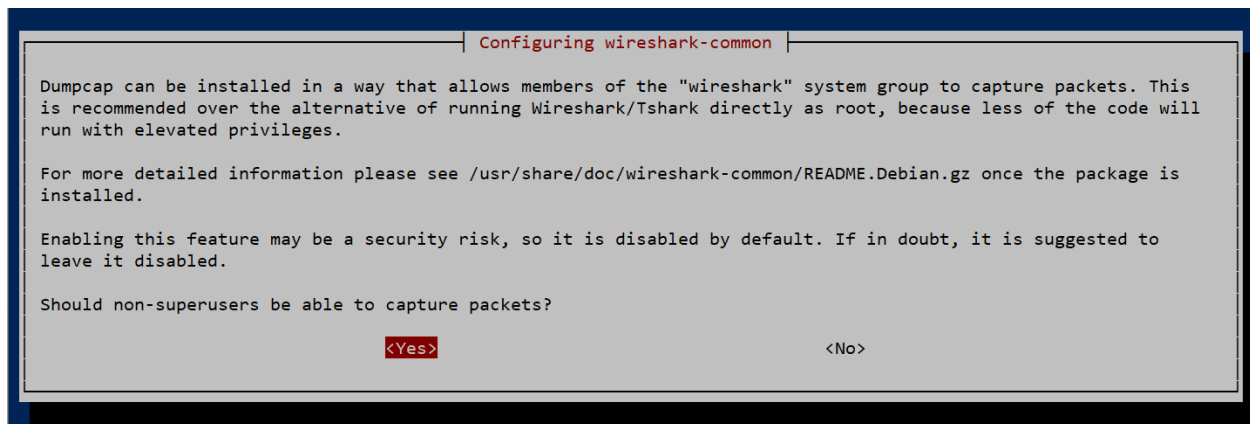
Make sure the second line of the file is **SPLUNK\_HOME="/opt/splunk"**

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

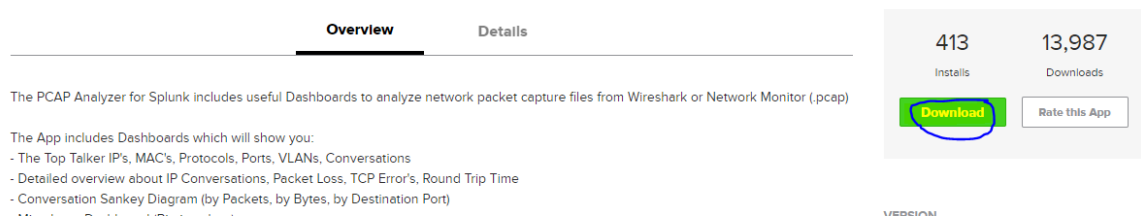
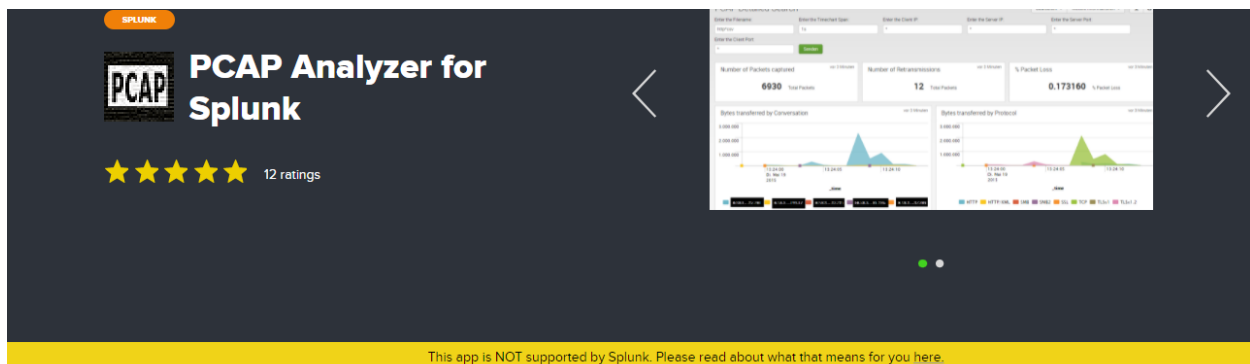
- **sudo apt-get update | sudo apt-get upgrade -y**

- **sudo apt install tshark -y**

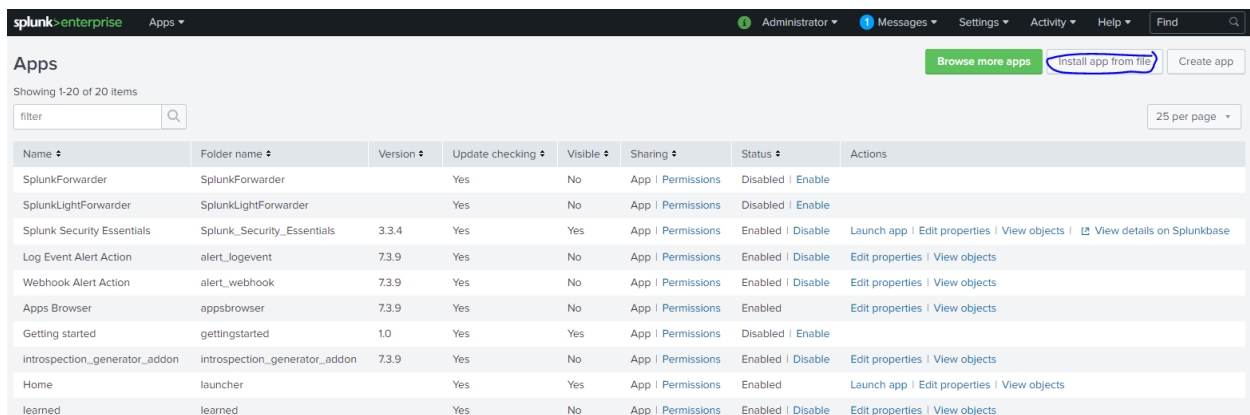
Select yes at the screen below to allow non-superusers to capture packets



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



5- Login in Splunk and install the PCAP Analyzer.



The screenshot shows the Splunk Enterprise Apps interface. At the top, there's a navigation bar with 'splunk>enterprise' and 'Apps' dropdown. Below it, the 'Apps' section is active, showing 'Showing 1-20 of 20 items'. A search filter box is present. On the right, there are buttons for 'Browse more apps', 'install app from file' (circled in blue), and 'Create app'. Below these is a table listing various apps.

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App   Permissions	Disabled   Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App   Permissions	Disabled   Enable	
Splunk Security Essentials	Splunk_Security_Essentials	3.3.4	Yes	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   View details on Splunkbase
Log Event Alert Action	alert_logevent	7.3.9	Yes	No	App   Permissions	Enabled   Disable	Edit properties   View objects
Webhook Alert Action	alert_webhook	7.3.9	Yes	No	App   Permissions	Enabled   Disable	Edit properties   View objects
Apps Browser	appsbrowser	7.3.9	Yes	No	App   Permissions	Enabled	Edit properties   View objects
Getting started	gettingstarted	1.0	Yes	Yes	App   Permissions	Disabled   Enable	
Introspection_generator_addon	introspection_generator_addon	7.3.9	Yes	No	App   Permissions	Enabled   Disable	Edit properties   View objects
Home	launcher		Yes	Yes	App   Permissions	Enabled	Launch app   Edit properties   View objects
learned	learned		Yes	No	App   Permissions	Enabled   Disable	Edit properties   View objects

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/**

Administrator
Messages
Settings
Ac

Add Data
Select Source
Done
Back
Next

Files & Directories
Upload a file, index a local file, or monitor an entire directory.
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.
TCP / UDP
Configure the Splunk platform to listen on a network port.
Scripts
Get data from any API, service, or database with a script.
PCAP File Location
Location of PCAP files to be analyzed

Location of PCAP files to be analyzed
name \*
WRCCDC
path \*
Please specify the full path of the PCAP file location
/home/zanmitay/PCAP/
More settings

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

Files & Directories
Upload a file, index a local file, or monitor an entire directory.
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.
TCP / UDP
Configure the Splunk platform to listen on a network port.
Scripts
Get data from any API, service, or database with a script.
PCAP File Location
Location of PCAP files to be analyzed

Interval
Interval
Number of seconds to wait before running the command again, or a valid cron schedule. (leave empty to run this script once)
Source type
Set sourcetype field for all events from this source.
Set sourcetype
Automatic
Set to automatic and Splunk will classify and assign sourcetype automatically. Unknown sourcetypes will be given a placeholder name.
Host
Set the host with this value.
Host
siem
Index
Set the destination index for this source.
Index
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.



