**Feeding entrada by PCAP files**

The section describes how to feed entrada by pcap files. Since entrada installed in namenode server, the data should be sent to that node to specific location.

**Configuration of the sender:**

* Install ssh server and ssh.
* Install sshpass.
* Install wireshark in the sender node (check capinfos command).

**Configuration of the namenode:**

* Enough storage in the namenode server to handle the big data.
* Install ssh server and ssh client.
* Create folders for each server (e.g. DNS1-PRI, DNS1-SEC, DNS2-PRI, DNS2-SEC) in the captures file in the home of namenode server.

-----------------------------------------------------------------------------------------------------------------

1. The data can be stored in any node in the cluster or any device that can communicate with namenode.
2. Specify the requirements in the bash script
   * username="entrada"
   * server\_ip=192.168.100.1
   * path\_to\_destination="/home/entrada/captures"
   * location=PCAP\_DATA
   * pass="12345"
3. check that all the requirement is installed before running the script.

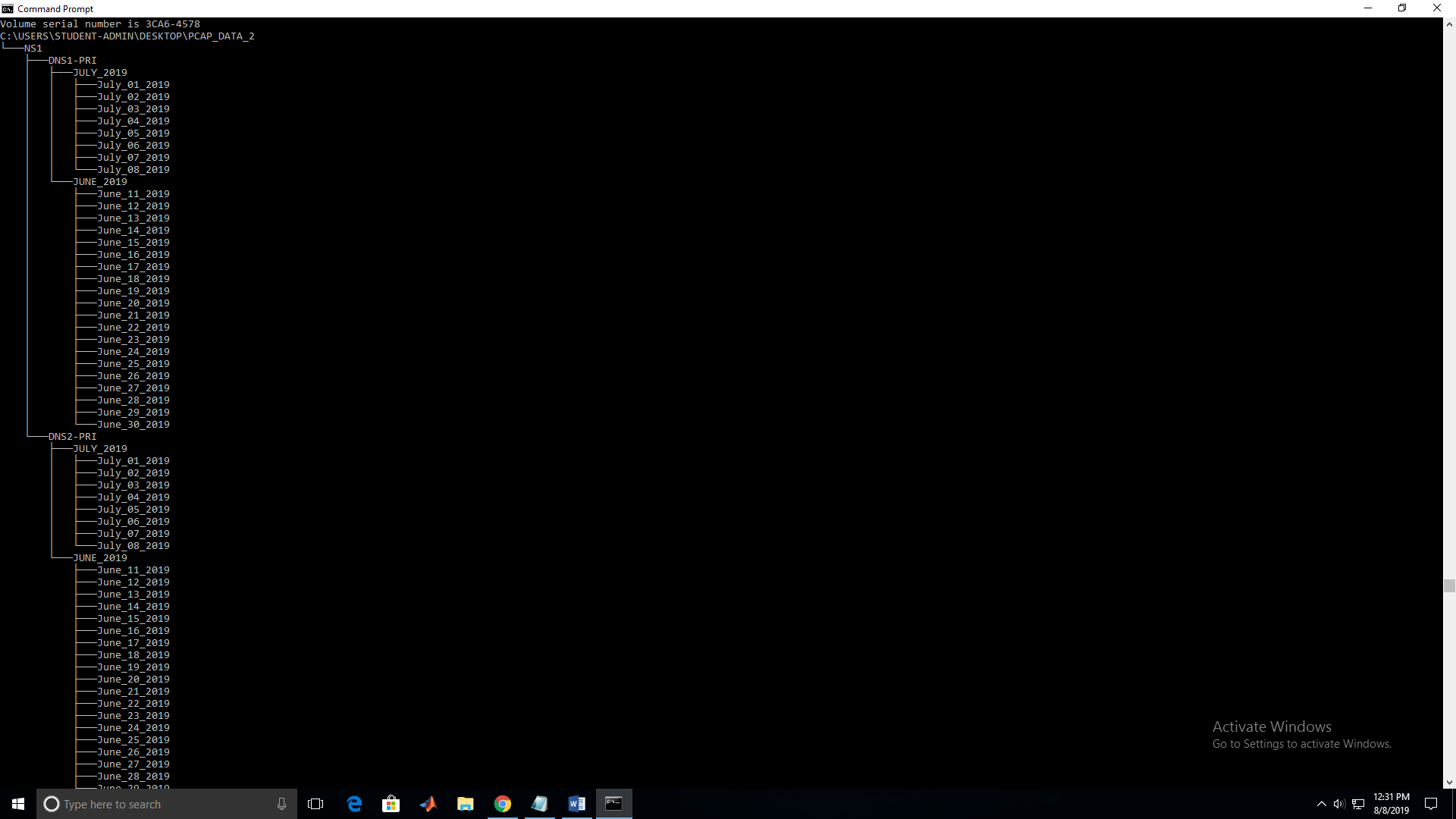
**PCAP\_DATA Directory Tree:**

PCAP\_DATA/NS1/DNS1-PRI/MONTH\_YEAR/month\_day\_year/anyname.pcap

PCAP\_DATA/NS1/DNS2-PRI/MONTH\_YEAR/month\_day\_year/anyname.pcap

PCAP\_DATA/NS2/DNS1-SEC/MONTH\_YEAR/month\_day\_year/anyname.pcap

PCAP\_DATA/NS2/DNS2-SEC/MONTH\_YEAR/month\_day\_year/anyname.pcap



**PCAP Files Script:**

1)Copy the PCAP\_DATA to the home Directory in Namenode4

2) Run the script (shell\_test2.sh ) using “ sudo ./shell\_test2.sh PCAP\_DATA/”

3) switch to Namenode 1 and open Grafana in the browser at [http://192.168.9.102:3000](http://192.168.9.102:3000/)

**Grafana**

Grafana Documentation Page: <https://grafana.com/docs/guides/getting_started/>

1. In Namenode 1, open Grafana in the browser at [http://192.168.9.102:3000](http://192.168.9.102:3000/)
2. Click on the Dashboard Dropdown located in the top left corner of the screen
3. Choose “DNS Analysis” or any other dashboard you want to show.

Grafana Variables:

Query : entrada.\*

Regex: DNS[1-2].\*

**Cleaning old data for a fresh start: (Create a script)**

1. In Namenode1, remove all files in /opt/graphite/storage/whisper/entrada using the command “ sudo rm –rf /opt/graphite/storage/whisper/entrada/\* “
2. Remove all the files in the locations :

* /home/captures/
* /home/pcap/incoming/
* /home/pcap/processing/
* /home/pcap/prossesed/archive

1. Remove the files :

* /home/entrada-latest/tmp/DNS1-PRI-pcap-process.hist
* /home/ entrada-latest /tmp/DNS2-PRI-pcap-process.hist
* /home/ entrada-latest /tmp/DNS1-SEC-pcap-process.hist
* /home/ entrada-latest /tmp/DNS2-SEC-pcap-process.hist

#! /bin/bash

//Script to Clean files for a fresh start

sudo rm –rf /opt/graphite/storage/whisper/entrada/\*

rm /home/captures/\*

rm /home/pcap/incoming/\*

rm /home/pcap/processing/\*

rm /home/pcap/incoming/\*

rm /home/entrada-latest/tmp/DNS1-PRI-pcap-process.hist

rm /home/entrada-latest/tmp/DNS2-PRI-pcap-process.hist

rm /home/entrada-latest/tmp/DNS1-SEC-pcap-process.hist

rm /home/entrada-latest/tmp/DNS2-SEC-pcap-process.hist

**Entrada and Hue ( SQL Queries )**

“The ENTRADA data model support many types of SQL queries which can be used to a extract interesting information from the captured network data. You might be interested in resolver behavior, domain name usage or the use of certain types of DNS attributes. Here we display some example queries, below each query, we show its (fictional) result.”

1. Open [http://192.168.9.102:8889](http://192.168.9.102:8889/) in the browser
2. Enter a SQL query and click the execute button or CTRL+ENTER

For Example: to show all data for the first 50 rows enter

“ SELECT \* FROM queries LIMIT 100; ”

1. Some examples can be found in <https://entrada.sidnlabs.nl/query_examples/>