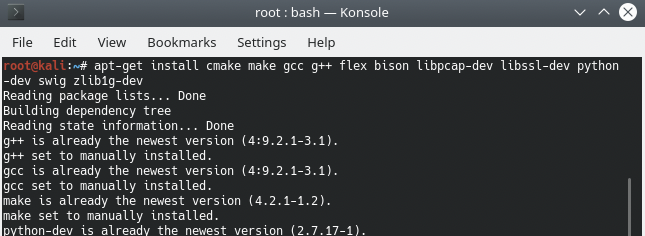
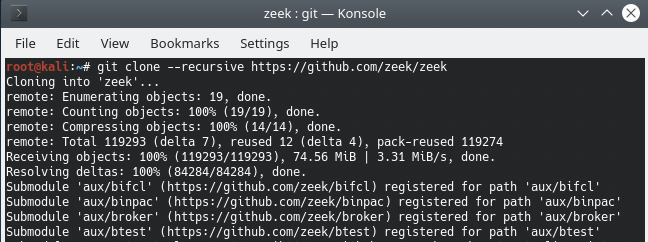
Install Zeek/bro

First, do **#apt-get update** to the **kali**,  
and then  
**#apt-get install git cmake make gcc g++ flex bison libpcap-dev libssl-dev python-dev swig zlib1g-dev**



then

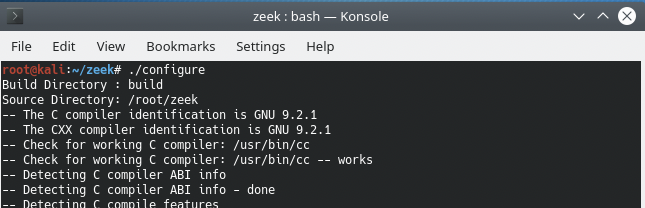
**#git clone --recursive https://github.com/zeek/zeek**



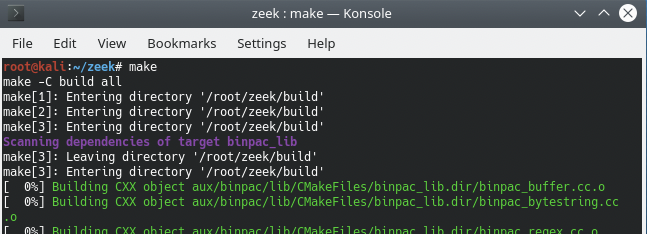
If necessary, you will need to install CMAKE with the machine as required **#apt-get install cmake**  
Or not

Once installed, you will enter the ZEEK home directory cd Zeek And Run the following command

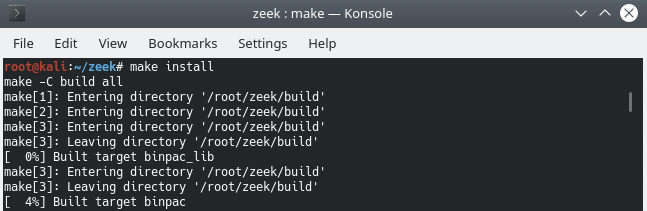
**#./configure and press enter**



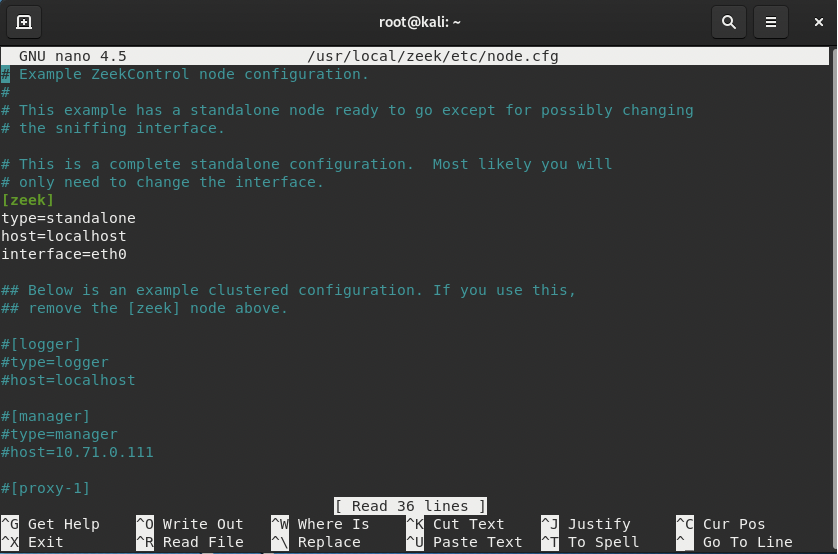
**#make** and press enter  
The make installation can take few minutes



**#make install** and press enter

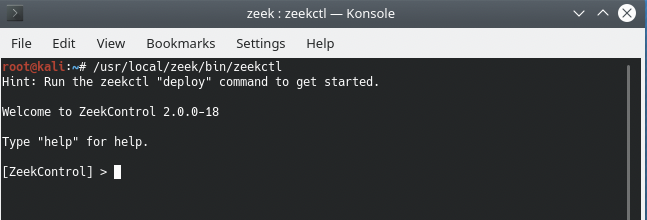


After installation, editing the configuration file in this path: **/usr/local/zeek/etc/node.cfg** Use nano to configuration the file

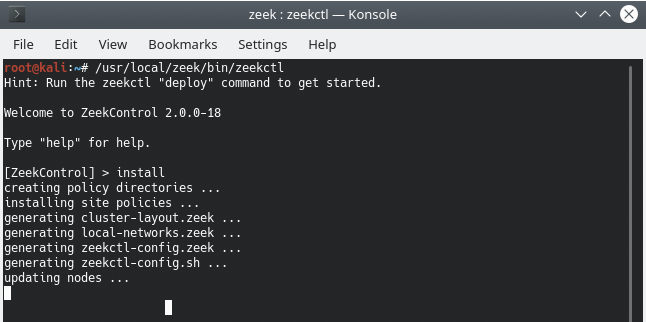


Please verify the interface name to the correct one. If it’s no need to change anything and just save the file and continue to the next step.

Now turn on ZEEK **/usr/local/zeek/bin/zeekctl** press enter



And type install



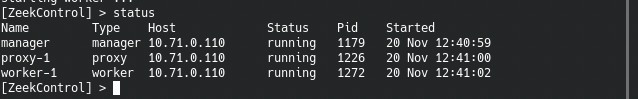
checking your work use command check and press enter



start

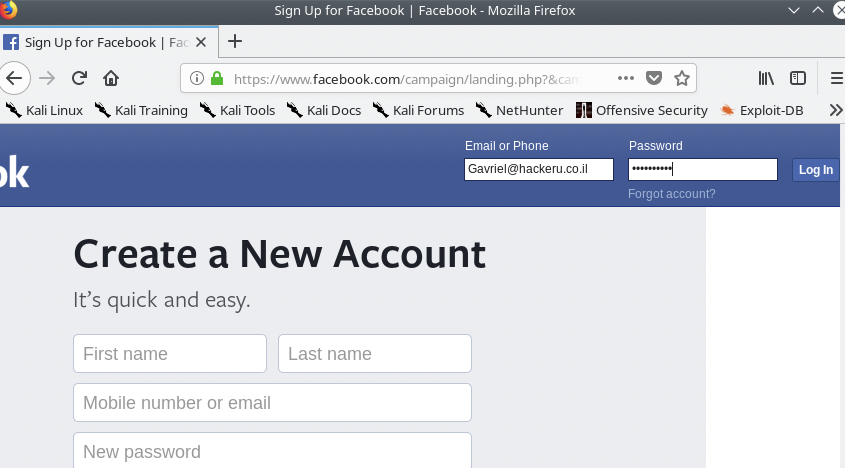
page9image43591008

status

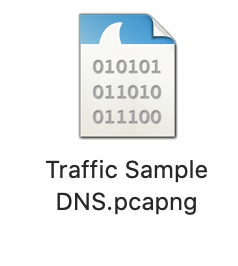


Once we know that everything is fine.

The next step is to create a log and filter inside it, in your machine you will go to a website that you will need to enter a username and password and log in.



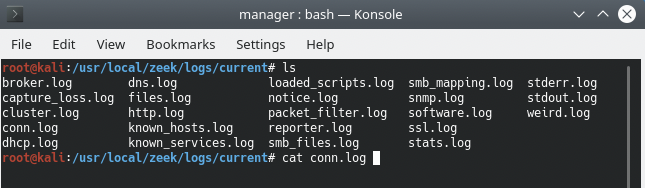
Make sure you’ve file:

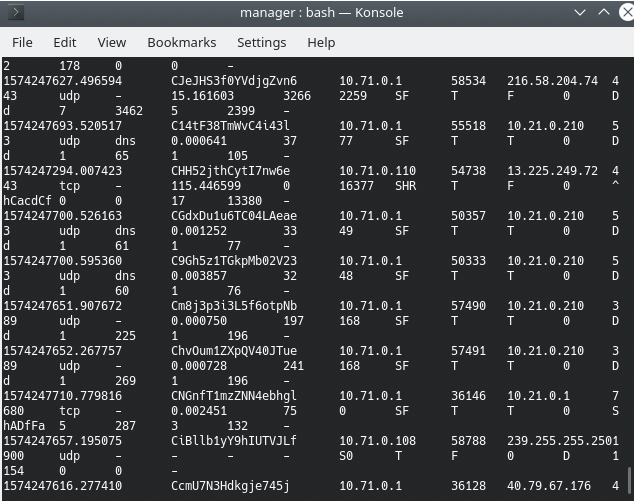


To convert pcap file, use

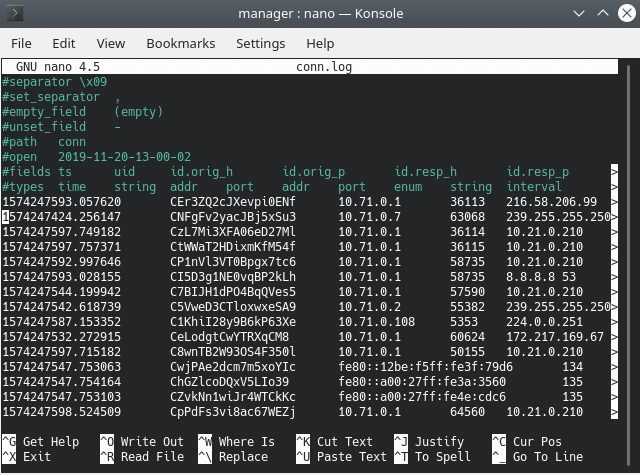
**#./zeek -Cr Traffic\ Sample\ DNS.pcapng**

Go to the next lane: **cat /usr/local/zeek/logs/current/conn.log**



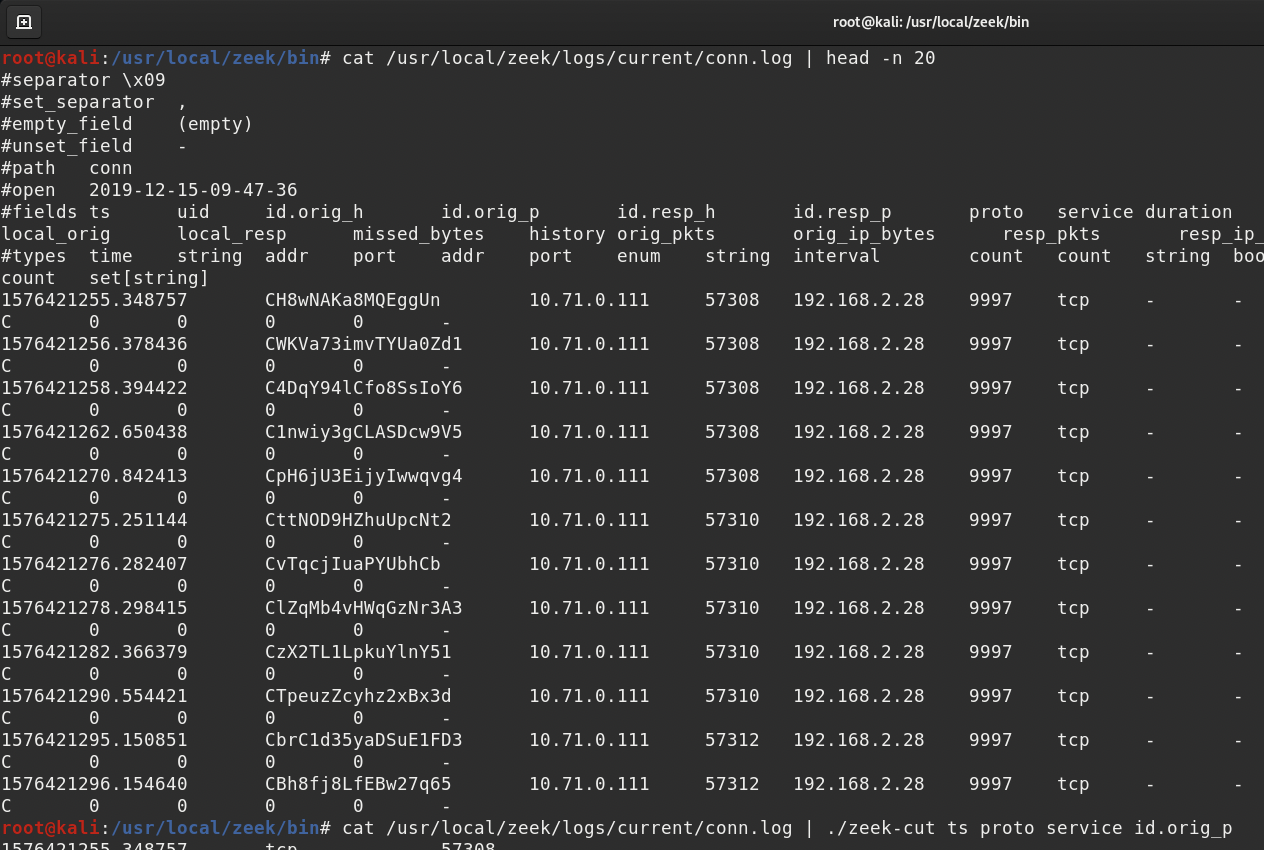


Or use nano conn.log



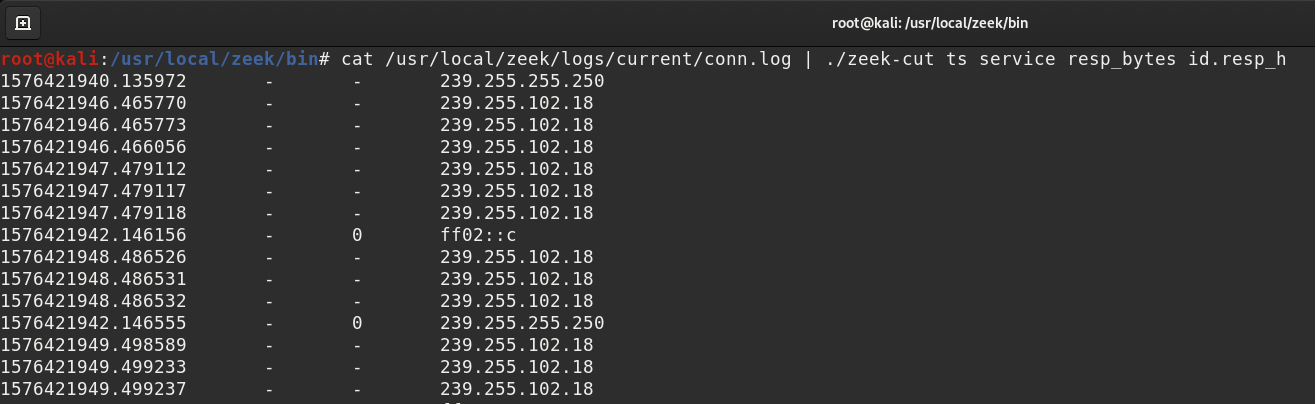
Using pipes, the output can be filtered and searched.

**#cat /usr/local/zeek/logs/current/conn.log | head**



**Command filtered:**

**#cat conn.log | zeek-cut ts service resp\_bytes id.resp\_h**



Command filtered : Example  
**#cat conn.log | zeek-cut ts service resp\_bytes id.resp\_h | awk '$2 == "ssl" && $3 > 1000 {print $4}'**

**#cat /usr/local/zeek/logs/current/conn.log | ./zeek-cut ts proto service id.orig\_p | awk '$4>58000 {print $4}'**

**#cat /usr/local/zeek/logs/current/conn.log | ./zeek-cut ts proto service id.orig\_p | awk '$4>58000 {print $1,$4}'**

